THE PENTEST EXPERTS.

WHITEPAPER

PLANUNG UND DURCHFÜHRUNG VON PENETRATIONSTESTS

Schaffhausenstraße 77, 72072 Tübingen, Deutschland
+49 (0)7071 - 40 78 56-0
info@syss.de
www.syss.de

Sebastian Schreiber

Über den Geschäftsführer

1993 – 1999	Studium der Informatik, Physik, Mathematik und BWL an der Eberhard Karls Universität Tübingen
1996 – 1998	Mitarbeiter bei Hewlett Packard
1996	MicroGold (USA)
1998 – heute	Geschäftsführer der SySS GmbH

Zahlreiche Veröffentlichungen, Vorträge im In- und Ausland.

Stand: Mai 2023

Autoren
Sebastian Schreiber
Moritz Abrell
Fidelis Abt
Micha Borrmann
Philipp Buchegger
Matthias Deeg
Thomas Heumann
Franz Jahn
Gerhard Klostermeier
Torsten Lutz
Daniel Reutter
Steffen Tacke
Wolfgang Zejda

Qualitätssicherung
Marcus Bauer
Stefanie Hütter
Dr. Julia Kerscher

Inhaltsverzeichnis

1 Penetrationstests

Seit 1998 führt die SySS Sicherheitstests durch. Die dadurch gewonnenen Erkenntnisse bilden das Fundament dieses Whitepapers. Dabei hat die SySS ihre Erfahrung sowohl bei großen multinationalen als auch bei traditionellen mittelständischen Unternehmen gesammelt. Die in diesem Whitepaper aufgeführten Empfehlungen basieren auf den praktischen Erfahrungen unserer IT Security Consultants und auf der intensiven Kommunikation mit unseren Kunden.

Sicherheits- oder Penetrationstests versteht die SySS als aktive Qualitätskontrolle der IT-Sicherheit. Das vorliegende Whitepaper unterstützt Sie dabei, die richtigen Testgegenstände und die zu diesen passenden Testverfahren aus dem Angebot der SySS auszuwählen. Zudem wird dargestellt, welche Voraussetzungen nötig sind, damit ein Test effizient und erfolgreich durchgeführt werden kann. Ein besonderer Schwerpunkt liegt dabei auf den Entscheidungen und Maßnahmen, die erforderlich sind, damit der Test auch intern in Ihrem Unternehmen als positive und für alle Beteiligten nutzbringende Dienstleistung wahrgenommen wird.

1.1 Gestaltungsmöglichkeiten

Aufgrund der Unterschiedlichkeit der diversen Testgegenstände können Sicherheitstests nicht nach einem festen, standardisierten Verfahren ablaufen, sondern müssen flexibel gestaltet werden. Diese Gestaltung ist von mehreren Faktoren abhängig:

- Zu testende Systeme, Anwendungen oder sonstige IT-Komponenten (siehe Abschnitt 1.1.1)
- Gewählte Testmodule (siehe Abschnitt 1.3.2)
- Mögliche Schwerpunkte (siehe Abschnitt 1.1.2)
- Regelmäßigkeit der Tests (siehe Abschnitt 1.1.2)
- Perspektive, aus der der Test durchgeführt wird (siehe Abschnitt 1.1.4)
- Interne Koordination des Testablaufs (siehe Abschnitt 1.1.5)
- Besonderheiten beim Testverfahren (siehe Abschnitt 1.1.5)
- Umgang mit Denial-of-Service (DoS)-Potenzialen (siehe Abschnitt 1.2.3)
- Zur Verfügung stehendes Budget

1.1.1 Testgegenstand und Testabdeckung

Sowohl bei externen als auch bei internen Tests sind die Testgegenstände beispielsweise Systeme, die durch ihre IP-Adressen identifiziert werden. Aus der Gesamtheit der IP-Adressen wählt der Kunde entweder eine repräsentative Stichprobe aus, oder es werden alle getestet. Beim Test von Webapplikationen oder Webservices ist der Testgegenstand der jeweilige Dienst selbst bzw. dessen bereitgestellter Funktionsumfang – zum Beispiel eine webbasierte Anwendung oder eine XML-basierte Schnittstelle.

Bei der Untersuchung von WLANs (Wireless LANs) ist der Testgegenstand wiederum die WLAN-Infrastruktur an einem Standort des Kunden oder daraus ausgewählte Funknetze. Die Testabdeckung beschreibt hier zum Beispiel die Größe des zu untersuchenden Campus oder die Anzahl der zu prüfenden Gebäude.

Der Testgegenstand und die Testbreite werden bei der Angebotserstellung berücksichtigt. Hier wird auch der Zeitbedarf kalkuliert. Aufgrund der Vielfalt an Systemen und Anwendungen, die bei allen Testgegenständen zum

Einsatz kommen können, sind pauschale Aussagen schwierig. Wir empfehlen Ihnen daher, den Testgegenstand vorab direkt mit uns zu besprechen.

Im Allgemeinen wird – insbesondere bei großen Unternehmen – im Rahmen eines Tests nicht das gesamte interne Netz oder die vollständige externe Angriffsfläche geprüft, sondern eine sinnvolle Auswahl getroffen. Als Sonderform ist es möglich, dass die SySS aus einem oder mehreren Netzen selbstständig Stichproben auswählt.

Stellt entweder der Kunde oder die SySS während eines Tests fest, dass Änderungen sinnvoll sein könnten, so sind Anpassungen unbürokratisch möglich. Sie werden in direkter Absprache zwischen dem durchführenden Consultant und dem Ansprechpartner des Kunden vorgenommen.

1.1.2 Testtiefe und Testfrequenz

Die Testtiefe ergibt sich automatisch aus dem gewählten Testgegenstand und der zur Verfügung stehenden Zeit. Ist ein Testziel beispielsweise die Überblicksgewinnung über eine große Anzahl von Systemen in vergleichsweise kurzer Zeit, so ist die Testtiefe bei einem einzelnen System niedrig und die Suche nach sehr hohen Risikopotenzialen hat Priorität. Steht dagegen viel Zeit für wenige Systeme zur Verfügung, so können zum Beispiel selbst Fehlkonfigurationen erfasst werden, von denen kein direktes Sicherheitsrisiko ausgeht, die aber die Funktionstüchtigkeit nicht optimal ausschöpfen.

Die Schwerpunktsetzung bei der Untersuchung des im Angebot definierten Testgegenstands wird in einer in der Regel telefonisch durchgeführten Besprechung vor Testbeginn (KICKOFF, siehe Abschnitt 1.3.1 auf Seite 16) näher bestimmt. Generelles Ziel ist es, innerhalb des Testzeitfensters festzustellen, wie das aktuelle Sicherheitsniveau des Testgegenstands aussieht und von welchen Sicherheitslücken das größte Risiko ausgeht. In der Regel wird der durchführende Consultant mehr Aufwand in den Nachweis von Sicherheitslücken investieren, die ein Eindringen Dritter ermöglichen, als in die detaillierte Untersuchung von Fehlern, die lediglich ein minimales Risiko darstellen.

Endgültiges Ziel ist es, ein möglichst umfassendes Gesamtbild über den Sicherheitszustand des Testgegenstands zu gewinnen, Risiken klar zu benennen und Vorschläge zur Behebung zu unterbreiten. Dies alles wird in einem ausführlichen Abschlussbericht (DOCU, siehe Abschnitt 1.3.3 auf Seite 18) festgehalten.

Wenn die Notwendigkeit erkannt wird, während des Tests die Schwerpunktsetzung oder Testtiefe zu ändern, so ist auch dies im direkten Gespräch zwischen Consultant und Ansprechpartner möglich. Da Sicherheitstests keinem linearen Ablauf folgen, bietet die SySS hier die nötige Flexibilität.

Sicherheitstests können ihre maximale Wirkung auf den Sicherheitsprozess nicht entfalten, wenn sie nur einmalig stattfinden – denn die Maßnahmen, die nach einem Test zur Behebung festgestellter Sicherheitslücken durchgeführt werden, sollten für die Mitarbeiter oder Dienstleister zur Routine werden. Auch Softwareupdates oder das Hinzufügen oder Entfernen von Modulen o. Ä. können zu neuen Sicherheitslücken führen. Zudem werden immer wieder neue Angriffstechniken entwickelt und Schwachstellen veröffentlicht, die auch bei einem bereits geprüften Testgegenstand relevant sind und nur durch regelmäßige Prüfungen erfasst werden können.

Für nachhaltige Ergebnisse sollte der Sicherheitstest vollständig in den Sicherheitsprozess integriert und turnusmäßig durchgeführt werden. Unternehmen, die einen hohen Wert auf IT-Sicherheit legen, konzipieren Testpläne, die zwei bis drei Jahre in die Zukunft reichen, zum Beispiel:

	Q2 2023	Q3 2023	Q4 2023	Q1 2024	Q2 2024	Q3 2024	Q4 2024
Sicherheitstest der Systeme im Internet (Modul IP-RANGE)							
Untersuchung der Webapplikationen (Modul WEBAPP)							
Interner Penetrationstest (Modul LAN)							
WLAN-Test (Modul WLAN)							

Dabei muss der permanente Wandel von IT-Netzen und Anwendungen berücksichtigt werden. Die Planung sollte etwa halbjährlich überdacht und aktualisiert werden. Der Testgegenstand sollte so gewählt werden, dass sich der Nutzen maximiert und keine Routine im Sinne einer Gleichgültigkeit gegenüber den Testergebnissen eintritt. Der Testplan sollte langfristig angelegt sein, denn nur so lassen sich auftretende Schwachpunkte identifizieren und ein professionelles Qualitätsmanagement nachweisen.

1.1.3 Testmodelle (Black-, White- und Greybox)

Bei einem Sicherheitstest wird sowohl eine bestimmte Perspektive eingenommen (siehe Abschnitt 1.1.4 auf der nächsten Seite) als auch von einem bestimmten Wissensstand des potenziellen Angreifers ausgegangen. Die SySS orientiert sich bei Bedarf an dem Blackbox-, Whitebox- und Greybox-Modell.

Blackbox-Modell

Bei diesem Modell werden durch den Kunden nur minimale Informationen zum Testgegenstand übermittelt. Ein Blackbox-Test darf dabei aber keinesfalls als Test missverstanden werden, bei dem keinerlei Informationsfluss zwischen Tester und Kunde stattfindet und Ziele völlig selbstständig gewählt und geprüft werden. Rechtliche Gegebenheiten erlauben das Testen von fremden Systemen ohne ausdrückliche Erlaubnis des tatsächlichen Betreibers nicht.

Vor einer Prüfung muss stets verifiziert werden, ob ein Test des Systems oder des Netzes unter organisatorischen und technischen Gesichtspunkten sinnvoll ist. Falls sich die Auswahl aufwendig gestaltet, kann vorab eine Perimetererkennung (siehe Abschnitt 2.12.1 auf Seite 67) durchgeführt werden. Dabei identifiziert die SySS Testziele weitgehend selbstständig. Die Ergebnisse und die Stichprobenauswahl werden mit dem Kunden besprochen, der die Testfreigabe erteilt und die nötigen Genehmigungen beschafft.

Whitebox-Modell

Bei Tests im Rahmen des Whitebox-Modells werden umfangreiche Informationen über den Testgegenstand übermittelt. Beispielsweise kann es von Vorteil sein, im Rahmen einer Webapplikationsanalyse eine begleitende Sichtung des Quelltextes sicherheitsrelevanter Funktionen der Applikation durchzuführen.

Greybox-Modell

Sicherheitstests der SySS folgen in der Regel diesem Modell. Dabei werden vom Kunden exakt die Informationen zur Verfügung gestellt, die zur effizienten Durchführung eines Sicherheitstests nötig sind. Falls höherer Informationsbedarf besteht, werden Rückfragen an den Ansprechpartner des Kunden gestellt. Die für ein Testmodul notwendigen Informationen werden in diesem Whitepaper jeweils unter „Mitwirkung des Kunden" innerhalb des entsprechenden Modulabschnitts aufgeführt. Aufgrund ihrer langjährigen Erfahrung erachtet die SySS dieses Modell für die häufigsten Testziele als die effizienteste Herangehensweise.

1.1.4 Testperspektive

Die unterschiedlichen Positionen, die ein potenzieller Angreifer einnehmen kann, werden durch unterschiedliche Testabläufe nachgestellt. Es kann beispielsweise erst einmal geprüft werden, welche Infrastruktur des Kunden überhaupt aus dem Internet erreichbar ist. Auf diese Weise wird ein realistisches Bild über die externe Angriffsfläche des Kunden gewonnen (siehe ebenso Abschnitt 2.12.1 auf Seite 67). Dies kann auch als Inventarisierungsmaßnahme verstanden werden. Es kann jedoch auch geprüft werden, welches Risiko konkret von im Internet erreichbaren Systemen durch nicht autorisierte Nutzer ausgeht. Hierzu werden diese Systeme einem externen Sicherheitstest unterzogen (siehe Abschnitt 2.1 auf Seite 21).

Davon zu unterscheiden ist der Test von Webapplikationen, Webservices oder Mobile Apps (siehe Abschnitte 2.2, 2.3 und 2.8). Er findet primär aus der Perspektive von regulären, angemeldeten Nutzern einer Anwendung statt. Der Tester kann zusätzlich auch die Perspektive eines unangemeldeten Nutzers einnehmen, um beispielsweise auch das Authentisierungsverfahren auf Schwachstellen zu prüfen.

Der interne Sicherheitstest prüft das Firmennetzwerk aus der Perspektive des Innentäters (siehe Abschnitt 2.4 auf Seite 30). Als Innentäter kann auch ein Angreifer agieren, dem es gelungen ist, ein einzelnes System innerhalb des Firmennetzwerks unter seine Kontrolle zu bringen. Bei einem internen Test sind in der Regel sehr viele Systeme erreichbar, die ihrerseits auch viele Dienste anbieten. Daher muss die Art der Durchführung hier oftmals angepasst werden. Dies umfasst unter anderem eine Konzentration auf die Feststellung von schwerwiegenden Sicherheitslücken, die leicht ausgenutzt werden können („Low-Hanging Fruits"). Auch spezielle Teilkomponenten einer internen IT-Landschaft können geprüft werden. Als Beispiele seien Netzwerkkomponenten, die VoIP-Infrastruktur oder spezielle Anwendungsumgebungen (Active Directory, SAP usw.) genannt.

Bei den Sicherheitstests von WLANs wird zunächst einmal die Perspektive eines Angreifers in der Reichweite eines WLAN Access Points eingenommen. Hier wird geprüft, ob beispielsweise die unberechtigte Nutzung eines Netzes möglich ist oder bestehende Verbindungen von Teilnehmern kompromittiert werden können.

Mehr und mehr Produkte sind heutzutage internetfähig (Internet of Things), sodass der Analyse von Hardwarekomponenten und ihren Schnittstellen zum Internet eine immer größere Bedeutung zukommt. Dabei soll vermieden werden, dass sich hier Sicherheitslücken auftun, die Angreifer leicht ausnutzen können (siehe Abschnitt 2.10 auf Seite 57).

Ferner bietet die SySS Red Teaming Assessments an (siehe Kapitel 3 auf Seite 80), bei denen ganz bewusst die Rolle von Angreifern simuliert wird, die nicht nur auf technische Weise versuchen, an sensible Informationen und Daten zu gelangen, sondern sich auch nicht scheuen, Social Engineering anzuwenden oder sich selbst in Gebäude einzuschleusen.

1.1.5 Angekündigte oder unangekündigte Prüfungen – verdeckte oder offensichtliche Tests

Das Ziel von Penetrationstests ist die Aufdeckung von technischen und nicht von menschlichen Defiziten. Unangekündigte Tests können aber häufig von den Betroffenen als Letzteres verstanden werden. Dies hat für den Kunden den großen Nachteil, dass Testergebnisse infrage gestellt werden können und die Motivation der Mitarbeiter, dringende Sicherheitsmaßnahmen umzusetzen, erheblich sinken kann. Das Ziel eines Sicherheitstests wird daher in der Regel nicht erreicht, sondern schlichtweg verfehlt, wenn er unangekündigt durchgeführt wird.

Der nachhaltige Erfolg der SySS besteht darin, dass sowohl die Ansprechpartner der Kunden als auch deren Systemverantwortliche und Administratoren der Dienstleistung „Sicherheitstest" Vertrauen statt Misstrauen entgegenbringen. Ein zentraler Faktor ist hierbei das Angebot an alle Beteiligten, dem Test persönlich beizuwohnen.

Tipp von Sebastian Schreiber

Sprechen Sie mit allen Beteiligten über geplante Tests. Damit erreichen Sie, dass der Sicherheitstest als nützliche Dienstleistung aufgefasst wird und die Ergebnisse effizient bearbeitet werden.

Der zweite zentrale Faktor ist eine positive Fehlerkultur. Die bei einem Penetrationstest gefundenen Fehler sollten als Lernchancen, als Gelegenheiten für neue Denkansätze und Möglichkeiten zur Weiterentwicklung verstanden werden.

Tipp von Sebastian Schreiber

Nehmen Sie entdeckte Fehler nicht zum Anlass, nach dem „Schuldigen" zu suchen. Dies führt im Zweifelsfall zu Vertuschung und Vertrauensverlust. Nur vor dem Hintergrund einer positiven Fehlerkultur kann ein Penetrationstest seine komplette Wirkung entfalten.

Social Engineering, eine unangekündigte und verdeckte Methode, gehört neben allen technischen Möglichkeiten zu den wirksamsten Mitteln, um an sensible Daten zu gelangen. Social Engineering bedeutet im Kontext von IT-Sicherheit, sensible Daten durch Täuschung eines Menschen zu erlangen. Betrüger, die Social Engineering betreiben, geben sich beispielsweise als befugte Techniker oder externe Dienstleister aus und schaffen es durch ein angepasstes Auftreten, gewünschte Informationen abzufragen. In der Regel haben sie auch hinreichende Kenntnisse der Unternehmenskultur, um hektische Situationen (z. B. IT-Umstellungen in großem Maßstab, Umzüge, geschäftige und betriebsame Situationen aller Art usw.) ausnutzen zu können.

Social Engineering birgt eine enorme Gefahr für Unternehmen. Die Diskussion über Maßnahmen zur Eingrenzung dieses Gefahrenpotenzials ist durchaus berechtigt. Allerdings gibt es einen entscheidenden Unterschied zu allen anderen Testmöglichkeiten: Der Testgegenstand ist hierbei der Mensch und keine technische Komponente. Die Tests sind nicht deterministisch und dienen in der Regel dazu, bestehende Prozesse im Unternehmen sowie die Sensibilisierung bei Mitarbeiterinnen und Mitarbeitern zu testen.

Prüfer nehmen bei solchen Tests eine falsche Identität an, um Firmenmitarbeiter über E-Mails, Telefonate oder sonstige direkte Interaktion dazu zu bringen, sensible Daten herauszugeben. Außerhalb von scharf kontrollierten Bedingungen ist dies rechtlich kritisch und organisatorisch heikel. Aus diesem Grund müssen solche Tests im Rahmen von Awareness-Maßnahmen immer angekündigt werden.

Bei Sicherheitstests wird – wie bereits erwähnt – nicht verdeckt agiert, mit Ausnahme von Red Teaming-Tests. Der durchführende Consultant trifft keinerlei besondere Maßnahmen, die Testaktivitäten zu verbergen. Die Erfahrung zeigt, dass Maßnahmen, die zum Beispiel geeignet sind, den Test vor automatisierten Erkennungs- oder

Abwehrsystemen zu verbergen, die Testdauer massiv erhöhen – meistens mehr als einem normalen Projektablauf zuträglich ist.

Anhand des im Rahmen der Dokumentationsphase erstellten Berichts kann zusätzlich nachvollzogen werden, ob beispielsweise die Tests, die Sicherheitslücken mit hohem Risikopotenzial nachgewiesen haben, von automatischen Systemen erkannt wurden.

1.1.6 Besondere Vorgehensweise

Spezialisierung

Die SySS ist auf die Durchführung von Sicherheitstests spezialisiert. Dieser extrem hohe Spezialisierungsgrad sorgt für einen großen Erfahrungsschatz bei allen Consultants, der durch die regelmäßigen Tests ständig weiter ausgebaut wird.

Die SySS kennt dadurch die Bedürfnisse ihrer Kunden sehr genau und kann ein präzises Testergebnis liefern. Sie bietet den kritischen, aber umfassenden Blickwinkel des Externen auf das Sicherheitsniveau. Beratungsleistungen bei der Behebung von erkannten Sicherheitslücken sind dabei nur in minimalem Umfang nötig – denn um die Umsetzung der nötigen Maßnahmen kümmern sich unsere Kunden sehr erfolgreich selbst.

Transparenz

Die SySS legt Wert darauf, dass ihre Kunden ohne Weiteres nachvollziehen können, wie Sicherheitslücken erkannt und im Rahmen des Tests ausgenutzt worden sind. Hacking als geheimnisvollen, fremdartigen Ablauf zu betrachten, ist kontraproduktiv, wenn es darum geht, die IT-Sicherheit eines Unternehmens zu verbessern.

Die notwendige Transparenz wird durch die folgenden Punkte erreicht:

- Eine hochwertige Dokumentation wird mit dem erklärten Ziel erstellt, Sicherheitsprobleme nachvollziehbar zu machen.
- Es ist hilfreich, wenn der Kunde seine von Tests betroffenen Mitarbeiter und Dienstleister einlädt, entweder teilweise oder ganz dem Sicherheitstest beizuwohnen. Dabei ist die SySS jederzeit bereit, dem Kunden mit ihrem Wissen zu dienen.
- Auf Wunsch wird eine Ergebnispräsentation durch den Consultant gehalten, der den Test geleitet hat. Falls es sich anbietet, können einzelne Angriffe in diesem Rahmen auch nochmals demonstriert werden.

Nur durch diese Offenheit ist eine positive Wahrnehmung von Sicherheitstests bei Ihren Mitarbeitern möglich.

Flexibilität

Bei der Durchführung von Tests arbeitet die SySS nicht nach einem festen Schema, sondern flexibel. Ein festes Schema wäre eine Verkennung der Natur eines Angriffs, denn jedes Netz ist anders und jeder Schritt während des Tests hängt vom vorherigen ab. Zusätzlich sind sinnvolle Schwerpunktänderungen während des Tests durch ein Gespräch zwischen Ansprechpartner und dem durchführenden Consultant möglich.

Qualitätssicherung

Die Qualitätssicherung der Berichte wird von einem weiteren, nicht am Projekt beteiligten Consultant vorgenommen. Damit wird die Nachvollziehbarkeit der Testergebnisse gewährleistet. Zudem sichert das Technical Editing der SySS die sprachliche und formale Qualität des Berichts.

Expertenmeinungen

In den Abschlussberichten von Penetrationstests werden Feststellungen stets bewertet. Die Experten der SySS sind ausgezeichnet ausgebildet und erfahren, sie diskutieren in strittigen Fällen die Sachverhalte untereinander und geben ihren erworbenen Erfahrungsschatz regelmäßig an ihre Kollegen weiter.

Um die Neutralität unserer Berichte und Gutachten nicht zu beeinflussen, nimmt die Geschäftsführung der SySS keinen Einfluss auf die Gutachten der Consultants. Der Consultant bewertet immer nach bestem Wissen und Gewissen.

In seltenen Fällen kommt es vor, dass die SySS-Consultants bei der Bewertung von Schwachstellen keinen Konsens finden. Dies beruht nicht auf fehlender Expertise oder nicht zu Ende gedachten Schlüssen, sondern auf unterschiedlichen Betrachtungsweisen. Diese Meinungsvielfalt kommt nicht ausschließlich bei den Consultants der SySS vor. Ein Beispiel für eine typische unterschiedliche Bewertung durch IT-Sicherheitsexperten sind Verschlüsselungslösungen. Während die eine Gruppe die strikte Ende-zu-Ende-Verschlüsselung als ideal ansieht, legt die andere mehr Wert darauf, den Nutzer bestmöglich vor schädlichen Inhalten zu schützen, wofür eine strikte Ende-zu-Ende-Verschlüsselung kontraproduktiv wäre.

Werkzeuge

Sowohl der genaue Ablauf eines Tests als auch die Auswahl der Werkzeuge liegen in der Verantwortung des testenden Consultants. Dieser passt auf der Basis seiner Erfahrung den Ablauf an den Testgegenstand und insbesondere an die Testtiefe an und wählt die optimalen Werkzeuge aus. Sowohl die Qualität und Nutzbarkeit als auch die Lizenzbedingungen einer Soft- oder Hardware können sich kurzfristig ändern.

Die folgende Übersicht ist daher auch nur eine beispielhafte Auswahl an Werkzeugen, die regelmäßig bei der Prüfung von Systemen zum Einsatz kommen:

- Für System- und Diensterkennung werden Portscanner wie Nmap, ZMap oder von der SySS selbst entwickelte Scanner eingesetzt.
- Als automatisierte Schwachstellenscanner oder Analyse-Frameworks kommen z. B. Nessus, Recon-ng, BloodHound, Metasploit, Powersploit oder das IPv6 Attack Toolkit infrage.
- Für die weitere Überprüfung einzelner Dienste steht eine sehr große Anzahl von Werkzeugen zur Verfügung, wie beispielsweise Relay-Scanner, Smtpmap/Smtpscan, Ike-Scan, Dnswalk oder die Hping-Familie.
- Manuelle Überprüfungen werden von Telnet, Netcat, Socat, OpenSSL oder Stunnel unterstützt. Auch bei derartigen Tests ist das Metasploit-Framework ein ständiger Begleiter.

Für Webapplikationstests setzt die SySS Proxy-Tools wie die Burp Suite Professional und viele eigens entwickelte Scanner und Systeme ein. Zum Test von WLAN-Infrastrukturen nutzt die SySS vor allem die Aircrack-ng-Suite. Zudem kommen Werkzeuge wie Hostapd, airgeddon und eaphamme – teilweise mit eigenen Anpassungen – zum Einsatz.

Die Entscheidung, welche Werkzeuge genau eingesetzt werden, basiert zum einen auf dem zu erwartenden Erkenntnisgewinn und zum anderen auf der Testtiefe. Nicht jedes Werkzeug ist für jede Software einsatztauglich. Der Einsatz eines jeden Werkzeuges hat eine bestimmte Mindestlaufzeit; überschreitet diese den geplanten Testzeitraum jedoch erheblich, muss auf den Einsatz verzichtet werden. Falls der geplante Testzeitraum es zulässt,

können auch Werkzeuge zum Einsatz kommen, die beispielsweise erst nach Testbeginn veröffentlicht wurden. Gerne kann der geplante Werkzeugeinsatz auch im Vorfeld eines konkreten Projekts bei dem das Projekt leitenden Consultant erfragt werden.

1.2 Grenzen und Risiken

Ein Sicherheitstest wird durchgeführt, um Sicherheitsschwächen verschiedenster Art erkennen und anschließend beseitigen zu können.

1.2.1 Grenzen von Sicherheitstests

Ein Sicherheitstest stellt eine Analyse des Ist-Zustands dar. Risiken, die sich durch mögliche Konfigurationsänderungen oder neue Erkenntnisse in der Zukunft ergeben könnten, lassen sich nur schwer erkennen – derartige Überlegungen haben immer spekulativen Charakter. Um Schlagkraft zu besitzen, müssen Sicherheitstests daher regelmäßig durchgeführt werden. Zudem sind die Sicherheitslücken, die entdeckt werden können, von der Testperspektive abhängig.

Ein weiteres Problem ist Budgetknappheit: Werden große Netze oder komplexe Webapplikationen in einem kurzen Zeitraum geprüft, besteht die Gefahr, dass Sicherheitslücken schlichtweg aus Zeitmangel nicht identifiziert werden können. Ein potenzieller Angreifer, der sich ausreichend Zeit für eine tiefergehende Untersuchung nimmt, kann diese Sicherheitslücken aufdecken und ausnutzen.

1.2.2 Abgrenzung von Sicherheitstests gegenüber anderen Prüfungen

Im Vergleich zu IT-Grundschutz-Audits oder Zertifizierungen nach ISO 27001 ist ein Sicherheitstest vor allem konkret – er schafft überprüfbare Fakten und benennt direkte Bedrohungen für die IT-Sicherheit.

Sicherheitslücken können auch nachgewiesen werden, wenn vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierte Software eingesetzt wird und ein ISO 27001-Zertifikat vorliegt. Daher sind autonome, von Spezialisten durchgeführte Sicherheitstests den Sicherheitsprüfungen im Rahmen entsprechender Audits vorzuziehen. Sie stehen dabei nicht in Konkurrenz zu derartigen Maßnahmen, sondern eignen sich ideal zur Unterstützung – vor allem, da die Ergebnisse vergleichsweise zügig vorliegen und in ein bestehendes Audit integriert werden können.

1.2.3 Risiko Denial-of-Service

Denial-of-Service (DoS)-Potenzialen kommt eine besondere Bedeutung zu. Zum einen können diese durch Fehler in Diensten selbst auftreten, zum anderen durch Fehlkonfigurationen. Generell ist es nicht das Ziel eines Sicherheitstests, Systeme oder Anwendungen außer Kraft zu setzen, sondern zu überprüfen, ob dies möglich ist und welche Gefahr hiervon ausgehen kann.

Folgendes Vorgehen hat sich bei der Erkennung von DoS-Potenzialen besonders bewährt: Wird ein solches gefunden, kontaktieren wir zuerst den Ansprechpartner des Kunden. Im direkten Gespräch wird entschieden, ob die SySS den tatsächlichen Nachweis führen soll (also die Störung auslösen) oder nicht. Das Ausnutzen eines DoS-Potenzials kann sinnvoll sein, wenn der Kunde ein klares Signal wünscht, dass an einem bestimmten System Änderungen (Wartung, Abschottung oder gar Ersatz) nötig sind.

Tests, deren Ziel es ist, durch den Verbrauch von Bandbreite die Verfügbarkeit zu beeinträchtigen, führt die SySS nicht durch. Das Risiko durch derartige Angriffe besteht immer und kann durch die Betrachtung der zur Verfügung stehenden Bandbreite jederzeit ermittelt werden.

Da es sich bei einem Sicherheitstest um eine aktive Kontrolle handelt, kann nie völlig ausgeschlossen werden, dass die zu testenden Systeme beeinträchtigt werden. Beeinträchtigungen können sowohl bei Funktionen einzelner Dienste, dem getesteten Dienst selbst als auch bei dem gesamten getesteten System auftreten.

Insbesondere beim Test von Webapplikationen wird normalerweise nicht von DoS-Potenzialen ausgegangen. Da aber während eines Tests Abfragen an die Datenbank gestellt werden können, die reguläre Anwender nicht erzeugen, bestehen diese Risiken auch hier. Oft ist es schwer, derartige Probleme vorherzusehen. Gibt es jedoch klare Indikatoren dafür, kann wie bereits dargestellt vorgegangen werden.

Einen Sicherheitstest durchzuführen, der keinerlei Risiken birgt, ist nicht möglich. Bei kritischen Systemen kann es sinnvoll sein, Penetrationstests nicht auf dem Produktiv-, sondern auf einem Testsystem durchzuführen, um so Rückschlüsse auf Schwachstellen im Produktivsystem ziehen zu können.

Zwei Umstände sind nach Erfahrung der SySS für Denial-of-Service bei Sicherheitstests verantwortlich: Zum einen können Systeme oder Anwendungen, die auch mit der nur moderaten Last eines Tests bereits an ihre Grenzen kommen, DoS auslösen. Zum anderen bergen sehr alte und ungepflegte Dienste ein nicht unerhebliches DoS-Potenzial. Generell sollte bei der Vorbesprechung (KICKOFF, siehe Abschnitt 1.3.1 auf Seite 16) berücksichtigt werden, ob alte oder sehr alte Systeme getestet werden (z. B. mit stark veraltetem Patchstand) oder ob Lastprobleme ohnehin bei bestimmten Systemen auftreten. Um letzteres Problem zu umgehen, kann auch vereinbart werden, bestimmte Prüfungen außerhalb von Spitzenlastzeiten durchzuführen.

Penetrationstests unterscheiden sich nur punktuell von Funktions-, Last- und Verbindungstests. In gleicher Weise wie bei derartigen Tests muss bei einer Sicherheitsüberprüfung mit einem bestimmten Datenvolumen gerechnet werden, das die beteiligten Systeme wie im normalen Betrieb abarbeiten müssen.

Der Hauptunterschied zu anderen Testverfahren ist, dass bei einem Sicherheitstest verschiedene Dienste mit Anfragen konfrontiert werden, die im Alltag nicht auftreten. Dies ist exakt das grundlegende Vorgehen zum Erkennen von Sicherheitsdefiziten aller Art, von dem nicht abgewichen werden kann, es sei denn, man möchte auf technische Maßnahmen vollständig verzichten. Um also möglichst viele Risikopotenziale zu vermeiden, geht die SySS wie folgt vor:

- Durchführung des Tests durch ausgebildete und erfahrene Spezialisten
- Durchführung von Penetrationstests nur nach schriftlichem Auftrag und eindeutiger Testfreigabe für die zu prüfenden Systeme
- Prüfung der vom Kunden gelieferten Daten auf Korrektheit (z. B. IP-Ranges), Rücksprache bei Unklarheiten
- Durchführung eines Kick-off-Gesprächs anhand eines erprobten Verfahrens inkl. Erstellung eines schriftlichen Protokolls
- Fortwährende Betreuung im laufenden Projekt durch einen Ansprechpartner seitens des Kunden
- Minimierung des Risikos durch Gestaltung des Prüfprojekts: Langsame Scans (Reduktion der Bandbreite) erhöhen allerdings die Testdauer massiv.
- Tests können auch außerhalb der Geschäftszeit (z. B. nachts/am Wochenende) durchgeführt werden; wird dieses Vorgehen gewünscht, muss in dieser Zeit ein Ansprechpartner des Kunden direkt zur Verfügung stehen.
- Prüfung von Testsystemen: Entspricht das Testsystem nur in wenigen Punkten dem produktiven System, muss die SySS im Abschlussbericht stets auf diesen Umstand hinweisen, um die Aussagekraft des Berichts nicht zu verfälschen.
- Abbruch des Tests bei erkannten Schwierigkeiten: Indirekt erzeugte Probleme sind für Externe generell nicht erkennbar; daher muss der Ansprechpartner des Kunden in der Lage sein, auftretende Probleme eindeutig dem Test zuordnen zu können und vor allem die SySS zu informieren.
- Wahl von nicht invasiven Prüfmethoden: Die damit einhergehende Reduktion des Erkenntnisgewinns muss in Kauf genommen werden; Spekulationen werden als solche im Bericht von der SySS stets gekennzeichnet.

Die SySS möchte an dieser Stelle explizit auf die permanente Verfügbarkeit eines Ansprechpartners des Kunden während eines Tests hinweisen, denn ohne diesen kann eine Reihe der oben genannten Punkte unter keinen Umständen erfüllt werden. Insbesondere sollte der Ansprechpartner über die Kompetenz verfügen, mit der SySS zusammen einen anderen Testverlauf zu planen und gegebenenfalls Schwerpunkte eines Tests zu ändern. Die organisatorischen Prozesse sollten eine gewisse Flexibilität zulassen. Sind beispielsweise die üblichen Ansprechpartner während eines Tests nicht verfügbar, so sind Vertreter zu benennen und mit den entsprechenden Vollmachten auszustatten.

Aufgrund der Erfahrungen der SySS können die DoS-Risiken auf vier technische Ursachen zurückgeführt werden, die im Folgenden dargestellt werden.

1. Last bei Webapplikationstests: Bei Webapplikationstests wird, ähnlich wie bei Funktionstests, Last auf der Datenbank erzeugt, die die Webapplikation versorgt. Dies kann beispielsweise eine Suche über alle Felder sein, die dem Nutzer der Anwendung scheinbar nicht möglich ist. Ist das System, auf dem die Datenbank läuft, sehr knapp kalkuliert oder schlichtweg veraltet, kann dies zu Beeinträchtigungen führen. An dieser Stelle ist eine manuelle Betreuung der Datenbank durch Mitarbeiter des Kunden nötig – denn von externer Seite aus kann nur die Frequenz der Suchanfragen verändert werden, die Priorität einer Suche gegenüber anderen nicht.

Die SySS empfiehlt, derartige Systeme nicht auf ein sehr niedrig geschätztes Nutzungsvolumen auszulegen, sondern hinreichende Leistungsreserven vorzusehen. Diese können auch durch Optimierungen an der Datenbank und der Suchroutine in der Webapplikation gewonnen werden. Allerdings sind bei der Verwendung von Alt- oder Uraltsystemen der Lastreduzierung durch Optimierung an der Datenbank klare Grenzen gesetzt.

2. E-Mails an interne Adressen: Über entsprechende Funktionen können über die Webapplikation E-Mails verschickt werden, zum Beispiel Produkt- oder Kontaktanfragen. Diese dürfen sich weder für Spamversand noch für das Fälschen von E-Mails missbrauchen lassen. Probleme ergeben sich hier ebenfalls durch am Mailversand beteiligte Systeme, die eine Serie automatisch erzeugter Nachrichten nicht schnell genug abarbeiten können. Auch an dieser Stelle ist eine manuelle Betreuung der beteiligten Systeme nötig, da von externer Seite aus über die Komposition der beteiligten Systeme nur Annahmen getroffen werden können.

3. Ausfall von Infrastrukturkomponenten: Sicherheitstests erzeugen einen gewissen Netzwerkverkehr, den die beteiligten Komponenten, Router und Switches abwickeln müssen. Von ihnen wird dabei dasselbe korrekte Funktionieren wie im regulären Betrieb erwartet. Die bei einem Sicherheitstest entstehende Last entspricht in ihrer Natur auch der Last, wie sie eine intensive Nutzung zahlreicher Kommunikationsdienste hervorrufen würde. Infrastrukturkomponenten, die bei solchen Tests ausfallen statt einfach langsamer zu werden, sind extrem kritisch zu betrachten. Auch wenn sie höher liegt als bei legitimer Nutzung, so ist die Last eines Sicherheitstests nicht einmal ansatzweise mit der eines verteilten Angriffs (DDoS) zu vergleichen. Zudem besteht das Risiko, dass die Systeme auch natürlich auftretende Lastspitzen nicht abfangen können. Dies kann zum Beispiel die positive Annahme eines neuen Angebots durch den eigenen Kundenstamm sein oder Reaktionen der Öffentlichkeit auf Nachrichten. In der Regel lassen sich derartige Vorfälle eindeutig auf die eingesetzte Hardware bzw. die auf ihnen laufende Software zurückführen. Wird diese ohnehin vom Hersteller nicht mehr unterstützt, so empfiehlt die SySS ein Upgrade oder eine Migration. Reduziert werden kann das Risiko durch ein langsameres Vorgehen beim Testen, das aber die für das Projekt nötige Zeit leicht vervielfachen kann.

4. Nicht ausreichende Leitungskapazität: Die SySS verwendet für Tests hauptsächlich Root-Server im Internet. Sowohl vergleichbare Systeme als auch ein Großteil der eingesetzten Werkzeuge selbst sind allgemein verfügbar. Die bei einem Sicherheitstest nötige Last kann daher von Dritten mit vergleichsweise geringem finanziellen Aufwand ebenfalls erzeugt werden.

Bestimmend für das Risiko ist neben der Leitungskapazität ausschließlich der Faktor Zeit. Eine Reduktion der benötigten Bandbreite wird immer mit einer längeren Dauer des Tests verkauft. Alternativ sind nur Stichproben möglich. Da die Leitungskapazität von externer Seite nur indirekt und unpräzise festgestellt werden kann, ist die SySS daher auf präzise und widerspruchsfreie Informationen ihres Kunden angewiesen. Die SySS hat diesbezüglich keine Einsicht in die Verträge oder Absprachen des Kunden mit seinen Providern und kann daher diese Informationen nicht selbst ermitteln.

Generell empfiehlt die SySS, die Leitungskapazität modernen Erfordernissen anzupassen. Werden beispielsweise mehrere Class-C-Netze von einer 2-Mbit-Strecke versorgt, so gibt es in der Regel bereits Beeinträchtigungen durch die nicht ausreichende Bandbreite. Auf der anderen Seite können Kosten reduziert werden, indem einzelne Systeme im Ganzen oder teilweise extern gehostet werden. Ist dies nicht möglich, weil zum Beispiel Leitungen mit entsprechender Kapazität vor Ort nicht für einen angemessenen Preis zu haben sind, empfiehlt die SySS, ein klares Konzept für den Fall aufzustellen, dass die Leitung versehentlich – keinen bösen Willen vorausgesetzt – überlastet wird und die alltägliche Nutzung dann nicht mehr möglich ist. Der Ansprechpartner des Kunden sollte in diesem Fall der jeweilige Provider sein.

Zehn Tipps von Sebastian Schreiber

1. Verstehen Sie Penetrationstests nicht als einzelnes Projekt, sondern als Prozess. Dies ermöglicht und erzwingt eine kontinuierliche Vorgehensweise, deren Effizienz viel größer ist als bei einer separaten Projektsicht.
2. Penetrationstests sind sehr einfach in der Planung und Vorbereitung, wenn man sie frühzeitig terminiert. Gute Unternehmen sind zwar auch in der Lage, kurzfristig große Projekte zu stemmen, doch erzeugt dies stets einen vermeidbaren Mehraufwand.
3. Wohnen Sie dem Sicherheitstest bei! Dies bringt Ihnen einerseits einen nicht alltäglichen Perspektivenwechsel und andererseits ist es ein besonderes Erlebnis, die eigenen Systeme „unter Beschuss" zu sehen.
4. Während manche Prüfungen notwendigerweise unangemeldet durchgeführt werden müssen (wie z. B. bei Fahrkartenkontrollen, WKD), empfehlen wir, Penetrationstests anzukündigen. Dies schafft Vertrauen im Unternehmen und stärkt die Zusammenarbeit.
5. Oft sind Kunden unschlüssig, ob sie einen Blackbox- oder Whitebox-Test wählen sollen. Wir empfehlen den goldenen Mittelweg: Statten Sie den Penetrationstester gezielt mit den Informationen aus, die er für sein Projekt benötigt und die ein realistischer Hacker ohnehin selbst ermitteln könnte (Greybox).
6. Die Neutralität des Prüfers ist seine wichtigste Eigenschaft. Diese ist in Gefahr, wenn der Prüfer bei der Entstehung des Prüfgegenstands involviert war oder das Ergebnis einer Prüfung ihm Nutzen oder Schaden bringt. Sicherheitslücken können niemals mit derselben Denkweise gelöst werden, mit der sie entstanden sind (frei nach Albert Einstein).
7. Oftmals fehlt es an einem passenden Budget oder Zeitfenster zur Durchführung eines Penetrationstests. Es wäre jedoch falsch, als Konsequenz gänzlich auf den Test zu verzichten. Selbst ein kompakter Test nutzt der eigenen IT-Sicherheit.
8. Sogenannte Distributed Denial-of-Service (DDoS)-Angriffe offenbaren, ob ein System Sabotageangriffen standhält oder nicht. IT-Ressourcen wie Bandbreite oder CPU-Leistung sind aber prinzipiell auch ohne Penetrationstest erschöpfbar. Nach unserer Auffassung sollten solche Attacken vermieden werden, weil der zu erwartende Erkenntnisgewinn in keinem attraktiven Verhältnis zu möglichen negativen Auswirkungen steht.
9. Es ist offensichtlich, dass niemals sämtliche Systeme einer exakten Prüfung unterzogen werden können. Daher ist die Wahl einer repräsentativen Stichprobe wesentlich für einen effizienten Test. Diese ergibt sich aus einem sinnvollen Clustering, bei dem sich die Prüfgegenstände innerhalb eines Clusters stark ähneln, die Cluster selbst jedoch verschieden sind. Wird aus jedem Cluster ein Repräsentant untersucht, so erhält man eine sinnvolle Balance zwischen Aufwand und Ertrag.
10. Wir erleben häufig, dass der Nachtest immer wieder verschoben wird mit dem Ziel, vorher alle Lücken zu beheben. Das verschleppt die Durchführung des Nachtests und lähmt den Prozess der kontinuierlichen Verbesserung. Wir empfehlen daher, den Nachtest auch dann durchzuführen, wenn noch nicht alle Lücken geschlossen sind, zum Beispiel vier Wochen nach Abschluss des Haupttests. In der Regel handelt es sich bei einem Nachtest um ein vergleichsweise kleines Projekt, sodass eine Wiederholung des Nachtests nach weiteren sechs Wochen verglichen mit dem Gesamtbudget nicht wesentlich ins Gewicht fällt.

1.3 Standardtestphasen

Ein Sicherheitstest besteht aus einem Rahmenprojekt, Standardtestphasen und einzelnen Testmodulen. Abbildung 1.1 auf der nächsten Seite verdeutlicht den Projektablauf und dessen Gestaltungsmöglichkeiten: Dieser Abschnitt befasst sich mit den Standardtestphasen, die in der Regel feste Bestandteile eines Penetrationstests bilden. Die detaillierte Beschreibung der Testmodule, die je nach Testgegenstand variieren, finden Sie in Kapitel 2.

1.3.1 KICKOFF: Vorbesprechung des Projekts

In einer Vorbesprechung – in der Regel in der Form eines telefonischen Kick-off-Gesprächs – wird der Projektablauf gemeinsam geplant. Der Consultant, der den Test leitet, geht daher mit einem Ansprechpartner des Kunden unter anderem folgende Themen durch:

- Testzeitraum und Testzeitfenster
- Ansprechpartner und deren Erreichbarkeit
- Besprechung des Testgegenstands
- Notwendige Voraussetzungen (beschrieben beim jeweiligen Modul)
- Umgang mit der Erkennung von DoS-Potenzialen
- Allgemeines zur Durchführung (beschrieben beim jeweiligen Modul)
- Festlegen der Sprache, in der der Bericht geschrieben werden soll (Deutsch oder Englisch)
- Anzahl der gedruckten Exemplare des Berichts
- Fragen und Wünsche zum Testablauf

Je nach speziellem Testgegenstand und je nach gewählten Modulen gibt es individuelle Abweichungen. Wenn von der Durchführung eines Tests, wie bei den einzelnen Modulen beschrieben, abgewichen werden muss, wird dies ebenfalls zu diesem Zeitpunkt besprochen. Die Ergebnisse des Kick-off-Gesprächs werden protokolliert und dem Kunden zeitnah zur Verfügung gestellt.

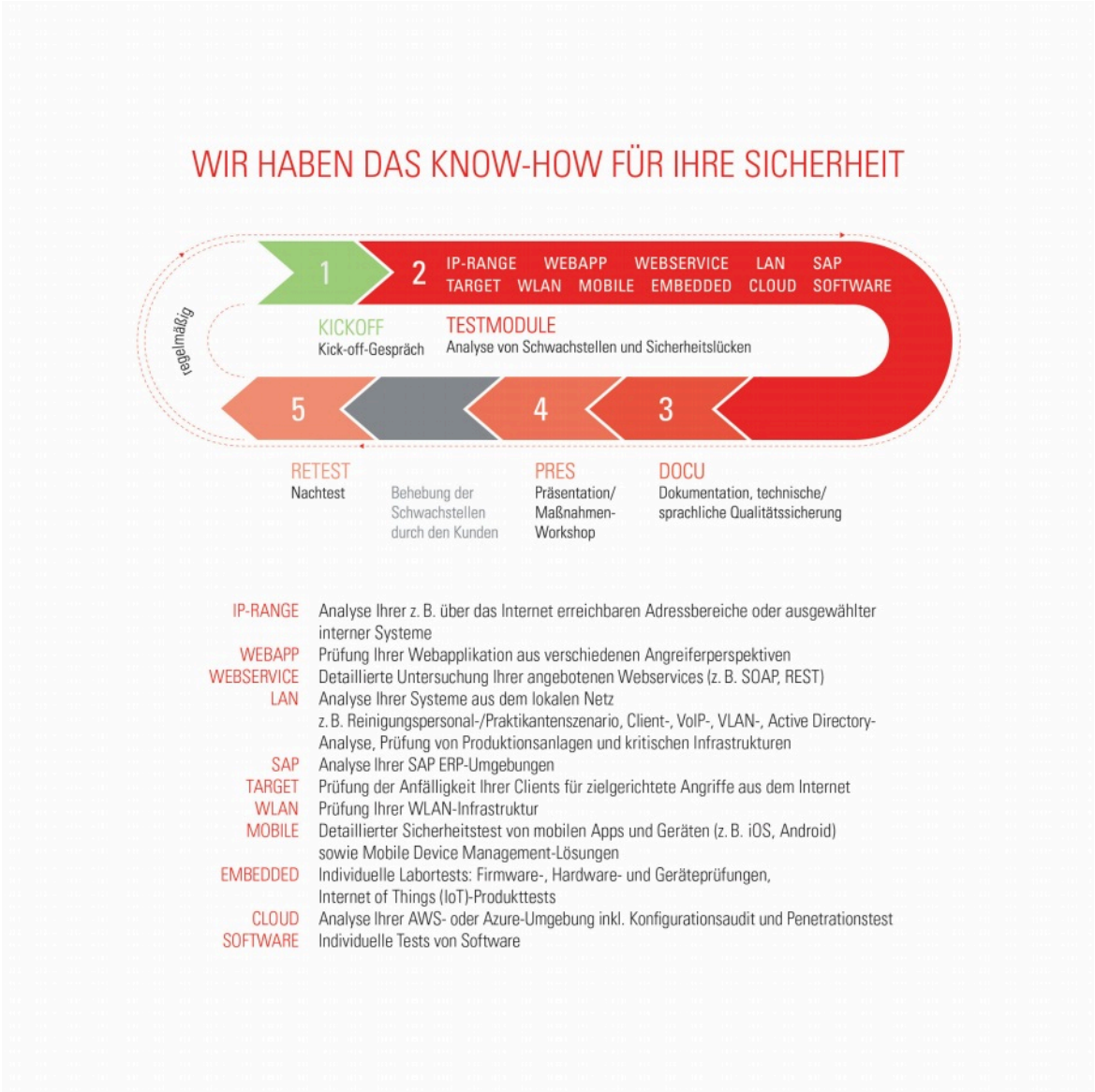

Abbildung 1.1: Ablaufschema eines Penetrationstests

Tipp von Sebastian Schreiber

Prüfen Sie vor dem Kick-off-Gespräch die im jeweiligen Modulabschnitt unter „Mitwirkung des Kunden" genannten Punkte und Tipps! Je mehr Zeit Sie sich für die Vorbereitung und die Durchführung des Kick-off-Gesprächs nehmen, desto effizienter wird der Test und desto mehr wird er Ihrem Unternehmen nützen!

1.3.2 MODULE: Durchführung der Sicherheitsprüfung (gewählte Module)

Die Durchführung des vom Kunden in Auftrag gegebenen Sicherheitstests wird durch die gewählten Module bestimmt. Diese bilden das Kernstück eines jeden Projekts und betten den Testgegenstand in seinen Kontext ein. Die Module geben ganz allgemein vor, welche Voraussetzungen für die Sicherheitsüberprüfung notwendig sind und wie die Durchführung des Tests grob verlaufen wird. Sie fungieren als Rahmen des durchzuführenden Sicherheitstests und geben lediglich Anhaltspunkte zum möglichen Ablauf, denn im Detail verläuft jeder Sicherheitstest individuell gemäß dem vom Kunden festgelegten Testgegenstand.

Die einzelnen möglichen Testmodule werden in Kapitel 2 ausführlich beschrieben und illustrieren die Vielfalt an Gestaltungsmöglichkeiten für jegliche Sicherheitstests. Durch unsere Erfahrung können wir selbst auf ausgefallene Testanliegen unserer Kunden eingehen. Ebenso ist die Liste der Module dynamisch, denn sie wird stetig erweitert und den gegenwärtigen Anforderungen, Wünschen und Bedürfnissen unserer Kunden angepasst.

1.3.3 DOCU: Dokumentation

Alle Testergebnisse werden am Ende des Projekts in einem Bericht zusammengefasst. Der Bericht umfasst die folgenden Bestandteile:

- Zusammenfassung der Ergebnisse („Executive Summary“) und Einschätzung des allgemeinen Sicherheitsniveaus
- Liste der festgestellten Schwachstellen mit Risikoeinschätzung[1] und Maßnahmen zur Behebung
- Nachvollziehbare Darstellung des Nachweises jeder erkannten Schwachstelle
- Auszüge aus den Ausgaben der Testwerkzeuge, wo dies sinnvoll erscheint
- Dokumentation von Besonderheiten während des Testablaufs
- Falls explizit gewünscht, Kommunikationsnachweis mit dem Kunden

Der Kunde teilt mit, wie viele gedruckte Exemplare des Berichts benötigt werden. Der Bericht wird SySS-intern gedruckt und gebunden. Er wird dem Kunden als Einschreiben mit Rückschein (auch ins Ausland) verschickt. Zusätzlich erhält der Kunde den Bericht als PDF-Datei. Auf Wunsch erhält der Kunde die beim Test entstandenen Rohdaten (Ausgaben der Testwerkzeuge). Allerdings werden diese unbearbeitet zur Verfügung gestellt, beispielsweise werden Falsch-Positive aus den Ergebnissen der Schwachstellenscanner nicht entfernt. Soweit nicht anders vereinbart, löscht die SySS die Rohdaten drei Monate nach Testende bzw. drei Monate nach einem eventuellen Nachtest.

Der Dokumentationsaufwand ist bei internen Tests erheblich höher, da insbesondere das Testvorgehen detaillierter beschrieben werden muss. Die Maßnahmen zur Behebung der Schwachstellen werden zudem mit dem Ansprechpartner während des Dokumentationsprozesses besprochen. Die Tabelle auf der folgenden Seite ist ein Beispiel für eine Liste von Sicherheitsschwächen mit Maßnahmenvorschlägen:

Risiko	Feststellung	Empfehlung	Referenz
H1.1	**www.kunde.de** Konfigurationsdatei enthält gültige Anmeldedaten für das TYPO3-Back-End	Betroffene Datei vom Server entfernen oder Zugriff durch ACL unterbinden	2.1.1 Seite 7
H2.1	**198.51.100.1** Der Router verwendet ein vom Hersteller gesetztes Standardpasswort	Nutzername und Passwort ändern	3.1.1 Seite 19
M1.1	**www.kunde.de** Anmeldedaten sowie das Session-Cookie werden über eine unverschlüsselte Verbindung übertragen	Anmeldedaten und Session-Cookies ausschließlich über verschlüsselte Verbindungen übertragen	2.2.2 Seite 9
M2.1	**198.51.100.111** Der SMB-Dienst gestattet lesenden Zugriff auf Netzwerkfreigaben	Dienst an der Firewall filtern	3.4.7 Seite 29

Fortsetzung nächste Seite …

[1] Auf Wunsch bieten wir auch eine Bewertung gemäß gängiger Scoring-Schemata wie CVSS oder CWSS an.

Risiko	Feststellung	Empfehlung	Referenz
L1.1	**www.kunde.de** Die Passwortrichtlinie erlaubt die Vergabe von trivialen Passwörtern	Passwortrichtlinie überarbeiten	2.3.9 Seite 14
I1.1	**www.kunde.de** Die Anmeldeseite kann zur Benutzerenumeration missbraucht werden	Keine Rückmeldung über die Existenz eines Benutzers geben	2.3.9 Seite 13

1.3.4 PRES: Präsentationsworkshop

Die Ergebnisse des gesamten Tests können in Form einer Präsentation mit Workshopcharakter beim Kunden vor Ort dargestellt werden. Bewährt hat sich eine zweiteilige Vorgehensweise:

Begonnen wird mit dem Briefing für die Entscheidungsebene („Management Summary“) mit einer Dauer von etwa 30 Minuten. Hier werden grundlegende Ergebnisse des Tests auf strategischer und organisatorischer Ebene besprochen. Für diesen Teil steht auf Wunsch auch der Geschäftsführer der SySS, Sebastian Schreiber, zur Verfügung.

Der zweite Teil ist ein technischer Workshop, der für Systemverantwortliche und Administratoren gedacht ist. An dieser Stelle gibt es die Möglichkeit, tiefgreifende Fragen zu stellen und mögliche Lösungsansätze zu diskutieren. Dieser Teil wird vom leitenden Consultant des Tests übernommen.

1.3.5 RETEST: Nachtest

Der Nachtest hat die Aufgabe, die Wirksamkeit der Maßnahmen zur Behebung von Sicherheitsschwächen zu messen, die in vorangegangenen Tests erkannt wurden.

Nach der Identifikation der Sicherheitslücken durch einen Test ist deren Behebung fällig. In der Regel ist hierfür keine besondere Beratungsleistung nötig, dennoch sollten die Ergebnisse dieser Maßnahmen zur Behebung verifiziert werden. Aus diesem Grund ist es ratsam, etwa nach zwei bis vier Wochen, aber spätestens nach einem halben Jahr, einen Nachtest durchzuführen. Hierbei wird in der Regel nicht nach neuen Verwundbarkeiten gesucht, sondern der Status der bereits bekannten Sicherheitslücken untersucht und dokumentiert. Das Vorgehen wird im Vorfeld besprochen. Als Dokumentation wird der bereits erzeugte Bericht des Haupttests zugrunde gelegt und das „Executive Summary“ angepasst. Eine Abschätzung des für einen Nachtest erforderlichen Aufwands ist erst dann sinnvoll zu leisten, wenn die Ergebnisse aus dem Haupttest bekannt sind.

1.4 Penetrationstests in agilen Umgebungen

Bei einem Penetrationstest beziehen sich die Befunde immer auf den konkreten Zeitpunkt der Analyse. Wird der Test zum Beispiel ein Jahr später wiederholt, so ist die vorgefundene Situation stets eine veränderte, was vor allem an den folgenden beiden Punkten liegt:

– Die Angriffswerkzeuge/Hacking-Methoden sind mächtiger und/oder effizienter geworden.
– Der Prüfgegenstand selbst hat sich verändert.

Neben turnusmäßigen Penetrationstests sind anlassbezogene Penetrationstests von großer Bedeutung, insbesondere bei agilen Entwicklungen wie Applikationen, mobilen Apps etc. Um Änderungen am Prüfgegenstand gerecht zu werden, wird ein Penetrationstest oft vor jedem Release durchgeführt. So stellt der Penetrationstest ein „Quality Gate" dar, das vor dem Livegang des neuen Release passiert werden muss. Teilweise ist ein bestandener Penetrationstest sogar ein im Werkvertrag vereinbartes Abnahmekriterium.

Bei agilen Entwicklungen werden hochfrequent neue Releases erstellt. Erhöht man im gleichen Maße die Penetrationstests, so vervielfachen sich mit dem Anstieg der Releases auch die Kosten für das Pentesting – und die Sicherheit droht am Kostenfaktor zu scheitern. Um dies zu verhindern, bieten sich die folgenden Alternativen zu hochfrequenten Penetrationstests:

- Verzicht auf situative Penetrationstests bei agilen Entwicklungen
- Tests von z. B. nur jedem dritten Release bzw. jedem Release, das vom Product Owner anerkannt wurde
- Differenzielle Penetrationstests: Prüfung nur jener Komponenten, die seit dem letzten Penetrationstest ergänzt bzw. geändert wurden

Die dritte Alternative scheint attraktiv zu sein. Voraussetzung hierfür wäre jedoch, dass feststellbar ist, welche Pfade in einer Webapplikation besucht werden müssen, um genau jene Webseiten und Formulare zu untersuchen, deren Sicherheit möglicherweise von einer konkreten Quelltextänderung betroffen ist. Enthält das neue Release eines Webshops zum Beispiel zum ersten Mal eine Zahlungsschnittstelle, so wird ausschließlich diese dem Penetrationstest unterzogen. Wird allerdings die Effizienz einer Applikation oder das Interface zur Datenbank optimiert oder eine große Anzahl kleiner Änderungen programmiert, dann kann dies Auswirkungen auf die Sicherheit sämtlicher Applikationsteile haben: Es ergäbe sich wieder ein Volltest.

Alle drei Alternativen scheinen Nachteile zu haben und erwecken zunächst den Eindruck, man könnte in agilen Umgebungen keine guten Penetrationstests durchführen. Dies ist jedoch ein Trugschluss. Ihm liegt der Gedanke zugrunde, dass Schwachstellen „nur" deswegen aufgespürt werden, um sie schließlich beheben zu können. Gerade bei Entwicklungen empfehlen wir eine erweiterte Perspektive: Parallel zur Ausbesserung der Schwachstellen müssen auch die internen Prozesse und die Denkweisen der Entwickler optimiert werden, denn nach der Entwicklung ist vor der Entwicklung! Wer nur die Findings in der Schwachstellenliste des Penetrationstests sukzessive mit „behoben" kennzeichnet, dem entgeht ein wichtiger Nutzen. Es ist bedeutend, das Übel an der Wurzel zu packen, also durch Penetrationstests nachhaltig bei der Entwicklung zu helfen – und genau dieser Nutzen ist völlig unabhängig von der Frequenz der Releases.

Tipp von Sebastian Schreiber

Nutzen Sie die durchgeführten Penetrationstests in agilen Umgebungen nicht nur für eine reine Schwachstellenbehebung, sondern vor allem als Prüfstand der Entwicklung Ihres Produkts. Dazu lohnt es sich, die folgenden zentralen Fragen zu stellen und nach Antworten zu suchen:

- Was ist bei uns schiefgelaufen, dass unser Produkt die Schwachstelle XY hatte?
- Was haben wir bei der Planung nicht berücksichtigt?
- Wie können wir besser werden und sicherstellen, dass diese Schwachstelle in Zukunft nicht mehr auftritt?

2 Penetrationstests – Testmodule

Dieses Kapitel enthält detaillierte Beschreibungen einiger unserer Standardtestmodule. Sollten Sie darüber hinaus eine Prüfung eines Testgegenstands wünschen, der sich nicht über eines unserer Standardtestmodule abdecken lässt, so wird eine individualisierte Testvorgehensweise erarbeitet und vorgeschlagen.

2.1 IP-RANGE: Analyse ausgewählter Systeme

Zusammenfassung

Ausgewählte interne oder über das Internet erreichbare IP-Adressen oder auch ganze IP-Adressbereiche werden auf konkrete Sicherheitsschwächen hin geprüft und die von ihnen ausgehenden Risiken werden bewertet.

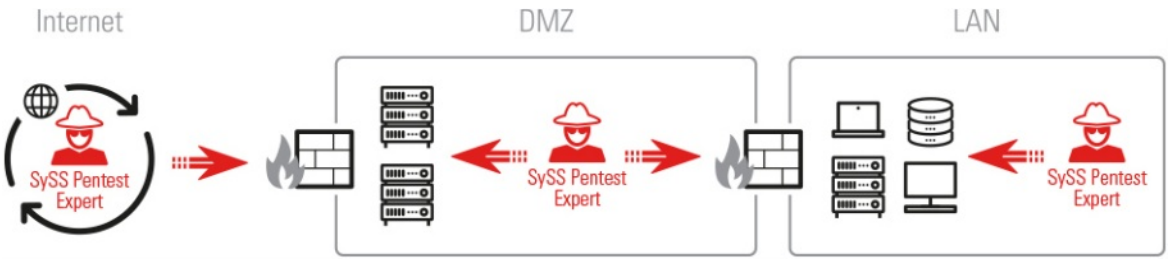

Abbildung 2.1: Mögliche Ausprägungen des Moduls IP-RANGE

Ausgangslage

Im Rahmen dieses Moduls werden einzelne Systeme oder auch Gruppen (Cluster) von Systemen auf Schwachstellen hin analysiert. Dies können zum einen ausgewählte interne Systeme sein, wie zum Beispiel die Infrastruktur einer wichtigen Applikationsumgebung oder auch die Analyse „kritischer Infrastrukturen", wie beispielsweise das Netzsegment für Industriesteuerungsanlagen und SCADA-Systeme. Zum anderen kann es sich aber auch um direkt aus dem Internet erreichbare und somit besonders exponierte Systeme handeln, die beispielsweise innerhalb einer eigenen Demilitarized Zone (DMZ) betrieben werden.

Insbesondere beim Betrieb von Systemen im Internet bestehen mehrere Arten von Risiken. So können Sicherheitsschwächen in einzelnen Diensten bestehen, die Dritten folgende Möglichkeiten erlauben:

- Sie können unter Umständen Informationen über die Systeme und eingesetzte die Software erlangen, die für weitere Angriffe dienlich sind.
- Sie können vertrauliche Daten und Informationen einsehen, die nicht system- oder softwarebezogen sind.
- Sie können in das System eindringen und es für eigene Zwecke oder weitere Angriffe nutzen.
- Sie können Daten manipulieren.
- Ebenso kann die Erreichbarkeit der Systeme eingeschränkt werden.

Zielsetzung

Ziel eines Sicherheitstests im Rahmen des Moduls IP-RANGE ist, die zu testenden Systeme abhängig von der Testtiefe auf die oben genannten Risiken zu prüfen. Wie in Abschnitt „Risiko Denial-of-Service“ (siehe Abschnitt 1.2.3 auf Seite 11) beschrieben ist, besteht das Ziel eines Tests nicht darin, Systeme oder Dienste zum Stillstand zu bringen, sondern derartige Potenziale lediglich aufzudecken.

Im Rahmen des Moduls IP-RANGE werden Webapplikationen oder Webservices nicht geprüft, dafür sind die Module WEBAPP (siehe Abschnitt 2.2 auf der nächsten Seite) respektive WEBSERVICE (siehe Abschnitt 2.3 auf Seite 27) vorgesehen. Eine Werthaltigkeitsanalyse der gefundenen Daten wird nicht durchgeführt, da die Erfahrung zeigt, dass unsere Kunden dies ohne Weiteres selbst vornehmen können und auch müssen.

Durchführung

Die Art der Durchführung wird vom leitenden Consultant bestimmt, läuft jedoch im Normalfall nach diesem Schema ab:

- Überprüfung der vom Kunden zur Verfügung gestellten Daten auf Korrektheit
- Identifizierung von Betriebssystemen und erreichbaren Diensten
- Test der erkannten Dienste mit Schwachstellenscannern
- Überprüfung der Ergebnisse, Verifizierung von erkannten Sicherheitslücken
- Einsatz von Werkzeugen, die Gebiete abdecken, die von Schwachstellenscannern nicht berücksichtigt werden
- Manuelle Prüfungen
- Nachweis von DoS-Potenzialen nach Absprache mit dem Kunden

Anhand der vorliegenden Informationen wählen die testenden Consultants die Werkzeuge aus, die den Erfolg des Tests am besten unterstützen. Einige Beispiele finden Sie unter „Werkzeuge“ (siehe Abschnitt 1.1.6 auf Seite 10).

Durch die von der SySS entwickelte Pentestbox (siehe Abschnitt 2.4.7 auf Seite 38) kann der IP-Range-Test, der das Ziel hat, interne oder in einer DMZ betriebene Systeme zu analysieren, auch aus der Ferne (remote) durchgeführt werden.

Mitwirkung des Kunden

Damit ein Sicherheitstest effizient und mit hohem Nutzen für den Kunden durchgeführt werden kann, braucht es einige Rahmenbedingungen. Ansonsten wird der Test erschwert oder es treten Verzögerungen und zusätzliche Kosten auf.

- Die IP-Adressen der zu testenden Systeme müssen rechtzeitig vor dem eigentlichen Testbeginn vorliegen.
- Für den Test von Systemen Dritter muss deren schriftliches Einverständnis vorliegen.
- Bei der Wahl der Testzeit (im Rahmen des Kick-off-Gesprächs wie in Abschnitt 1.3.1 auf Seite 16 beschrieben) müssen Wartungsfenster, Zeitzonenabhängigkeiten (beim Test von Systemen im Ausland) und Feiertage beachtet werden.
- Innerhalb der oben genannten Testzeit sollten Ansprechpartner tatsächlich erreichbar und handlungsfähig sein.
- Die Ansprechpartner sollten einen Überblick über die internen Zuständigkeiten bei den getesteten Systemen haben; dies reduziert den Kommunikationsaufwand während des Tests.
- Unsere Quell-IP-Adressen sollten in möglicherweise zum Einsatz kommenden Schutzmechanismen wie Intrusion Prevention-Systemen temporär freigeschaltet werden.
- Die Zuständigkeiten sollten geklärt sein.

Sie können die Testqualität weiter erhöhen, wenn Sie Ihre Dokumentation über die zu testenden IP-Adressen vor dem Test prüfen lassen.

Tipp von Sebastian Schreiber

Stellen Sie vor dem Test sicher, dass die betroffenen Mitarbeiter und Systembetreuer informiert sind, damit der Test positiv aufgenommen wird.

2.2 WEBAPP: Prüfung von Webapplikationen

Zusammenfassung

Ausgewählte Webapplikationen werden aus verschiedenen Perspektiven auf ihre Sicherheit hin getestet. Dabei werden Sicherheitslücken gesucht, die auf der eingesetzten Software, ihrer Konfiguration oder der Applikationslogik beruhen. Auch zugrunde liegende Systeme (Providing Infrastructure), wie zum Beispiel Web-, Applikations- oder Datenbankserver, werden auf Schwachstellen hin untersucht.

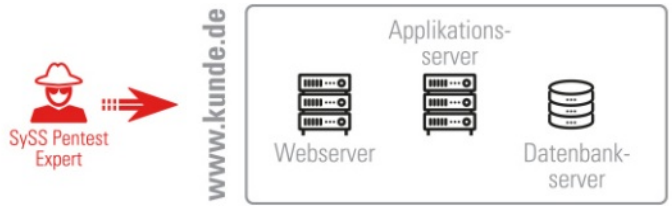

Abbildung 2.2: Modul WEBAPP

Ausgangslage

Bei Webapplikationen besteht grundsätzlich ein hohes Risiko, dass unautorisiert auf Daten sowohl des Kunden als auch von Dritten zugegriffen werden kann, was einem Verlust an Vertraulichkeit gleichkommt. Zusätzlich ist die Interaktion des Benutzers mit der Website relevant, denn besonders durch Cross-Site Scripting (XSS)-Schwachstellen können sowohl externe als auch interne Benutzer gefährdet werden.

Eine Besonderheit bei Webapplikationen ist die meist komplexe Abhängigkeit von anderen Systemen, zum Beispiel Applikations- oder Datenbankservern. Diese können durch Schwachstellen in der Applikation ebenfalls beeinträchtigt werden. Im Falle einer Datenbankanbindung könnten unter Umständen sogar schützenswerte Informationen aus der Datenbank gewonnen werden. Diese Abhängigkeiten können auch bezüglich eingesetzter Middleware und – im organisatorischen Sinn – bezüglich herangezogener Lieferanten bestehen. Zudem kann die Sicherheit einer Webapplikation nicht allein durch die Applikation selbst, sondern auch durch ein möglicherweise als Grundlage verwendetes Content Management System (CMS) bestimmt werden.

Eine weitere Besonderheit von Webapplikationen ist, dass viele Sicherheitsprobleme nach deren Bekanntwerden auch von Laien nachvollzogen werden können. Dies geht oft mit einem Imageschaden und Vertrauensverlust einher.

Zielsetzung

Auch bei diesem Testmodul besteht die Aufgabe darin, festzustellen, ob die oben genannten Risiken vorliegen. Die Bewertung des Risikos einer einzelnen Schwachstelle erhält bei diesem Test eine höhere Bedeutung, denn das Vorhandensein eines konkreten Risikos deutet meistens auf ein allgemeines Problem hinsichtlich der Anwendungsentwicklung hin: Beispielsweise weist eine XSS-Lücke auf eine generell unsauber implementierte serverseitige Eingabevalidierung hin.

Ein weiterer Testschwerpunkt behandelt die Frage, ob es möglich ist, durch Ausnutzung der typischen Schwachstellen von Webapplikationen Einsicht in Daten des Kunden oder Dritter zu erhalten. Das Sicherheitsniveau der Anwendung wird abschließend eingeschätzt und Maßnahmen zur Behebung eventueller Schwachstellen werden vorgeschlagen.

Durchführung

Die Durchführung eines Penetrationstests ist bei Webapplikationen stark von deren Funktion und Aufbau abhängig. Ein festes Schema für den Testablauf kann daher nicht aufgestellt werden, der Ablauf entspricht aber grob dem folgenden Muster:

Prüfung der Providing Infrastructure: Wird lediglich eine Prüfung der Webanwendung, nicht jedoch auch eine gründliche Analyse der Providing Infrastructure beauftragt, so werden weitere möglicherweise auf dem Webserver erreichbare Dienste nicht mitgeprüft. Wird die Analyse der Providing Infrastructure explizit gewünscht, so finden zusätzlich Portscans zur Ermittlung weiterer auf diesen Systemen erreichbarer Dienste statt. Im Anschluss werden sämtliche Dienste einer Schwachstellenanalyse unterzogen (wie im Modul IP-RANGE, siehe Abschnitt 2.1 auf Seite 21). Zum Beispiel werden auch Schwächen in der Konfiguration des eingesetzten Webservers selbst sowie in eingesetzten SSL/TLS-Komponenten analysiert. Hierbei kommen in Abhängigkeit von den erreichbaren Diensten unterschiedliche Werkzeuge zum Einsatz. Schwachstellenscanner wie z. B. Nessus gehören zum Standardrepertoire bei derartigen Tests. Ziel dieser Überprüfung ist es, auch Schwachstellen abseits der für die Webapplikation bereitgestellten Dienste zu identifizieren.

Strukturermittlung: Bezüglich des eigentlichen Tests der Webapplikation wird in einer ersten Phase die Struktur der zu prüfenden Webanwendung analysiert. Hierfür kommen neben verschiedenen automatisierten Methoden (Spider/Crawler) auch manuelle Verfahren zum Einsatz. Das vorrangige Ziel dieser Phase ist, die für einen Angreifer interessanten Bereiche der Anwendung zu identifizieren.

Test des Authentifizierungskonzepts und der Sitzungsverwaltung: Erfordert die Anwendung eine Benutzeranmeldung, so werden in einem nächsten Schritt mögliche Angriffe gegen das Authentifizierungskonzept eruiert. Hierbei werden neben rein technischen (z. B. Umgehung der Authentifizierung durch SQL Injection-Angriffe) auch programmatisch-konzeptionelle Schwachstellen (z. B. Möglichkeiten der Benutzerenumeration, Passwort-Reset-Funktionen, Passwort-Rate-Angriffe, Kontensperrungen usw.) betrachtet. Alle weiteren Tests werden optimalerweise unter Verwendung mehrerer Benutzerkonten mit – wenn möglich – unterschiedlichen Rollen durchgeführt. Anschließend erfolgt – falls vorhanden – eine Untersuchung des implementierten Sitzungskonzepts. Im Fokus stehen hierbei grundsätzliche Schwachstellen, die die Durchführung von Identitätsdiebstählen ermöglichen können. Geprüft werden unter anderem Sitzungsbezeichner, Cookie-Attribute, Session Handling und Pre-Authentication-Schwachstellen.

Prüfung der Eingabevalidierung: Im Vordergrund steht hierbei eine Prüfung der Funktionalität der serverseitigen Payload-Verifikation mittels klassischer Angriffsvektoren (verschiedene Formen des Cross-Site Scripting, SQL Injection, URL Injection, LDAP Injection, OS Command Injection, XPath Injection, XML Injection usw.). Hierfür werden neben manuellen Eingabeprüfungen auch Payload-Manipulationen unter Verwendung von Browser-Plug-ins und Analyseproxys, wie z. B. der Burp Suite Professional, durchgeführt. Wo bedingt durch Umfang und Komplexität der Anwendung angebracht, kommen automatisierte Webapplikationsscanner zum Einsatz, deren Ergebnisse im Anschluss manuell verifiziert werden.

Analyse der Applikationslogik und des Autorisierungskonzepts: In einem weiteren Schritt wird die Applikation auf möglicherweise fehlerhafte Konsistenz- oder Plausibilitätsprüfungen innerhalb der Anwendungslogik untersucht. Klassische Beispiele wären an dieser Stelle die Möglichkeit einer Preismanipulation innerhalb eines Webshops, Anfälligkeiten für gefälschte Antworten von eingebundenen Drittsystemen – etwa Zahlungsdienstleister – oder unerlaubte Verzweigungen innerhalb der Anwendungslogik, etwa durch Manipulation von in den Client verlagerten Logikkomponenten, die beispielsweise über Hidden Fields transportiert werden. Zudem wird das von der Anwendung umgesetzte Autorisierungskonzept geprüft. Auch hierfür sollten idealerweise mehrere Testkonten zur Verfügung gestellt werden, um Zugriffsmöglichkeiten auf Daten und Funktionen anderer Benutzer bzw. Rollen effizient prüfen zu können.

Reverse Engineering: Optional können vom Server ausgelieferte (auch binäre) Clientkomponenten analysiert werden, z. B. Java-Applets oder Flash-Anwendungen. Hierfür werden spezielle Decompiler sowie Reverse Engineering-Techniken eingesetzt. Grundsätzlich wird – abhängig von den jeweils gemachten Feststellungen – eine als Proof of Concept (PoC) geeignete Angriffssoftware entwickelt. Ziel ist hierbei in erster Linie die Verifikation der Feststellungen sowie die Erlangung weiterer Informationen oder Berechtigungen.

OWASP Top 10: Bei der Suche nach Schwachstellen orientiert sich die SySS stark an den jeweils aktuellen OWASP Top 10. Das Open Web Application Security Project (OWASP) pflegt seit vielen Jahren eine Liste der zehn häufigsten Risiken bei Webapplikationen. Diese Liste ist dynamisch und wird regelmäßig überarbeitet. Darüber hinaus wird auch eine Reihe weiterer Schwachstellenklassen geprüft, die entweder nicht in den OWASP Top 10 enthalten sind oder seitdem neu veröffentlicht wurden.

Schwachstellenscannern kommt bei diesem Testmodul nur eine unterstützende Rolle zu. Dies gilt auch für diejenigen, die speziell für den Test von Webapplikationen vorgesehen sind, da Scanner nur sehr eingeschränkt in der Lage sind, kontextbezogene Informationen zu verwerten und zu beurteilen. Daher ist das Hauptwerkzeug bei der Untersuchung von Webapplikationen immer ein Browser, mit dem manuelle Prüfungen durchgeführt werden. Bevorzugt wird hier Mozilla Firefox eingesetzt, da für diesen Browser eine große Auswahl an Add-ons zur Verfügung steht. Zusätzlich werden zur Verifizierung und Demonstration von Schwachstellen bei Bedarf eigene Skripte geschrieben.

Dennoch kann die Untersuchung von Webapplikationen durch den Einsatz von Security-Scannern bzw. entsprechenden Proxys sinnvoll unterstützt werden. Zum Einsatz kommen hier unter anderem Nessus, SQLmap und Burp Suite Professional.

Mitwirkung des Kunden

Für den Test muss auf jeden Fall die URL der Webapplikation mitgeteilt werden. Ferner muss definiert werden, welche Bereiche der Webapplikation geprüft werden sollen. Beispiele hierfür sind öffentlich erreichbare Bereiche der Seite, nur für angemeldete Benutzer verfügbare Funktionen sowie zu einem möglicherweise zum Einsatz kommenden Content Management System gehörende Bereiche, zum Beispiel Administrationsoberflächen. Zudem muss geklärt werden, von wo aus der Test erfolgt (über das Internet, aus einem bestimmten Intranetbereich heraus o. Ä.).

Ansprechpartner: Die Analyse von Webapplikationen unterscheidet sich nicht nur beim Vorgehen erheblich von anderen Testmodulen. Wie bereits erwähnt, können Sicherheitsprobleme in der Webapplikation auch weitere Dienste betreffen, insbesondere Datenbanken und E-Mail-Dienste.

Darüber hinaus kommen Webapplikationen bzw. deren Funktionalität in der Regel nicht aus einer Hand: Die Gestaltung kann in den Händen einer Agentur liegen, das Programmieren der Webapplikation kann sowohl von internen als auch von externen Programmierern übernommen werden. Die Hardware selbst kann wiederum von einem Webhoster gestellt und auch betreut werden.

Insbesondere zur Behebung der festgestellten Sicherheitsschwächen ist es notwendig, mit denjenigen Personen Kontakt aufzunehmen, die für die jeweils betroffenen Elemente zuständig sind. Daher ist es für den durchführenden Consultant von sehr großer Bedeutung, die Kontaktdaten der Ansprechpartner zu kennen.

Ist kein direkter Ansprechpartner definiert oder verfügbar, können daraus zweierlei Probleme entstehen:

– Rückfragen während des Tests, die zur Verifizierung von Sicherheitsschwächen dienen, können nicht beantwortet werden, was wiederum zu Verzögerungen führt.
– Sind die Verantwortlichen für eine Funktion, die von einer Sicherheitslücke betroffen ist, nicht bekannt, verzögert sich die Behebung der Schwachstelle erheblich.

Aus diesem Grund sollte rechtzeitig vor dem Test mit der Klärung der Zuständigkeiten und Feststellung der Verantwortlichen begonnen werden, auch wenn dies im ersten Schritt aufwendig zu sein scheint. Anschließend sollten die Betroffenen über Termin und Ziel des Tests informiert werden. Ebenso wie bei anderen Testmodulen können sie auf Wunsch dem Test beiwohnen. Falls Dritte betroffen sind, müssen diese der Durchführung des Tests zustimmen (in Form einer schriftlichen Einverständniserklärung). Zusätzlich sollte während des Tests ein Ansprechpartner, der mit der Webapplikation aus der Benutzerperspektive vertraut ist, für Rückfragen zur Verfügung stehen.

Die Tests erfolgen stets in enger Zusammenarbeit mit den Ansprechpartnern. Hierdurch wird zum einen garantiert, dass eventuell auftretende Verfügbarkeitsprobleme zeitnah erkannt und ausgeräumt werden können. Zum anderen wird sichergestellt, dass vor allem die kritischen Schwachstellen sofort behoben werden können.

Abhängigkeiten: Organisatorische und technische Abhängigkeiten sollten der SySS mitgeteilt werden. Dies kann im Rahmen des Kick-off-Gesprächs geschehen.

Status der Webapplikationen: Die zu testenden Funktionen müssen möglichst durchgängig verfügbar sein. In der sehr frühen oder mittleren Umsetzungsphase einer neuen Webapplikation bringt ein Test keine nachhaltigen Ergebnisse. Er kann aber dennoch sinnvoll sein, wenn möglichst früh entscheidungsrelevante Ergebnisse vorliegen müssen.

Zudem sollte davon abgesehen werden, während der Testzeit Updates durchzuführen. Das hat den Hintergrund, dass sich zum einen die Testtiefe verringern kann, da während des Updates keine Tests durchgeführt werden können. Zum anderen kann keine zuverlässige Aussage über den aktuellen Sicherheitsstand der Applikation getroffen werden, wenn sich während der Testzeit Funktionalitäten ändern und dadurch nicht umfassend geprüft werden.

Anmeldeinformationen: Viele Webapplikationen bieten zusätzliche Funktionen in einem internen Bereich an, der erst nach erfolgreicher Anmeldung sichtbar wird, beispielsweise bei einem Kundenportal.

Für den Test dieser Funktionen benötigt die SySS mindestens zwei Benutzerkonten mit unterschiedlichen Berechtigungsstufen, aus deren Sicht der Test durchgeführt werden soll. Stehen keine entsprechenden Konten zur Verfügung, kann ein Test nur aus der Perspektive eines Besuchers der Webseite durchgeführt werden. Dies führt meist zu lediglich geringen Erkenntnissen bezüglich des Sicherheitsniveaus der Webapplikation. Die Erfahrung zeigt, dass ein Angreifer mit genügend Zeit und dem Einsatz von Social Engineering-Techniken mit hoher Wahrscheinlichkeit in der Lage ist, einen Benutzer zu übernehmen. Daher wird empfohlen, diese Testnutzer zur Verfügung zu stellen, vor allem, weil der Penetrationstest in einem beschränkten zeitlichen Rahmen stattfindet. Um sinnvolle Ergebnisse zu erhalten, dürfen die Rechte der Benutzerkonten gegenüber denen regulärer Anwender nicht eingeschränkt sein. Wie diese Konten erzeugt werden, wird beim Kick-off-Gespräch (siehe Abschnitt 1.3.1 auf Seite 16) besprochen.

Testdaten oder Testsystem: Falls der Test nicht mit produktiven Daten oder auf produktiven Systemen durchgeführt werden soll, kann auch an einem Produktivsystem mit Testdaten oder nur an einem Testsystem gearbeitet werden. Testdatensätze, auf die die für den Test verwendeten Benutzerkonten zugreifen können, sollten bereits vor Testbeginn zur Verfügung stehen.

Bei der Arbeit mit reinen Testsystemen ist das Ergebnis des Sicherheitstests nur aussagekräftig, wenn ihre Funktionalität zu großen Teilen mit der des Produktivsystems übereinstimmt.

Sollte keine Möglichkeit zur Bereitstellung einer Testinstanz bestehen, so wird die Vorgehensweise entsprechend justiert. Beispielsweise soll dadurch verhindert werden, dass die Benutzer einer zu testenden, produktiven Webapplikation Verfügbarkeitsbeeinträchtigungen während des Tests ausgesetzt sind. Insbesondere die automatisierten Schwachstellenscans werden in einem solchen Fall sehr moderat konfiguriert oder nur bei ausgewählten Funktionen eingesetzt.

Tipps von Sebastian Schreiber

Um bei einem Webapplikationstest festgestellte Schwächen zu beseitigen, benötigen Sie die Kooperationsbereitschaft des Verantwortlichen für das betroffene Element. Versuchen Sie, alle Zuständigen und Betroffenen daher frühzeitig zu ermitteln und zu informieren – nur so wird eine schnelle Reaktion gewährleistet.

Unterrichten Sie alle Beteiligten, auch diejenigen, die beim Test selbst keine aktiven Aufgaben haben. So schaffen Sie zusätzliches Vertrauen in die Dienstleistung „Sicherheitstest" und stärken die Position der IT-Sicherheit im Unternehmen. Stehen uns für den Test keine Anmeldeinformationen zur Verfügung, dann ist meist ein nur wenig aussagekräftiger Test möglich.

2.3 WEBSERVICE: Prüfung von Schnittstellen (APIs)

Zusammenfassung

Ausgewählte Webservices werden aus unterschiedlichen Testperspektiven auf Sicherheitsschwächen hin analysiert, die es einem Angreifer ermöglichen, die Vertraulichkeit und Integrität von Daten zu gefährden oder die Verfügbarkeit der bereitgestellten Webservicefunktionalität zu stören.

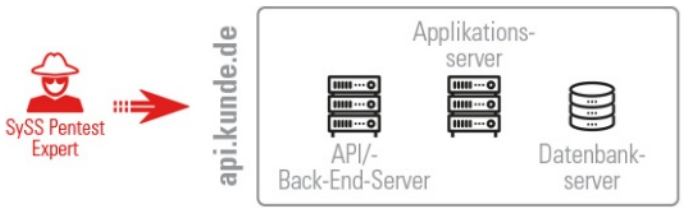

Abbildung 2.3: Modul WEBSERVICE

Ausgangslage

Wie bei klassischen Webapplikationen (siehe Modul WEBAPP, Abschnitt 2.2 auf Seite 23) besteht auch bei Webservices ein hohes Risiko, dass auf nicht autorisierte Weise auf Daten zugegriffen werden kann, was einen Verlust der Vertraulichkeit bedeutet. Überdies besteht die Gefahr, dass Daten auf nicht autorisierte Weise manipuliert werden können, wodurch deren Integrität verletzt wird. Darüber hinaus stellt die Störung der Verfügbarkeit von Webservices (Denial-of-Service) oftmals ebenfalls ein hohes Risiko dar, da kritische Geschäftsprozesse ohne entsprechende Webservicefunktionalität nicht mehr ordnungsgemäß funktionieren.

Webservices greifen auf verschiedene Webtechnologien und -protokolle zurück, die größtenteils auch bei klassischen Webapplikationen zum Einsatz kommen. In der Regel werden hierbei spezielle Formate oder eine spezielle Syntax innerhalb gewöhnlicher HTTP-Anfragen verwendet (z. B. in Form einer REST API oder des XML-basierten SOAP). Neben typischen Schwachstellen in Back-End-Anwendungen, wie beispielsweise Buffer Overflow, SQL Injection-Schwachstellen oder (De)Serialization, existieren ferner Webservice-spezifische Sicherheitsschwächen, wie etwa XML/XPath Injection oder XML Signature Wrapping, die für Webservices ein Sicherheitsrisiko darstellen können.

Zielsetzung

Im Rahmen des Sicherheitstests wird der ausgewählte Webservice aus unterschiedlichen Perspektiven auf Schwachstellen geprüft. Je nach Testschwerpunkt und Funktionalität des Webservice, beispielsweise im Kontext von Business-to-Consumer (B2C)- oder Business-to-Business (B2B)-Geschäftsprozessen, kann der Fokus auf unterschiedliche Schutzziele (z. B. Vertraulichkeit, Verfügbarkeit, Integrität) gelegt werden. Des Weiteren wird auch bei jeder Sicherheitsanalyse einer Mobile App[1] der dazugehörige Webservice getestet. Lastbasierte Denial-of-Service-Angriffe führt die SySS nicht durch, jedoch wird geprüft, wo es zu DoS durch Fehlkonfiguration des Servers bzw. durch eine fehlerhafte Implementierung des Webservice kommen kann.

Auch etwaige zum Einsatz kommende Authentisierungsprotokolle wie OpenID Connect (OIDC) oder OAuth und Single Sign-on-Dienste wie Active Directory Federation Services (ADFS) sowie deren konkrete Implementierung werden geprüft.

Durchführung

Die Durchführung eines Sicherheitstests von Webservices richtet sich primär nach den eingesetzten Technologien und Architekturen (z. B. SOAP, RESTful, JSON-basiert usw.) sowie nach der bereitgestellten Funktionalität, die in der Webservicespezifikation dokumentiert ist.

Der Testablauf entspricht in der Regel dem folgenden Muster:

- Analyse der Webservicespezifikation
- Bedrohungsanalyse zur Identifikation möglicher Angriffe, beispielsweise zum unautorisierten Zugriff auf fremde Daten oder der unautorisierten Manipulation fremder Daten
- Überprüfung von Schwachstellen in Back-End-Systemen (z. B. Buffer Overflow, SQL Injection, XML Injection, (De)Serialization)
- Überprüfung von weiteren bei Webservices auftretenden Schwachstellen (z. B. XML/XPath Injection, XML Signature Wrapping)
- Überprüfung der Zugriffskontrolle/Sitzungsverwaltung (sofern vorhanden)
- Suche nach Fehlern in der Anwendungslogik bereitgestellter Funktionen

[1] Weitere Informationen zur Analyse von mobilen Apps können Abschnitt 2.8.2 auf Seite 50 entnommen werden.

Für die Durchführung der Sicherheitsanalyse werden sowohl spezielle Softwaretools wie SoapUI, Burp Suite Professional oder Postman als auch manuelle Prüfmethoden eingesetzt.

Mitwirkung des Kunden

Für den Sicherheitstest eines Webservice müssen dessen URL sowie dessen Spezifikation bzw. Schnittstellenbeschreibung, beispielsweise als WSDL- oder OpenAPI-Datei, bereitgestellt werden. Darüber hinaus sollten jeweils Beispiele für Anfragen bereitgestellt und die mögliche Authentifizierung beschrieben werden. Dies ist dann wichtig, wenn die Authentifizierung von einem Identity Provider vorgenommen wird, der jedoch nicht Teil des Tests ist. Die Erfahrung hat gezeigt, dass die Schnittstellenbeschreibung oft nicht ausreicht, um eine fehlerfreie Kommunikation mit dem Service herzustellen.

Die Sicherheitsanalyse von Webservices entspricht im Wesentlichen der von Webapplikationen, weshalb dieselben organisatorischen und technischen Aspekte zu berücksichtigen sind (siehe Modul WEBAPP, Abschnitt 2.2 auf Seite 23).

Ansprechpartner: Die Klärung von Zuständigkeiten sowie die Feststellung verantwortlicher Personen sollte rechtzeitig vor einem geplanten Sicherheitstest geschehen. Ferner sollten alle Projektbeteiligten vorab über den Termin und das Ziel des Tests informiert werden. Während des Projektzeitraums sollte zudem ein Ansprechpartner für Rückfragen bezüglich des zu testenden Webservice zur Verfügung stehen.

Abhängigkeiten: Organisatorische und technische Abhängigkeiten des Webservice sollten der SySS mitgeteilt werden, wozu zum Beispiel die Weiterleitung von Daten an weitere Dienste zählt. Dies kann im Rahmen des Kick-off-Gesprächs geschehen. Werden der Webservice oder die nachgelagerten Dienste von Dritten bereitgestellt, benötigt die SySS vor Testbeginn eine schriftliche Testgenehmigung.

Anmeldeinformationen: Sollte für die Nutzung des zu testenden Webservice eine Zugriffskontrolle implementiert sein, benötigt die SySS mindestens zwei Benutzerkonten pro Berechtigungsstufe, aus deren Perspektive der Sicherheitstest durchgeführt werden soll. Stehen keine entsprechenden Anmeldedaten zur Verfügung, kann ein Test nur aus der Perspektive eines externen Angreifers ohne gültige Anmeldedaten erfolgen. Aus einer solch eingeschränkten Testperspektive heraus können Sicherheitsschwächen in einem authentifizierten Kontext eines Webservice in der Regel nicht gefunden werden. Des Weiteren sollte auch beschrieben werden, wie die Authentifizierung durchgeführt wird. Wenn die Authentifizierung beispielsweise von einem Identity Provider vorgenommen wird, der nicht Teil des Tests ist, taucht dieser unter Umständen nicht in der Dokumentation des Webservice auf.

Testdaten/Testsystem: Wie auch bei Sicherheitstests von Webapplikationen gilt bei der Analyse von Webservices, dass sowohl produktive Systeme mit entsprechenden Nutzdaten als auch reine Testsysteme mit Testdaten im Rahmen der Sicherheitsanalyse untersucht werden können. Testdatensätze, auf welche die für den Sicherheitstest bereitgestellten Benutzerkonten zugreifen können, sollten bereits vor Testbeginn eingerichtet werden.

Darüber hinaus ist bei der Arbeit mit reinen Testsystemen zu beachten, dass Ergebnisse des Sicherheitstests nur dann aussagekräftig sind und auf das produktive System übertragen werden können, wenn ihre Funktionalität und Architektur zu großen Teilen identisch sind.

Tipp von Sebastian Schreiber

Stellen Sie dem Consultant bei einem solchen Projekt möglichst immer sämtliche vorhandenen Dokumentationen über die zu testenden Schnittstellen bereit (inkl. Schnittstellenbeschreibung und Beispielanfragen) – dies spart wertvolle Testzeit!

2.4 LAN: Sicherheitstest im internen Netz

Zusammenfassung

Verschiedene Angriffsszenarien in lokalen Netzwerken werden beleuchtet und die von ihnen ausgehenden Risiken bewertet. Ohne kundenspezifische Vorgaben liegt der Schwerpunkt auf der Feststellung möglicher Rechteeskalationswege. Grundsätzlich existiert zwar eine Vielzahl an Möglichkeiten für interne Sicherheitsanalysen, im Laufe der Jahre haben sich jedoch einige immer wieder angefragte Testszenarien herauskristallisiert, für die die SySS daher konkret beschriebene Testmodule anbietet. Grundsätzlich sind den Testmöglichkeiten jedoch keine Grenzen gesetzt und die SySS findet auch für individuelle Anliegen immer die passende Herangehensweise.

Ausgangslage

Im Gegensatz zu Systemen im Internet, die Risiken seitens eines nicht einzuschränkenden Benutzerkreises ausgesetzt sind, geht es im internen Netz (Corporate Network) um das von Innentätern ausgehende Risiko. Konkret ist damit ein Benutzer mit Zugang zum internen Netz gemeint. Dieser hat aufgrund seiner Position automatisch einen höheren Kenntnisstand über das Netz. Hierbei muss es sich keinesfalls um einen eigenen Mitarbeiter mit bösen Absichten handeln, denn auch Besucher eines Gebäudes haben potenziell Zugriff auf das Corporate Network. Angriffe können zudem auch über kompromittierte Zugangsdaten oder über von Malware befallene Systeme der eigenen Mitarbeiter erfolgen.

Je nachdem, welches Prüfszenario evaluiert werden soll, werden die Tests aus unterschiedlichen Perspektiven heraus initiiert. Eine Ausgangslage ist zum Beispiel, dass dem Consultant der SySS ausschließlich ein physischer Netzzugang zur Verfügung steht, jedoch darüber hinaus keine weitergehenden Informationen (siehe Modul LAN/CLEAN, Abschnitt 2.4.1 auf Seite 32). In einer weiteren Ausgangslage agiert der Consultant aus der Rolle eines „Praktikanten" heraus (siehe Modul LAN/TRAINEE, Abschnitt 2.4.2 auf Seite 33). Es können jedoch auch gezielte Analysen bestimmter Anwendungsumgebungen oder eingesetzter Technologien durchgeführt werden. Beispiele hierfür sind die Module LAN/VOIP/UC und SAP (siehe Abschnitte 2.4.5 und 2.5). Ab Modul LAN/CLEAN werden die verschiedenen klassischen Testmodule der SySS im Detail beschrieben.

Im Folgenden werden zunächst einige generelle Aspekte erläutert, die es bei der Durchführung eines LAN-Tests zu beachten gilt.

Zielsetzung

Ziel ist es, je nach eingenommener Perspektive und durchgeführtem Prüfmodul die etwaig vorhandenen Risiken im Corporate Network aufzudecken, zu bewerten und Vorschläge zu deren Behebung aufzuführen. Dabei werden nicht nur reine Sicherheitslücken betrachtet, sondern auch Konfigurationen oder die Verfügbarkeit bestimmter Software, die einem internen Angreifer Ansatzpunkte für einen erfolgreichen Angriff geben könnten. Hierbei wird nicht nur die Verwundbarkeit von einzelnen Systemen eingeschätzt, sondern auch die Kommunikation von Diensten untereinander, um Man-in-the-Middle-Anfälligkeiten oder andere protokollbasierte Angriffspotenziale festzustellen. Falls andere Sicherungsmaßnahmen (Update, Konfigurationsänderung, Ersatz) sich als nicht effektiv erweisen, wird in der Regel eine interne Abschottung der betroffenen Systeme empfohlen.

Die SySS führt hierbei keine organisatorische Dateizugriffsberechtigungsprüfung durch. Derartige Kontrollen sind oft durch Externe nicht möglich.

Durchführung

Grundsätzlich ist die Durchführung bei vielen Prüfszenarien des Moduls LAN an die des Moduls IP-RANGE angelehnt, sofern die netzbasierte Analyse bestimmter Systeme vorgesehen ist:

- Prüfung der Systeme auf erreichbare Dienste
- Test der Dienste mit automatischen Schwachstellenscannern
- Verifizierung der Ergebnisse
- Begleitende und manuelle Prüfungen

Hinzu kommen einige Prüfaspekte, die sich nur in internen Netzwerken realistisch umsetzen lassen, wie zum Beispiel die Durchführung von Man-in-the-Middle-Angriffen oder Angriffe, die physischen Zugriff auf ein System erfordern.

Die konkrete Durchführung der klassischen internen Prüfszenarien der SySS wird ab Abschnitt 2.4.1 auf der nächsten Seite erläutert.

Mitwirkung des Kunden

Für einen internen Test müssen gewisse logistische Voraussetzungen erfüllt werden, da ein solcher Test keine autarke Dienstleistung darstellt.

Auswahl von Stichproben: Aufgrund der enormen Anzahl von testbaren Diensten, die typischerweise in internen Netzen zur Verfügung stehen, kommt der Auswahl sinnvoller Stichproben eine hohe Bedeutung zu. Dies sollte beim Kick-off-Gespräch (siehe KICKOFF, Abschnitt 1.3.1 auf Seite 16) unbedingt berücksichtigt werden.

Bei der Auswahl der Stichproben sollte darauf geachtet werden, dass die Systeme repräsentativ für weitere Systeme sind. Optimalerweise werden Integrations- oder Testsysteme näher untersucht – insbesondere, wenn die produktiven Systeme für kritische Aufgaben benötigt werden.

Bei sehr großen oder sehr komplexen internen Netzen kann die SySS bei der Auswahl geeigneter Stichproben helfen und gegebenenfalls auch eine interne Inventarisierung durchführen (siehe Modul RECON, Abschnitt 2.12.1 auf Seite 67).

Ansprechpartner: Ein Ansprechpartner sollte während der gesamten Testzeit gut und kurzfristig erreichbar sein. Er kann dem Test gerne beiwohnen. Da der Test in der Regel vor Ort stattfindet, sollten alle organisatorischen Rahmenbedingungen bereits bei Testbeginn erfüllt sein.

Information der Beteiligten: Alle Systemverantwortlichen, Administratoren und anderen betroffenen Mitarbeiter sollten vor Beginn des Projekts über den Test und seine Zielsetzung informiert werden. Ihre Kooperation kann während des Tests nötig sein, ist aber vor allem für die Behebung eventuell gefundener Schwachstellen von essenzieller Bedeutung. Gegebenenfalls sollte geprüft werden, ob es Sinn ergibt, die Unternehmens-IT-Sicherheit oder die Mitarbeitervertretung bei der Vorbereitung des Tests miteinzubeziehen.

Arbeitsplatz: Für jeden Consultant sollte ein Arbeitsplatz zur Verfügung stehen. Für den Test interner Netzwerkkomponenten ist Folgendes erforderlich:

- Mindestens ein Netzanschluss (Ethernet), von dem aus die zu testenden Netzwerkkomponenten erreicht werden können
- Stromanschluss für Notebook und Switch (Steckdosenleiste)
- Platz für ca. zwei Notebooks, Switch und Unterlagen
- Möglichst ruhige Umgebung
- Internetzugang für Dokumentation und gegebenenfalls Recherche
- Je nach Prüfmodul wird auch ein Referenzgerät benötigt (z. B. Standardclient wie Desktop-PC oder Notebook, Thin Client oder VoIP-Phone)

– Für manche Szenarien wird zudem mindestens ein Benutzerkonto benötigt (z. B. Active Directory-Benutzer mit Standardrechten)

Zugang zu Gebäuden und Netz: Der Consultant sollte am Testtag das betroffene Gebäude mit seiner Ausrüstung betreten und den oben beschriebenen Arbeitsplatz erreichen und einrichten können. Eventuell notwendige Genehmigungen sollten daher rechtzeitig beschafft werden.

Falls zudem ein Mechanismus zur Netzwerkzugangskontrolle im Einsatz sein sollte (z. B. 802.1X mit Clientzertifikaten), so sollten entsprechende Zugangsdaten für den Consultant vorbereitet und diesem zu Testbeginn übergeben werden.

Umgang mit instabilen Systemen und Altlasten: In internen Netzen werden häufig Systeme eingesetzt, die nicht besonders widerstandsfähig gegen Angriffe sind und teilweise weit über ihren durch den Händler angekündigten End-of-Life (EOL) hinaus betrieben werden. Das Risiko, dass solche Systeme beim Test abstürzen, ist nicht zu vernachlässigen. Dies gilt insbesondere für produktionsnahe Maschinen. Daher ist bei der Prüfung eine enge Koordination mit dem Ansprechpartner nötig. Idealerweise wird der SySS vor Testbeginn eine Liste solcher Systeme zur Verfügung gestellt.

Generell empfiehlt die SySS, Systeme, die ihren EOL erreicht haben oder seit mehreren Jahren nicht mehr gepflegt wurden, nur zu testen, wenn der direkte Nachweis erbracht werden soll, dass Systeme abzuschotten oder zu ersetzen sind, und der entstehende Schaden vom Kunden in Kauf genommen werden kann. Falls möglich, sollten auch für solche Tests Systeme ausgewählt werden, die keine kritischen Funktionen erfüllen. Eine Haftung für alle aus eventuellen Abstürzen oder anderen Beeinträchtigungen entstehenden Schäden wird durch unsere Allgemeinen Geschäftsbedingungen (AGB) ausgeschlossen.

Tipps von Sebastian Schreiber

Sie können das Ergebnis eines internen Tests qualitativ aufwerten, wenn Sie die Auswahl der zu testenden Systeme mit sehr viel Sorgfalt vornehmen.

Bei vielen identischen Systemen ist fast immer der tiefergehende Test von zwei als Stichproben ausgewählten Systemen sinnvoller als eine grobe Prüfung aller Systeme.

Ziel eines Sicherheitstests ist es, technische Defizite aufzudecken. Informieren Sie daher alle Beteiligten vor Testbeginn, sodass der Test als positive, die eigene Sicherheit stärkende Maßnahme wahrgenommen wird.

2.4.1 LAN/CLEAN: Reinigungspersonalszenario

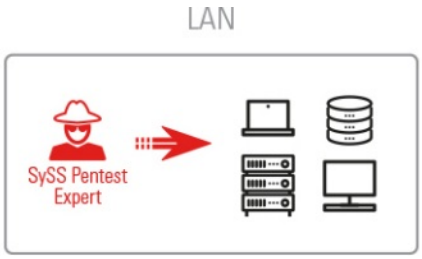

Abbildung 2.4: Modul LAN/CLEAN

Dieses Szenario simuliert den Angriff von unternehmensfremden Personen, die die Möglichkeit haben, Zugang zum Netz des Kunden zu erhalten, was über gepatchte Netzwerkdosen in öffentlichen Räumen der Fall sein könnte oder über Fremdgeräte, die in das Unternehmensnetz gebracht und angeschlossen werden. Der Consultant wird mit einem eigenen Notebook die Sicherheit des Kundennetzwerks analysieren. Hierbei wird er insbesondere

nach offensichtlichen, leicht ausnutzbaren Schwachstellen („Low-Hanging Fruits") Ausschau halten. Ein typischer Ablauf eines solchen Tests gestaltet sich wie folgt:

– Prüfung eventuell vorhandener Netzwerkzugangskontrollen
– Ermittlung genutzter interner Netzbereiche
– Identifizierung aktiver Systeme und Dienste
– Schwachstellenanalyse und -ausnutzung
– Rechteeskalation und Ausbreitung

Das Ziel dieser Vorgehensweise besteht darin, einen möglichst genauen Überblick über das Sicherheitsniveau der internen Netzlandschaft zu erhalten. Tests können sowohl in der Breite erfolgen – das heißt, es wird keine Einschränkung bezüglich der zu testenden Systeme getroffen – als auch in der Tiefe. Bei letzterer Vorgehensweise stellt der Kunde eine sinnvolle und repräsentative Liste zu testender Systeme zusammen, auf die sich der Consultant dann konzentriert.

Der Consultant wird – je nach Kundenwunsch – Wege aufzeigen, über die er beispielsweise seine Berechtigungen innerhalb des Unternehmensnetzes ausweiten kann, über die er auf vertrauliche Daten Zugriff erlangen kann oder über die es ihm gezielt gelingt, bestimmte Systeme zu kompromittieren.

Tipp von Sebastian Schreiber

Wenn Sie dem Consultant die intern genutzten Netzbereiche – beispielsweise in Form eines Netzwerkplans – bei Projektbeginn vorlegen, lässt sich wertvolle Zeit einsparen, die dann wiederum in die eigentliche Schwachstellenanalyse investiert werden kann.

2.4.2 LAN/TRAINEE: Praktikantenszenario

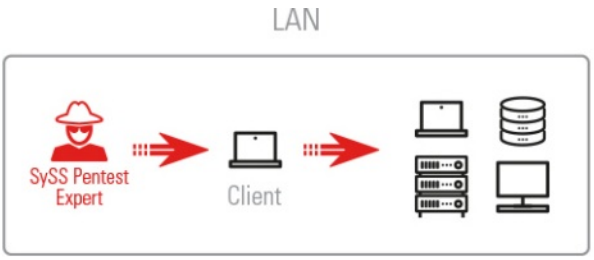

Abbildung 2.5: Modul LAN/TRAINEE

Bei diesem Szenario simuliert die SySS einen Angriff, der mit den Rechten eines Mitarbeiters bzw. Praktikanten im internen Netz des Kunden durchgeführt wird. Hierfür benötigt der Consultant einen Standardclient sowie eine Benutzerkennung mit üblichen Rechten. Aus dieser simulierten Sicht wird anschließend der Versuch unternommen, sowohl lokal auf dem Client als auch innerhalb des Netzes die eigenen Rechte auszuweiten.

Die Kernelemente dieser Untersuchung sind unter anderem folgende:

– Physische Angriffsmöglichkeiten wie Booten von externen Medien
– Softwareinventarisierung und Ermittlung des Patchstands
– Konfigurationsanalyse
– Prüfung auf Härtungsmaßnahmen
– Lokale Dateisystemanalyse (z. B. NTFS-Zugriffsberechtigungen)
– Sichtung von Netzlaufwerken und -freigaben

Tipps von Sebastian Schreiber

Stellen Sie unserem Consultant einen möglichst realitätsgetreuen Client zur Verfügung, wie er auch einem neuen Mitarbeiter, z. B. einem Praktikanten, bereitgestellt wird. Sorgen Sie zudem frühzeitig für die Beantragung eines Testbenutzerkontos, sodass dieses dem Consultant zu Testbeginn vorliegt. Das Benutzerkonto sollte mit typischen Berechtigungen ausgestattet sein.

2.4.3 LAN/CLIENT bzw. LAN/SERVER: Härtungsanalyse eines Clients oder Servers

Abbildung 2.6: Modul LAN/CLIENT bzw. LAN/SERVER

LAN/CLIENT

Dieses Szenario simuliert den Umstand, wenn ein Endgerät in fremde Hände gerät (zum Beispiel, wenn ein Laptop verloren geht). Hierbei wird von unterschiedlichen Zuständen (Laptop ausgeschaltet, eingeschaltet aber gesperrt oder entsperrt) ausgegangen. Im Gegensatz zu dem in Abschnitt 2.4.2 beschriebenen Praktikantenszenario wird im Zuge des Moduls LAN/CLIENT eine gründliche, umfassende Härtungsanalyse eines Clients durchgeführt, bei der sämtliche Angriffsaspekte beleuchtet werden – unter anderem auch Angriffe gegen eine etwaige Festplattenverschlüsselungslösung sowie deren Pre-Boot-Authentifizierung. Weitere Prüfpunkte sind:

- Virtualisierung des Image, Speicheranalyse usw.
- Boot- und hardwarebasierte Angriffe (Booten externer Medien, PXE, Direct Memory Access-basierte und Cold-Boot-Angriffe)
- Systemanalyse (Zugriff auf vertrauliche Daten, Data Loss-Szenarien, Device Control, Zugriffsrechte, Malware-Anfälligkeit/Trojanisierung, Konfiguration)
- Rechteausweitung (Bordmittel, Betriebssystem- und Softwareschwachstellen, Exploits)
- Analyse von Drittsoftware (Antivirenlösung, Endpoint Protection, Softwareverteilung etc.)
- Netzbasierte Analyse (Port- und Security-Scans, manuelle Prüfung, Trafficanalyse, Eindringen in das Firmennetz, z. B. per VPN)

LAN/SERVER

Mit dem Modul LAN/SERVER bieten wir auch eine fundierte Härtungsanalyse eines Server-Image bzw. einer Server-Referenzinstallation an. Hierbei werden unter anderem die folgenden Aspekte beleuchtet:

- Dienstekonfiguration (insbesondere die Konfiguration der Netzwerkdienste wird aus Sicherheitssicht evaluiert; Beispiele: Webserver wie Apache oder Nginx, Applikationsserver wie Tomcat oder WildFly, SSH, MySQL, MSSQL, SNMP, Drittanbieter-Agents u. v. m.)
- Rechteanalyse (Welche Benutzer haben effektive Rechte an dem Server?)
- Rechteausweitung (Bordmittel, Betriebssystem- und Softwareschwachstellen, Exploits)
- Analyse von Drittsoftware (Antivirenlösung, Endpoint Protection, Softwareverteilung etc.)
- Netzbasierte Analyse (Port- und Security-Scans, manuelle Prüfung, Trafficanalyse)

– Ggf. Prüfung auf Einhaltung von IT Security-Vorgaben oder Best Practice-Empfehlungen von Organisationen wie dem BSI oder dem NIST

Die Durchführung der Module LAN/CLIENT bzw. LAN/SERVER wird beispielsweise im Zuge einer bevorstehenden Migration von einem älteren auf ein neueres Betriebssystem angeraten (z. B. Ablösung von Windows 7 durch Windows 10 oder Red Hat Enterprise Linux 7.x durch Red Hat Enterprise Linux 8.x). Vor dem eigentlichen Rollout wird unser Consultant im Zuge dieser Prüfung eruieren, ob die umgesetzten Härtungsmaßnahmen greifen und ob zusätzliche Schutzmechanismen implementiert werden sollten.

Tipp von Sebastian Schreiber

Der ideale Zeitpunkt für die Durchführung einer solchen gründlichen Client- oder Serveranalyse ist **vor** dem flächendeckenden Rollout oder **vor** dem produktiven Einsatz. Dank der beispielsweise in Form von Gruppenrichtlinien zur Verfügung stehenden Möglichkeiten können identifizierte Schwachstellen in der Regel jedoch auch nachträglich behoben werden.

2.4.4 LAN/AD: Sicherheitsanalyse der Active Directory-Umgebung

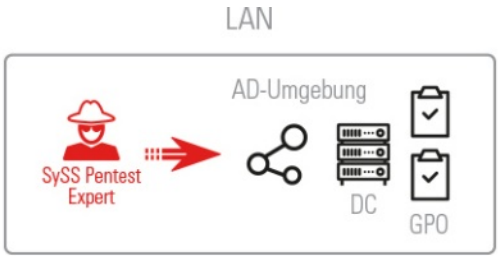

Abbildung 2.7: Modul LAN/AD

Der Active Directory (AD)-Verzeichnisdienst ist quasi omnipräsent und kommt beinahe in jedem Unternehmen zur Verwaltung der IT-Landschaft zum Einsatz. Nicht nur Benutzer, Gruppen und Computer lassen sich hierüber in Form von Objektcontainern zentral administrieren, auch Konfigurationen und Sicherheitseinstellungen sind mit Active Directory-Mitteln in Form von Gruppenrichtlinien mittlerweile in vielen Variationen steuerbar. Auch Angreifern sind diese Vorzüge nicht unbekannt. Oftmals sind es gerade diese vom Active Directory angebotenen Features, die eine weitreichende Ausbreitung eines Angreifers im Netzwerk oder eine Rechteeskalation überhaupt erst ermöglichen. Daher sollte der Absicherung dieses bedeutungsvollen Dienstes sowie der Nutzung der zahlreichen angebotenen Security-Funktionalitäten eine zentrale Bedeutung beigemessen werden, wenn es um den Schutz der eigenen IT-Infrastruktur geht.

Die SySS bietet daher dedizierte Sicherheitsanalysen einer Active Directory-Umgebung des Kunden an. Hierbei stehen in der Regel die folgenden Prüfschritte im Fokus:

– Ermittlung der Active Directory-Struktur (z. B. Sites, Forests, Domains, Subdomains, OUs usw.)
– Identifikation der Vertrauensstellungen zwischen verschiedenen Teilbereichen der Active Directory-Umgebung (z. B. External Trusts, Forest Trusts, Crosslinks usw.)
– Analyse der sicherheitsrelevanten Konfigurationsoptionen (z. B. Sichtung der bereits umgesetzten Gruppenrichtlinien sowie Empfehlungen für zusätzliche, sicherheitsrelevante Gruppenrichtlinien)
– Bewertung der (verschiedenen) Passwortrichtlinien
– Least Privilege-/Berechtigungsanalyse (Ermittlung der Anzahl „kritischer" Konten wie z. B. die von offensichtlichen und versteckten lokalen Administratoren oder Domänenadministratoren auf kritischen Systemen durch rekursives Gruppenauflösen)

– Analyse einer etwaigen Anbindung an bzw. Vernetzung mit Microsoft Azure AD

Durchgeführt wird eine derartige Analyse in der Regel in enger Zusammenarbeit mit den Ansprechpartnern des Kunden. Beispielsweise findet eine Konfigurationssichtung idealerweise in Form eines gemeinsamen Walk-Through durch die verschiedenen Gruppenrichtlinien statt. Bestimmte Teilaspekte hingegen lassen sich auch autark durch den Consultant umsetzen. Beispielsweise kann dieser mithilfe von Bordmitteln wie der PowerShell bereits sehr viele Informationen über die Active Directory-Umgebung in Erfahrung bringen.

Das Ziel dieser Sicherheitsanalyse besteht darin, den Kunden bei der zusätzlichen Härtung seiner Active Directory-Umgebung zu unterstützen. Insbesondere zielen die Empfehlungen der SySS darauf ab, die Ausbreitung eines bereits erfolgreich in das Netz eingedrungenen Angreifers deutlich zu erschweren. Dies kann größtenteils schon mit Active Directory-Bordmitteln bewerkstelligt werden.

Dieses spezielle Prüfmodul lässt sich ideal mit den beiden klassischen Innentäterszenarien (Module LAN/CLEAN und LAN/TRAINEE) kombinieren, da dem Consultant hierdurch bereits nahezu alle technischen Voraussetzungen zur Verfügung stehen.

Tipp von Sebastian Schreiber

Stellen Sie dem Consultant – zumindest auf Abruf – geeignete „Interviewpartner" zur Verfügung! Auf diese Weise können gezielte Fragen direkt vom jeweils zuständigen Ansprechpartner beantwortet werden. Zudem kann der jeweilige Ansprechpartner dem Consultant bestimmte Sicherheitseinstellungen durch ein gemeinsames Sichten der Konfiguration „belegen", ohne dass der Consultant ein hochprivilegiertes (Test-)Benutzerkonto benötigt.

2.4.5 LAN/VOIP/UC: VoIP-Analyse

Abbildung 2.8: Modul LAN/VOIP/UC

Die Kommunikation mithilfe von Voice-over-IP (VoIP)[2] ist schon seit Jahren gängige Praxis und in vielen Unternehmensbereichen zu finden. Neben der traditionellen Telefonie stellen auch Audio- und Videokonferenzen, Chatfunktionen, Softphones, aber auch zum Beispiel die Kommunikation über den Browser die derzeitigen Anforderungen an diese Technologie. Dieser Verbund an Kommunikationsmöglichkeiten wird auch als Unified Communication (UC) bezeichnet.

[2] Voice over Internet Protocol

Da dieses Bündel an Funktionen oft eine fundierte Integration in die vorhandene Infrastruktur erfordert, bergen VoIP-Systeme neben den spezifischen Bedrohungen der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität übermittelter, teils hochkritischer und schützenswerter Daten auch Risiken und Gefahren gegenüber der restlichen IT-Infrastruktur.

In diesem Zusammenhang ist die Wirtschaftsspionage zu nennen. Sie ist ein mittlerweile gängiges und äußerst lukratives Motiv für Angreifer geworden, über Schwachstellen bei VoIP beispielsweise die Wettbewerbsfähigkeit der Konkurrenz in Erfahrung zu bringen, um diese dann schwächen bzw. die eigene stärken zu können.

Bei diesem Testszenario wird das Risiko zugrunde gelegt, das von einem Angreifer mit Zugriffsmöglichkeit auf einen Netzwerkanschluss im Unternehmensnetz ausgeht.

Die SySS untersucht im Rahmen der Prüfung vor allem den möglichen Mitschnitt von Medien- und Kontrollverbindungen, Angriffe gegen andere Identitäten sowie die Ausbreitungsmöglichkeiten in die angrenzende Infrastruktur. Des Weiteren werden auch Schwachstellen und Konfigurationen involvierter Systeme gründlich untersucht.

Im Detail werden unter anderem die folgenden Punkte bei der VoIP-Analyse berücksichtigt:

- Passive und aktive Trafficanalyse (Signalisierungs-, Konfigurations- und Sprachdaten)
- Analyse des zentralen Verwaltungs- und Provisionierungssystems
- Netzbasierte Angriffe sowohl gegen VoIP-Client als auch -Server
- Angriffe gegen einen VoIP-Client mit physischem Zugriff
- Bootangriffe gegen VoIP-Telefone, Mitschnitt und Auswertung eines Bootvorgangs
- Lauschangriffe (Man-in-the-Middle, Logging-Funktionen im integrierten Webserver usw.)

Für die Testdurchführung werden seitens der SySS zwei standardmäßig konfigurierte VoIP-Clients (z. B. Deskphones) sowie zwei konfigurierte Unified Communication-Clients aus dem Unternehmensbestand benötigt.

2.4.6 LAN/VLAN: VLAN-Analyse

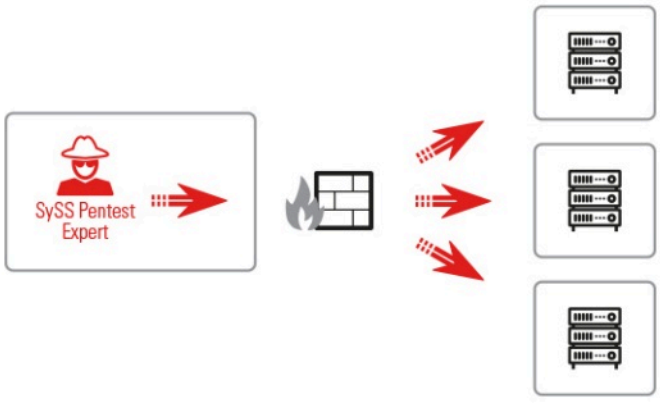

Abbildung 2.9: Modul LAN/VLAN

Gerätegruppen wie Server, Clients, VoIP-Systeme, Drucker etc. werden häufig in eigene Netzwerke aufgeteilt. Diese Netzwerkseparierung erfolgt meist auf logischer Ebene mithilfe dedizierter VLANs.

Neben den organisatorischen Vorteilen bietet eine Netzwerkseparierung auch die Möglichkeit, den netzwerkübergreifenden Datenverkehr an zentraler Stelle kontrollieren und reglementieren zu können. Teilweise wird die Separierung mit einer Netzwerkzugangskontrolle ergänzt, sodass ausschließlich legitimierten Systemen Zugriff auf die Unternehmensnetzwerke erlaubt wird.

Enthalten Switche, Paketfilter und Zugangskontrollsysteme Konfigurationsschwächen, besteht die Gefahr einer nicht legitimierten Eingliederung eines Angreifers ins Unternehmensnetzwerk sowie die Gefahr einer Ausbreitung in schützenswerte und kritische Netzwerkbereiche (z. B. Servernetzwerk).

Bei dem Modul LAN/VLAN wird vom Risiko eines Angreifers mit Zugriffsmöglichkeit auf einen Netzwerkanschluss im Unternehmensnetz ausgegangen.

Die SySS untersucht im Rahmen der Prüfung vor allem eine mögliche Umgehung der Zugangskontrollsysteme sowie die netzwerkübergreifenden Kommunikationsmöglichkeiten.

Im Detail werden unter anderem die folgenden Punkte bei der VLAN-Analyse berücksichtigt:

– Integration von Fremdgeräten ins Unternehmensnetzwerk
– Passive Trafficanalyse (Information Leaks wie VLAN-Tags usw.)
– Prüfung der Abschottungswirkung/Inter-VLAN-Routing
– Trunking-Angriffe
– Durchlässigkeitsanalyse in andere, auch physisch getrennte Netze

Für die Testdurchführung wird seitens der SySS lediglich ein Netzwerkanschluss zum Unternehmensnetzwerk benötigt. Idealerweise erhält der Consultant eine detaillierte Auflistung der konfigurierten Netzwerkssegmente inklusive VLAN-ID und IP-Adressen.

Tipp von Sebastian Schreiber

Legen Sie unserem Consultant idealerweise einen Netzwerkplan bereit, auf dem sämtliche genutzte Netzsegmente inklusive VLAN-ID dargestellt werden. Dies spart bei einer Durchlässigkeitsanalyse sehr viel Zeit ein.

2.4.7 PENTESTBOX: Sicherheitstest per VPN

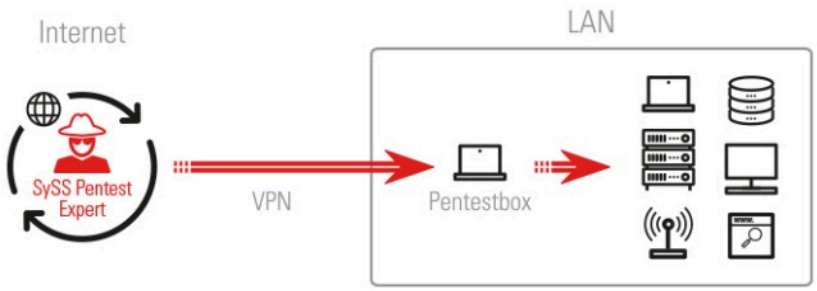

Abbildung 2.10: Modul PENTESTBOX

Klassischerweise führen die IT Security Consultants der SySS die Module LAN/CLEAN und LAN/TRAINEE vor Ort beim Auftraggeber durch. In manchen Fällen ist dies sinnvoll und hat seine Berechtigung, vor allem da es zu einer realen Begegnung und Zusammenarbeit kommt, die meist zu einer besseren Kundenbindung und zu einem positiven Projektverlauf auf beiden Seiten führt.

Doch nicht immer ist es praktikabel und manchmal sogar unmöglich, für Tests beim Kunden vor Ort zu sein. Aus diesem Grund hat die SySS die „Pentestbox" entwickelt, die es ermöglicht, jegliche On-site-Szenarien via VPN von extern aus durchzuführen. Die Pentestbox wird anstelle eines IT Security Consultants zum Auftraggeber geschickt und über diese führt der Consultant den Test remote durch. Dies erhöht nicht nur die Flexibilität und verringert die Kosten, sondern trägt auch zu einem besseren ökologischen Fußabdruck bei.

Generell kann jedes Modul, das klassischerweise vor Ort durchgeführt wird, auch mit der Pentestbox realisiert werden. Neben zielgerichteten Angriffen gegen einzelne Komponenten über das Modul TARGET/TECH (siehe Abschnitt 2.6.1 auf Seite 42) bis hin zur Überprüfung einzelner Clientsysteme im Modul LAN/CLIENT (siehe Abschnitt 2.4.3 auf Seite 34) ist die Pentestbox flexibel einsetzbar. Sogar die Sicherheit des vor Ort vorhandenen Drahtlosnetzwerks (siehe Modul WLAN, Abschnitt 2.7 auf Seite 46) kann über die Pentestbox überprüft werden.

Um die Pentestbox einsetzen zu können, muss sie zunächst einmal zum Kunden gelangen. Hierfür schickt die SySS ein Paket, bestehend aus einem Laptop, USB-Ethernet-Adapter und Netzteil, an den Auftraggeber. In einem separaten Brief erhält dieser eine Smartcard, um die verschlüsselte Laptop-Festplatte entsperren zu können, sowie eine Anleitung für die Inbetriebnahme der Pentestbox. Durch die Vollverschlüsselung der Festplatte wird sichergestellt, dass keine Daten auf dem Postweg verloren gehen bzw. von Dritten abgegriffen werden können.

Für den Auftraggeber ist die Inbetriebnahme in der Regel sehr einfach und benötigt kaum Zeit – der Laptop wird lediglich über das mitgelieferte Netzteil an den Strom angeschlossen und gestartet. Mit der Smartcard wird das Notebook einmalig entsperrt und kann ab dann eingeschaltet bleiben.

Die Pentestbox wird mit dem internen Netzwerk des Auftraggebers verbunden, und über ein weiteres Netzwerk (LAN, WLAN oder über mobiles Internet) verbindet sich die Pentestbox automatisch mit einem von der SySS kontrollierten Server. Für eine bestmögliche Verbindung ist für dieses weitere Netzwerk ein unbeschränkter Zugriff ins Internet beziehungsweise zum entsprechenden Server der SySS ideal. Sollte es aus organisatorischen oder technischen Gründen nicht möglich sein, eine Internetverbindung via LAN oder WLAN herzustellen, wird die Pentestbox automatisch versuchen, sich via mobilem Internet zum Server der SySS zu verbinden.

Durch die Vorkonfiguration der Pentestbox durch den Consultant der SySS entsteht für den Auftraggeber kaum zusätzlicher Aufwand, um das System nach initialer Inbetriebnahme weiter zu konfigurieren oder zu warten.

Sobald die VPN-Verbindung aufgebaut ist, hat der Consultant die Möglichkeit, den Test über die Pentestbox zu beginnen. Dabei verhält sich die Pentestbox so wie ein mitgebrachter Laptop bei einem On-site-Test – er ist für den Auftraggeber also klar zu erkennen.

Wie auch bei anderen Testmodulen ist eine enge Absprache zwischen Auftraggeber und Consultant immens vorteilhaft, um etwaigen technischen und organisatorischen Problemen bereits im Vorfeld entgegenzuwirken. So steht der Consultant dem Kunden bei Bedarf zu jeder Zeit über Telefon- und/oder Videokonferenzen beratend zur Seite, um beispielsweise die Pentestbox initial in Betrieb zu nehmen. Sollte es während des Projektes zu Problemen mit der Pentestbox kommen, kann der Auftraggeber über einen dedizierten Nutzer unter Anleitung eines SySS-Consultants „Bugfixing“ betreiben.

Nach Testabschluss werden sämtliche Daten gelöscht, indem die Pentestbox und der dazugehörige Server vollständig zurückgesetzt werden. Durch dieses Zurücksetzen können die Pentestboxen im Nachhinein keine VPN-Verbindung mehr aufbauen. Diese Maßnahmen gewährleisten die Integrität der Daten – vor dem Projekt, während des Tests und auch nach Projektabschluss.

Neben den oben vorgestellten LAN/CLEAN- und LAN/TRAINEE-Szenarien (siehe Abschnitt 2.4.1 auf Seite 32 und Abschnitt 2.4.2 auf Seite 33) können auch Module wie LAN/CLIENT (siehe Abschnitt 2.4.3 auf Seite 34) durchgeführt werden. Dafür sendet der Auftraggeber ein Notebook an den durchführenden Consultant der SySS. Dieses Notebook wird dann von der SySS wieder über die Pentestbox beim Auftraggeber in dessen internes Netzwerk zurückgeführt. Daher bietet es sich an, die Module LAN/CLEAN oder LAN/TRAINEE mit dem Modul LAN/CLIENT zu kombinieren, da die Pentestbox für LAN/CLIENT beim Auftraggeber sein muss.

2.5 SAP: Sicherheitsanalyse von SAP ERP-Umgebungen

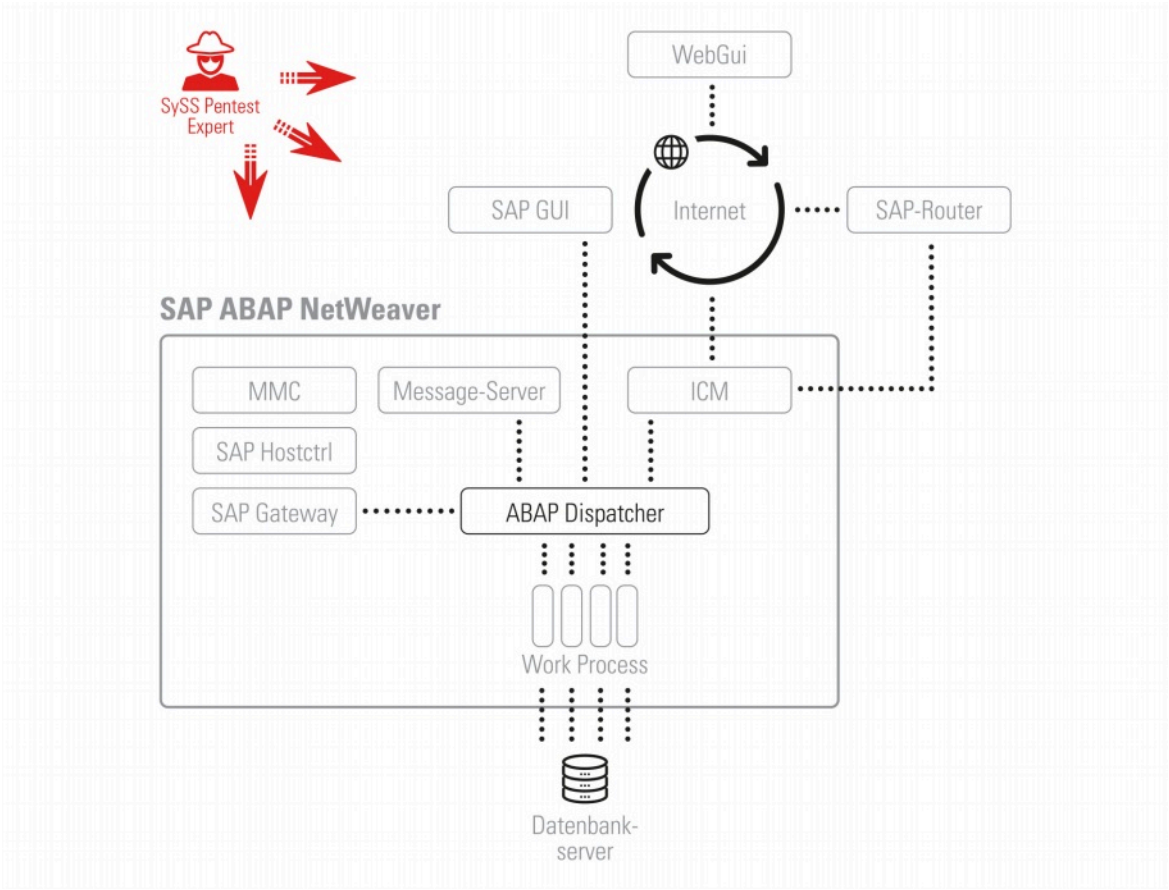

Abbildung 2.11: Modul SAP

Das Produkt SAP ERP des Softwareherstellers SAP ist die marktführende Lösung zur Abwicklung von Geschäftsprozessen wie beispielsweise Buchführung, Controlling, Vertrieb oder Personalwesen in Firmen beliebiger Größe. Darüber hinaus bietet SAP die Möglichkeiten, solche Geschäftsprozesse individuell und auf die jeweiligen Bedürfnisse eines Unternehmens abzubilden. Die aus spezifischen Anforderungen und Individualität resultierende Komplexität sowie die Kritikalität der verarbeiteten Daten schaffen zusätzlich ein sehr lukratives Ziel für eine breite Palette von Angreifern, das mit den „10KBLAZE Exploits" im Jahr 2019 ein mediales Echo erlangte.[3] Deshalb sollten gerade in kritischen Umgebungen wie SAP regelmäßige Sicherheitsüberprüfungen durchgeführt werden, um beispielsweise Wirtschaftsspionage oder Sabotageangriffen vorzubeugen.

Die SySS bietet im Rahmen einer solchen Sicherheitsanalyse verschiedene Prüfszenarien bzw. Testgegenstände an, die der Komplexität der eingesetzten SAP-Softwarelösung gerecht werden:

- Berechtigungsanalyse (auf Rollenbasis, via SAP GUI/WebGUI)
- Analyse der Providing Infrastructure
- Analyse der eingesetzten Datenbankanbindung und -konfiguration
- Analyse der SAP-spezifischen Konfiguration auf Clientsystemen
- Analyse der SAP-Systemkonfiguration (inklusive z. B. SAP-Router)
- Test der eingesetzten SAP-Webapplikation(en)

Die Vorgehensweise im Rahmen der verschiedenen Testszenarien gestaltet sich in der Regel sehr unterschiedlich und ist optimal auf die jeweiligen Kundenbedürfnisse abgestimmt. Auch die eingesetzten Werkzeuge unterschei-

[3] https://github.com/gelim/sap_ms/blob/master/10KBLAZE.md

den sich von den anderen Modulen, selbst bei der Durchführung einer Prüfung über das Internet. Beispielsweise kann es im Rahmen eines solchen Tests möglich sein, auf aktive Dienste des Internet Communication Manager (ICM) zuzugreifen. Ein Worst-Case-Szenario wäre hier eine vollständige Kompromittierung des internen SAP-Systems sowie eine Rechteeskalation und Ausweitung im internen Netzwerk.

Im Rahmen der internen Sicherheitsanalyse stehen vorrangig die System- und Konfigurationsanalyse, die Berechtigungsprüfung von unterschiedlichen SAP-Benutzerrollen sowie die Providing Infrastructure der SAP-Landschaft im Fokus. Sofern ein SAP-Router eingesetzt wird, rückt auch dieser in den Mittelpunkt der System- und Konfigurationsanalyse. Die erwähnte Berechtigungsanalyse der zur Verfügung gestellten SAP-Rollen wird in der Regel über die auf Clientsystemen zumeist installierte SAP GUI durchgeführt. Nur selten kommt eine Prüfung über die aktivierte WebGUI infrage. In der Regel werden dafür ein paar der im Unternehmen verwendeten Rollen ausgewählt. Im Rahmen dieser Prüfung werden zusätzliche spezifische Systemparameter aus sicherheitstechnischem Blickwinkel identifiziert und bewertet sowie mögliche Risiken daraus abgeleitet. Für jegliche Art der detaillierten Untersuchung benötigt die SySS in jedem Fall einen vorab bereitgestellten administrativen SAP-Benutzer.

Als weiterer wichtiger Aspekt muss der besondere Schutzbedarf der Providing Infrastructure einer SAP-Umgebung und ihrer verschiedenen Kommunikationsschnittstellen (RFC, DIAG oder SOAP) hervorgehoben werden. Die im Rahmen einer solchen Prüfung erreichbaren Dienste, wie beispielsweise das Gateway, der Message-Server, die Management Console oder auch der ICM, werden auf Aktualität und konfigurative Fehler hin überprüft. Dabei wird vorrangig nach unautorisierten Zugriffsmöglichkeiten gefahndet, mit denen auf hochkritische Unternehmensdaten, wie zum Beispiel geheime Projektinformationen oder personenbezogene Angestellten-, Kunden- oder Dienstleisterdaten, zugegriffen werden kann. Ferner werden auch die Möglichkeiten der Ausbreitung auf andere SAP-Systeme analysiert. Denn die enge Verzahnung der verschiedenen SAP-Systeme ermöglicht es einem Angreifer, von einem kompromittierten SAP-System auf weitere Systeme Zugriff zu erlangen.
Neben dem eigentlichen SAP-Applikationsserver und dessen Komponenten werden im Rahmen der Untersuchung sowohl die SAP-spezifische Konfiguration der Windows-Clients als auch die Konfiguration der eingesetzten Datenbanklösung (z. B. Oracle, MSSQL, DB2, MaxDB, SyBase sowie HANA) einer gründlichen Analyse unterzogen.

Die SySS setzt für die Durchführung dieser Testgegenstände unterschiedliche Security- und Verwundbarkeitsscanner sowie Exploit-Sammlungen ein, wie z. B. das Metasploit-Framework. Zudem werden bei Sicherheitstests im entsprechenden Kontext selbst entwickelte Softwaretools der SySS herangezogen. Darüber hinaus kommen SAP-typische Werkzeuge wie SAP GUI, SQL-Clients, PySAP, Bizploit (oder Sapyto) und weitere öffentlich zugängliche Tools zum Einsatz.

Tipp von Sebastian Schreiber

Egal, ob ganzheitliche oder stichprobenartige Untersuchung: Stellen Sie in jedem Fall sicher, dass dem durchführenden Consultant ein administrativer SAP-Benutzer bereitgestellt wird. Nur so kann eine fundierte Aussage über das Sicherheitsniveau getroffen werden.

2.6 TARGET: Simulation zielgerichteter Angriffe („Targeted Attacks“)

Die vergangenen Jahre haben gezeigt, dass Unternehmen immer öfter Opfer von zielgerichteten Angriffen – sogenannten „Targeted Attacks“ – werden. Bei diesen Angriffen liegt der Fokus nicht mehr auf der wahllosen Übernahme von Perimetersystemen oder einem Eindringen in die DMZ über Schwachstellen, die Systeme ausnutzen, die aus dem Internet erreichbar sind, sondern auf der Kompromittierung ausgewählter Ziele im internen Unternehmensnetz: den Clients. Angreifer machen sich hierfür Techniken wie Social Engineering, Phishing, Spear Phishing, Whaling oder Waterholing zunutze. Folglich ist oftmals eine simple E-Mail mit einem gefährlichen Anhang oder der Aufruf einer vermeintlich harmlosen Webseite Auslöser einer Kompromittierung.

Um die Anfälligkeit eines Unternehmens gegenüber solchen realitätsnahen Angriffen zu messen, bietet die SySS zwei Testmodule an. Zum einen wird im Rahmen des Moduls TARGET/TECH eruiert, welche technischen Schutzmaßnahmen bereits implementiert sind, um derartige Angriffe zu erschweren, und wie gut diese im Falle eines Angriffs auch wirklich greifen. Zum anderen kann über das Modul TARGET/PHISH ermittelt werden, ob sich derartige Angriffe auch schon im Bewusstsein der eigenen Mitarbeiter verankert haben. Beide Prüfszenarien werden in den folgenden Abschnitten beschrieben.

2.6.1 TARGET/TECH: Technische Prüfung der Schutzmaßnahmen

Zusammenfassung

Die SySS prüft die Widerstandsfähigkeit ausgewählter Arbeitsumgebungen des Kunden (z. B. Notebook, Desktop-PC oder Thin Client/Terminalserver) gegenüber Angriffen aus dem Internet. Hierbei werden sowohl die lokal auf dem Endgerät implementierten Schutzmaßnahmen als auch die möglicherweise auf Zwischensystemen installierten Filter evaluiert.

Abbildung 2.12: Modul TARGET/TECH

Ausgangslage

Auf Clientsystemen ist eine Vielzahl von Softwarekomponenten installiert, die beispielsweise von Browsern in Form von Plug-ins verwendet und so indirekt gestartet werden können. Eben diese Komponenten stellen – besonders im Falle der Verwendung von veralteten Versionen – ein lohnendes Ziel im Rahmen von Targeted Attacks dar. Prominente Beispiele hierfür sind Adobe Flash, Word-Makros oder die Oracle Java-Laufzeitumgebung. Die Übernahme eines oder mehrerer Clientsysteme kann eine weitreichende Kompromittierung des Corporate Network nach sich ziehen und stellt auch im Falle eines Advanced Persistent Threat (APT) oftmals den ersten Schritt einer dauerhaften Infiltration dar.

Zielsetzung

Dieser Spezialfall einer internen Sicherheitsprüfung bildet den zielgerichteten Angriff auf ein ausgewähltes Clientsystem ab. Die SySS versucht, durch die Verwendung von bekanntem, angepasstem bzw. eigenem Schadcode das zur Verfügung gestellte Clientsystem zu übernehmen. Ziel ist zum einen, die Performanz der bereits vorhandenen Schutzmaßnahmen zu evaluieren, und zum anderen, zusätzliche Härtungsmaßnahmen zu empfehlen. Als Nebeneffekt dieser Prüfung wird gezeigt, inwiefern vorhandene Gateway Security-Lösungen die Durchführung derartiger Angriffe erschweren.

Durchführung

Die SySS wird bei diesem Modul sowohl die Angreifer- als auch die Opferperspektive einnehmen. Hierzu findet der Test beim Kunden vor Ort statt. Der Consultant wird ausgehend von einem Referenzclient beispielsweise versuchen, den Schadcode von einem eigenen Root-Server der SySS nachzuladen oder per E-Mail-Anhang an das Zielsystem zu versenden. Unter anderem wird Folgendes geprüft:

- Eingesetzte Browser und Browser-Plug-ins
- Dokumentbetrachter und Medienabspielsoftware (z. B. präparierte PDF-Dateien oder Office-Dokumente mit Makros)
- Malware in E-Mail-Anhängen
- Drittsoftware wie Oracle Java
- Überlisten von Zwischenstationen wie Mailfilter, AV-Gateways, URL-Filter, Content Inspection usw.
- Umgehung von lokalen Schutzmaßnahmen wie z. B. der UAC oder der eingesetzten Endpoint Protection- und Antivirenlösungen (AV)

Mitwirkung des Kunden

Vorbereitungen: Die folgenden Voraussetzungen müssen seitens des Kunden erfüllt werden:

- Bereitstellung eines Referenzclients (z. B. Desktop-PC, Notebook oder Thin Client)
- Bereitstellung eines Standardbenutzerkontos mit Zugriffsmöglichkeiten auf E-Mails und Internet

Ansprechpartner: Wie bei den anderen Modulen ist es auch bei diesem wichtig, dass ein Ansprechpartner während des Testzeitraums kurzfristig verfügbar ist.

Tipps von Sebastian Schreiber

Targeted Attacks sollten stets durch unsere Consultants simuliert werden, die dabei sowohl in die Täter- als auch die Opferrolle schlüpfen. Auf diese Weise kann der Consultant sehr effizient arbeiten. Weiterhin bietet dies die Möglichkeit, das Szenario eines Mitarbeiters zu behandeln, der aus Unwissenheit heraus Angriffe durch Fehlverhalten auslöst. Somit wird getestet, ob die Technik auch in einem solchen Fall bestmöglichen Schutz bietet.

2.6.2 TARGET/PHISH: Simulation eines Phishing-Angriffs

Zusammenfassung

Im Rahmen dieses Moduls führt die SySS im Auftrag des Kunden die Simulation eines Phishing-Angriffs durch und liefert als Ergebnis eine anonymisierte, statistische Auswertung der Rückläufer.

Abbildung 2.13: Modul TARGET/PHISH

Ausgangslage

Phishing ist kein neues Phänomen. Jeder Nutzer wird fast täglich mit dieser Angriffsform konfrontiert. Doch während die üblichen „Rechnungs-E-Mails“ eher breitgefächert sind und keinen bestimmten Adressaten, sondern „die Masse“ erreichen sollen, werden im Rahmen von gezielten Phishing-Angriffen auf ein bestimmtes Unternehmen individuell zugeschnittene E-Mails an ausgewählte Empfänger versandt. Diese werden speziell für bestimmte Mitarbeiter täuschend echt verfasst, um die Wahrscheinlichkeit eines erfolgreichen Angriffs zu erhöhen. In diesem Rahmen wird von Spear Phishing oder Whaling gesprochen, wenn sich die Adressaten insbesondere aus den „dicken Fischen“ des Unternehmens zusammensetzen.

Inhalt solcher gezielten Phishing-Mails sind oftmals mit Schadcode versehene Anhänge – beispielsweise vermeintliche Rechnungen – oder Links zu Webseiten, auf denen der Empfänger zur Eingabe seiner Zugangsdaten verleitet wird. Das Ziel der Angreifer besteht in der Regel darin, einzelne Benutzerkonten oder gar Systeme innerhalb des Unternehmens unter ihre Hoheit zu bringen, um von dort aus zum Beispiel schützenswertes, geistiges Eigentum der Firma zu kopieren und sich dadurch einen Wettbewerbsvorteil zu verschaffen. Industriespionage und Ausspähaktionen sind ebenfalls kein neues Phänomen. Immer wieder erscheinen Pressemeldungen über erfolgte Phishing-Angriffe in den Medien und rücken diese Problematik ins öffentliche Bewusstsein.

Zielsetzung

Im Rahmen dieses Moduls wird die SySS einen solchen Phishing-Angriff gegen das beauftragende Unternehmen durchführen. An dieser Stelle ist es besonders wichtig zu betonen, dass hierbei auf keinen Fall das Fehlverhalten einzelner Individuen aufgedeckt werden soll. Vielmehr wird die SySS den Angriff auf eine möglichst anonymisierte Weise durchführen und als Ergebnis eine quantitative, statistische Auswertung des Angriffsresultats liefern (siehe Abbildung Abbildung 2.14 auf der nächsten Seite). Das Ergebnis kann vom Kunden beispielsweise als Sensibilisierungsverstärker in Security Awareness-Veranstaltungen verwendet werden.

Durchführung

Der Ablauf dieses Moduls entspricht in der Regel dem folgenden Muster:

- Der Kunde stellt der SySS eine gewisse Anzahl von E-Mail-Adressen zur Verfügung (z. B. 200 Empfänger).
- Die SySS bereitet den Phishing-Angriff vor. Hierzu werden Informationen über das Unternehmen gesammelt und der Inhalt der E-Mail gestaltet sowie eventuelle Phishing-Seiten vorbereitet.
- Die SySS versendet die E-Mail an eine zufällige Auswahl der bereitgestellten E-Mail-Adressen.
- Nach einer gewissen Frist (in der Regel nach wenigen Tagen) wird die SySS das Ergebnis auswerten und dem Kunden in Form einer anonymen, statistischen Dokumentation zur Verfügung stellen.
- Phishing ist ebenfalls per SMS möglich. Hierbei kann die SySS eine beliebige Telefonnummer als Absender hinterlegen.

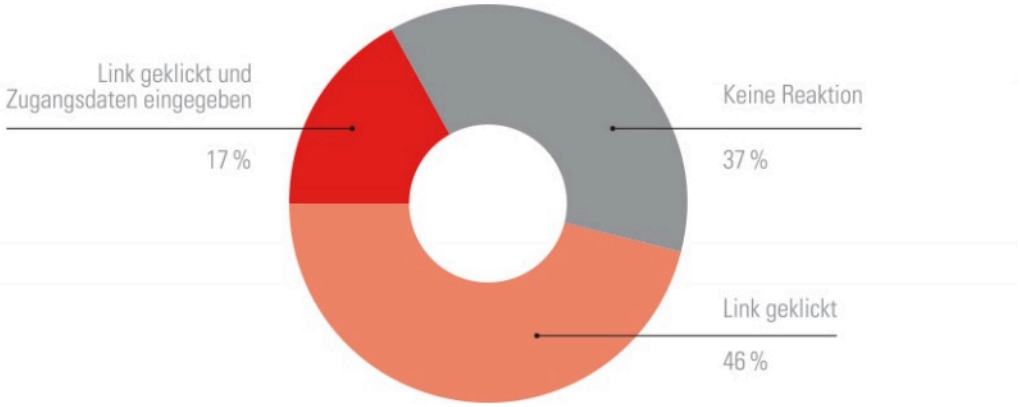

Abbildung 2.14: Beispielhaftes Ergebnis eines Phishing-Angriffs

Mitwirkung des Kunden

Vorbereitungen: Die Vorbereitungsaufgaben des Kunden bei diesem Modul sind sehr überschaubar. Der SySS muss lediglich die Liste der E-Mail-Empfänger (siehe „Durchführung") zur Verfügung gestellt werden. Gerne kann der Kunde der SySS auch Informationen bereitstellen, die die Glaubwürdigkeit der Phishing-E-Mail erhöhen.

Ansprechpartner: Die SySS rät dazu, den Phishing-Angriff vorab mit dem Ansprechpartner des Kunden durchzuspielen. Hierdurch kann zum Beispiel verhindert werden, dass der Angriff aufgrund von möglicherweise eingesetzten Filtermechanismen scheitert und die E-Mails ihre Empfänger erst gar nicht erreichen. Derartige Eventualitäten werden vor der Durchführung des Moduls auf jeden Fall gemeinsam besprochen.

Der Kunde sollte sich zudem darauf vorbereiten, dass der Phishing-Angriff im Unternehmen auffällt und Rückfragen gestellt werden. Umso wichtiger ist es zum einen, den Angriff zeitlich stark einzuschränken, und zum anderen, unmittelbar nach Beendigung des Angriffs für Aufklärung und Entwarnung zu sorgen!

Eine Erreichbarkeit des Ansprechpartners während der Moduldurchführung ist, wie auch bei den anderen Modulen, obligatorisch. Beispielsweise könnten beim Versand der Phishing-E-Mails unvorhersehbare Hürden auftauchen. Zudem sollte der Ansprechpartner auch für die Empfänger stets für Rückfragen zur Verfügung stehen.

2.7 WLAN: Test des Drahtlosnetzwerks

Zusammenfassung

Die WLAN-Infrastruktur des Kunden wird vor Ort auf Sicherheitsschwächen hin untersucht. Zusätzlich kann auch die Clientsicherheit geprüft werden, beispielsweise in Bezug auf eine Verbindung mit sogenannten „Rogue Access Points". Auch eine Prüfung der Abschottung der verschiedenen WLAN- von sonstigen internen Netzbereichen kann durchgeführt werden.

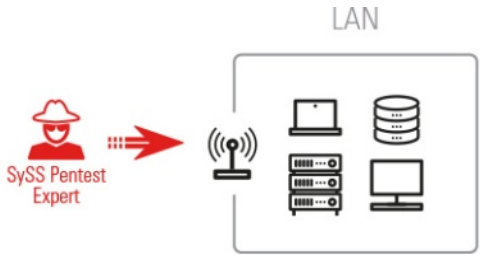

Abbildung 2.15: Modul WLAN

Ausgangslage

WLAN kann – im Gegensatz zu drahtgebundenen Netzen – jederzeit von Dritten erreicht und empfangen werden, oftmals auch von außerhalb des eigenen Firmengeländes. Hieraus resultiert die Gefahr des Missbrauchs der WLAN-Infrastruktur. Die Bedrohung besteht einerseits in der unberechtigten Nutzung des WLAN und andererseits in der Ausspähung der übermittelten Daten durch Unbefugte. Dies betrifft dann den Teil des Unternehmensnetzes, der per WLAN erreichbar ist.

Zielsetzung

Um die oben genannten Risiken ausschließen zu können, werden sowohl die Zugangspunkte (Access Points) als auch die WLAN-Clients (z. B. Notebooks oder Mobiltelefone) untersucht. Der Untersuchungsgegenstand umfasst in erster Linie die eingesetzten Verschlüsselungs- und Authentifizierungsverfahren sowie die Clientkonfiguration. Bei dieser wird bei der Untersuchung ein Schwerpunkt auf Resistenz gegen Man-in-the-Middle-Angriffe gelegt. Zudem kann geprüft werden, ob sich Clients auch mit sogenannten „Rogue Access Points" verbinden würden.

Zusätzlich kann eine WLAN-Sichtbarkeitsanalyse zum Beispiel in Form einer Begehung des Firmengeländes erfolgen, wobei neben der Sichtbarkeit auch die Parametrisierung des WLAN ermittelt wird.

Durchführung

Der WLAN-Test findet vor Ort statt. Das genaue Vorgehen hängt stark von der zu testenden Lokation und der verwendeten WLAN-Infrastruktur ab. Der Ablauf entspricht in etwa dem folgenden Muster:

- Inventarisierung und Parametrisierung: Was ist sichtbar, was gehört zur Kundeninfrastruktur?
- Verifizierung: Entspricht das Vorgefundene den Erwartungen und Informationen?
- Erkennung von Zugangspunkten
- Untersuchung der Netze hinsichtlich Authentifizierung und Verschlüsselung
- Angriff gegen festgestellte Authentifizierung und Verschlüsselung
- Untersuchung der WLAN-Clients

Bei der Untersuchung von Funknetzwerken sind Denial-of-Service-Angriffe zwangsläufiger Bestandteil. Diese können aber auf ausgewählte Systeme (z. B. einen Referenzclient) beschränkt werden. Eine Auswahl von möglichen Testwerkzeugen wird unter „Werkzeuge“ (siehe Abschnitt 1.1.6 auf Seite 10) vorgestellt.

Die SySS prüft dabei WLANs nach dem IEEE-Funkstandard 802.11 auf 2.4 und 5 GHz. Andere Funknetze (basierend auf DECT, UWB, IEEE 802.15.4, Z-Wave, Bluetooth usw.) sind nicht Bestandteil eines WLAN-Tests.

Mitwirkung des Kunden

Vorbereitungen: Vor Beginn des Tests sollten Informationen über die WLAN-Infrastruktur, insbesondere den eingesetzten Access Point-Typ und die Art der Authentifizierung zur Verfügung gestellt werden, am besten im Rahmen des KICKOFF. Des Weiteren sollten alle Beteiligten und Systemverantwortlichen für das WLAN über den Test und seine Intention informiert werden und während des Tests für Rückfragen zur Verfügung stehen.

Ansprechpartner: Da WLAN-Tests immer vor Ort stattfinden, sollte wie beim internen Test stets ein Ansprechpartner zur Verfügung stehen. Der Ansprechpartner sollte während des Testzeitraums gut erreichbar sein und dem Consultant auch Zugang zu den zu untersuchenden Gebäuden ermöglichen können. Die Erfahrung zeigt, dass es am effizientesten ist, wenn der Ansprechpartner diese Zugangsberechtigungen selbst besitzt und sie zusätzlich erteilen kann.

Falls der Consultant Lokationen ohne Begleitung testen soll, sollte pro zu besuchender Örtlichkeit eine Person zugegen sein, die den Zugang zu Gebäuden und zum Gelände ermöglicht und über den Test bzw. Besuch informiert ist. Optional kann der Consultant mit entsprechenden Unterlagen ausgestattet werden.

Zugang zu Gebäuden und zum Gelände: Die hierfür erforderlichen Genehmigungen müssen zu Testbeginn vorliegen. Dies betrifft sowohl den Zugang für den Consultant selbst als auch für seine Ausrüstung.

Bei der Wahl des Testzeitraums sollten vor allem Öffnungs- und allgemeine Arbeitszeiten berücksichtigt werden. Falls Begehungen nötig sind, sollten diese ausschließlich bei Tageslicht durchgeführt werden. Wenn WLAN-Clients getestet werden, sollten Referenzclients zur Verfügung stehen oder Stichproben ausgewählt werden. Sollen mehrere Örtlichkeiten an einem Tag getestet werden, müssen bei der Wahl des Testzeitraums und der Testdauer auch Faktoren wie Verkehrsfluss usw. in Betracht gezogen werden.

Tipps von Sebastian Schreiber

Beschaffen Sie die notwendigen Genehmigungen für den Zutritt zu Gebäuden rechtzeitig und informieren Sie die Beteiligten. So werden lange und unproduktive Wartezeiten vermieden. Das Informieren der Beteiligten hilft, dass sie den Test als eine positive Maßnahme und nicht als eine störende Kontrolle wahrnehmen. Sollten sich unter Ihren Mitarbeitern Personen befinden, die Bedenken haben, so laden Sie diese einfach ein, dem Test beizuwohnen.

2.8 MOBILE: Sicherheitstest von mobilen Endgeräten, Apps und Mobile Device Management-Lösungen

Mobile Endgeräte wie Smartphones oder Tablets haben in den vergangenen Jahren vermehrt auch Einzug in die Unternehmens-IT erhalten. Neben E-Mails und Kontakten werden teils auch weitere kritische Unternehmensdaten auf die Geräte synchronisiert, die dadurch zu einem weiteren interessanten Angriffsziel werden. Die SySS bietet daher auch in diesem Bereich verschiedene Testmodule an, um zu eruieren, ob die Daten auf den Geräten des Kunden gut vor eventuellen Angriffen geschützt sind. Typische Prüfszenarien sind beispielsweise eine Analyse der Gerätekonfiguration (MOBILE/DEVICE), ein Sicherheitstest eingesetzter Mobile Apps (MOBILE/APP) oder eine Bewertung der zur Verwaltung eingesetzten Mobile Device Management-Lösung (MOBILE/MDM).

2.8.1 MOBILE/DEVICE: Sicherheitstest von mobilen Endgeräten

Zusammenfassung

Ausgewählte mobile Endgeräte – vor allem Smartphones oder Tablets – werden aus unterschiedlichen Perspektiven auf Sicherheitsschwächen hin untersucht, die es einem Angreifer ermöglichen, auf nicht autorisierte Weise auf lokal gespeicherte Daten zuzugreifen sowie über das mobile Endgerät Zugriff auf das Unternehmensnetzwerk zu erlangen.

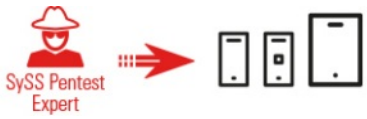

Abbildung 2.16: Modul MOBILE/DEVICE

Ausgangslage

Auf mobilen Endgeräten wie Smartphones oder Tablets werden häufig sensible Informationen wie etwa personenbezogene Daten oder unternehmenskritische Dokumente (E-Mails, PDF-/Office-Dateien usw.) gespeichert. Darüber hinaus bieten solche mobilen Geräte oftmals einen Zugang zum Unternehmensnetzwerk, um etwa Personal Information Management (PIM)-Funktionalitäten nutzen zu können. Dazu gehört beispielsweise die Synchronisation von E-Mails, Kontakten und Terminen. Dieser Umstand macht mobile Endgeräte zu einem interessanten und auch lohnenswerten Ziel für Angreifer. Da die Geräte ständig unterwegs eingesetzt werden, liegt zudem ein erhöhtes Diebstahlrisiko vor.

Zielsetzung

Im Rahmen des Sicherheitstests wird das ausgewählte mobile Endgerät aus unterschiedlichen Perspektiven auf Schwachstellen geprüft. Je nach Testschwerpunkt des jeweiligen Sicherheitstests werden dabei Angriffsszenarien aus der Perspektive eines externen Angreifers und/oder aus der Perspektive eines autorisierten Benutzers des Gerätes durchgeführt. Ziel ist es, zusätzliche Härtungsmaßnahmen aufzuzeigen.

Durchführung

Die mobilen Endgeräte werden im SySS-Labor auf Sicherheitsschwächen hin untersucht. Je nach Gerätetyp, Betriebssystem und Testschwerpunkt kommen dabei unterschiedliche Werkzeuge und Methoden zum Einsatz. Mögliche Angriffsszenarien werden im Folgenden aufgeführt.

Angriffe aus der Perspektive eines externen Angreifers:

- Angriffe über Netzwerkschnittstellen des Gerätes (WLAN, Bluetooth)
- Angriffe gegen Netzwerkdienste
- Man-in-the-Middle-Angriffe gegen genutzte Apps (E-Mail-Synchronisation, VPN-Zugriff, Dokumentenverwaltung etc.)
- Angriffe mit physischem Zugriff auf das Gerät (Diebstahlszenario): nicht autorisierter Zugriff auf lokal gespeicherte Daten; Manipulation des Gerätes (beispielsweise Installation von Schadsoftware)

Angriffe aus der Perspektive eines autorisierten Benutzers:

- Zugriff auf Daten fremder Benutzer via PIM-Funktionalität
- Manipulation des Gerätes (z. B. Jailbreak oder Rooting, Installation nicht genehmigter Apps)
- Sicherheitsanalyse ausgewählter Apps (Dokumentenverwaltung, Fernzugriff auf Systeme im Unternehmensnetzwerk, Mobile-Banking)

Implementierte Schutzmechanismen, die beispielsweise von eingesetzten Mobile Device Management-Lösungen bereitgestellt werden, können im Rahmen des Sicherheitstests ebenfalls überprüft werden. Dazu gehören etwa eine PIN-/Passwort-/Biometrie-Anmeldung, das Löschen von Benutzerdaten nach einer bestimmten Anzahl fehlgeschlagener Anmeldeversuche am Gerät, die Erkennung von sogenannten Jailbreak- oder Rooting-Versuchen oder das Zurücksetzen von Geräten aus der Ferne (Remote Wipe).

Mitwirkung des Kunden

Testvorbereitung: Vor Testbeginn sollten Informationen über die zu testende Hardware, die Betriebssystemversion sowie relevante Angriffsszenarien im Rahmen des KICKOFF mitgeteilt werden. Des Weiteren sollten alle Beteiligten wie etwa Systemverantwortliche für E-Mail- oder Mobile Device Management-Server über den Sicherheitstest informiert werden und innerhalb des Testzeitraums für Rückfragen zur Verfügung stehen.

Ansprechpartner: Um den Test eines mobilen Endgerätes durchzuführen, müssen vor allem logistische Voraussetzungen erfüllt werden. So muss der Transport der Geräte organisiert werden und wie bei anderen Tests muss auch ein Ansprechpartner für Rückfragen zur Verfügung stehen.

2.8.2 MOBILE/APP: Sicherheitstest von mobilen Apps

Zusammenfassung

Die auf einem mobilen Endgerät installierbaren Applikationen (Mobile Apps) werden bei dieser Sicherheitsprüfung auf Schwachstellen hin getestet. Die Mobile Apps werden mithilfe von Decompilern und Debuggern einer statischen und dynamischen Analyse unterzogen, außerdem werden die lokal gespeicherten Daten analysiert. Zusätzlich werden Tools zur Laufzeitmanipulation herangezogen. Der Datenverkehr zum Server wird analysiert und die Verschlüsselung im Rahmen einer Man-in-the-Middle-Attacke geprüft. Neben der Prüfung der über das Internet erreichbaren Back-End-Server und der Anbindung der Mobile Apps an diese werden Sicherheitseinstellungen innerhalb der Mobile Apps analysiert und unter Berücksichtigung des geforderten Schutzbedarfes bewertet.

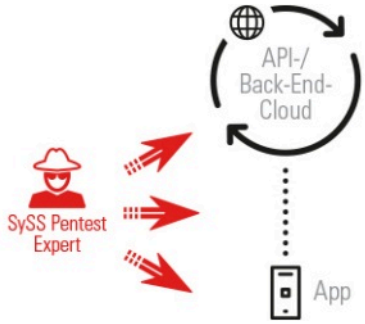

Abbildung 2.17: Modul MOBILE/APP

Ausgangslage

Auf mobilen Endgeräten wie Smartphones oder Tablets werden häufig sensible Informationen gespeichert. Da bei der Eigenentwicklung von Mobile Apps zahlreiche Sicherheitsmaßnahmen oftmals selbst implementiert werden, empfiehlt die SySS, diese vor dem Go-Live einer Analyse zu unterziehen – insbesondere dann, wenn personenbezogene Daten oder Informationen mit einem hohen Schutzbedarf von den entsprechenden Mobile Apps verarbeitet werden. Ein weiterer Anlass für eine gründliche Sicherheitsbewertung von Mobile Apps – auch wenn diese nicht selbst entwickelt wurden – kann eine Zugriffsmöglichkeit über die Mobile Apps auf interne Firmenressourcen darstellen (z. B. VPN-Funktionalität o. Ä.).

Zielsetzung

Im Rahmen des Sicherheitstests werden die Mobile Apps nach Absprache in der jeweiligen, für den entsprechenden Application Store entwickelten Version (z. B. Android oder iOS) auf Schwachstellen hin geprüft. Neben der Erfüllung der Sicherheitsanforderungen wird auch der Datenverkehr überwacht. Die Prüfung der Mobile Apps erfolgt auf Wunsch zudem aus unterschiedlichen Perspektiven heraus. Abschließend schätzt die SySS das Sicherheitsniveau ein und schlägt Maßnahmen zur Behebung oder Abschwächung eventueller Schwachstellen vor.

Durchführung

Die Mobile Apps werden im Prüflabor der SySS auf Sicherheitsschwächen hin untersucht. Je nach Testschwerpunkt kommen dabei unterschiedliche Werkzeuge und Methoden zum Einsatz. Die zu testende Mobile App wird beispielsweise auf einem Gerät mit Jailbreak bzw. Root-Rechten installiert, um während der Analyse vollen

Zugriff auf die Dateisystem- und Speicherinhalte zu haben. Gegebenenfalls wird vorab eruiert, ob sich eine im Einsatz befindliche Rooting/Jailbreak Detection umgehen lässt. Im Nachgang wird die Mobile App zum Beispiel dekompiliert und sowohl einer statischen Code- als auch einer dynamischen Laufzeitanalyse unterzogen. Mögliche weitere Angriffsszenarien sind außerdem Man-in-the-Middle- oder sonstige trafficbasierte Angriffe gegen die Datenübertragung zwischen der Mobile App, anderen Apps und ihrem Server-Back-End. Augenmerk kann auch auf potenzielle Verletzungen der Privatsphäre gelegt werden. Je nach Bedarf werden eigene Tweaks für die Umgehung von Sicherheitsmaßnahmen entwickelt.

Mitwirkung des Kunden

Für einen Test von Mobile Apps müssen je nach Testszenario folgende Anforderungen erfüllt werden:

Testvorbereitung: Die zu testende Mobile App muss vom Kunden in der zu testenden Version (pro zu berücksichtigendem Betriebssystem) bereitgestellt werden, falls diese nicht über einen Application Store zur Verfügung steht. Einige Mobile Apps lassen sich zudem erst nach erfolgreicher Authentisierung innerhalb der Mobile App bedienen. Für Tests aus einer solchen Perspektive heraus benötigt die SySS entsprechende Benutzerkonten. Vor Testbeginn ist es zudem sinnvoll, dem Consultant z. B. im Rahmen des KICKOFF organisatorische und technische Abhängigkeiten, Informationen über die zu testende Mobile App (z. B. Dokumentationen) sowie relevante Angriffsszenarien mitzuteilen.

Ansprechpartner: Da die Analyse der Mobile App idealerweise im Prüflabor der SySS stattfindet, sollte der Verantwortliche der zu testenden App als Ansprechpartner innerhalb des Testzeitraums zumindest telefonisch erreichbar sein. Für Detailfragen ist es hilfreich, wenn direkter Kontakt zu den Entwicklern oder zu technischen Ansprechpartnern besteht.

Tipp von Sebastian Schreiber

Wenn Sie eine Mobile App für mehrere Betriebssysteme anbieten und testen lassen möchten – beispielsweise für iOS und Android – teilen Sie dem Consultant unbedingt vorab mögliche Schnittmengen mit, damit keine wertvolle Testzeit verloren geht. Ein klassisches Beispiel hierfür ist eine von unterschiedlichen Mobile App-Versionen gemeinsam genutzte Webserviceschnittstelle.

2.8.3 MOBILE/MDM: Prüfung von Mobile Device Management-Lösungen

Zusammenfassung

Diese Sicherheitsprüfung dient dazu, die für die Verwaltung der mobilen Endgeräte wie Smartphones oder Tablets eingesetzte Mobile Device Management (MDM)-Lösung zu evaluieren. Die SySS analysiert hierbei zum einen die Serverinfrastruktur – hierzu zählen auch die meist webbasierte Managementoberfläche sowie weitere angebotene Netzwerkdienste der MDM-Lösung. Zum anderen werden auch die über die MDM-Lösung ausgerollten Sicherheitseinstellungen gemäß dem geforderten Schutzbedarf bewertet.

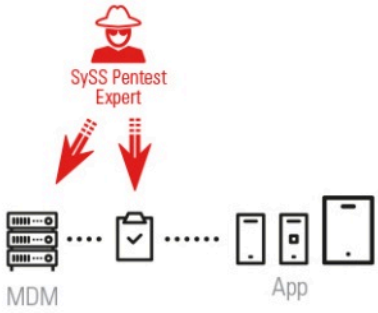

Abbildung 2.18: Modul MOBILE/MDM

Ausgangslage

Um mobile Endgeräte in das Unternehmensnetzwerk einzugliedern und die darauf gespeicherten Daten den Sicherheitsrichtlinien konform zu verwalten, wird in der Regel eine Mobile Device Management (MDM)-Lösung eingesetzt. Damit die darüber verwalteten Geräte von überall aus beispielsweise aktualisierte Konfigurationen erhalten können, sind die MDM-Server auch aus dem Internet erreichbar. Da über diese Server zudem eine hohe Konzentration an unternehmenskritischen Daten erreicht werden kann, stellen MDM-Server ein ertragreiches Angriffsziel dar. Auch die über das MDM verwalteten Gerätekonfigurationen sind unternehmenskritisch, da diese direkten Einfluss auf das Sicherheitsniveau der mobilen Endgeräte nehmen.

Zielsetzung

Im Rahmen dieses Testmoduls prüft die SySS zunächst die Infrastruktur, die zur Anbindung der mobilen Endgeräte an das Unternehmensnetzwerk zuständig ist. Dabei wird zum Beispiel sowohl der Zugriff auf den E-Mail-Server als auch der restliche Datenverkehr im Hinblick auf die Erfüllung der Sicherheitsanforderungen analysiert. Auch der Registrierungs- und Provisionierungsprozess sowie die dabei stattfindende Überprüfung, ob das Mobile Device den Unternehmensrichtlinien entspricht, werden untersucht. Dabei geht die SySS vor allem der Frage nach, ob ein Gerät, dessen Sicherheit kompromittiert wurde, sich mit dem Unternehmensnetzwerk verbinden kann, und analysiert dafür unter anderem die implementierte Jailbreak/Rooting-Erkennung der MDM-Lösung. Ein weiteres Ziel ist eine kritische Betrachtung der ausgerollten Gerätekonfigurationen. Hierbei gilt es, Empfehlungen auszusprechen, die das von einem kompromittierten Gerät ausgehende Risiko senken.

Durchführung

Der Penetrationstest der MDM-Lösung kann wahlweise aus dem SySS-Labor über das Internet oder direkt beim Kunden vor Ort durchgeführt werden. Die SySS prüft den kompletten „Lebenszyklus“ von der Provisionierung bis zur Stilllegung des Gerätes. Dabei wird versucht, Schwachstellen in der Umsetzung der Sicherheitsrichtlinien aufzuzeigen. Auf spezielle Sicherheitsbedürfnisse und Anforderungen des Kunden sowie auf besondere Testszenarien kann ebenfalls eingegangen werden. Besteht beispielsweise die Anforderung, dass die Mobile Devices ausschließlich in einem klar definierten Zustand betrieben werden dürfen, versucht die SySS, diesen Zustand zu kompromittieren.

Im Rahmen von Data Loss-Szenarien wird untersucht, über welche Schnittstellen Informationen das Unternehmen verlassen können. Hierbei betrachtet die SySS die Frage, welche Vorkehrungen getroffen werden, damit ein Mitarbeiter nicht durch Nachlässigkeit Unternehmensdaten auf ein anderes, unsicheres Gerät kopieren kann. Falls eine Container-Lösung entsprechende Exportfunktionen anbietet oder das Backup sich auf einem privaten Computer durchführen lässt, werden diese Schwachstellen aufgezeigt.

Zusammengefasst sind unter anderem die folgenden Prüfszenarien denkbar:

– Netzbasierte Sicherheitsanalyse der beteiligten MDM-Infrastrukturserver
– Webbasierte Sicherheitsanalyse der Managementoberfläche
– Sicherheitsbewertung der Konfigurationsprofile und -richtlinien
– Schwachstellenanalyse der MDM-App
– Analyse von Prozessen: Provisionierung, Konfigurationsupdate, Fernlöschung, Deprovisionierung etc.
– Trafficanalyse, Identifizierung protokollbasierter Schwachstellen

Mitwirkung des Kunden

Testvorbereitung: Für einen Test der MDM-Infrastruktur müssen je nach Testszenario folgende Anforderungen erfüllt werden:

– Eine Testfreigabe für den über das Internet erreichbaren MDM-Server muss vorliegen.
– Eine Möglichkeit zur Einsicht in die MDM-Profile/-Richtlinien muss gewährleistet sein.
– Eine Möglichkeit, Testgeräte selbst einzurichten, muss gegeben sein.
– Die zu testende MDM-App muss bereitgestellt werden, falls diese nicht im jeweiligen App Store steht.

Ansprechpartner: Der Test der MDM-Infrastruktur hat zahlreiche Schnittpunkte mit anderen Bereichen. Der Ansprechpartner für die Absicherung des über das Internet erreichbaren MDM-Servers sollte ebenso wie der Ansprechpartner für das lokale Netzwerk und das WLAN einbezogen werden. Sobald auch private Geräte (Stichwort: Bring Your Own Device, BYOD) involviert sind, sollten die Prozesse mit dem Betriebsrat abgestimmt werden. Da bei der Prüfung kurzzeitige Verfügbarkeitsprobleme nicht ausgeschlossen werden können, empfiehlt die SySS, alle Mobile Device-Nutzer – auch zur Schaffung von Security Awareness – zu informieren.

2.9 CLOUD

Cloud Computing ist ein wichtiger Trend der letzten Jahre. Die Bündelung von Serverkapazitäten und der Eindruck eines unbegrenzten Speicherplatzes machen Cloud-Dienste für Nutzer sehr attraktiv. Auch der bequeme Zugriff per Internet mit diversen Clients wie dem eigenen Computer, aber auch Smartphones und Tablets trägt zur wachsenden Beliebtheit von Cloud Computing bei. Leider hat Praktikabilität auch einen Haken: Wo Neues entsteht, sind meist auch Hacker nicht weit, die Angriffe gegen Cloud-Dienste entwickeln. Die SySS bietet mit dem Modul CLOUD Sicherheitsprüfungen von Amazon Web Service-Umgebungen und Microsoft Azure-Infrastrukturen an. In den folgenden Abschnitten werden die Ausprägungen dieses Prüfmoduls im Detail beschrieben.

Abbildung 2.19: Modul CLOUD

2.9.1 CLOUD/AWS: Sicherheitsanalyse und Härtungsempfehlungen für Amazon Web Services-Projekte

Zusammenfassung

Bei der Sicherheitsanalyse einer AWS-Umgebung, die sowohl ein Konfigurationsaudit als auch Elemente des Penetrationstests umfasst, werden die Cloud-Infrastruktur und darin genutzte Services auf Schwachstellen und mögliche Härtungsmaßnahmen hin überprüft.

Abbildung 2.20: Modul CLOUD/AWS

Ausgangslage

Um Kosten zu optimieren und Skalierungsmöglichkeiten zu schaffen, kommt kaum ein Unternehmen mehr an der Cloud vorbei. Einer der größten Anbieter in diesem Bereich ist Amazon mit den Amazon Web Services (AWS). Egal, ob ein Cloud-Projekt gerade aufgebaut wird oder bereits in Betrieb ist: Eine Sicherheitsanalyse deckt Schwachstellen auf und projektspezifische Härtungsempfehlungen verbessern das Sicherheitsniveau des Cloud-Projektes. Neben grundlegenden Funktionalitäten wie der Überprüfung des Rollen- und Berechtigungskonzeptes und des Schlüsselmanagements zum Schutz von sensiblen Daten prüft die SySS auch Speicherablageberechtigungen, zum Beispiel von S3 (Simple Storage Service) oder Datenbanken. Wird die Infrastruktur dynamisch erzeugt und hierbei mit „Terraform" oder „CloudFormation" gearbeitet, überprüft die SySS die Sicherheit der Systeme, die in Zukunft im Einsatz sein werden. Neben den Templates wird auch die Sicherheit der Image-Quellen und Auto Scaling Groups untersucht.

Auch eine umfangreiche Netzwerkkonfiguration, bestehend aus VPCs, Subnetzen, Sicherheitsgruppen (Security Groups) und Gateways, wird auf offene Angriffsflächen hin analysiert und Verbesserungspotenzial wird erarbeitet.

Auch das Auditieren von organisatorisch-technischen Themen wie Monitoring, Logging und den Alert-Workflows fällt in den Kompetenzbereich der SySS. Hierbei wird zum Beispiel geprüft, ob die richtigen Sicherheitsmeldungen bei den richtigen Mitarbeitern ankommen und ob diese nicht unnötigerweise mit zu vielen Informationen überhäuft werden.

Sollte das Projekt auf einer serverlosen Infrastruktur (Serverless Infrastructure) aufbauen, betrachtet die SySS die zugeschnittene Implementierung mit Services wie beispielsweise AWS Lambda, AWS DynamoDB oder AWS Cognito.

Bei einem IoT-Projekt werden der Enrollment-Prozess, die Kommunikation mit dem IoT Core und die Konfiguration der entsprechenden Regeln (Topic Rules) analysiert, damit die Geräte und deren Benutzer nach dem Least Privilege-Prinzip konfiguriert werden.

Zielsetzung

Die SySS versucht, gemeinsam mit dem Kunden das Cloud-Projekt auf ein hohes Sicherheitsniveau zu heben oder ihm ein solches zu bestätigen. Die SySS arbeitet neben einem Katalog an Schwachstellen auch differenziert eine Liste für empfohlene und mögliche Härtungsmaßnahmen aus.

Durchführung

Die Cloud-Audits finden in der Regel remote statt. Hierfür erhält die SySS einen Benutzer mit Leseberechtigungen auf dem entsprechenden Projekt. Ergänzt wird diese Herangehensweise durch Telefoninterviews mit zuständigen Personen, um offene Fragen zu klären oder einen Einblick in die organisatorische Struktur zu erhalten. Hierbei soll beispielsweise auch ermittelt werden, ob es Themengebiete gibt, die bisher im Projekt nicht abgebildet worden sind. Beispiele hierfür sind regelmäßige Vulnerability-Scans von Instanzen oder ein fehlender Notfallaccount bei einem Ausfall der Multi-Faktor-Geräte.

Mitwirkung des Kunden

Bei einem Audit kann nur das bewertet werden, was auch eingesehen werden kann. Daher ist es besonders wichtig, dass die benötigten Leseberechtigungen für das Projekt gesetzt sind.

Hierbei lohnt es sich, vor der Übergabe der Auditor-Accounts an die SySS zu überprüfen, ob die eingerichteten Berechtigungen ausreichen, um alles Relevante sehen zu können.

Die Kombination aus folgenden Berechtigungen hat sich hierbei als besonders zielführend herausgestellt:

- `arn:aws:iam::aws:policy/job-function/ViewOnlyAccess`
- `arn:aws:iam::aws:policy/SecurityAudit`

Neben den Auditorberechtigungen, die eine Sicht „von oben" ermöglichen, ist auch die Bereitstellung von Benutzeraccounts des jeweiligen Projektes sinnvoll, um Szenarien aus der Perspektive eines Benutzers überprüfen zu können.

2.9.2 CLOUD/AZURE: Sicherheitsanalyse und Härtungsempfehlungen für Azure-Infrastrukturen

Zusammenfassung

Bei der Sicherheitsanalyse einer Office 365-Umgebung, die sowohl ein Konfigurationsaudit als auch Elemente des Penetrationstests umfasst, werden die Cloud-Infrastruktur und darin genutzte Services auf Schwachstellen und mögliche Härtungsmaßnahmen hin überprüft. Auch das Sicherheitsniveau der Office 365-Konfiguration wird evaluiert.

Abbildung 2.21: Modul CLOUD/AZURE

Ausgangslage

Eine IT-Firmenstruktur auf Basis von Microsoft Active Directory, Windows-Servern und Windows Office-Clients ist heute allgegenwärtig. Um diese Infrastruktur dynamischer skalieren zu können und die Arbeit von der Ferne aus einfacher zu gestalten, ist der Schritt in die Azure-Cloud eine Möglichkeit, die Anforderungen nach mehr Flexibilität zu erfüllen. Egal, ob Kunden gerade die ersten Schritte in der Azure-Cloud machen, bereits größere Umzüge und Projekte realisiert haben oder sogar auf „Cloud only" setzen: Die SySS unterstützt sie, ihre Azure-Infrastruktur

auf ein hohes Sicherheitsniveau zu bringen, oder bestätigt ihnen bestenfalls, dass ihre Azure-Umgebung bereits sehr gut abgesichert ist.

Bei einer Azure-Überprüfung wird in der Regel im ersten Schritt das Azure Active Directory analysiert. Hierbei wird geprüft, ob die Benutzer- und Gruppenrechte sowie die Authentifizierung in einem Zustand sind, der zu den Sicherheitsanforderungen des Kunden passt. Sowohl bei Infrastrukturen mit virtuellen Maschinen oder Kubernetes als auch bei komplett serverlos auf- und ausgebauten Infrastrukturen sorgt die SySS dafür, dass keine Konfigurationsfehler zu Schwachstellen oder gar Datenverlust führen. In einem Audit, das sowohl manuelle als auch automatisierte Tests umfasst, wird die jeweilige Konfiguration auf sicherheitsrelevante Fehlkonfigurationen und den Einsatz von Best Practice-Methoden getestet. Auch das Monitoring, das Logging und den Alert-Workflow nimmt die SySS unter die Lupe und gibt einen Überblick, was möglich und nötig ist, um die Azure-Umgebung nachhaltig zu stärken.

In einem Office 365-Konfigurationsaudit geht es in erster Linie darum, herauszuarbeiten, ob die Daten und E-Mails von Mitarbeiterinnen und Mitarbeitern vor ungewollten Zugriffen untereinander und durch Dritte geschützt sind. Hierbei werden unter anderem die folgenden Aspekte betrachtet:

- Benutzerberechtigungseinstellungen und Rollenverteilung in Office 365 und Azure AD-Audit von Office Secure Score-Einsatz und OneDrive-Konfiguration
- Datenspeicherung und Prüfung von Anhängen z. B. Ablage von kritischen Daten und Malware-Erkennung
- Überprüfung der Datenstromüberwachung (OneDrive, SharePoint etc.)
- Überprüfung des Anmeldemonitorings bzw. von Angriffsmonitoring/Benachrichtigung bei administrativen Handlungen (z. B. der richtige Einsatz von Azure Advanced Threat Protection)

Wir teilen auch gerne unsere Kompetenzen in der Sicherheitsanalyse bei Azure IoT-Umgebungen. Hierbei werden die folgenden Themen bearbeitet:

- Enrollment-, Registrierungs- und Authentifizerungsprozess des IoT-Gerätes
- Überprüfung der Datenkommunikation zwischen IoT-Gerät und Azure IoT Hub auf Schwachstellen hin
- Der sichere Einsatz von Azure Event Hubs und Azure Functions
- Das passende Monitoring, um kompromittierte Geräte zu detektieren
- Der Best Practice-Einsatz des Azure IoT SDK auf den Geräten
- Überprüfung einer eventuell vorhandenen Mandantentrennung der IoT-Landschaft auf die Möglichkeit von Rechteeskalationen

Zielsetzung

Die SySS versucht, gemeinsam mit dem Kunden das Cloud-Projekt auf ein hohes Sicherheitsniveau zu heben oder ihm ein solches zu bestätigen. Die SySS arbietet neben einem Katalog an Schwachstellen auch differenziert eine Liste für empfohlene und mögliche Härtungsmaßnahmen aus.

Durchführung

Die Cloud-Audits finden in der Regel remote statt. Hierbei erhält die SySS einen Benutzer mit Leseberechtigungen auf den Tenant oder die Projektressourcen und das AAD. Ergänzt wird diese Herangehensweise durch Telefoninterviews mit zuständigen Personen, um offene Fragen zu klären oder einen Einblick in die organisatorische Struktur zu erhalten. Hierbei soll beispielsweise auch ermittelt werden, ob es Themengebiete gibt, die bisher im Projekt nicht abgebildet worden sind. Beispiele sind hier regelmäßige Vulnerability-Scans von Instanzen oder ein fehlender Notfallaccount bei einem Ausfall der Multi-Faktor-Geräte.

Mitwirkung des Kunden

Bei einem Audit kann nur das bewertet werden, was auch eingesehen werden kann. Daher ist es besonders wichtig, dass die benötigten Leseberechtigungen für das Projekt gesetzt sind.

Hierbei lohnt es sich, vor der Übergabe der Auditor-Accounts an die SySS zu überprüfen, ob die eingerichteten Berechtigungen ausreichen, um alle wichtigen Konfigurationen sehen zu können.

Je nach Projektumfang sollte hier ein Benutzer mit den Berechtigungen des „Global Reader" auf dem Tenant bereitgestellt werden. Weiterhin sollte eine Berechtigung für die projektrelevanten Ressourcengruppen ermöglicht werden.

Neben den Auditorberechtigungen, die eine Sicht „von oben" ermöglichen, ist auch die Bereitstellung von Benutzeraccounts des Projektes sinnvoll, um Szenarien aus der Sicht eines Benutzers überprüfen zu können.

Tipp von Sebastian Schreiber

Die Cloud ist mehr als das Auslagern von virtuellen Maschinen. Sie ist ein neues Ökosystem, das seine eigenen Regeln hat und insbesondere auch die Sicherheit betrifft. Große Projekte lassen sich in kürzester Zeit realisieren und werden oft von einem Team umgesetzt, das nicht aus der klassischen IT des Unternehmens entstanden ist. Achten Sie daher auch in diesem neuen Ökosystem darauf, dass Sicherheit einen wichtigen Stellenwert einnimmt.

2.10 EMBEDDED: Embedded Security (ES)

Zusammenfassung

Über die Module des Bereichs Embedded Security (ES) bietet die SySS vielfältige Sicherheitsanalysen der unterschiedlichsten eingebetteten Systeme an. Sie reichen von einer Analyse der extern erreichbaren Schnittstellen per Kabel- oder Funkübertragung bis hin zur Untersuchung der intern verbauten Komponenten und der dort verwendeten Software. Selbst für die Analyse einzelner Protokolle oder Steuergeräte aus dem Automobilbereich können eigene Untermodule angeboten werden.

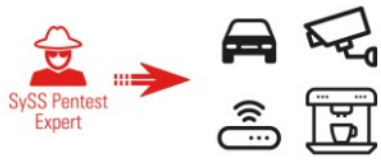

Abbildung 2.22: Modul EMBEDDED

Im Folgenden werden zunächst allgemeine Voraussetzungen und Empfehlungen für die Durchführung der Testmodule dargestellt. Im Anschluss werden diese detailliert beschrieben und mögliche Angriffsszenarien aufgezeigt.

Ausgangslage

Auf Hardwarekomponenten werden häufig sensible Informationen wie Zugangsdaten für ein Back-End-System, Clientzertifikate oder Passwörter für Wartungszugänge hinterlegt. Außerdem gelten interne Funktionsweisen – beispielsweise Algorithmen, die Sensordaten verarbeiten – meist als Betriebsgeheimnisse. Da die Geräte in der

Regel der physischen Kontrolle des Herstellers entzogen sind, können Dritte durch Angriffe versuchen, hinterlegte Daten zu extrahieren oder das Gerät anderweitig zu manipulieren.

Zielsetzung

Im Rahmen des Sicherheitstests werden nach Absprache die Hardware, deren angebotene Schnittstellen, Verbindungen zum Back-End und die Firmware selbst auf Schwachstellen geprüft. Eine Analyse des Back-End, das oftmals in Form einer Webserviceschnittstelle – z. B. mittels SOAP oder REST – umgesetzt wird, kann auf Wunsch ebenfalls durchgeführt werden (siehe Modul WEBSERVICE, Abschnitt 2.3 auf Seite 27). Je nach Hardwaretyp kann das Ziel beispielsweise darin bestehen, zu verifizieren, ob die darauf abgelegten oder die darüber übertragenen Daten ausreichend vor Fremdzugriffen geschützt sind. Auch der Schutz der Firmware vor unbefugtem Kopieren oder Manipulieren kann eine solche Analyse motivieren.

Durchführung

Die Hardwarekomponenten werden, wenn möglich, im Labor der SySS auf Sicherheitsschwächen untersucht. Je nach Testmodul kommen dabei unterschiedliche Werkzeuge und Methoden zum Einsatz. Bei invasiven Tests kann es beispielsweise dazu kommen, dass einzelne Chips, wie z. B. Speicherbausteine, ausgelötet und analysiert werden. Die im Folgenden aufgezählten Schwachstellen beschreiben exemplarische Verwundbarkeiten, die bei derartigen Tests häufig aufgedeckt werden:

- Firmware-Extraktion: Die Hardware weist keine wirksamen Maßnahmen auf, die vor einer Extraktion der Firmware schützen.
- Wartungszugänge: Über Wartungsdienste, wie beispielsweise einen Konsolenzugang über eine serielle Schnittstelle, können Daten extrahiert oder die Funktionsweise des Geräts kann manipuliert werden.
- Trivialpasswörter: Zugangsdaten für den Bootloader oder Wartungsschnittstellen sind bekannt oder leicht zu erraten.
- Unverschlüsselte Speicherbausteine: Unverschlüsselte Speicherbausteine können ausgelötet und anschließend ohne Beschränkung ausgelesen werden.
- Anmeldedaten werden im Klartext gespeichert: Die in der zu testenden Hardware abgelegten Zugangsdaten sind besonders schützenswert, da sie für weitere Angriffe eingesetzt werden können. Dennoch kann eine Extraktion möglich sein, wenn Schutzmaßnahmen (beispielsweise des Betriebssystems bzw. der Firmware) umgangen werden können.
- Man-in-the-Middle-Angriff auf Verbindung: Bei nicht ordnungsgemäßer Implementierung von verschlüsselten Verbindungen kann ein Angreifer in geeigneter Position im Netzwerk den Datenverkehr abhören und modifizieren.
- Replay-Angriffe: Durch erneutes Absenden bereits aufgezeichneter Kommunikation können bekannte Aktionen ausgelöst werden.
- Statische Schlüssel: Durch Extraktion des statischen Schlüsselmaterials kann die Verschlüsselung gebrochen werden.
- Verletzung des Principle of Least Privilege

Die konkrete Durchführung der einzelnen spezifischen Module wird ab Abschnitt 2.10.1 auf Seite 60 erläutert.

Mitwirkung des Kunden

Während des Penetrationstests sollten die Ansprechpartner telefonisch oder per E-Mail zur Verfügung stehen. Hierzu zählen Ansprechpartner zur Einrichtung des Systems, Entwickler der Schnittstellen und Betreuer eventuell

weiterer Dienste, mit welchen das Gerät kommuniziert. Da sich im Laufe des Penetrationstests auch Fragen zur Hardware selbst ergeben können, sollten auch hierfür Ansprechpartner benannt werden.

Testvorbereitung

Die SySS empfiehlt, für den Penetrationstest mindestens zwei Ausgaben des zu testenden Geräts bereitzustellen. So kann überprüft werden, ob ein durchgeführter Angriff auch auf weitere Geräte übertragbar ist oder diese sich durch einen Angriffsvektor beeinflussen lassen. Auch für einen möglichen Ausfall des Geräts ist damit vorgesorgt. Ist das Modul ES/INTERNAL (siehe Abschnitt 2.10.4) geplant, sollte im Idealfall noch eine dritte Ausführung bereitstehen. Die Geräte sollten der SySS bereits mehrere Tage vor Testbeginn vorliegen. So kann die erwartete Funktionalität der zu testenden Geräte schon im Vorfeld geprüft werden.

Um die Testqualität zu verbessern, empfiehlt die SySS, sämtliche Dokumentationen zur Inbetriebnahme und den verfügbaren Schnittstellen und Prozessen bereitzustellen. Hilfreich sind auch Architekturdiagramme, (Protokoll-)Spezifikationen oder technische Handbücher und Härtungsrichtlinien. Zusätzlich können zum Zweck der Zeitersparnis etwaige vom Kunden genutzte Testwerkzeuge/Software oder vorab erlangte Erkenntnisse mit der SySS geteilt werden.

Vor Beginn des Penetrationstests sollte das Gerät in einem gemeinsamen Workshop initial eingerichtet werden. Gleichermaßen ist eine Einführung in die Verwendung und Konfiguration der Geräte sinnvoll. Der Workshop kann gemeinsam im Labor der SySS, beim Kunden vor Ort oder über eine Telefon- bzw. Videokonferenz erfolgen. Dabei sollten nicht nur die Endverbraucherseite, sondern auch die Provisionierung und die Administration der Geräte betrachtet werden.

Bei der Verwendung externer Dienste (Cloud) kann es nötig sein, beim entsprechenden Dienstleister eine Genehmigung für den Penetrationstest einzuholen. Diese Fragen können im Rahmen des initialen Kick-off-Gesprächs (siehe Abschnitt 1.3.1 auf Seite 16) geklärt werden.

Ansprechpartner

Da die Prüfung der Hardwarekomponenten idealerweise im Labor der SySS durchgeführt wird, sollte der Verantwortliche der zu testenden Hardwarekomponente während des Testzeitraums zumindest telefonisch als Ansprechpartner erreichbar sein. Für Detailfragen ist es hilfreich, wenn der direkte Kontakt zu den Entwicklern oder einem anderen technischen Ansprechpartner hergestellt wird.

Abhängigkeiten

Organisatorische und technische Abhängigkeiten sollten der SySS mitgeteilt werden. Dies kann im Rahmen des Kick-off-Gesprächs geschehen. Wenn es sich bei der Teststellung beispielsweise nicht um ein völlig autonomes System handelt, das getrennt von anderen Systemen getestet werden kann, dann muss der SySS mitgeteilt werden, von welchen weiteren Systemen der Testgegenstand abhängt. Auch eventuelle Testeinschränkungen (zeitlich, technisch, organisatorisch) müssen der SySS mitgeteilt werden.

Tipps von Sebastian Schreiber

Schätzen Sie den Zeitbedarf für einen Hardwaretest sehr großzügig ein! Prüfen Sie, mit welchen Systemen Ihr Produkt kommuniziert. In der Regel ist ein vollständiger Test dieser Systeme sinnvoll, wenn es sich ohnehin um eine organisatorische und technische Einheit handelt. Wählen Sie anschließend die passenden Prüfmodule für den Test.

2.10.1 ES/AUTOMOTIVE: Sicherheitsanalyse von Steuergeräten und Sensoren

Steuergeräte und Sensoren im Automobilbereich verarbeiten Daten und regeln auf deren Grundlage die Systeme des Fahrzeugs. Ein sicherer und störungsfreier Betrieb der Systeme kann daher lebenswichtig sein. Zusätzlich spielt das Thema Intellectual Property eine sehr große Rolle. Für Automobilhersteller sind beispielsweise Leistungskurven und Algorithmen zur Motorsteuerung besonders wertvoll. Im Bereich der E-Mobilität kann auch das Lademanagement der Batteriezellen von großer Bedeutung sein.

Abbildung 2.23: Modul ES/AUTOMOTIVE

Die SySS bietet mit dem Untermodul ES/AUTOMOTIVE eine IT-Sicherheitsüberprüfung der oben genannten Komponenten an. Testgegenstände können Testaufbauten mit mehreren Komponenten oder gegebenenfalls ganze Fahrzeuge sein. Auch einzelne Komponenten wie ECUs, Head Units, Sensoren etc. können einer Sicherheitsüberprüfung unterzogen werden. Die Vorgehensweise dieses Moduls ähnelt zwar durchaus derer bei den Modulen ES/EXTERNAL (siehe Abschnitt 2.10.2) und ES/INTERNAL (siehe Abschnitt 2.10.4), im Automobilbereich werden jedoch häufig besondere Protokolle und Technologien eingesetzt, die speziell für diesen Bereich entwickelt wurden. Die SySS passt daher die eingesetzten Werkzeuge und Angriffstechniken entsprechend an. Unterschiede ergeben sich auch in der Einstufung der gefundenen Sicherheitslücken. Diese werden mit speziellem Fokus auf die Automotive-Industrie beschrieben und bewertet.

Fragestellungen

Während des Penetrationstests klärt die SySS unter anderem die folgenden Fragestellungen:

- Analyse der Diagnosefunktionen: Sind die verwendeten Diagnoseprotokolle ausreichend abgesichert? (Stichwort: Security Access)
- Schwächen in der Bus-Kommunikation (CAN, FlexRay, LIN, Ethernet): Welche Protokolle kommen zum Einsatz und wie sind diese konfiguriert?
- Tamper Detection der ECU: Lässt sich die ECU öffnen und manipulieren, ohne dass dies vom System bemerkt wird?
- Können sensible Daten – z. B. Daten zur Motorsteuerung – von der ECU ausgelesen werden?
- Wie reagieren die Akteure auf fehlerhafte Sensordaten?
- Kann die Firmware extrahiert und modifiziert werden?

2.10.2 ES/EXTERNAL: Sicherheitsanalyse kabelgebundener Schnittstellen

Über die diversen Schnittstellen können verschiedene Geräte miteinander kommunizieren und Daten austauschen. Bei der Kommunikation von Geräten untereinander handelt es sich häufig um schützenswerte Daten, deren Bekanntwerden oder Manipulation immensen Schaden verursachen kann. Auch über unzureichend abgesicherte Konfigurationsschnittstellen kann großer Schaden entstehen.

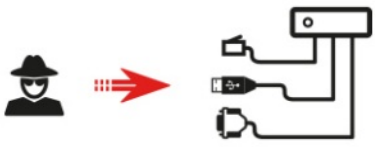

Abbildung 2.24: Modul ES/EXTERNAL

Das Untermodul ES/EXTERNAL überprüft das Schutzniveau dieser kabelgebundenen Schnittstellen. Das Gerät wird dabei nicht geöffnet. Untersucht werden lediglich die von außen erreichbaren Schnittstellen. Hierzu zählen beispielsweise Ethernet, serielle Verbindungen oder optische Sensoren. Auch weitere Schnittstellen, z. B. proprietäre, können untersucht werden. Dieses Modul eignet sich vor allem für eine initiale Sicherheitsbetrachtung und lässt sich ergänzend optimal mit den Modulen ES/INTERNAL (siehe Abschnitt 2.10.4) und ES/PROTOCOL (siehe Abschnitt 2.10.5) für eine tiefergreifende Analyse der Produkte oder einzelner Schnittstellen kombinieren.

Hinweis: Soll lediglich die Webanwendung oder ein Webservice, der vom Testgerät angeboten wird (Beispiel: Konfigurationsseite eines Routers), überprüft werden, sind die Module WEBAPP (siehe Abschnitt 2.2 auf Seite 23) oder WEBSERVICE (siehe Abschnitt 2.3 auf Seite 27) geeignet.

Fragestellungen

Während des Penetrationstests klärt die SySS unter anderem die folgenden Fragestellungen:

- Überprüfung der Verschlüsselung: Werden die übertragenen Daten ausreichend verschlüsselt? Kann die Verschlüsselung gebrochen oder umgangen werden?
- Gibt es Schwachstellen im Autorisierungs- und Authentifizierungssystem?
- Manipulation der übertragenen Daten: Ist es möglich, eine Man-in-the-Middle-Position einzunehmen, um hierdurch sensible Daten mitzuschneiden oder zu manipulieren?
- Replay-Angriffe: Können aufgezeichnete Sequenzen erneut abgespielt werden, um eine Aktion im Gerät auszulösen? (Beispiel: Deaktivierung von Schließ- oder Alarmsystemen)
- Können über einen Missbrauch der Schnittstellen sensible Daten extrahiert werden?
- Kann ein Gerät über die vorhandenen Schnittstellen kompromittiert werden?

2.10.3 ES/FIRMWARE: Sicherheitsanalyse von Firmware

Kaum ein elektronisches Produkt funktioniert heutzutage noch ohne entsprechende Firmware. Genauso wie sich die Produkte unterscheiden, so unterscheiden sich auch die Ausprägungen der implementierten Firmware, die häufig auf den jeweiligen Anwendungsfall des Produkts ausgerichtet ist. Dies gilt beispielsweise für ein angepasstes Linux-System, eine barebone-Firmware, die ohne Abstraktion direkt mit Hardwarekomponenten kommuniziert, oder ein Real-Time Operating System (RTOS). Die Vielzahl an Möglichkeiten macht es häufig sehr komplex, die Firmware entsprechend sicher zu gestalten. Auch Themen wie die Konzipierung und Umsetzung eines sicheren Updatemechanismus „Over-the-Air" (OTA) oder die Problematik eines sicheren Lizenzierungsverfahrens können Herausforderungen darstellen.

Abbildung 2.25: Modul ES/FIRMWARE

Die Sicherheitsprüfung des Moduls ES/FIRMWARE zielt auf eine Analyse eben dieser Bereiche ab.

In den meisten Fällen wird in diesem Modul eine statische Codeanalyse oder Reverse Engineering durchgeführt. Aus diesem Grund empfiehlt die SySS, die Firmware als Datei bereitzustellen. Falls die Firmware verschlüsselt ist, sollte zusätzlich eine unverschlüsselte Version zur Verfügung stehen. Obwohl lediglich die Software des Geräts überprüft wird, empfiehlt die SySS dennoch, die entsprechende Hardware mitzuliefern. Nur so können festgestellte Schwachstellen vollumfänglich nachvollzogen und überprüft werden.

Fragestellungen

Während des Penetrationstests klärt die SySS unter anderem die folgenden Fragestellungen:

- Welche Art Firmware wird verwendet? (Linux-Image, binäres Image-Format etc.)
- Funktionieren die Verschlüsselung und Signierung der Updatedateien zuverlässig?
- Wie funktioniert der Updateprozess?
- Wie funktionieren die Autorisierungs- und Authentifizierungsprozesse?
- Gibt es Schwächen in den bereitgestellten Diensten? (Remote Code Execution, SQL Injection etc.)
- Lassen sich geheime Schlüssel extrahieren, die für weitere Angriffe (z. B. gegen die Cloud-Infrastruktur) verwendet werden können?

2.10.4 ES/INTERNAL: Sicherheitsanalyse interner Schnittstellen und Speicherkomponenten

Auf modernen Geräten werden häufig sensible Informationen wie Zugangsdaten für ein Back-End-System, Clientzertifikate oder Passwörter für Wartungszugänge hinterlegt. Außerdem gelten interne Funktionsweisen – beispielsweise Algorithmen, die Sensordaten verarbeiten – meist als Betriebsgeheimnisse. Da die Geräte in der Regel der physischen Kontrolle des Herstellers entzogen sind, können Dritte durch gezielte Angriffe versuchen, die hinterlegten Daten zu extrahieren oder das Gerät anderweitig zu manipulieren.

Abbildung 2.26: Modul ES/INTERNAL

Das Untermodul ES/INTERNAL konzentriert sich daher auf Angriffsvektoren bei einem Angriff mit physischem Zugriff auf den Testgegenstand. Die SySS analysiert dabei Angriffsmöglichkeiten auf interne Datenspeicher (z. B. eMMC, Flash-ROM), Schnittstellen (z. B. UART, I²C, JTAG, CAN) und die verwendeten Komponenten (z. B. Controller, Crypto-IC). Hierfür ist es notwendig, ein Gerät zu öffnen und/oder zu zerlegen. So kann es beispielsweise dazu kommen, dass zusätzliche Leitungen an die Platine angebracht werden oder einzelne Chips, wie Speicherbausteine, entlötet und losgelöst vom Produkt untersucht werden. Eine Bereitstellung des Produkts in mehrfacher Ausführung ist daher dringend zu empfehlen.

Fragestellungen

Während des Penetrationstests klärt die SySS unter anderem die folgenden Fragestellungen:

- Gibt es wirksame Maßnahmen, die vor einer Extraktion der Firmware schützen?
- Sind Zugangsdaten für den Bootloader oder Wartungsschnittstellen bekannt oder leicht zu erraten?
- Kann der Inhalt von Speicherbausteinen durch das Anbringen von Leitungen oder das Chip-off-Verfahren extrahiert werden?
- Können Zugangsdaten oder private Schlüssel extrahiert werden? (Diese können für weitere Angriffe eingesetzt werden, z. B. gegen ein Cloud-Back-End)
- Bus-Snooping: Ungeschützte Schnittstellen auf der Platine können bei einem Angriff abgehört werden. Können auf diese Weise Geheimnisse ausgelesen oder kann eine nachfolgende Verschlüsselung umgangen werden?
- Fehlender Schutz vor Manipulation (Tampering): Kann die Funktionsweise von Geräten verändert werden oder können Geheimnisse abhanden kommen, ohne dass dies auffällt?

2.10.5 ES/PROTOCOL: Sicherheitsanalyse von Protokollen

Ein Gerät kommuniziert über verschiedene Protokolle mit anderen Systemen. Hierbei werden Daten ausgetauscht oder Kommandos übermittelt. Da es sich hierbei häufig um schützenswerte Daten handelt, deren Manipulation hohen Schaden verursachen kann, sind die Sicherheitsmechanismen dieser Protokolle von besonders großer Bedeutung.

Abbildung 2.27: Modul ES/PROTOCOL

Die hierfür verwendeten, oftmals proprietären Protokolle werden in diesem Modul genauer untersucht. Typische Ziele der Untersuchung sind die Stärke der Verschlüsselung und der Schutz der Integrität der übertragenen Daten. Auch die Untersuchung auf Logikfehler, die häufig zu Sicherheitsvorfällen führen können, sind Teil des Penetrationstests. Bei der Verwendung komplexerer Protokolle kann zusätzlich das Umgehen von Sicherheitsmechanismen zur Autorisierung und Authentifizierung untersucht werden.

Hinweis: Im Gegensatz zum Untermodul ES/EXTERNAL (siehe Abschnitt 2.10.2), mit dem Möglichkeiten zur Kompromittierung über extern erreichbare Schnittstellen untersucht werden, liegt der Fokus dieses Untermoduls auf einer tiefergreifenden Untersuchung eines spezifischen Protokolls.

Fragestellungen

Während des Penetrationstests klärt die SySS unter anderem die folgenden Fragestellungen:

- Wie stark ist die Verschlüsselung des Protokolls? Lässt sich diese aushebeln oder lassen sich sensible Daten extrahieren?
- Können Daten manipuliert werden?
- Können die Geräte über Logikfehler zu unerwünschtem Verhalten gebracht werden?
- Replay-Angriffe: Können aufgezeichnete Sequenzen erneut abgespielt werden, um eine Aktion im Gerät auszulösen? (Beispiel: Deaktivierung von Schließ- oder Alarmsystemen)

2.10.6 ES/WIRELESS: Sicherheitsanalyse funkbasierter Schnittstellen

Über die diversen Funktechnologien können verschiedene Geräte miteinander kommunizieren, um Daten auszutauschen oder um sich gegenseitig Steuersignale zu senden. Sowohl im privaten als auch im industriellen Umfeld sind funkbasierte Verbindungen nicht mehr wegzudenken: sei es die Vernetzung großer Industrieanlagen, seien es Zugangskontrollen zu Gebäuden oder auch kontaktloses Bezahlen oder die Verwendung kabelloser Kopfhörer. Die entsprechenden Daten sind häufig schützenswert und ihre Manipulation kann hohen Schaden verursachen. Eine Übernahme der Steuerung kann überdies mitunter die Sicherheit von Personen gefährden. Daher ist die Sicherheit dieser Kommunikationswege von besonders hoher Bedeutung. Insbesondere spielt die Tatsache, dass für einen Angriff lediglich physische Nähe, aber kein physischer Zugriff bestehen muss, eine nicht zu vernachlässigende Rolle. Gegebenenfalls können Geräte auf diese Weise sogar vollständig kompromittiert werden.

Abbildung 2.28: Modul ES/WIRELESS

Die Sicherheitsprüfung des Moduls ES/WIRELESS zielt auf die Analyse dieser funkbasierten Technologien und der verwendeten Kommunikationsprotokolle ab. Die SySS analysiert dabei Angriffsmöglichkeiten, unter anderem

auf Bluetooth/BLE, Zigbee, LoRaWAN, ZWave, WLAN oder auch NFC/RFID. Selbst eine Analyse von Daten, die über Mobilfunk (z. B. LTE) übertragen werden, ist denkbar. Neben der Implementierung der Protokoll-Stacks steht dabei insbesondere auch die Suche nach Konfigurationsfehlern der jeweils verwendeten Technologie im Fokus.

Hinweis: Die Analyse weiterer, auch proprietärer, Funkprotokolle ist potenziell möglich, solange der SySS die dafür nötige Hard- und Software bereitgestellt wird. Hierfür stehen wir gerne beratend zur Verfügung. Für die Überprüfung von WLAN-Infrastrukturen im Unternehmensumfeld sollte das Modul WLAN (siehe Abschnitt 2.7 auf Seite 46) verwendet werden.

Das Untermodul ES/WIRELESS ist prinzipiell ohne ein Öffnen des Geräts im Blackbox-Ansatz (siehe Abschnitt 1.1.3 auf Seite 6) durchführbar. Es wird jedoch empfohlen, funkbasierte Penetrationstests mindestens im Graybox-Ansatz (siehe Abschnitt 1.1.3) (Bereitstellung von Dokumentation, Spezifikationen etc.) durchzuführen, da dies erfahrungsgemäß ein effizienteres und ökonomischeres Ergebnis liefert. Die Funktionsweise der Protokolle und mögliche Testszenarien können im Vorfeld in einem gemeinsamen Workshop besprochen werden. Für eine tiefergehende Analyse sollten zudem die Module ES/INTERNAL (siehe Abschnitt 2.10.4) und ES/PROTOCOL (siehe Abschnitt 2.10.5) in Erwägung gezogen werden.

Fragestellungen

Im Folgenden sind für verschiedene Technologien beispielhafte Fragestellungen aufgelistet, die während des Penetrationstests geklärt werden können:

Bluetooth Smart (BLE)

- Kann die Kommunikation im Klartext mitgelesen werden?
- Können Characteristics/Services ohne Authentifizierung gelesen/geschrieben werden?
- Welche Daten werden über BLE übertragen und können diese manipuliert werden?
- Welcher Security Mode wird verwendet?
- Sind BLE-Man-in-the-Middle-Angriffe möglich, beispielsweise durch Spoofing der BLE-MAC-Adresse? Toolauswahl: Sniffle, nRF Sniffer for Bluetooth LE, nRF52 Dongle, nRF52 DK

RFID und NFC

- Können Karten geklont oder emuliert werden?
- Können Zugangsberechtigungen manipuliert werden?
- Sind die hinterlegten Daten ausreichend abgesichert?
- Können sensible Daten extrahiert werden? Toolauswahl: Proxmark3, Kartenlesegeräte, NFC-fähiges Smartphone

WLAN

- Wie ist das aufgespannte WLAN abgesichert (Authentifizierung)?
- Sind gängige Schutzmaßnahmen aktiv (z. B. Protected Management Frames)?
- Sind Teilnehmer untereinander isoliert bzw. sollten sie es sein?
- Gibt es konfigurative Schwächen (z. B. Passwortwiederverwendung, schwache Passwörter etc.)?

ZIGBEE

- Werden Pakete korrekt verschlüsselt?
- Existiert eine Verschlüsselung auf Netzwerk- oder Anwendungsebene?
- Wie werden die Schlüssel ausgetauscht?
- Wie werden neue Geräte angelernt (Gibt es einen Master-Key)?

2.11 SOFTWARE: Sicherheitsanalyse von Softwarelösungen

Zusammenfassung

Softwarekomponenten und -produkte werden im Rahmen dieser Sicherheitsprüfung auf Schwachstellen hin untersucht. Der Fokus der Sicherheitsanalyse liegt dabei auf sicherheitsrelevanten Funktionen wie beispielsweise Authentifizierung, Autorisierung und Verschlüsselung. Unter Einsatz verschiedener Analysemethoden wird nach möglichen Sicherheitsschwächen der zu testenden Software gesucht, die sich aus unterschiedlichen Angreiferperspektiven ausnutzen lassen. Bekannte Beispiele für Softwareschwachstellen sind Fehler in der Verarbeitung von Benutzereingaben, die etwa missbräuchlich zur Ausführung beliebigen Programmcodes genutzt werden können, oder Fehler im Berechtigungskonzept, die einen unautorisierten Zugriff auf Funktionen oder Daten ermöglichen.

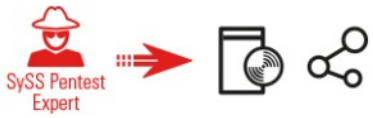

Abbildung 2.29: Modul SOFTWARE

Ausgangslage

Software stellt einen integralen Bestandteil moderner informationstechnischer Systeme und Prozesse dar. Softwareprodukte und einzelne Softwarekomponenten besitzen einerseits eine große Bedeutung für die ordnungsgemäße Funktionsweise von Arbeitsabläufen und Geschäftsprozessen sowie andererseits für die Gewährleistung der Informationssicherheit. Sicherheitsrelevante Funktionen wie Authentifizierung, Autorisierung und Verschlüsselung sind hierbei wichtige Elemente, die keine Sicherheitsschwachstellen aufweisen sollten.

Zielsetzung

Im Rahmen des Sicherheitstests werden nach Absprache sicherheitsrelevante Funktionen des zu testenden Softwareprodukts auf Schwachstellen hin analysiert. Hierbei wird überprüft, ob definierte Schutzziele – wie beispielsweise die Vertraulichkeit, die Verfügbarkeit und die Integrität – gefährdet werden können.

Je nach Softwareprodukt kann das Ziel eines möglichen Angriffs beispielsweise darin bestehen, unautorisierten Zugriff auf bereitgestellte Funktionen oder Daten zu erhalten, eine Rechteausweitung auf dem Zielsystem über das installierte Softwareprodukt durchzuführen, implementierte Schutzmechanismen – wie zum Beispiel eine digitale Rechteverwaltung (Digital Rights Management) – zu umgehen oder geistiges Eigentum (Intellectual Property) bezüglich der Funktionalität des Softwareprodukts zu stehlen.

Durchführung

Die Sicherheitsanalyse von Softwareprodukten findet, sofern möglich, im Labor der SySS innerhalb einer entsprechenden Testumgebung statt. In Abhängigkeit von den verwendeten Technologien des Softwareprodukts, wie beispielsweise Programmiersprachen und Laufzeitumgebungen, sowie von Anforderungen an die Zielplattform, wie etwa Prozessorarchitektur und Betriebssystem, werden hierbei unterschiedliche Werkzeuge und Analysemethoden eingesetzt.

Die Funktionsweise vieler Softwareprodukte ist aufgrund fehlenden Zugangs zum Quelltext (Closed-Source-Produkte) im Gegensatz zu sogenannter Open-Source-Software nicht unmittelbar ersichtlich. Daher werden für die Schwachstellenanalyse von Softwareprodukten, die lediglich in kompilierter Form vorliegen, verschiedene Reverse Code Engineering-Methoden eingesetzt. Hierzu zählen einerseits die statische Codeanalyse von Binärprogrammen unter Verwendung von Softwaretools wie Decompiler (z. B. ILSpy für .NET-Anwendungen oder JD-GUI für Java-Anwendungen) und Disassembler (z. B. IDA Pro oder Hopper für verschiedene ausführbare Dateiformate unterschiedlicher Plattformen) und andererseits die dynamische Codeanalyse unter Verwendung von Softwaretools wie Debuggern (z. B. OllyDbg, x64dbg, dnSpy oder GNU Debugger) und sogenannter Dynamic Binary Instrumentation Tools (z. B. Frida oder DynamoRIO).

Kann der Quelltext für die zu testende Software in Teilen oder vollständig bereitgestellt werden, wird dies für eine Reduzierung des Testaufwands und für eine Verbesserung der Testdurchführung der Sicherheitsanalyse dringend empfohlen.

Mitwirkung des Kunden

Testvorbereitung: Um einen Sicherheitstest einer Softwarekomponente oder eines Softwareprodukts durchführen zu können, muss der SySS die entsprechende Software entweder in lauffähiger Form für die Untersuchung im SySS-Labor oder durch einen entsprechenden Zugang zu einer Testinstanz bereitgestellt werden. Für bestmögliche Testergebnisse sollten keine Einschränkungen bezüglich der Nutzung des Softwareprodukts vorhanden sein. Idealerweise hat die SySS die vollständige Kontrolle über das Testsystem mit der zu untersuchenden Software. Bei Whitebox-Tests von Softwareprodukten sollten der SySS der Quelltext der zu prüfenden Software und Unterlagen wie Handbücher und technische Dokumentationen zur Verfügung gestellt werden.

Ansprechpartner: Die verantwortlichen Ansprechpartner für den Sicherheitstest eines Softwareprodukts sollten innerhalb des Testzeitraums erreichbar sein.

Abhängigkeiten: Organisatorische und technische Abhängigkeiten sollten der SySS mitgeteilt werden. Dies kann im Rahmen des Kick-off-Gesprächs geschehen. Wenn das zu untersuchende Softwareprodukt bzw. die Softwarekomponente beispielsweise nicht isoliert funktionsfähig ist und daher nicht getrennt von anderen Systemen getestet werden kann, muss der SySS mitgeteilt werden, welche Tests an abhängigen Systemen durchgeführt werden können und welche Ansprechpartner in diesem Fall zur Verfügung stehen.

Tipps von Sebastian Schreiber

Schätzen Sie den Zeitbedarf für den Sicherheitstest eines Softwareprodukts großzügig ein! Prüfen Sie, welche Abhängigkeiten, Kommunikationsbeziehungen und Vertrauensstellungen des Softwareprodukts zu anderen Systemen existieren. In der Regel ist ein vollständiger Test dieser Systeme sinnvoll, wenn es sich ohnehin um eine organisatorische und technische Einheit handelt. Wählen Sie anschließend die passenden, flankierenden Prüfmodule für den Test.

2.12 Weitere Module

Zusätzlich zu den bisher vorgestellten klassischen Testmodulen haben sich in den letzten Jahren einige weitere, fokussiertere Prüfszenarien bewährt, die in den folgenden Abschnitten beschrieben werden.

2.12.1 RECON: Inventarisierung der Angriffsfläche

Zusammenfassung

Die SySS identifiziert in Abhängigkeit von der Prüfperspektive die durch einen Dritten sichtbare Angriffsfläche des Kunden. Dies können z. B. die aus dem Internet direkt erreichbaren und anhand öffentlich verfügbarer Informationen aufspürbaren IP-Adressen und IP-Adressbereiche sowie Webapplikationen und -services sein. Auch innerhalb von Firmennetzwerken kann eine Analyse der von einer bestimmten Ausgangsposition aus erreichbaren Netzbereiche wichtige Erkenntnisse bringen. Dieses Testmodul unterstützt Inventarisierungsmaßnahmen und die Auswahl zu testender Systeme für weitere Module (z. B. IP-RANGE, WEBAPP, LAN sowie PIVOT).

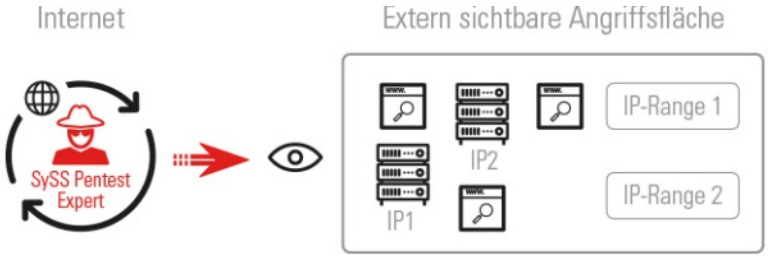

Abbildung 2.30: Modul RECON

Ausgangslage

Insbesondere bei größeren Unternehmen mit diversifizierten IT-Abteilungen kommt es häufig vor, dass ein umfänglicher Gesamtüberblick der eigenen IT-Infrastruktur nicht bis in letzter Konsequenz existiert. Unterschiedliche Bereiche wie z. B. andere Abteilungen oder sonstige Organisationseinheiten, andere Standorte oder auch Tochterfirmen arbeiten häufig ohne Absprache. Dies kann einer der Gründe dafür sein, dass die „Schatten-IT" innerhalb des Unternehmens wächst, was bedeutet, dass nicht erfasste und dadurch auch nicht durch Maßnahmen wie ein automatisiertes Patchmanagement verwaltete Systeme über das Internet erreichbar sind oder im eigenen Netz existieren und ein potenzielles Sicherheitsrisiko darstellen können.

Kleinere Unternehmen dagegen kämpfen eher mit dem Problem, die eigene IT-Verwaltung komplett ausgelagert zu haben. Daher fehlt ihnen der eigene Überblick über möglicherweise existierende Einfallstore.

In solchen Fällen, aber auch dann, wenn ein vorbildlich umgesetztes Asset-Management existiert, kann es interessant sein, ein realistisches Bild über die eigene, aus verschiedenen Perspektiven heraus sichtbare Angriffsfläche zu erhalten.

Zielsetzung

Normalerweise werden Sicherheitstests nur auf IP-Adressen und Dienste durchgeführt, die vom Kunden vorher – auch gerne mit Unterstützung der SySS – ausgewählt und benannt worden sind. Wenn insbesondere bei großen, international verteilten Netzen des Kunden eine solche Auswahl nicht möglich ist oder wenn die Prüfobjekte,

die getestet werden sollten, erst identifiziert werden müssen, kann eine Inventarisierung, wie in diesem Modul vorgesehen, durchgeführt werden.

Das Ziel besteht also darin, beispielsweise eine Übersicht von Systemen (IP-Adressen oder IP-Adressbereichen) oder Webapplikationen und -services zu erstellen, die explizit dem Kunden zuzuordnen und von einer bestimmten Angreiferposition aus sichtbar sind. Typische Durchführungsformen dieses Moduls sind:

- Identifikation der öffentlichen IP-Adressbereiche, die dem Unternehmen zuzuordnen sind
- Ermittlung der aus dem Internet erreichbaren Systeme (Perimeter)
- Identifikation der vom Kunden im Internet veröffentlichten Webapplikationen und -services
- Sammeln von im Internet veröffentlichten E-Mail-Adressen oder Mitarbeiterinformationen des Kunden
- Identifikation aktiver Systeme und deren Erreichbarkeit in ausgewählten internen Netzbereichen

Zusätzlich können eventuelle Fehler in der Zuordnung (z. B. fehlerhafte Regional Internet Registry (RIR)-Einträge) aufgedeckt und gegebenenfalls an dieser Stelle Kandidaten für einen anschließenden Sicherheitstest ausgewählt werden. Letzteres geschieht nach Verifikation durch den Kunden selbst. Dieser hat hierbei auch die Möglichkeit, Fehler in der eigenen Dokumentation zu korrigieren oder Dienstleister (wie z. B. ISPs) dazu anzuweisen. Aufgrund rechtlicher Rahmenbedingungen kann die SySS hier nicht selbstständig agieren, denn es ist in jedem Fall auszuschließen, dass Dritte beeinträchtigt werden.

Durchführung

Je nach Prüfszenario kommen unterschiedliche Vorgehensweisen zum Einsatz. Bei der klassischen Identifikation der externen Angriffsfläche werden auf Basis bereits bekannter Informationen (z. B. Domain- oder Hostnamen, E-Mail-Adressen o. Ä.) öffentliche Quellen wie RIR-Datenbanken (in Europa: RIPE) oder das DNS abgefragt. Auch das Mail-Routing des Kunden und Inhalte von Webseiten, die eventuell Aufschlüsse über Unternehmensverknüpfungen geben, werden hierbei berücksichtigt.

Bei Inventarisierungen innerhalb von Firmennetzwerken scannt die SySS aus vom Kunden zu benennenden Netzbereichen heraus, welche weiteren Netzbereiche erreichbar und welche Systeme darin aktiv sind. Dies kann auch sehr gut mit einer Abschottungsanalyse kombiniert werden (technische Verifikation des Firewallregelwerks). Verschiedene Portscans bilden hierbei den Schwerpunkt der Testaktivitäten.

Mitwirkung des Kunden

Testvorbereitung: Je nach Erwartungshaltung können der SySS bereits bekannte Informationen wie IP-Adressbereiche oder Domain-/Hostnamen mitgeteilt werden. Dies kann die weitere Recherche durchaus beschleunigen. Andernfalls kann jedoch auch die Blackbox-Perspektive eingenommen werden.

Ansprechpartner: Um Kundensysteme von denen Dritter unterscheiden und Ergebnisse mit der kundeneigenen Dokumentation abstimmen zu können, sollte auch bei diesem Modul ein Ansprechpartner erreichbar sein.

Tipps von Sebastian Schreiber

Definieren Sie im Rahmen des Kick-off-Gesprächs Ihre genauen Erwartungen an das Projekt! Standardmäßig wird unser Consultant bei der Ermittlung der externen Angriffsfläche beispielsweise nur nach IP-Adressinformationen und (Sub-)Domainnamen Ausschau halten. Wenn Sie zusätzlich daran interessiert sind, welche E-Mail-Adressen sich z. B. aus dem Internet ermitteln lassen, teilen Sie dies dem Consultant unbedingt vor Projektbeginn mit!

2.12.2 SOCIAL: Social Engineering

Zusammenfassung

Beim Datenklau sind Angreifern alle Mittel recht, um an wertvolle Informationen zu kommen. Angesichts dessen, dass es seit vielen Jahren üblich ist, Hardware, Software, Applikationen oder Netzwerke technisch gegen Angreifer abzusichern, finden Angriffe zunehmend auf zwischenmenschlicher Basis statt. Solche Angriffe werden als „Social Engineering" (SE) bezeichnet. Dieses Modul hat zum Ziel, Ihre Mitarbeiter dabei zu unterstützen, sich besser gegen Manipulationsversuche zu schützen, ihr Bewusstsein dafür zu schärfen, wie dreist und skrupellos Angreifer mitunter vorgehen und keine Hemmungen haben, sich durch Lügen und gefälschte Tatsachen sowohl Zugriff auf Daten als auch Zutritt zum Firmengebäude zu verschaffen. Das Modul hilft Ihnen dabei zu erfassen, ob Ihre bis dato getroffenen Maßnahmen gegen Social Engineering greifen und wo Sie Bedarf zur Nachjustierung haben. Social Engineering ist besonders perfide, weil es mit grundsätzlichen menschlichen Werten und unserer Erziehung zu sozialen, die Anderen achtenden Menschen spielt und diese pervertiert. Daher ist hier ein besonders behutsames Vorgehen vonnöten.

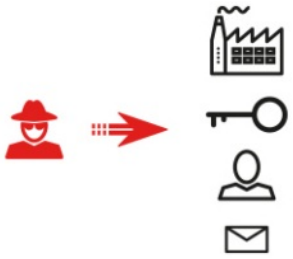

Abbildung 2.31: Modul SOCIAL

Ausgangslage

„Ich habe unerlaubten Zugang zu einigen der weltweit größten Unternehmen erlangt und erfolgreich einige der hartnäckigsten Computersysteme geknackt, die jemals entwickelt worden sind. Dabei habe ich mich technischer und nicht-technischer Mittel bedient, um mir den Quellcode verschiedener Betriebssysteme und Telekommunikationsgeräte zu beschaffen, damit ich ihre Schwachstellen und internen Funktionsweisen studieren konnte." (Kevin Mitnick: Die Kunst der Täuschung)

Wie Kevin Mitnick es treffend beschreibt, verwenden „moderne" Hacker nicht mehr nur ausschließlich technische Mittel, um Zugang zu Unternehmen zu erlangen, die sie angreifen wollen. Immer häufiger kommt es zu sogenannten Social Engineering-Angriffen, bei denen die Mitarbeiter – sprich der Faktor Mensch – eine zentrale Rolle spielen. Derartige Angriffe sind häufig sehr erfolgreich. Um Ihnen auch in dieser Hinsicht eine umfassende Analyse Ihrer Sicherheit liefern zu können, bietet die SySS zusätzlich zu den gängigen, auf Technik basierenden Tests auch Social Engineering als eigenes Modul an. Social Engineering kann entweder unabhängig von anderen Tests oder in Kombination mit anderen Modulen durchgeführt werden.

Zielsetzung

Auch wenn Social Engineering-Angriffe den Menschen und seine Schwachpunkte im Fokus haben, ist es niemals das Ziel eines Social Engineering-Tests, einzelne Mitarbeiter bloßzustellen oder zu diskreditieren. Bei diesen Tests geht es vielmehr darum, Awareness-Maßnahmen zu prüfen, Prozesse sowohl zu analysieren als auch zu verbessern sowie die Sensibilisierung der Mitarbeiter für diese Art von Angriffen zu erhöhen. Social Engineering-Techniken werden auch in Modulen wie Physical Assessment (siehe Abschnitt 2.12.3 auf Seite 72) oder Red

Teaming (siehe Kapitel 3 auf Seite 80) verwendet, wenn dort keine andere Möglichkeit existiert, die vom Kunden gesteckte Zielsetzung zu erreichen.

Dabei verfolgt der Test das Ziel, die folgenden Fragen zu beantworten:

- Wie sensibilisiert sind Ihre Mitarbeiter?
- Greifen Awareness-Maßnahmen?
- Sind Prozesse, die solche Angriffe erschweren oder verhindern sollen, bekannt und werden sie in der Praxis umgesetzt?
- Funktionieren die technischen Vorkehrungen?
- Gibt es Lücken beim Vorgehen im Verdachtsfall?

Durchführung

Grundsätzlich werden Social Engineering-Angriffe ausschließlich von speziell ausgebildeten und sensibilisierten Mitarbeitern der SySS durchgeführt, welche im Hinblick auf rechtliche und ethische Aspekte (siehe Abschnitt 3.3 auf Seite 84) geschult worden sind. Dabei gehen sie mit der Thematik stets sehr verantwortungsvoll und vorsichtig um. Die verwendeten Techniken werden immer auf das jeweilige Modul und die jeweilige Situation angepasst. Prinzipiell kommen die folgenden gewaltfreien Techniken zum Einsatz, mit denen Mitarbeiter bei ihrer normalen Arbeit rechnen müssen:

- **Phishing- und Spear Phishing-Mails:** Mitarbeiter werden per E-Mail kontaktiert und aufgefordert, eine bestimmte Handlung (häufig die Eingabe von Zugangsdaten auf einer Webseite) durchzuführen.
- **Pre-Texting:** Ein Angreifer versucht ein erfundenes Szenario zu schaffen, das eine vorgesehene Handlung legitimiert, zum Beispiel, um unbefugten Zugang zu einem Gebäude oder Gelände zu erlangen oder um einen Mitarbeiter dazu zu bewegen, bestimmte Informationen preiszugeben.
- **Anrufe und SMS:** Außer per E-Mail können Mitarbeiter auch per Telefon oder SMS kontaktiert werden. Hierbei wird auf öffentlich zugängliche Kontaktdaten zurückgegriffen. Ebenso können durch diese Technik Anrufe beantwortet werden, die Mitarbeiter aufgrund gefälschter Angaben in Gesprächen oder E-Mail-Signaturen tätigen.
- **Versand von Briefen:** In seltenen Fällen sieht ein Prozess oder eine Richtlinie vor, dass die Kommunikation über den Postweg stattfinden muss. Aus diesem Grund kann auch das Versenden von Briefen Teil eines solchen Tests sein. In diesem Zusammenhang kann es vorkommen, dass Unterschriften kopiert werden müssen. Dies geschieht jedoch nur nach schriftlicher Genehmigung der betroffenen Person.
- **Personenrecherche unter Zuhilfenahme von öffentlichen Business Community-Profilen:** Um im Rahmen des Pre-Texting ein möglichst authentisches Szenario schaffen zu können, sind Hintergrundinformationen elementar. Hierfür dienen der SySS hauptsächlich öffentlich zugängliche Informationen im Internet. Jegliche Netzwerkplattformen, aber auch Printmedien, Radio oder TV-Reportagen können interessante Fakten über ein Unternehmen oder einzelne Mitarbeiter liefern.
- **Vor-Ort-Techniken:** Falls das gewählte Testmodul vorsieht, dass der Test auch vor Ort stattfindet, können hierbei weitere Techniken wie das Entwenden von unbeaufsichtigten Security-Token, das Kopieren von Mitarbeiterausweisen, Verkleidung und Vorgabe einer falschen Identität oder das Anbringen von Remote-Zugängen im Firmennetzwerk verwendet werden.

Bei der Durchführung der Tests wird stets darauf geachtet, dass die Privatsphäre der Mitarbeiter des Kunden gewahrt wird. Aus diesem Grund benennt die SySS weder in persönlichen Gesprächen noch im Abschlussbericht Namen von betroffenen Mitarbeitern.

Mitwirkung des Kunden

Da es sich beim Modul Social Engineering um ein sehr anspruchsvolles Testmodul handelt, ist eine umfassende Vor- und Nachbereitung des Tests unerlässlich. Bei der Vorbereitung eines solchen Tests werden die Rahmenbedingungen einschließlich der verwendeten Techniken in einem gemeinsamen Workshop definiert. Zusätzlich müssen während der Vorbereitung alle Mitarbeiter, die potenziell Teil eines Social Engineering-Tests sein könnten, darüber informiert werden, dass Tests dieser Art durchgeführt werden, falls SE-Tests nicht sowieso schon Teil der Unternehmenskultur sind. Während des Tests muss jederzeit ein Mitarbeiter als Ansprechpartner für die SySS erreichbar sein, sodass kritische Situationen schnell und unkompliziert entschärft werden können. Der Schutz betroffener Mitarbeiter steht hierbei jederzeit im Vordergrund. Auch der Umgang mit den Testergebnissen ist erfahrungsgemäß bei SE-Modulen anspruchsvoller als bei klassischen technischen Penetrationstests. Dennoch gilt: Selbst wenn ein konkreter Mitarbeiter angegriffen wurde, ist das Problem an dieser Stelle der nicht beachtete/nicht definierte Prozess oder die mangelnde Vorbereitung bzw. Schulung der Mitarbeiter. Wie in der SE-Ethik (siehe Abschnitt 3.3 auf Seite 84) definiert ist, werden im Abschlussbericht weder Namen noch andere Interna genannt.

Tipps von Sebastian Schreiber

Bereiten Sie Ihre Mitarbeiter auf Social Engineering-Tests vor, indem Sie regelmäßig, aber auch mit Angabe von konkreten Zeiträumen Tests ankündigen. Dadurch steigern Sie die Akzeptanz dieser Tests und vermeiden Unzufriedenheit und Ärger. Gleichzeitig schaffen Sie Awareness für echte Angriffe. Prüfen Sie im Vorfeld des Tests, ob die betroffenen Mitarbeiter ausreichend gut informiert sind, um mit Sondersituationen umgehen zu können, und schaffen Sie Prozesse, die Ihre Mitarbeiter im Ernstfall gut unterstützen.

2.12.3 PHYSICAL: Physical Assessment

Zusammenfassung

Nicht nur Webapplikationen, Rechner oder Netzwerke, die aus mehr oder weniger großer Ferne erreicht werden können, sind lohnende Angriffsziele. Es gibt auch eine Reihe von Daten, die gerade dadurch gestohlen werden können, dass ein Angreifer sich Zugang zu Gebäuden verschafft und körperlich anwesend ist. Im Rahmen eines Physical Assessment untersucht die SySS jegliche Möglichkeiten, unbefugt ins Gebäude einzudringen, Zugriff auf Geräte zu nehmen und so Daten abgreifen zu können.

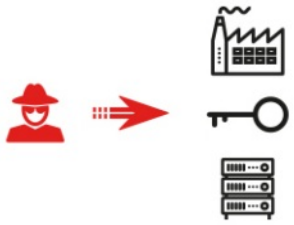

Abbildung 2.32: Modul PHYSICAL

Ausgangslage

Bei jeder Firmenimmobilie besteht das Risiko, dass sich unberechtigte Personen Zugang zum Gelände, zum Gebäude bzw. zu Räumen und Einrichtungen (z. B. die Forschungs- und Entwicklungsbereiche eines Industrieunternehmens) verschaffen. Dadurch können:

- Sachwerte geschädigt oder entwendet werden,
- Personen im Gebäude einer Gefährdung ausgesetzt sein,
- Manipulationen an technischen Systemen vorgenommen werden oder
- erleichterter Zugriff auf Daten durch den direkten Zugang zu Rechnersystemen, Kopierern, mobilen Geräten und nicht zuletzt zur Netzwerkinfrastruktur möglich sein.

Nach Art. 5 Datenschutz-Grundverordnung (DSGVO) müssen Verarbeiter von personenbezogenen Daten technische und organisatorische Maßnahmen zum Schutz der Daten vor Zugriff durch unbefugte Personen getroffen haben.

Zielsetzung

Ziel eines Physical Assessment ist es, die Gebäudesicherheit zu prüfen. Diese Form des Tests soll helfen, Bedrohungen zu erkennen, deren Eintrittswahrscheinlichkeit und Schadenspotenzial zu beurteilen und daraus das Risiko für die Organisation abzuschätzen. Neben den technischen Vorkehrungen werden auch die Zutritts-, Zutrittskontroll- und Überwachungsprozesse getestet. Folgende Fragen werden durch den Test beantwortet: Sind die Sicherheitskonzepte ausreichend? Gibt es Lücken im Sicherheitskonzept? Funktionieren die technischen Vorkehrungen? Werden die vorgesehenen Abläufe gelebt? Gewährleisten die technischen und organisatorischen Maßnahmen einen ausreichenden Schutz personenbezogener Daten?

Durchführung

Grundsätzlich versucht der Consultant, sich auf verschiedene Art und Weise Zutritt zum Gebäude bzw. den vereinbarten Räumlichkeiten zu verschaffen. Hierzu beschafft er sich zunächst unterschiedliche Informationen, die

auch einem Angreifer zur Verfügung stehen (Informationen im Internet, Beobachtungen etc.). Physical Assessment-Tests haben im Wesentlichen den folgenden Ablauf:

- Beschaffung von Informationen aus öffentlichen Quellen
- Beobachtung des Gebäudes, des Geländes und der Umgebung
- Analyse der Zutrittsmöglichkeiten
- Identifikation von Zutrittskontrollen
- Beobachtung der Authentifizierungsmaßnahmen für Mitarbeiter und Gäste
- Analyse der Zutrittskontrollen auf ihre Wirksamkeit
- Suche nach Umgehungsmöglichkeiten der installierten Schutzmaßnahmen

Bei den Tests kommen auch Social Engineering-Methoden zum Einsatz (siehe Abschnitt 2.12.2 auf Seite 69). Beispielsweise könnte ein Consultant versuchen, mittels Tailgating in ein Gebäude zu kommen – also sich schlicht einem Mitarbeiter anzuschließen, der gerade die Tür geöffnet hat. Auch ungeplante Wartungsarbeiten oder – von einer externen Telefonnummer aus mit einem vorgetäuschten internen Namen – ein durch den Angreifer selbst angekündigter Besuch wären möglich. Die Grenze ziehen wir bei der Durchführung der Tests immer spätestens bei solchen Methoden, die darauf abzielen, Mitarbeiter unter besonderen Stress zu setzen, Notsituationen vorzutäuschen oder Ähnliches. Daher setzen wir für diese Tests nur besonders geschulte Consultants ein. Grundlage unserer Arbeit sind in jedem Fall unsere Ethikgrundsätze für Social Engineering, wie sie in Abschnitt 3.3 auf Seite 84 erläutert werden.

Mitwirkung des Kunden

Bei einem aktiven Test von Zutrittskontrollen wird der Versuch unternommen, physische Sicherheitsmaßnahmen zu umgehen, was durchaus als Einbruch gewertet werden kann. Deshalb ist es hier besonders wichtig, dass Sie uns die Umstände, unter denen der Test stattfinden soll, im Detail erläutern. Je nach Sicherung des Gebäudes mag es erforderlich sein, dass unsere Consultants mit einem „Freischein" ausgestattet werden, sodass bei einem erfolglosen oder aufgedeckten Eindringungsversuch beispielsweise nicht gleich die Polizei gerufen wird. Bei geteilten Gebäuden oder in Sondersituationen sind gegebenenfalls zusätzliche Informationen erforderlich. So ist zum Beispiel zu definieren, in welche Bereiche aus Sicherheitsgründen keinesfalls eingedrungen und auch kein Versuch dazu gestartet werden sollte. Wie bei allen Tests mit Social Engineering-Methoden ist im Vorfeld des Tests eine Besprechung notwendig, bei der wir zulässige und auszuschließende Methoden, die vor- oder nachgelagerte Aufklärung der Mitarbeiter und Ähnliches klären. Der Umgang mit den Testergebnissen ist erfahrungsgemäß bei diesem und anderen Social Engineering-Modulen anspruchsvoller als bei klassischen technischen Penetrationstests. Selbst wenn ein konkreter Mitarbeiter angegriffen wurde, ist das Problem an dieser Stelle der nicht beachtete/nicht definierte Prozess oder die mangelnde Vorbereitung bzw. Schulung der Mitarbeiter.

Tipps von Sebastian Schreiber

Bereiten Sie Ihre Mitarbeiter auf Physical Assessment- und andere Social Engineering-Tests vor. Sie vermeiden Unzufriedenheit und Ärger über den Test und schaffen gleichzeitig ein Bewusstsein für echte Angriffe. Niemand möchte bei einem Test durchfallen. Ein aufmerksamer Mitarbeiter ist immer hilfreich, wenn es darum geht, Schindluder und den damit einhergehenden Schaden zu verhindern! Prüfen Sie im Vorfeld des Tests, ob die betroffenen Mitarbeiter ausreichend gut darüber informiert sind, wie sie mit Sondersituationen umgehen müssen. Stellen Sie sicher, dass es eine Verfahrensanweisung oder einen Prozess zum Umgang mit unbefugten Personen auf dem Betriebsgelände gibt.

2.12.4 PIVOT: Kompromittierte Demilitarized Zone (DMZ)

Zusammenfassung

Dieses Modul geht von dem Szenario aus, dass es einem Angreifer gelingt, mindestens ein System in der demilitarisierten Zone (Demilitarized Zone; DMZ) – zum Beispiel einen Webserver – zu übernehmen. Die SySS wird beispielsweise durch Ausnutzung von Vertrauensstellungen oder weiteren Schwachstellen versuchen, weiter in die DMZ oder die internen Netzsegmente einzudringen oder aufzuzeigen, welche Informationen ein Angreifer in der DMZ erbeuten kann.

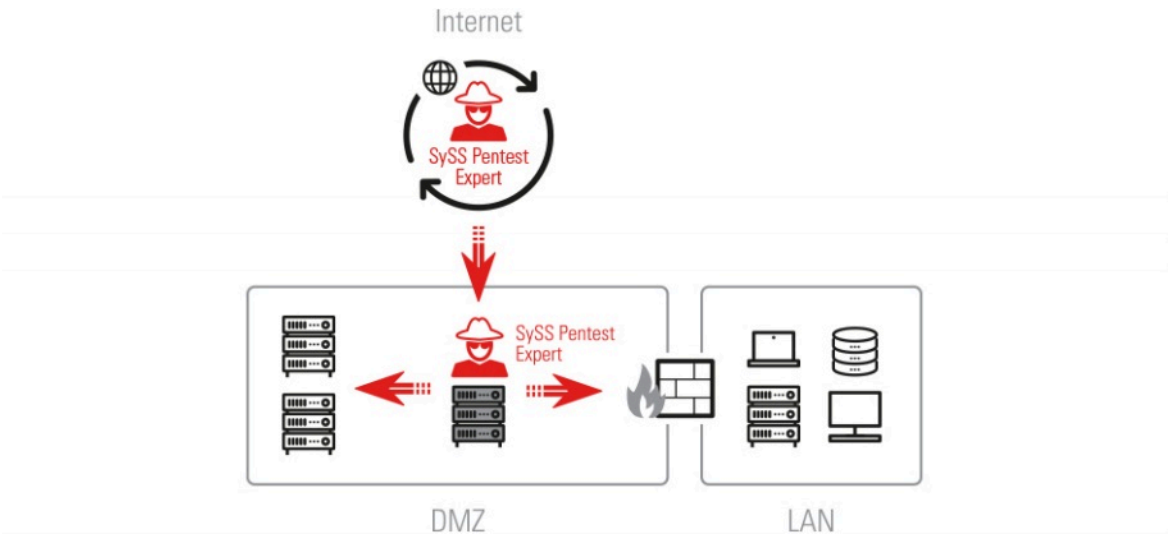

Abbildung 2.33: Modul PIVOT

Ausgangslage

Häufig besteht das Ziel von Angreifern darin, durch Ausnutzung von Schwachstellen wie SQL Injection Informationen aus an Webapplikationen gekoppelten Datenbankmanagementsystemen zu kopieren. Hierbei interessieren sich die Angreifer in vielen Fällen für Daten wie Passwörter, E-Mail-Adressen oder in der Datenbank gespeicherte Bezahlinformationen, um diese dann gewinnbringend zu veräußern.

Verfolgen Angreifer jedoch die Absicht, gezielt einem bestimmten Unternehmen Schaden zuzufügen, so nutzen sie derartige Schwachstellen lediglich als Einstiegspunkt für weiterführende Angriffsaktivitäten und die betroffenen Server als sogenannte Pivot-Systeme. Ihre eigentliche Motivation besteht in der Regel darin, in das interne Unternehmensnetz einzudringen, um kritische Daten des Unternehmens, beispielsweise geistiges Eigentum

(Intellectual Property), zu veruntreuen bzw. zu stehlen. Im schlimmsten Fall ist ein solcher Angriff Teil eines Advanced Persistent Threat (APT), bei dem weitere Angriffstechniken wie Social Engineering- oder Phishing-Methoden zum Einsatz kommen.

Zielsetzung

Im Rahmen dieses Moduls wird die SySS analysieren, welche Möglichkeiten sich für Angreifer ergeben, die durch einen erfolgreichen Angriff einen Server in der DMZ kompromittieren konnten. Dieses System wird anschließend als Pivot genutzt, um tiefergehende Angriffe darüber weiterzuleiten. Hierdurch können unter anderem die Vertrauensstellungen zwischen diesem und weiteren Servern ausgenutzt werden, um Angriffe gegen Systeme durchzuführen, die nicht direkt aus dem Internet erreichbar sind. Ziel ist es, tiefer in die DMZ oder interne Netzbereiche einzudringen.

Durchführung

Da sich vor einem Projekt nicht abschätzen lässt, ob es der SySS beispielsweise im Rahmen einer Webapplikationsanalyse (siehe Modul WEBAPP in Abschnitt 2.2 auf Seite 23) aus eigener Kraft gelingen wird, in die DMZ des Kunden einzudringen, wird der SySS in der Regel der Zugang zu einem Server in der DMZ eingerichtet. Dies macht das Modul PIVOT zudem unabhängig von anderen Testmodulen. Der Ablauf entspricht grob dem folgenden Muster:

- Hochladen der erforderlichen Werkzeuge (z. B. einer Proxy-/VPN-fähigen Payload) auf das Pivot-System
- Analyse des Pivot-Systems (z. B. Berechtigungen, lokale Credentials, Netzwerkschnittstellen, offene Verbindungen usw.)
- Pivoting (häufig auch „Island Hopping“ genannt), was die Prüfung der Erreichbarkeit weiterer Systeme innerhalb der DMZ sowie in internen Netzbereichen als auch die Analyse weiterer Systeme umfasst

Zusätzlich können bei Bedarf auch die folgenden Prüfungen stattfinden:

- Gezielter Versuch, bestimmte interne Systeme anzugreifen (z. B. Datei- oder Mailserver)
- Durchlässigkeitsprüfung für dedizierte Netzbereiche (technische Verifikation des Firewallregelwerks)

Mitwirkung des Kunden

Testvorbereitung: Für den Test muss der SySS auf jeden Fall ein Zugang zu einem System in der DMZ eingerichtet werden. Üblicherweise handelt es sich bei diesem System um einen Web- oder Applikationsserver. Auch Datenbankserver, die häufig in separaten demilitarisierten Zonen untergebracht sind, können hierzu herangezogen werden. Um den produktiven Betrieb nicht zu beeinträchtigen, wird idealerweise ein technisch identischer Klon eines solchen Systems verwendet. Wichtig ist, dass das System eine mit der Produktivinstanz möglichst identische Konfiguration aufweist. Dadurch stehen der SySS sämtliche Angriffsmöglichkeiten bereit, die auch einem realen Angreifer zur Verfügung stehen könnten.

Der Zugang wird idealerweise per SSH eingerichtet. Der SySS sollten die gleichen Berechtigungen eingeräumt werden, über die beispielsweise auch das Dienstkonto eines Web- oder Applikationsservers verfügt. Der Hintergrund hierzu ist, dass ein Angreifer sehr wahrscheinlich mit diesen Rechten ausgestattet ist, wenn er erfolgreich eine Schwachstelle in einer Webapplikation ausnutzen konnte.

Alternativ kann auch ein spezieller VPN-Zugang (End-to-End) eingerichtet und dann auf Protokolle wie RDP oder VNC zurückgegriffen werden.

Ansprechpartner: In den vorangegangenen Modulbeschreibungen wurden bereits einige Gründe genannt, weshalb (technische) Ansprechpartner sowie deren Erreichbarkeit während des Testzeitraums sehr wichtig sind. Diese gelten insbesondere auch für dieses Modul. Ansprechpartner können unter anderem eventuelle Rückfragen während des Tests beantworten, die beispielsweise zur Verifizierung von Sicherheitsschwächen dienen, oder über mögliche Probleme wie eine eingeschränkte oder unterbrochene Erreichbarkeit des Pivot-Systems oder anderer Systeme informiert werden und diese folglich zeitnah beheben.

Besonders der zweitgenannte Punkt – eine durchgehende, ununterbrochene Erreichbarkeit des Pivot-Systems – ist im Rahmen dieses Moduls von äußerster Wichtigkeit, da sämtliche Tests über dieses System hinweg erfolgen.

Tipp von Sebastian Schreiber

Wenn Sie für dieses Testmodul einen „künstlichen Zugang" auf eines Ihrer DMZ-Systeme einrichten, achten Sie unbedingt darauf, dass z. B. per Access Control List sichergestellt ist, dass dieser Zugang ausschließlich von den SySS-IP-Adressen aus genutzt werden kann!

2.12.5 TERMSERV: Sicherheit von Remote Access-Lösungen

Zusammenfassung

Im Rahmen dieses Moduls werden Remote Access-Lösungen auf mögliche Schwachstellen hin untersucht. Sowohl die Authentisierung als auch das Berechtigungskonzept stehen hierbei im Fokus. Zum Beispiel kann im Zuge einer „Ausbruchsanalyse" geprüft werden, ob ein Zugriff auf weitere als die vorgesehenen Applikationen möglich ist oder ob ausgehend vom Terminalserver durch verschiedene Rechteeskalationen weitere Ressourcen im Firmennetzwerk angegriffen werden können.

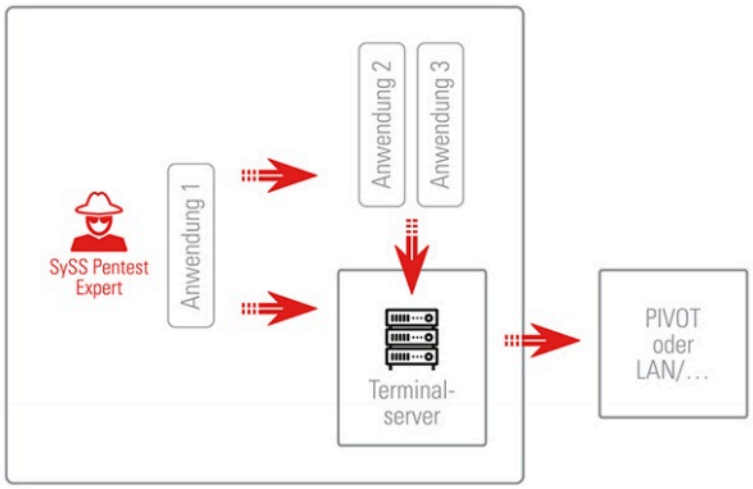

Abbildung 2.34: Modul TERMSERV

Ausgangslage

Viele Unternehmen bieten ihren Mitarbeitern oder auch externen Dienstleistern einen eingeschränkten Fernzugriff auf ausgewählte, interne Ressourcen an. Gängige technische Lösungen sind hier Citrix XenApp, Microsoft Remote Desktop Gateway oder VMware Horizon. Da diese Technologien somit eine aus dem Internet erreichbare

Schnittstelle des eigenen Unternehmensnetzwerks darstellen, sollte deren Sicherheitsniveau eine hohe Bedeutung beigemessen werden. Ausgehend von verschiedenen Prüfperspektiven eruiert die SySS im Rahmen dieses Moduls, ob eventuelle Schwachstellen in der Umsetzung der Remote Access-Lösung existieren.

Zielsetzung

Im Rahmen dieses Testmoduls werden Möglichkeiten identifiziert, über die sich ein Angreifer die Remote Access-Lösung zunutze machen kann, um unautorisiert auf kritische Unternehmensressourcen zuzugreifen. Hierbei wird beispielsweise der Versuch unternommen, die Authentisierung zu umgehen, definierte Nutzerrichtlinien auszuhebeln, aus dem Kontext einzelner Anwendungen auszubrechen oder eine sonstige Rechteeskalation zu erreichen. Sofern gewünscht, wird die SySS auch versuchen, weitere vom Terminalserver aus erreichbare Netzwerkressourcen zu identifizieren und anschließend zu kompromittieren. Das Ziel des Testmoduls besteht darin, potenzielle und konkrete Verwundbarkeiten zu identifizieren und Maßnahmen zu empfehlen, deren Umsetzung zu einer optimalen Härtung der Remote Access-Lösung führt. In manchen Fällen jedoch soll lediglich festgestellt werde, ob eine einzeln bereitgestellte Applikation den Zugriff auf das zugrunde liegende System ermöglicht. Hier ist es wichtig, die für Sie relevante Fragestellung konkret zu definieren.

Durchführung

Je nach zu prüfender Technologie und einzunehmender Prüfperspektive wird die SySS unter anderem die folgenden Aspekte berücksichtigen:

- Angriffe auf Systemebene (siehe Modul IP-RANGE in Abschnitt 2.1 auf Seite 21)
- Angriffe gegen die Authentisierung (1-Faktor, 2-Faktor etc.)
- Ausbruch aus Einzelanwendungen
- Rechteeskalation auf dem Terminalserver bzw. innerhalb der Virtual Desktop-Umgebung
- Netzbasierte Angriffe gegen weitere Systeme

Hierzu macht sich die SySS beispielsweise Ausbruchstechniken über Systemdialoge, nicht gesperrte Tastaturkürzel oder Bordmittel sowie, falls möglich, selbst geschriebene Angriffsskripte zunutze, um idealerweise Zugriff auf eine Kommandozeile wie die CMD oder die PowerShell zu erhalten. Falls dies gelingt, werden weitere Testaktivitäten begünstigt, wie z. B. Passwort-Rate-Angriffe gegen andere Benutzerkonten.

Werden auf dem lokalen System über Local Privilege Escalation-Techniken zudem Administrator- oder Systemrechte erlangt, können weitere interessante Informationen aus dem Speicher, dem Dateisystem oder der Registry extrahiert werden. Auch netzbasierte Angriffe sind mit dieser Rechtestellung effizienter durchführbar.

Die SySS prüft zudem, ob es möglich ist, einen alternativen Kommunikationskanal – wie z. B. eine Reverse Shell zu einem SySS-Root-Server im Internet – aufzubauen, oder welche weiteren Möglichkeiten es gibt, interne Unternehmensdaten über die Remote Access-Lösung zu exfiltrieren (z. B. Copy-and-Paste per Zwischenablage etc.).

Mitwirkung des Kunden

Testvorbereitung: Vor Testbeginn wird die SySS im KICKOFF mit dem Kunden die gewünschten Angriffsszenarien sowie den Testumfang besprechen und Zugangsdaten für die Remote Access-Lösung anfordern.

Ansprechpartner: Auch bei diesem Testmodul ist die telefonische Erreichbarkeit des Ansprechpartners während der Testzeiten wichtig, damit beispielsweise ein gesperrter Zugang zeitnah wieder entsperrt werden kann. Einige

Remote Access-Lösungen erlauben den Zugriff auf einen Terminalserver, auf dem sich mehrere Benutzer gleichzeitig aufhalten. Sollten wider Erwarten durch die Testaktivitäten Verfügbarkeitsbeeinträchtigungen entstehen, wird der Ansprechpartner unmittelbar informiert und kann für Abhilfe sorgen.

Tipps von Sebastian Schreiber

Unterschätzen Sie den zeitlichen Aufwand für die Vorbereitungen bei diesem Testmodul nicht! Die Beantragung eines Fernzugriffs kann je nach Unternehmensgröße durchaus mehrere Tage in Anspruch nehmen. Zudem muss oftmals noch ein zweiter Authentisierungsfaktor (z. B. Hardware-Token) per Post zur Verfügung gestellt werden.

2.12.6 REVIEW: Sicherheitsbewertung von Konzepten, Prozessen, Dokumenten und organisatorischen Vorgaben

Zusammenfassung

Die SySS bewertet vorhandene Sicherheitskonzepte und -architekturen, um bereits frühzeitig in einer Projektphase auf bisher unberücksichtigte Risiken aufmerksam zu machen. Zudem können im Zuge dieses Testmoduls sicherheitsrelevante interne Prozesse und Dokumentationen sowie organisatorische Vorgaben kritisch beleuchtet werden.

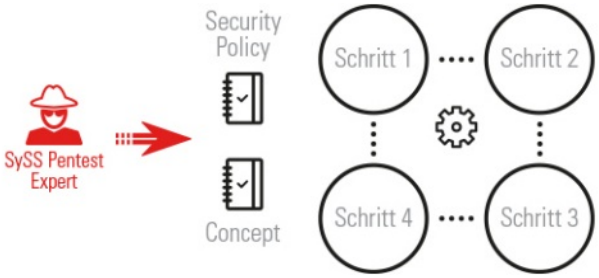

Abbildung 2.35: Modul REVIEW

Ausgangslage

IT-Sicherheit kann nur bei der Betrachtung als Prozess[4], nicht jedoch durch rein punktuelle Maßnahmen gewährleistet werden. Daher bietet die SySS auch Prüfungen der organisatorischen Vorgaben an, die die IT-Sicherheit definieren. Dies können unter anderem Sicherheitsrichtlinien und -handbücher, aber auch Regelsets innerhalb der IT-Infrastruktur sein. Das zu prüfende Material wird unseren Consultants zur Verfügung gestellt, die sich anschließend damit vertraut machen und Verbesserungen empfehlen. Auf Wunsch und wo sinnvoll, können die Reviews durch Gespräche oder Workshops flankiert oder abgeschlossen werden. Dieses Modul deckt die nicht technischen Untersuchungen im Rahmen von Sicherheitstests ab. Um den Status der tatsächlichen Umsetzung von Vorgaben bzw. Sicherheitsrichtlinien zu kontrollieren, empfehlen wir, eine Untersuchung über das jeweils passende Modul aus diesem Whitepaper durchführen zu lassen.

Dieses Testmodul ist auch im Rahmen von Entwicklungsprojekten neuer Anwendungen (Webapplikationen und -services, Mobile Apps etc.) sinnvoll, um die ausgearbeiteten Sicherheitskonzepte und -architekturen zu evaluieren. Auf diese Weise kann bereits frühzeitig auf eventuelle Sicherheitsrisiken aufmerksam gemacht werden, die bisher keine Berücksichtigung fanden.

[4] Schneier, Mai 2000, `https://www.schneier.com/crypto-gram-0005.html`

Zielsetzung

Die Zielsetzung des Projekts variiert in Abhängigkeit von dem zu bewertenden Gegenstand. Grundsätzlich wird die SySS jedoch versuchen, Verbesserungspotenzial zur Erhöhung des zu erzielenden Sicherheitsniveaus aufzuzeigen. Wie auch bei den technischen Sicherheitsanalysen wird hierbei die Sicht- und Denkweise eines Angreifers eingenommen, um mögliche Lücken zu identifizieren.

Durchführung

Auch die Durchführung eines Reviews hängt stark vom Projektcharakter ab. Geht es beispielsweise darum, Sicherheitsrichtlinien zu bewerten, so reicht oftmals eine gründliche Dokumentensichtung und -evaluation aus. Für Evaluationen von Architekturen oder fertigen Konzepten hingegen eignet sich ein Vor-Ort-Workshop hervorragend, um den Teilnehmern – zumeist Softwarearchitekten und Entwickler – zunächst die Gelegenheit zu geben, das zu Bewertende vorzustellen und im Anschluss in Form einer Diskussionsrunde gemeinsam eventuelles Gefahrenpotenzial zu identifizieren. Bewertungen sicherheitsrelevanter Prozesse und Abläufe wiederum werden idealerweise in Form von Interviews mit den jeweils Verantwortlichen durchgeführt.

Mitwirkung des Kunden

Testvorbereitung: Je nach Form des Reviews sind vorab entsprechende Zuständigkeiten zu klären, um ideale Interviewpartner oder Workshopteilnehmer zu benennen. Die Planung eines Workshops sollte frühzeitig angestoßen werden, da es hier oftmals eine Schnittmenge in zahlreichen Kalendern zu finden gilt. Bei einer Dokumentensichtung sollten die jeweiligen Dokumente der SySS in der zu bewertenden Version rechtzeitig vor Projektbeginn zur Verfügung gestellt werden.

Ansprechpartner: Idealerweise sollte für die Planung des Reviews ein zentraler Ansprechpartner benannt werden, der für Rückfragen, eventuell noch einzuholende Informationen oder die Terminkoordination zur Verfügung steht.

> **Tipp von Sebastian Schreiber**
>
> Kombinieren Sie die frühzeitige, konzeptionelle Sicherheitsbetrachtung mit einer direkt an die Umsetzung des Projekts anschließenden technischen Sicherheitsanalyse. Auf diese Weise decken Sie sowohl grundlegende Sicherheitsrisiken im Konzept als auch klassische Schwachstellen in dessen Umsetzung auf.

2.12.7 Spezieller, individueller Testfokus

Sollte Ihr Anliegen nicht von den in diesem Whitepaper vorgestellten Testmodulen abgedeckt werden, zögern Sie nicht, uns anzurufen und es uns im Detail darzulegen. Mit unseren Pentest-Architekten werden wir in fast allen Fällen eine Lösung für Sie finden, da wir über langjährige Erfahrung und Expertise in nahezu allen Beratungsbereichen der IT-Sicherheit verfügen. Gerne führen wir auf Wunsch auch einen gemeinsamen Workshop mit Ihnen durch, um ein mögliches Prüfprojekt zu konzipieren.

3 Red Teaming

Red Teaming ist eine Prüf- und Schulungsmethode, die ursprünglich aus dem Militärischen kommt und ihren Einzug in den ersten Jahren der 2010er in die Unternehmenswelt fand. Bei dieser Methode wird gezielt ein Team von Angreifern („Red Team") eingesetzt, um zu testen, wie es um die Abwehr der Firma steht, und um das entsprechende Team von Mitarbeitern („Blue Team") zu trainieren.

Die Mitarbeiter wissen nur, dass sie durchgehend angegriffen werden können. Dadurch erhöht sich die Sensibilität spürbar und sie erkennen durch die permanente Suche nach dem Angreifer-Team (Red Team) mehr tatsächliche Angriffe.

Abbildung 3.1: RED TEAMING

3.1 Ablauf Red Teaming

Die Zielsetzung eines klassischen Penetrationstests besteht darin, in einem klar definierten engen Rahmen alle Schwachstellen zu finden, welche das Zielobjekt aufweist, diese zu dokumentieren und Empfehlungen zu deren Behebung auszusprechen.

Ein Red Teaming Assessment jedoch verfolgt das Ziel, unter Zuhilfenahme von frei wählbaren Angriffsvektoren einen breitflächigen Angriff zu fahren. Dabei ist der Rahmen sehr weit gefasst und der Angreifer hat einen hohen kreativen Freiraum. Er nutzt nicht nur die technischen Möglichkeiten aus, die ihm zur Verfügung stehen, sondern er lotet mitunter auch aus, ob er durch Social Engineering an sensible Daten kommen und Wege finden kann, in die Firma einzudringen. Ein eingesetztes Blue Team hat die Aufgabe, die Angriffe des Red Teams aufzuspüren und zu verhindern. Dabei werden das Blue Team und dessen Abwehrmaßnahmen getestet und weiter ausgebaut. Auch wird diese Prüfmethode verwendet, um zu testen, ob es einem Angreifer in einem zeitlich gesetzten Rahmen gelingen kann, ein Firmennetzwerk aus einer externen Perspektive zu kompromittieren.

Ausgangslage

In den meisten kritischen Bereichen der Unternehmenswelt gibt es Übungen, um den Ernstfall zu proben. Im Bereich der IT-Sicherheit gab es dies bisher nur punktuell und nicht als ganzheitliches Szenario.

Red Teaming ermöglicht die komplette Simulation eines echten Angriffs. Dabei wird getestet, ob die Mitarbeiter sowohl technisch als auch in puncto Awareness ausreichend geschult sind und ob die definierten Notfallprozesse funktionieren.

In diesem simulierten Ansatz wird die interne IT Security bei der Detektierung von gezielten Angriffen (APT) weitergebildet. Auch in Firmen, die kein dediziertes IT-Sicherheitspersonal haben, kann ein Red Teaming Assessment sinnvoll sein, da in einem solchen Test die technischen Abwehrmaßnahmen auf ihre Effektivität hin geprüft werden können.

Red Teaming als Testmethode wird nach dem TIBER-EU- bzw. TIBER-DE-Framework, das im Mai 2018 bzw. Juli 2020 veröffentlicht wurde, für Banken vorgeschrieben. Demnach müssen in dieser Branche Red Teaming-Tests stattfinden.

Zielsetzung

Red Teaming hat den primären Fokus darauf, das Blue Team zu schulen und in einem spielerischen Ansatz weiterzubilden. Diese Art des Tests kann aber auch für andere Ziele verwendet werden, wie die nachfolgenden Beispiele zeigen:

- Überprüfung der ganzheitlichen Unternehmenssicherheit anhand eines breit aufgestellten Angriffsportfolios
- Simulation eines echten Angriffs, um die Effektivität der aktuellen technischen Schutzmaßnahmen zu überprüfen, Mitarbeiter und deren Handlungen zu testen und zu evaluieren, welche Prozesse es gibt und ob sie eingehalten werden
- Schulung des Blue Teams

Durchführung

Die Durchführung eines Red Teaming Assessment wird individuell an bestehende Kundenwünsche angepasst. Grob durchläuft die Prüfung die nachfolgenden elf Phasen. Im initialen Workshop können Schwerpunkte festgelegt werden.

Kick-off-Workshop

Im Rahmen eines Workshops wird gemeinsam mit dem Kunden der Umfang des Red Teaming-Projekts evaluiert. Anhand der folgenden Aspekte kann ein erster Eindruck über den Projektverlauf gewonnen werden, wobei individuelle Wünsche und Fragen berücksichtigt werden.

Analyse öffentlich zugänglicher Daten

In einer ersten Phase folgt eine Analyse von öffentlich zugänglichen Daten jeglicher Art zur Identifikation von möglichen Zielen für spätere Angriffe aus dem Internet und mit Social Engineering-Methoden.

Sammeln von Informationen

In dieser Phase soll ein möglichst realistisches Bild über die sichtbare Angriffsfläche von aus dem Internet erreichbaren Systemen und Diensten gezeichnet werden. Dazu wird versucht, möglichst viele Details über die eingesetzten Dienste- und Betriebssystemversionen in Erfahrung zu bringen.

Persistieren im Unternehmensnetzwerk

Nachdem die SySS sich einen temporären Zugang zum internen Netzwerk des Unternehmens verschafft hat, wird der Versuch unternommen, eine dauerhafte Verbindung sicherzustellen. Hierbei wird noch stärker als in den vorangegangenen Phasen darauf geachtet, so minimalinvasiv wie möglich vorzugehen, um von Erkennungs- und Abwehrsystemen unerkannt zu bleiben.

Social Engineering

Sollte es durch die vorangegangenen technischen Phasen nicht möglich gewesen sein, Zugang zum internen Unternehmensnetzwerk zu erlangen, werden Social Engineering-Methoden angewandt, um in den Besitz von Zugangsdaten zu gelangen. Aufgrund der ethischen Herausforderungen von Social Engineering und der gleichzeitig hohen Erfolgsquote hat es sich bewährt, dass der Kunde einen Mitarbeiter benennt, der das Verhalten eines Opfers simuliert und zum Beispiel auf den Link in einer Phishing-Mail klickt.

Kompromittierung von Systemen und Diensten

Abhängig davon, ob die initiale Kompromittierung über Server- oder Clientsysteme erfolgte, soll versucht werden, weitere Systeme im internen Netzwerk zu kompromittieren, sodass mit den gewonnenen Daten und Erkenntnissen im weiteren Testverlauf die Rechte innerhalb des internen Netzwerks erweitert werden können.

Ausweitung von Rechten

Die in den vorangegangenen Phasen gesammelten Daten und Informationen ermöglichen es einem Angreifer typischerweise, sich mit den eingeschränkten Rechten eines Standardbenutzers im Netzwerk zu bewegen. Außerdem verfügt ein Angreifer vielleicht bezüglich einzelner Systeme oder Dienste über weiterreichende Rechte. In dieser Phase wird zunächst angestrebt, die lokale Rechtestellung auszuweiten. Anschließend folgt die Analyse, welche weiteren Angriffsmöglichkeiten sich unter Nutzung eines Standardbenutzerkontos im Netz ergeben.

Erreichen von definierten Zielen

Diese Phase beschreibt die Zielerreichung des im Workshop vereinbarten Projektziels. Sofern es sich um Daten handelt, werden diese identifiziert und mit möglichst minimalinvasiven Mitteln extrahiert. Dabei wird ebenfalls analysiert, ob das Monitoring Anomalien im Netzwerkverkehr aufspürt.

Auslösen von Schutzsystemen und Prozessen

Wurde das vereinbarte Projektziel erreicht und ist der Angriff noch nicht aufgefallen, so werden weitere Wege ermittelt, mit denen das Ziel ebenfalls erreicht werden kann. Hierbei wird in jedem Durchgang die Aggressivität der Angriffe stetig gesteigert, um festzustellen, ab welcher Stufe interne Schutzsysteme und Prozesse greifen. Insbesondere wird hierbei geprüft, ob es gelingt, den Angriff erfolgreich und nachhaltig abzuwehren.

Bereinigung der Advanced Persistent Threat-Simulation

In dieser Phase soll die Wirksamkeit der Abwehrmaßnahmen und des Notfallkonzepts erprobt werden. Durch den erfolgten Zugriff aus den vorangegangenen Phasen ist es dem Angreifer gelungen, diverse Berechtigungen für verschiedene Systeme zu erlangen. Ziel auf Seiten des Kunden ist es, den Angreifer möglichst restlos aus dem Unternehmensnetz zu entfernen und alle Hintertüren zu schließen, die bereits geöffnet wurden. Begleitend zu den Maßnahmen des Blue Teams wird der Angriff auf Seiten des Red Teams weitergeführt. Hierbei werden Techniken eingesetzt, die schwierig zu detektieren sind und einen nachhaltigen und sicheren Zugriff auf das Netzwerk ermöglichen.

Dokumentation

In dieser Phase werden die Ergebnisse des Tests chronologisch in einer schriftlichen Dokumentation zusammengefasst. Die Dokumentation entspricht dem SySS-Standard und wird zweistufig qualitätsgesichert. Außerdem werden die Ergebnisse in einer Abschlusspräsentation, angepasst auf die jeweilige Zielgruppe, vorgestellt und erläutert.

Mitwirkung des Kunden

Red Teaming erfordert eine intensive Betreuung auf Seiten des Kunden. Aus der langjährigen Erfahrung bei der Durchführung von Red Teaming Assessments hat sich gezeigt, dass Statustelefonate mindestens alle zwei Wochen erheblich zum Erfolg des Tests beitragen. Auch sollte die SySS bereits in die Vorbereitung für den Test miteinbezogen werden.

Hier sollten gemeinsam Ziele definiert und kritische Systeme identifiziert werden. Aufgrund der Tatsache, dass Red Teaming ein vollständiger Blackbox-Test ist, kann die SySS erst nach einem initialen Scan erkennen, welche Art von Systemen in einem Netzwerksegment sind. Allerdings ist es möglich, dass es bei veralteten Systemen bereits durch einen solchen Scan zu Ausfällen kommt. Aus diesem Grund empfiehlt es sich bei kritischen Infrastrukturen, mit einem Whitelisting-Ansatz zu arbeiten. Hier erhält die SySS im Vorfeld eine Liste mit Subnetzen, die unkritisch sind.

Sollte die SySS im Rahmen eines Assessment Zugriff auf andere Netzwerkbereiche haben, muss das weitere Vorgehen detailliert abgestimmt werden. Während der Durchführung wird im Detail besprochen, welche Informationen an das Blue Team weitergegeben werden. In einzelnen Testphasen sollte eine Informationsweitergabe gänzlich vermieden werden, damit überprüft werden kann, ob Angriffe entdeckt werden oder nicht. Im Fall einer sehr fortgeschrittenen Kompromittierung kann es in der Phase „Bereinigung der Advanced Persistent Threat-Simulation“ sinnvoll sein, gezielt Informationen weiterzugeben.

3.2 Purple Teaming

Wie beschrieben, eignen sich Red Teaming-Tests insbesondere dafür, zu überprüfen, wie gut die eigene IT-Sicherheit auch bei der Erkennung und Abwehr von Angriffen aufgestellt ist.

Ist das Blue Team gerade erst im Aufbau begriffen, empfiehlt sich der Ansatz des „Purple Teaming“. Bei diesem Ansatz gibt es einen direkten Austausch zwischen dem Blue Team und dem Red Team. Das Blue Team wird zudem anfangs unterstützt. Sollte diese Unterstützung nicht notwendig sein, können die Schritte 1-3 des unten beschriebenen Vorgehens übersprungen werden.

Für eine optimale Umsetzung eines Purple Team Assessment empfiehlt die SySS das folgende Vorgehen:

Schritt 1

Unsere Mitarbeiter für Digitale Forensik und Incident Response besprechen im Vorfeld eines Red Teaming-Tests mit Ihnen Ihre Incident Detection-Methoden. In einem Workshop können dann bereits Verbesserungen erarbeitet werden.

Schritt 2

In einem zweiten Schritt empfehlen wir, die umgesetzten Änderungen bzw. die Ist-Situation zu testen. Dies kann beispielsweise in einem Rollenspiel geschehen. Hierbei werden Prozesse anhand von Beispielszenarien durchgespielt, wobei sich bereits wichtige Erkenntnisse ergeben. Die Szenarien werden auf Basis der Ergebnisse des initialen Workshops erarbeitet. Alternativ stellt das Red Team eine Beschreibung unterschiedlicher Szenarien bereit, aus welchen ausgewählt werden kann.

Schritt 3

Nachdem die Prozesse bereits ausgereifter sind, empfehlen wir, diese praktisch im produktiven Umfeld zu testen. Hierfür wird Ihr Blue Team weiter von unseren Mitarbeitern der Digitalen Forensik und Incident Response unterstützt, während das Red Team im Vorfeld abgesprochene Szenarien durchführt. Nach jedem Szenario wird im Detail durchgesprochen, was das Blue Team erkannt und welche Angriffsvektoren das Red Team durchgeführt hat. Dabei entwickelt Ihr Blue Team immer bessere Routinen, um Angriffe schnell zu erkennen und diese abzuwehren.

Schritt 4

Die Betreuung Ihres Blue Teams wird reduziert und die Angriffsszenarien des Red Teams werden komplexer. So wird Ihr Blue Team in die Selbstständigkeit überführt. Nach diesem Schritt empfiehlt es sich, ein separates Red Team Assessment durchzuführen, um die Umsetzung der Incident Detection- und Incident Response-Maßnahmen vollständig verdeckt zu testen.

Durch Netzwerkmonitoring bzw. andere Arten von Monitoring während eines Purple Teaming Assessment werden Daten gewonnen, die im Nachgang ausgewertet und zur Optimierung Ihrer Erkennungsmethoden (SIEM, Logauswertung etc.) verwendet werden können. Die Leistungen unseres Red Teams und unserer DFIR-Abteilung ergänzen sich an dieser Stelle, damit Sie einerseits Ihre Schwachstellen identifizieren und andererseits möglichst schnell reagieren und Ihre eigene Abwehr darauf vorbereiten können.

Idealerweise finden Purple Team Assessments häufig statt und bedienen unterschiedliche Szenarien, damit Ihre IT-Sicherheit sich kontinuierlich weiterentwickeln kann und bei einem echten Vorfall routiniert reagiert. Damit wird dann auch die Sicherheit nachhaltig verbessert und die Dauer eines Incident wird verkürzt.

3.3 Ethikgrundsätze für Social Engineering

Die SySS führt Social Engineering (SE)-Projekte durch. Diese werden nur von speziell ausgebildeten und sensibilisierten Mitarbeitern durchgeführt, die auch im Hinblick auf rechtliche und ethische Aspekte zuvor geschult worden sind.

Uns ist bewusst, dass ein SE-Test gezielt Schwächen von Menschen ausnutzt. Ein SE-Test wird nur dann durchgeführt, wenn a) keine andere Möglichkeit existiert, den Test auf andere Weise durchzuführen, und b) wenn SE als Mittel angemessen erscheint.

SySS-Mitarbeiter gehen dabei sehr verantwortungsvoll, vorsichtig und umsichtig vor. Social Engineering-Techniken dienen der Überprüfung von Awareness-Maßnahmen oder der Zielerreichung eines Red Teaming Assessment. Bei Social Engineering-Projekten beachten unsere Consultants die von uns aufgestellten zehn Regeln:

1. Die Privatsphäre des Mitarbeiters des Kunden wird gewahrt.
2. Tests müssen angekündigt werden oder sind bereits Teil der Unternehmenskultur.

3. Die SySS nennt keine Namen von Mitarbeitern, welche im Rahmen des Tests auffällig geworden sind.
4. Es werden ausschließlich Techniken eingesetzt, mit denen die entsprechenden Mitarbeiter bei ihrer normalen Arbeit rechnen müssen.
5. Die Kommunikation mit Mitarbeitern wird auf ein Minimum beschränkt. Eine passive Vorgehensweise wird in jedem Fall bevorzugt.
6. Jedes Vorgehen wird aus den beiden ethischen Perspektiven „Utilitarismus" und „Deontologie"[1] beurteilt. Nach Abwägen dieser Perspektiven wird ein Vorgehen gewählt oder verworfen.
7. Alle eingesetzten Social Engineering-Techniken sind gewaltfrei.
8. Es dürfen nur Geräte entwendet werden, die zu rein geschäftlichen Zwecken bestimmt sind.
9. Die Tests werden zum Nutzen des Unternehmens durchgeführt. Das Ziel der Tests ist die Aufdeckung von Schwachstellen in den Prozessen und/oder der unzureichenden Wirksamkeit von Sensibilisierungsmaßnahmen. Dabei geht es nie um den Nachweis von Unzulänglichkeiten eines einzelnen Mitarbeiters.
10. Das Vorgehen ist nicht destruktiv, nur in Ausnahmefällen wird z. B. auf Lockpicking zurückgegriffen.

Im Rahmen von Social Engineering Assessments kommen z. B. die nachfolgenden Techniken zum Einsatz:

- Phishing- und Spear Phishing-Mails
- Pre-Texting
- Anrufe und SMS
- Tailgating
- Kopieren von Mitarbeiterausweisen
- Verkleidung und Vorgabe einer falschen Identität
- Versand von Briefen
- Kopieren von Unterschriften nach schriftlicher Genehmigung der betroffenen Person
- Personenrecherche unter Zuhilfenahme von Social Community-Profilen
- Entwenden von unbeaufsichtigten Security-Token/Computersystemen

Welche Techniken im Rahmen eines Projekts verwendet werden, wird im Vorfeld in einem Workshop abgestimmt. Ebenso wird dort auf die jeweiligen Vor- und Nachteile hingewiesen.

[1] Utilitarismus (Nutzen/Vorteil): Eine Handlung ist genau dann moralisch richtig, wenn der Gesamtnutzen, also die Summe des Wohlergehens aller Betroffenen, maximiert wird. Deontologie: Schützt das Individuum mehr als es die Gemeinschaft schützt. Ist die Aktion richtig oder falsch für den Einzelnen? Zum Beispiel könnte während eines SE-Tests zu einem Mitarbeiter des zu testenden Unternehmens gesagt werden: „Ihr Kind hatte einen schweren Unfall". Der Utilitarismus betrachtet den Inhalt wie folgt: Falls dadurch eine Sicherheitsmaßnahme umgangen werden konnte (Wachposten verlässt seinen Platz), hilft diese Erkenntnis dem Unternehmen -> Maßnahmen müssen verbessert werden; nach Deontologie wäre ein solches Vorgehen moralisch absolut falsch.

4 Über die SySS

4.1 Firmengeschichte

Die SySS GmbH wurde 1998 von Diplom-Informatiker Sebastian Schreiber gegründet, um hochwertige Sicherheitstests anzubieten.

Die SySS hat fünf Geschäftsbereiche: Neben Penetrations- und Red Teaming-Tests bieten wir Digitale Forensik/Incident Response, Live-Hacking und Schulungen an.

Der Hauptsitz der SySS GmbH befindet sich in Tübingen, mit Niederlassungen sind wir in Frankfurt/M. und München vertreten. Des Weiteren hat die SySS GmbH eine Tochter in Österreich, die SySS Cyber Security GmbH.

Kunden der SySS sind Unternehmen aller Branchen und Größen. Hierzu zählen sowohl zahlreiche mittelständische Unternehmen als auch einheimische DAX-Konzerne.

Die SySS hält Fachvorträge auf nationalen und internationalen Kongressen sowohl im Inland als auch im europäischen und außereuropäischen Ausland.

Mitarbeiter der SySS sind immer wieder als Experten in diversen Print-, Funk- und Onlinemedien präsent, darunter Der Spiegel, Die Zeit, Financial Times Deutschland, Stuttgarter Zeitung, Süddeutsche Zeitung, ARD und ZDF, Südwestrundfunk, Hessischer Rundfunk, RTL, Pro7 und CHIP TV.

4.2 Grundlegende Ethik für Penetrationstester

Basierend auf schon existierenden Kodizes und über Jahre gesammelten Erfahrungswerten hat die SySS den ersten Vorstoß unternommen, eine grundlegende Ethik für Penetrationstester zu erstellen. Diese Ethik wurde in der Ausgabe 04/2009 in der IT-Zeitschrift „Datenschutz und Datensicherheit" (DuD) zum ersten Mal veröffentlicht und spiegelt die Einstellung und die Grundlage des Arbeitens bei der SySS wider. Auf der Basis dieser Ethik gestalten wir unsere Arbeit:

- **Unabhängigkeit:** Penetrationstests durchführende Firmen testen nur in solchen Unternehmen, in denen sie weder bei der Konzipierung der IT-Umgebung noch der Einrichtung von Sicherheitsmaßnahmen beteiligt gewesen sind und an die sie auch keine eigene Software verkauft haben oder verkaufen wollen. Nur so kann sichergestellt werden, dass die Testergebnisse objektiv sind.
- **Vertraulichkeit:** Sowohl die Identität der beauftragenden Firma als auch jegliche Einblicke in interne Netzwerke, Strukturen sowie in jegliche Daten – auch wenn diese dem Penetrationstester zur Verfügung gestellt werden – sind absolut vertraulich zu behandeln.
- **Provisionsverbot:** Die Annahme von Provisionen oder vergleichbaren Vorteilen ist untersagt.
- **Vorsicht:** Der Kunde ist über mögliche Risiken in Kenntnis zu setzen, die bei den Prüfungen entstehen können.
- **Professionalität und Qualitätsmanagement:** Die Arbeit hat professionell zu erfolgen und ist einem Qualitätsmanagement zu unterziehen. Dabei leistet der Penetrationstester seine Arbeit nach bestem handwerklichen Wissen und ethischem Gewissen.
- **Verbindlichkeit:** Vertraglich zugesicherte und in Beratungsgesprächen mündlich getroffene Zusagen sind von den Mitarbeitern der Penetrationstests durchführenden Firma verbindlich einzuhalten.

- **Objektivität, Neutralität und Transparenz:** Schlussfolgerungen müssen objektiv sein und sind nachvollziehbar darzustellen.
- **Interessenskonflikte:** Interessenskonflikte zwischen Penetrationstestern und Kunden sind zu vermeiden und gegebenenfalls anzuzeigen und auszuräumen.
- **Striktes Legalitätsprinzip:** Die Gesetze der von Penetrationstests betroffenen Länder sind strikt einzuhalten, auch wenn Teilergebnisse eines Penetrationstests selbst einen Interessenkonflikt mit der vorgefundenen Gesetzgebung darstellen könnten. So kann die Aufdeckung von Schwachstellen in bestimmten Fällen Verstöße gegen bestehendes Recht begünstigen. Penetrationstester sind daher verpflichtet, sich mit der jeweiligen Gesetzeslage vertraut zu machen und sorgfältig darauf zu achten, dass ihre Arbeit innerhalb der vorgegebenen Gesetzesgrenzen abläuft.
- **Respekt vor Menschen:** Social Engineering-Projekte sind Angriffe gegen das Verhalten von Menschen – diese werden, sofern sie überhaupt realisiert werden, ausschließlich angekündigt durchgeführt.
- **Korrektes Zitieren:** Wird fremdes Wissen bei der Arbeit herangezogen und verwertet, so sind die Quellen bzw. Urheber korrekt auszuweisen.

5 Ausgewählte Veröffentlichungen der SySS (seit 2012)

Die SySS veröffentlicht regelmäßig Artikel in Fachzeitschriften, auf Onlineplattformen oder im Rahmen von Kongressen. Im Folgenden finden Sie eine Auswahl. Weitere Informationen über unsere Publikationen finden Sie auf: https://www.syss.de/pentest-blog/category/know-how/ und https://www.syss.de/pentest-blog/pentest-library/.

Abrell, Moritz: Die Kommunikation geht neue Wege – Ende-zu-Ende-Verschlüsselung erhält eine neue Bedeutung. SySS-Publikation, Juni 2020: https://www.syss.de/fileadmin/dokumente/Publikationen/2020/2020_06_16_Die_Kommunikation_geht_neue_Wege.pdf (auch in englischer Sprache verfügbar)

Krauß, Thomas: Herausforderungen für die IT-Sicherheit bei der Elektromobilität und autonomem Fahren. In: Informatik Aktuell 8/2019: https://www.informatik-aktuell.de/betrieb/sicherheit/herausforderungen-fuer-die-it-sicherheit-bei-der-elektromobilitaet-und-autonomem-fahren.html

Lutz, Torsten: Mehr Sicherheit in SAP Town. In: Protektor und WiK 6/2019: https://www.syss.de/fileadmin/dokumente/Publikationen/2019/2019_06_14_SAP_Lutz.pdf

Bechler, Moritz: LDAP Swiss Army Knife – A directory server for LDAP client analysis and exploitation. SySS-Publikation, Mai 2019: https://www.syss.de/fileadmin/user_upload/2019_05_LDAP_Swiss_Army_Knife.pdf

Schreiber, Sebastian: Internet der Dinge – Smart genug? In: Protektor und WiK 3/2019: https://www.syss.de/fileadmin/dokumente/Publikationen/2019/2019_01_22_IoT_Schreiber.pdf

Buchegger, Philipp: Hacking Fingerprint Readers without Making a Mess – using tin foil instead of human skin. SySS-Publikation, November 2018: https://www.syss.de/fileadmin/dokumente/Publikationen/2018/Hacking_Fingerprint_Readers_without_Making_a_Mess.pdf

Vollmer, Dr. Adrian: Antivirus Evasion with Metasploit Web Delivery – Leveraging PowerShell to Execute Arbitrary Shellcode. SySS-Publikation, Juli 2018: https://www.syss.de/fileadmin/dokumente/Publikationen/2018/Antivirus_Evasion_Metasploit.pdf

Deeg, Matthias/Klostermeier, Gerhard: Rikki Don't Lose that Bluetooth Device – Exploiting the Obvious: Bluetooth Trust Relationships. SySS-Publikation, Juli 2018: https://www.syss.de/fileadmin/dokumente/Publikationen/2018/Rikki_Dont_Lose_That_Bluetooth_Device.pdf

Deeg, Matthias/Klostermeier, Gerhard: Case Study: Security of Modern Bluetooth Keyboards – SySS IT Security Research Project. SySS-Publikation, Juni 2018: https://www.syss.de/fileadmin/dokumente/Publikationen/2018/Security_of_Modern_Bluetooth_Keyboards.pdf

Vollmer, Dr. Adrian: Angriffe auf RDP – Wie man RDP-Sitzungen abhört. SySS-Publikation, November 2017: https://www.syss.de/fileadmin/dokumente/Publikationen/2017/2017_11_07_Vollmer_Angriffe_auf_RDP.pdf

Schreiber, Sebastian/Straßheim, Alexander: IoT-Penetrationstest. In: DuD Datenschutz & Datensicherheit 10/2017: https://www.syss.de/fileadmin/dokumente/Publikationen/2017/2017_09_07_Strassheim_Schreiber_IoT-Penetrationstest__DuD.pdf

Schreiber, Sebastian: Penetrationstests in der IT – Angreifbare Schwachstellen finden und schließen. In: unternehmermagazin 3/4, 2017: https://www.syss.de/fileadmin/dokumente/Publikationen/2017/2017_09_14_UMAG-03-04-2017-TT-24-25-Schreiber.pdf

Scholl, Edgar/Schreiber, Sebastian: Leider gehackt. In: impulse 07+08, 2017: https://www.syss.de/fileadmin/dokumente/Publikationen/2017/2017_07_01_Leider_gehackt.pdf

Deeg, Matthias/Klostermeier, Gerhard: Of Mice and Keyboards – On the Security of Modern Wireless Desktop Sets. SySS-Publikation, Juni 2017: https://www.syss.de/fileadmin/dokumente/Publikationen/2017/2017_06_01_of-mice-and-keyboards_paper.pdf

Nerz, Sebastian: Alltag und Arbeitsfelder der IT-Forensik. In: IT-Sicherheit 2/2017: https://www.syss.de/fileadmin/dokumente/Publikationen/2017/2017_05_Alltag_und_Arbeitsfelder_der_IT-Forensik_IT-SICHERHEIT_2_2017.pdf

Vollmer, Dr. Adrian: Attacking RDP – How to Eavesdrop on Poorly Secured RDP Connections. SySS-Publikation, März 2017: https://www.syss.de/fileadmin/dokumente/Publikationen/2017/2017_03_13_Attacking_RDP.pdf

Grasmück, Dr. Oliver/Mangold, Marcel: Safety first! In: smart engineering 1/2017: https://www.syss.de/fileadmin/dokumente/Publikationen/2017/2017_02_17_Safety_First_smart_engineering_1_17.pdf

Schreiber, Sebastian: Schwachstellen vor dem Hacker finden. In: Energie & Management 7/2016: https://www.syss.de/fileadmin/dokumente/Publikationen/2016/2016_07_04_Schwachstellen_vor_dem_Hacker_finden.pdf

Schreiber, Sebastian: Penetrationstests für Stadtwerke – Den Hacker nicht ins Netz lassen. In: ew Spezial 2/2016: https://www.syss.de/fileadmin/dokumente/Publikationen/2016/2016_05_23_Hacker_nicht_ins_Netz_lassen_ew_Spezial_02-2016.pdf

Stühler, Roman: Schadcode auf Smartphones – wie sicher sind Android-Geräte vor Angriffen? SySS-Publikation, März 2016: https://www.syss.de/fileadmin/dokumente/Publikationen/2016/2016-03_03_Schadcode_auf_Smartphones.pdf

Deeg, Matthias: Verantwortungsvoller Umgang mit Sicherheitsschwachstellen. SySS-Publikation, Dezember 2015: https://www.syss.de/fileadmin/dokumente/Publikationen/2015/2015_12_02_Verantwortungsvoller_Umgang.pdf

Deeg, Matthias: Deactivating Endpoint Protection Software in an Unauthorized Manner. Conference Paper, DeepSec, Wien, 19.11.2015: https://www.syss.de/fileadmin/dokumente/Publikationen/2015/Deactivating_Endpoint_Protection_Software_in_an_Unauthorized_Manner_-_DeepSec_2015.pdf

Deeg, Matthias: Privilege Escalation via Client Management Software. Conference Paper, BSidesVienna 0x7DF, Wien, 21.11.2015: https://www.syss.de/fileadmin/dokumente/Publikationen/2015/Privilege_Escalation_via_Client_Management_Software_-_BSidesVienna_2015.pdf

Borrmann, Micha: Attacking all your IPv4 devices at home from the Internet via Dual-Stack Lite. Hacktivity, Budapest, 10.10.2015: https://hacktivity.com/en/downloads/archives/397/

Steglich, Finn/Straßheim, Alexander: Digitaler Kassenraub. Austricksen von In-App-Bezahlfunktionen. In: iX 7/2015,
S. 52-55: http://www.heise.de/ix/inhalt/2015/7/52/

Nerz, Sebastian: IT-Sicherheit und die EU-Datenschutznovelle: Worauf deutsche Unternehmen sich einstellen müssen. SySS-Publikation, Mai 2015: https://www.syss.de/fileadmin/dokumente/Publikationen/2015/IT-Sicherheit_und_die_EU-Datenschutznovelle.pdf

Deeg, Matthias: Rechteausweitung mittels Client-Management-Software. SySS-Publikation, April 2015: https://www.syss.de/fileadmin/dokumente/Publikationen/2015/Rechteausweitung_mittels_Client-Management-Software.pdf (auch in englischer Sprache verfügbar)

Deeg, Matthias/Nerz, Sebastian/Sauder, Daniel: Ausgetrickst – Warum Schadprogramme trotz aktueller Antivirensoftware zum Zuge kommen. SySS-Publikation, August 2014: https://www.syss.de/fileadmin/dokumente/Publikationen/2014/Anit_Virus_Evasion_dt.pdf (auch in englischer Sprache verfügbar)

Borrmann, Micha: Thunderbird gibt falschem Absender das Echtheits-Siegel. In: c't 17/2013, S. 16: http://www.heise.de/security/meldung/Thunderbird-gibt-falschem-Absender-das-Echtheits-Siegel-2044405.html

Borrmann, Micha: Microsofts Hintertür – Zweifelhafte Updates gefährden SSL-Verschlüsselung. In: c't 17/2013, S. 16: http://www.heise.de/ct/ausgabe/2013-17-Zweifelhafte-Updates-gefaehrden-SSL-Verschluesselung-2317589.html

Schreiber, Sebastian: Komplexität bildet das Hauptproblem. In: isreport 10/2012

Schreiber, Sebastian: Wir bemerken eine zunehmende Professionalisierung der Angreifer. In: Bankmagazin 10/2012

Schreiber, Sebastian: Windows 8 – Der richtige Weg. In: CHIP 8/2012

Heitmann, Kirsten/Schreiber, Sebastian: Sicherheit bei Web-Shops. In: Ecommerce Vision 5/2012: http://www.ecommerce-vision.de, 16. Mai 2012

THE PENTEST EXPERTS

SySS GmbH Tübingen Germany +49 (0)7071 - 40 78 56-0 info@syss.de

WWW.SYSS.DE