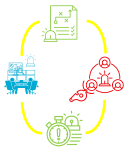
Produkt-Katalog Cyfidelity Security Services



Incident Response Framework

Unser Incident Response Framework besteht aus vier zentralen Bausteinen, die Unternehmen dabei unterstützen, auf Cyberangriffe vorbereitet zu sein, angemessen zu reagieren und ihre Sicherheitslage kontinuierlich zu verbessern.

1.1 Notfallplanung

Die Notfallplanung ist ein essenzieller Bestandteil der Sicherheitsstrategie eines Unternehmens. Sie umfasst die Erstellung strukturierter Maßnahmen, um auf Cyberangriffe vorbereitet zu sein und im Ernstfall schnell und effektiv reagieren zu können.

Modul 1: Einführung in die Notfallplanung für Cyberangriffe

- Aktuelle Bedrohungsszenarien: Überblick über relevante Cyberangriffe wie Ransomware, Advanced Persistent Threats (APTs) und Zero-Day-Exploits sowie deren potenzielle Auswirkungen.
- Branchenspezifische Risiken: Besonderheiten verschiedener Sektoren, z. B. Angriffe auf IT/OT-Schnittstellen in der produzierenden Industrie oder Gefahren für Lieferketten.
- Best Practices & Compliance: Einführung in regulatorische Vorgaben wie NIS-2, ISO 27001 oder den BSI IT-Grundschutz und deren Bedeutung für das Unternehmen.
- Kosten und Folgen eines Cyberangriffs: Bewertung der wirtschaftlichen, rechtlichen und reputationsbezogenen Auswirkungen von Sicherheitsvorfällen.
- Erwartete Herausforderungen: Typische Schwierigkeiten in der Notfallplanung und Strategien zu deren Bewältigung.
- Dauer: 90 Minuten
- Ergebnisdokumente: Handlungsempfehlungen zu allen Modulinhalten.

Modul 2: Vorgehensmodell zur Erstellung einer Notfallplanung

- Grundlagen der Notfallplanung: Definition von Schutzzielen, Identifikation kritischer Geschäftsprozesse und Bedrohungsszenarien.
- Struktur eines Notfallplans: Eskalationsstufen, technische Maßnahmen zur Eindämmung von Angriffen sowie Wiederherstellungsstrategien.

- Lessons Learned: Methoden zur kontinuierlichen Verbesserung des Incident-Response-Managements.
- Dauer: 90 Minuten
- Ergebnisdokumente: Strukturierte Notfallplanung mit Abgleich vorhandener Dokumentation.

Modul 3: Aufbau eines Krisenstabs & effektive Notfallkommunikation

- Zusammensetzung eines Krisenstabs: Klärung von Rollen, Verantwortlichkeiten und Entscheidungsstrukturen.
- Aktivierung und Arbeitsweise: Prozesse zur Einberufung des Krisenstabs und strukturierte Entscheidungswege unter Zeitdruck.
- Kommunikation im Krisenfall: Umgang mit internen und externen Stakeholdern, inklusive Strategien zur Vermeidung von Fake News und Social-Media-Risiken.
- Praxisübung: Simulation eines Krisenstabs-Meetings anhand eines realistischen Ransomware-Szenarios.
- Dauer: 90 Minuten
- Ergebnisdokumente: Strukturierte Krisenstabsplanung mit Abgleich vorhandener Dokumentation.

Modul 4: Entwicklung von Notfallmaßnahmen für kritische Systeme

- Identifikation geschäftskritischer Systeme: Definition von Mission-Critical- und Customer-Facing-Systemen.
- Technische Schutzmaßnahmen: Netzwerksegmentierung, Backup-Sicherheitskonzepte (Air-Gapped-Backups, Immutable Storage), Logging und Monitoring.
- Dauer: 90 Minuten
- Ergebnisdokumente: Strukturierte Notfallplanung mit Maßnahmenempfehlungen.

Modul 5: Entwicklung individueller Notfallpläne

- Erstellung eines unternehmensspezifischen Notfallplans: Integration der erarbeiteten Inhalte aus den vorherigen Modulen.
- Definition klarer Wiederherstellungsmaßnahmen für kritische Systeme und Entwicklung spezifischer Playbooks für verschiedene Cyberangriffsszenarien (z. B. Ransomware, Zero-Day-Exploits, Insider-Bedrohungen).
- Erstellung einer strategischen Roadmap: Umsetzungsplanung für organisatorische, technische und personelle Sicherheitsverbesserungen.
- Dauer: 90 Minuten
- Ergebnisdokumente: Detaillierte Notfallplanstruktur mit spezifischen Maßnahmen.

1.2 Notfallübung

Die Cyfidelity bietet eine strategische Notfallübung an. Für die Notfallübung werden praxiserprobte, aber auf die Bedürfnisse des Kunden zugeschnittene Szenarien genutzt, welche einerseits die aktuellen Cyberbedrohungen und Cyberrisiken aufzeigen und andererseits auch Bedrohungen nachstellen, die Infrastruktur und Dienstleister in den Fokus nehmen. Mit allen Szenarien werden die Fähigkeiten im Krisenmanagement des Kunden beleuchtet. Darüber hinaus sollen Optimierungspotenziale für den Krisenmanagement-Prozess im Bereich des Cyber- und IT-Sicherheitsmanagements aufgezeigt werden.

Die Notfallübung kann je nach Komplexität und Übungsgrundlage einen Tag dauern. Das Szenario besteht aus einer spezifischen Ausgangslage und mehreren lageverändernden Eingriffen, die von den Teilnehmern in kleinen Gruppen und unter Zeitdruck analysiert, diskutiert und technische sowie organisatorische Lösungsansätze erarbeitet werden.

Vorgehen

- Zieldefinition und Ausprägung eines oder mehrerer für den Kunden spezifizierten Szenarien, welche die Aufgaben und Fragen der jeweiligen Fachbereiche inkludiert.
- Durchführung der Notfallübung unter der Moderation der Cyfidelity
- Dokumentation und konkrete Lösungs- und Optimierungsvorschläge.

In der Phase der Ausprägung der Szenarien wird ausgeplant, wie das einzelne Szenario einen technischen und organisatorischen Erkenntnisgewinn herbeiführt, damit die Widerstandsfähigkeit des Kunden nachhaltig erhöht werden kann. Um ein Kunden-spezifisches Szenario zu entwickeln, werden Workshops mit ausgewählten Mitarbeitern durchgeführt. Diese Personen bringen ihre spezifischen Fähigkeiten und ihr Wissen aus den jeweiligen Organisationseinheiten mit ein, um ein realistisches Szenario zu entwickeln.

Die Workshop Teilnehmer zur Szenario-Entwicklung werden nicht aktiv an der Notfallübung beteiligt, sie werden bei Bedarf als Beobachter integriert und sie unterstützen bei der Bewertung der Ergebnisse.

Die aktiven Teilnehmer der Notfallübung hingegen dürfen zu keiner Zeit vor der Übung das Szenario kennen, damit eine realitätsnahe Krisen-Simulation entstehen kann.

Projektphasen

Phase 1: Zieldefinition

In der ersten Phase des Projektes wird mit dem Management und weiteren zuständigen Stellen des Kunden die Ziele der Notfallübung detailliert und die vorgeschlagenen Szenarien gegebenenfalls angepasst und weiterentwickelt.

Dabei werden insbesondere auch organisatorische Abläufe und Abhängigkeiten des Kunden betrachtet, die Inhalt der Notfallübung sein sollen.

Phase 2: Überarbeitung der Szenarien

Auf Grundlage der Ergebnisse der Phase 1 werden die vorgeschlagenen Szenarien überarbeitet oder gegebenenfalls durch andere Szenarien ersetzt.

Phase 3: Moderation und Durchführen der Notfall-Übung

Die Ergebnisse einer Notfallübung hängen stark von der Motivation der Teilnehmenden und deren organisatorischen Vorwissen und deren Kreativität ab, daher sollten die Teams mit relevanten Teilnehmern besetzt werden und die Teams sollten nicht zu groß werden. Eine ideale Größe sind Gruppen von 3-4 Teilnehmern und nicht mehr als 2-3 Gruppen.

Ausprägung der Notfallübung

Die Notfallübung kann als gekennzeichnetes Planspiel ausgeprägt werden. Das bedeutet alle vorgesehenen Teilnehmenden werden im Vorfeld über die Durchführung der Notfallübung informiert und ihre Anwesenheit oder Erreichbarkeit wird gewährleistet.

Alternativ kann die Notfallübung auch unangekündigt aber als Planspiel ausgeprägt werden. Das bedeutet, dass nicht alle vorgesehenen Teilnehmenden im Vorfeld informiert sind und ihre Anwesenheit und die Möglichkeit ihrer Teilnahme nicht gewährleistet ist und sich somit eine neue Situation ergeben kann. Über die Ausprägung der Notfallübung muss in der Phase 1 Ziel Definition entschieden werden.

1.3 Incident-Response-Preparation

- Optimierung der organisatorischen Abläufe der Notfallplanung
- Analyse er individuellen Notfallplanung des Kunden
- Definition klarer Wiederherstellungsmaßnahmen für kritische Systeme.
- Entwicklung spezifischer Playbooks für typische Cyberangriffsszenarien:
    - Playbook für Ransomware-Angriffe.
    - Playbook für Zero-Day-Exploits.
    - Playbook für Insider-Bedrohungen.

weitere Playbooks werden nach der spezifischen Situation des Kunden erstellt

- Erstellung einer strategischen Roadmap für weitere Maßnahmen
- Umsetzungsschritte für Verbesserungen in Organisation, Technik und Schulung.
- Vorbereitung auf eine spätere Notfallübung zur Praxisvalidierung.

Ergebnisdokumente: Optimierung der Notfallplanung mit wesentlichen Inhalten / Vorschlag für eine Krisenstabsstruktur

1.4 Incident Response & Digitale Forensik

Sofortige Reaktion und Analyse von Sicherheitsvorfällen

Unsere **Incident Response & Digitale Forensik (DFIR)-Dienstleistungen** bieten Unternehmen eine schnelle, strukturierte und effektive Unterstützung bei Cyberangriffen. Unser Ziel ist es, Sicherheitsvorfälle professionell zu analysieren, digitale Spuren gerichtsfest zu sichern und Schäden für Ihr Unternehmen zu minimieren, um eine schnelle Wiederherstellung des Geschäftsbetriebs zu ermöglichen.

- **Incident Response: Sofortige Reaktion & Bedrohungsanalyse**
  - **24/7-Einsatzbereitschaft:** Unsere Incident-Response-Experten sind rund um die Uhr verfügbar und reagieren sofort auf kritische Sicherheitsvorfälle.
  - **Flexibler Einsatz – Vor Ort & Remote:** Abhängig von der Bedrohungslage agieren unsere Spezialisten entweder direkt bei Ihnen vor Ort oder unterstützen Sie remote.
  - **Post-Incident-Analysen:** Nach einem Vorfall erstellen wir eine detaillierte Analyse, die Angriffsmuster, Schwachstellen und genutzte Vektoren aufzeigt. Daraus leiten wir gezielte Maßnahmen zur Verbesserung Ihrer Sicherheitslage ab.
- **Digitale Forensik & Beweissicherung**
  - **Gerichtsverwertbare Spurensicherung:** Anwendung internationaler Standards (z. B. **ISO/IEC 27037**) zur rechtssicheren Dokumentation digitaler Beweismittel. Jeder Schritt wird lückenlos protokolliert.
  - **Forensische Tiefenanalyse:** Identifikation und Nachverfolgung von Cyberangriffen bis auf tiefste Systemebene, inklusive der Analyse versteckter Spuren.
  - **Reverse Engineering von Schadsoftware:** Untersuchung und Dekonstruktion bösartiger Software, um Angriffstechniken zu verstehen und gezielte Verteidigungsmaßnahmen abzuleiten.
- **Langfristige Sicherheitsstrategie & Prävention**

Neben der reaktiven Incident Response bieten wir proaktive Maßnahmen, um Ihr Unternehmen langfristig widerstandsfähig gegen Cyberangriffe zu machen:

- **DFIR-Rahmenverträge:** Maßgeschneiderte Vereinbarungen mit definierten Reaktionszeiten, priorisiertem Zugang zu unseren Experten und regelmäßigen Sicherheitsprüfungen.
- **Cyber Threat Intelligence (CTI):** Überwachung gestohlener Daten im Darknet, Erkennung von Credential Leaks und gezieltes Threat Hunting zur Identifikation potenzieller Bedrohungen.
- **Workshops & Schulungen:** Individuelle Trainingsprogramme zur Verbesserung der Incident-Response-Fähigkeiten Ihrer internen Teams mit praxisnahen Übungen.

1.5 Cyber Threat Intelligence (CTI)

Bedrohungserkennung und Prävention

Cyber Threat Intelligence (CTI) beschreibt den systematischen Prozess der Sammlung, Analyse und Nutzung von Informationen über aktuelle und potenzielle Cyberbedrohungen. Ziel ist es, Unternehmen frühzeitig vor Angriffen zu warnen, neue Entwicklungen im Cybercrime-Umfeld zu überwachen und effektive Gegenmaßnahmen zu ermöglichen. Dabei liegt der Fokus nicht nur auf bereits bekannten Bedrohungen, sondern auch auf sich entwickelnden Angriffsmethoden, die von Cyberkriminellen genutzt werden. Durch kontinuierliche Überwachung und Analyse der Bedrohungslandschaft kann ein Unternehmen proaktiv handeln, bevor ein Sicherheitsvorfall eintritt.

Abgrenzung Threat Hunting:
TH beschreibt die proaktive Suche nach bisher unbekannten Bedrohungen im internen Netzwerk eines Unternehmens. Hierfür wird der Zugriff auf diverse Systeme wie beispielsweise das SOC benötigt. TI kann als Zulieferer für Angriffsmuster- und Methoden gesehen werden, während TH die Verwertung bzw Anwendung der bereit gestellten Informationen bezeichnet.

Cyfidelitys CTI umfasst ein breites Spektrum an Maßnahmen, die darauf ausgerichtet sind, kompromittierte Zugangsdaten, neue Entwicklungen sowie aufkommende Angriffsmuster relevanter Bedrohungsakteure frühzeitig zu erkennen. Diese Maßnahmen tragen dazu bei, das Risikomanagement zu verbessern und die Sicherheitsstrategie eines Unternehmens auf eine fundierte Basis zu stellen. Im Rahmen eines CTI-Assessments werden unter anderem die folgenden Aspekte untersucht:

Monitoring Credential Leaks

Zugangsdaten sind ein bevorzugtes Ziel von Cyberkriminellen. Bei einem Credential Leak gelangen Benutzername-Passwort-Kombinationen in die Hände von Angreifern, die diese zur unbefugten Anmeldung in Unternehmensnetzwerken nutzen können. Wir überwachen für eine definierte Unternehmensdomain verschiedene Quellen wie Datenlecks, Ransomware-Leaks und sogenannte Stealer-Logs – also Datensätze, die durch Malware von infizierten Systemen gestohlen wurden. Durch eine frühzeitige Identifikation solcher Leaks können betroffene Zugangsdaten gesperrt und die Nutzer informiert werden, bevor ein Angreifer diese aktiv nutzt.

Monitoring Domains – Schutz vor Phishing-Angriffen

Phishing-Angriffe basieren oft auf täuschend echt wirkenden Domains, die den Eindruck erwecken, eine legitime Unternehmenswebsite zu sein. Cyberkriminelle nutzen dabei Techniken wie homoglyphische Angriffe (z. B. "oediv.de" statt "oediv.services"), alternative Schreibweisen oder andere Top-Level-Domains, um Nutzer zu täuschen. Wir überwachen neu registrierte Domains und analysieren deren Potenzial für missbräuchliche Zwecke, sodass Unternehmen frühzeitig auf potenzielle Bedrohungen reagieren und entsprechende Schutzmaßnahmen einleiten können.

Bereitstellung von Tactics, Techniques und Procedures (TTPs)

Verschiedene Bedrohungsakteure verfolgen unterschiedliche Taktiken und Vorgehensweisen. Cyfidelity identifiziert und definiert gezielt die für Ihr Unternehmen relevanten Akteure. Auf dieser Grundlage

werden spezifische Techniken, Tools und Prozesse abgeleitet, die auf die Bedrohungslage Ihres Unternehmens zugeschnitten sind. So erhalten Sie eine fundierte Basis, um sich effektiv gegen die typischen Angriffsmuster der identifizierten Akteure zu schützen. Die Aufbereitung und das Format der Ergebnisse stimmen wir individuell auf Ihre Bedürfnisse ab.

Password Spraying – Identifikation schwacher Passwörter

Passwort-Spraying ist eine Angriffsmethode, bei der eine begrenzte Anzahl häufig verwendeter Passwörter (z. B. "123456", "Passwort1" oder "Sommer2024") systematisch gegen eine Vielzahl von Benutzerkonten getestet wird. Diese Angriffe bleiben oft unentdeckt, da sie keine massenhaften fehlgeschlagenen Anmeldeversuche erzeugen. Wir analysieren, ob die E-Mail-Adressen einer Organisation für solche Angriffe anfällig sind und unterstützen Unternehmen bei der Durchsetzung sicherer Passwort-Richtlinien, um das Risiko erfolgreicher Angriffe zu minimieren.

Monitoring von öffentlichen Code-Repositories (GitHub)

Viele Entwickler nutzen GitHub, um Quellcode zu speichern, zu verwalten und gemeinsam an Projekten zu arbeiten. Allerdings kommt es immer wieder vor, dass in öffentlichen Repositories versehentlich vertrauliche Informationen wie API-Keys, Zugangsdaten oder Konfigurationsdateien offengelegt werden. Durch die Analyse der öffentlichen Repositories von Unternehmen und deren Mitarbeitenden identifizieren wir potenzielle Risiken und zeigen auf, welche sensiblen Daten möglicherweise ungeschützt zugänglich sind.

Cyberangriffe sind heutzutage nicht mehr nur auf große Konzerne beschränkt, sondern betreffen Unternehmen aller Branchen und Größen. CTI ermöglicht es Unternehmen, Bedrohungen nicht nur zu erkennen, sondern auch gezielt auf diese zu reagieren. Die gesammelten Informationen helfen dabei, Sicherheitsstrategien kontinuierlich anzupassen und Angriffe bereits im Vorfeld zu vereiteln.

Durch die Kombination aus proaktiver Überwachung, gezielten Analysen und fundierten Handlungsempfehlungen bietet Cyfidelity mit Cyber Threat Intelligence einen entscheidenden Vorteil im Kampf gegen Cyberbedrohungen. Unsere Dienstleistungen helfen Unternehmen dabei, ihre digitale Resilienz zu stärken und sich effektiv gegen aktuelle und zukünftige Angriffsszenarien zu wappnen.

2 IT-Security Beratung

Die IT-Security Beratung umfasst gezielte Maßnahmen zur Absicherung von IT-Systemen und Architekturen sowie die Entwicklung und Implementierung von Sicherheitsstrategien. Ziel ist es, Unternehmen bei der Verbesserung ihrer Sicherheitslage zu unterstützen, indem potenzielle Schwachstellen identifiziert, Risiken minimiert und wirksame Schutzmechanismen etabliert werden. Cyfidelity bietet Unternehmen individuelle Beratung, um ihre IT-Sicherheit nachhaltig zu stärken.

2.1 TIBER-EU Framework

In Deutschland wird das TIBER-EU-Framework durch das TIBER-DE-Programm der Deutschen Bundesbank und des Bundesamtes für Sicherheit in der Informationstechnik (BSI) umgesetzt. TIBER-DE wurde speziell an die nationalen Gegebenheiten des deutschen Finanzmarktes angepasst und stellt ein einheitliches Testverfahren für Finanzinstitute bereit, um ihre Cyber-Resilienz systematisch zu verbessern.

Ziele von TIBER-DE

Das Hauptziel von TIBER-DE ist es, Finanzinstitute und kritische Marktinfrastrukturen gegen fortgeschrittene Cyberbedrohungen widerstandsfähiger zu machen. Dazu werden realitätsnahe Angriffsszenarien simuliert, die von professionellen Red-Teams durchgeführt werden. Das Programm verfolgt dabei folgende Kernziele:

Erhöhung der Cyber-Resilienz des deutschen Finanzsektors: Durch simulationsbasierte Tests sollen Schwachstellen identifiziert und Sicherheitsmaßnahmen verbessert werden.

Harmonisierung mit TIBER-EU: TIBER-DE orientiert sich an den Vorgaben von TIBER-EU, um eine europaweit einheitliche Testmethodik sicherzustellen.

Kooperation zwischen Finanzinstitutionen und Regulierungsbehörden: Die Deutsche Bundesbank arbeitet eng mit dem BSI und anderen Aufsichtsbehörden zusammen, um eine effektive Umsetzung zu gewährleisten.

TIBER-DE-Testprozess

Der Testprozess von TIBER-DE folgt einer klaren Struktur, die auf den Grundsätzen von TIBER-EU basiert:

Initiierungsphase:

Die beteiligten Finanzinstitute legen gemeinsam mit der Bundesbank den Umfang und die Ziele des Tests fest. Die Institutionen benennen ein White Team, das für die Koordination verantwortlich ist.

Bedrohungsanalyse (Threat Intelligence Phase):

Externe Threat Intelligence Provider (TI-Anbieter) sammeln aktuelle Bedrohungsinformationen zu spezifischen Angriffsszenarien. Diese Analysen werden in einem Targeted Threat Intelligence Report (TTIR) dokumentiert.

Red-Team-Phase (Simulierte Angriffe):

Ein Red Team führt gezielte Cyberangriffe auf die IT-Systeme der Organisation durch. Diese Angriffe basieren auf realen Methoden und Werkzeugen, die auch von Cyberkriminellen genutzt werden.

Blau-Team-Phase (Abwehranalyse und Reaktion):

Die internen Sicherheitsteams (Blue Teams) analysieren ihre Reaktionsfähigkeit auf die simulierten Angriffe.Es erfolgt eine detaillierte Bewertung der Erkennungs- und Reaktionsprozesse.

Regulatorische Einbindung und Harmonisierung mit DORA

TIBER-DE wurde so konzipiert, dass es mit den Anforderungen des Digital Operational Resilience Act (DORA) harmoniert. Dies stellt sicher, dass Finanzinstitute, die an TIBER-DE teilnehmen, gleichzeitig die europäischen Regulierungsanforderungen im Bereich der Cybersicherheit erfüllen. Die Bundesbank und das BSI stellen dabei sicher, dass sich die Umsetzung von TIBER-DE nahtlos in die europäische Cybersicherheitsstrategie einfügt (Bundesbank, 2023).

Die Dienstleistungen der Cyfidelity

Threat Intelligence Services (Threat Intelligence Phase)

- Echtzeit-Bewertung potenzieller Bedrohungen für Ihr Unternehmen
- Entwicklung gezielter Bedrohungsintelligenzberichte (TTIR) gemäß TIBER-EU
- Identifikation wichtiger Angriffsvektoren und gegnerischer Taktiken

Red-Team-Testing (Simulierte Angriffe)

- Durchführung kontrollierter Cyberangriffe zur Sicherheitsbewertung
- Simulation fortgeschrittener realer Angriffsszenarien
- Detaillierte Analyse von Schwachstellen und Sicherheitslücken

Purple Teaming (Abwehranalyse und Reaktion)

- Zusammenarbeit zwischen Red und Blue Teams
- Verbesserung der Erkennungs- und Reaktionsfähigkeiten durch Echtzeit-Feedback
- Optimierung der Cybersicherheitsstrategie durch Integration von Angriff und Verteidigung

2.2 Beratung zur Härtung von Systemen und Architekturen

Die Sicherheit von IT-Systemen beginnt mit einer fundierten Härtung der bestehenden Infrastruktur. Eine unzureichend konfigurierte Umgebung kann Angreifern Tür und Tor öffnen, während eine gut gehärtete Architektur Cyberangriffe erheblich erschwert oder gar verhindert.

Als erfahrene IT-Security-Berater analysieren wir gezielt die Schwachstellen von Endgeräten wie Laptops, Arbeitsplatzrechnern und Servern sowie der eingesetzten Betriebssysteme (Windows und Linux). Besonderes Augenmerk liegt auf der Absicherung von Active Directory-Umgebungen, die häufig Ziel von Angreifern sind. Fehlkonfigurationen in der Berechtigungsstruktur, unzureichende Passwortrichtlinien oder unsichere Netzwerkfreigaben können potenzielle Einfallstore für Angreifer darstellen.

Auch Cloud-Umgebungen, insbesondere Microsoft Azure mit Entra ID (ehemals Azure AD), sind ein zentraler Bestandteil der IT-Security Beratung. Da Cloud-Dienste über das Internet erreichbar sind, benötigen sie spezifische Sicherheitsmaßnahmen, um Angriffe, unautorisierte Zugriffe und Fehlkonfigurationen zu verhindern. Cyfidelity unterstützt Unternehmen dabei, ihre Cloud-Sicherheitsrichtlinien zu optimieren, Identitäts- und Zugriffsmanagement zu verbessern und kritische Ressourcen bestmöglich zu schützen.

Ein weiteres Kernthema ist die Analyse und Absicherung von Netzwerkinfrastrukturen. Sicherheitsmechanismen wie Network Segmentation, Zero-Trust-Architekturen und der Schutz kritischer Schnittstellen helfen dabei, Angriffsflächen zu minimieren. Unternehmen profitieren dabei von konkreten Maßnahmenempfehlungen, die auf die individuellen Bedürfnisse und technischen Gegebenheiten zugeschnitten sind. Unsere Experten stehen Ihnen zur Seite, um eine robuste und widerstandsfähige IT-Sicherheitsstrategie zu entwickeln.

Entwicklung und Implementierung von Sicherheitsmaßnahmen

Neben der Identifikation und Härtung von Schwachstellen ist die konsequente Umsetzung von Sicherheitsmaßnahmen essenziell. Eine solide IT-Sicherheitsstrategie basiert nicht nur auf präventiven Maßnahmen, sondern auch auf der kontinuierlichen Überprüfung der Implementierung und Wirksamkeit der getroffenen Schutzmaßnahmen.

Cyfidelity bietet umfassende Beratungsleistungen, um maßgeschneiderte IT-Security-Konzepte zu entwickeln, die sich sowohl an aktuellen Bedrohungsszenarien als auch an den spezifischen Anforderungen eines Unternehmens orientieren. Dazu gehören unter anderem:

- Die Überprüfung der Konfiguration von Security-Lösungen
- Die Härtung von Identitäts- und Zugriffsmanagementsystemen, insbesondere durch den Einsatz von Multi-Faktor-Authentifizierung (MFA) und sicheren Authentifizierungsverfahren.
- Die Implementierung von Sicherheitsrichtlinien in Active Directory und Cloud-Umgebungen, um die unbefugte Nutzung privilegierter Konten zu verhindern.

Nach der Umsetzung der Maßnahmen führen wir Wirksamkeitsprüfungen durch, um zu bewerten, ob die implementierten Sicherheitsmechanismen den gewünschten Schutz bieten. Dies kann durch

Sicherheitsaudits, Penetrationstests oder simulierte Angriffsszenarien erfolgen, bei denen überprüft wird, ob Angreifer weiterhin Schwachstellen ausnutzen könnten.

Ziel ist es, eine nachhaltige Sicherheitskultur im Unternehmen zu etablieren, die über reine technische Maßnahmen hinausgeht. IT-Sicherheit muss als kontinuierlicher Prozess verstanden werden, der regelmäßige Anpassungen an neue Bedrohungen und technologische Entwicklungen erfordert.

3 Wirksamkeitsprüfung

3.1 Red Team Engagement

Red Teaming ist eine ursprünglich aus dem Militärumfeld kommende Methode deren Hauptaufgabe die Prüfung der generellen Resilienz eines Objektes ist. Für die Überprüfung greift ein Angreiferteam "Red Team" das Objekt an, um die Verteidiger "Blue Team" herauszufordern und Lücken im Verteidigungskonzept aufzudecken. Übertragen auf das IT-Umfeld kann dieses Vorgehen möglicherweise Sicherheitslücken aufdecken, welche von traditionellen Penetrationstests übersehen werden. Der Grund dafür liegt darin, dass Red Teaming die gesamte Angriffsoberfläche eines Unternehmens untersucht und neben rein technischen Komponenten auch der Faktor Mensch mit Social Engineering Aspekten einbezieht. Da ein Red Teaming die Simulation eines echten aufwändigen Angriffes abbildet, wird für die Durchführung eines Assessments ein auch ein großer Zeitrahmen eingeplant.

Üblicherweise werden im Gegensatz zu einem Penetrationstests nur wenige Personen in das Assessment eingeweiht. Dies hilft sicherzustellen, dass die Ergebnisse realistischer sind, da das Blue Team und andere Mitarbeiter nicht im Voraus über den Test informiert werden. Bei der Durchführung eines Red Team Assessments wird typischerweise auch die Achtsamkeit des Blue Teams und diverse Incident Response Prozesse getestet.

Grober Ablauf

Eine Red Teaming läuft typischerweise in mehreren Phasen ab. Jedes Red Teaming ist individuell und hängt stark von der Infrastruktur sowie der Prozesse der Zielorganisation an. Aus diesem Grund ist es nicht möglich im Vorfeld alle Angriffsszenarien zu skizzieren. Während des gesamten Red Teamings besteht regelmäßige und kurzfristige Kommunikation zwischen dem Red Team und dem Kunden. Dies dient zum einen der Risikominimierung und zum anderen fördert der Regelmäßige Austausch den agilen Ablauf des Projektes. Die folgenden Eckpunkte werden allerdings in den meisten Red Team Assessments vorkommen.

Initialer Workshop

Da Red Team Assessments komplex sind, werden in einem gemeinsamen Workshop alle wesentlichen Fragen geklärt. Im Rahmen des Workshops werden individuelle Ziele und Meilensteine festgelegt, sowie der Scope des Assessments definiert. Dieser Termin findet optimalerweise einige Wochen vor Beginn des Projektes statt.

Recon

Bei Recon handelt es sich um die erste technische Phase des Assessments. Hierbei wird das Red Team zunächst die öffentliche Präsenz eines Unternehmens untersuchen. Eine intern vernetzte IT-Landschaft führt häufig dazu, dass ein bösartiger Akteur mehrere Unternehmen angreifen kann, um Zugang zu einem bestimmten Zielorganisation zu erhalten. Aus diesem Grund wird im Rahmen eines Red Team Assessments in der Regel die gesamte Unternehmensstruktur untersucht.

Perimeter Analyse

In der zweiten Phase werden die zuvor identifizierten Systeme und Dienste, mit dem Hauptfokus auf Schwachstellen, welche einen Zugang zum internen Netzwerk der Zielorganisation ermöglichen, untersucht. Das Vorgehen erfolgt zum großen Teil manuell und wird nur teilweise automatisiert, um möglichst unauffällig zu vorzugehen.

Phishing & Social Engineering

Sofern das Erlangen des Initialen Zugangs nicht auf einer rein technischen Ebene möglich ist, werden nach Absprache auch Social Engineering Techniken eingesetzt. Bei dieser Vorgehensweise wird das Red Team versuchen, Kontakt zu einzelnen Mitarbeitern der Zielorganisation aufzunehmen und sie dazu zu ermutigen, Schadsoftware auszuführen oder Zugangsdaten preiszugeben.

Lateral Movement

Sobald der Zugang zum internen Netzwerk hergestellt wurde, wird das Red Team die bereits erlangten Zugriffsrechte nutzen, um möglichst diskret die intern verfügbaren Dienste und Ressourcen zu erkunden, um sich im internen Netzwerk auszubreiten.

Privilege Escalation

Das Red Team wird eine Rechteerweiterung anstreben, klassischerweise handelt es sich dabei um Domänen Administrative Berechtigungen. Häufig wird diese Berechtigungsstufe als Meilenstein für ein Red Team Assessment definiert, da aus diesem Kontext heraus häufig die zuvor definierten weiteren Ziele erreicht werden können.

Actions on Objective

Nachdem die benötigte Berechtigungsstufe erlangt wurde, werden die Handlungen durchgeführt, welche zum Erreichen der zuvor gesetzten Ziele führen. Hierbei kann es sich beispielsweise um die Kompromittierung der Backup-Infrastruktur handeln. Diese Phase richtet sich stark nach den im gemeinsamen Workshop definierten Zielen und ist für jedes Projekt individuell.

Further Actions

Sofern erforderlich, können auch weitere Angriffsszenarien durchgespielt werden. So wäre es beispielsweise möglich gezielt Angriffe durchzuführen, welche bekannt dafür sind, dass sie häufig Alarme auslösen. Dabei liegt der Fokus darauf, die Monitoring Maßnahmen sowie die Incident Response Prozesse des Blue Teams zu testen.

Grundsätzlich sind Red Team Projekte flexibel, so dass Angriffsszenarien noch während der Projektzeit angepasst werden können.

Dokumentation

Ein detaillierter Abschlussbericht zeigt den Verlauf des Assessments auf und beschreibt die dabei ausgenutzten Schwachstellen. Neben der technischen Beschreibung der Vorgehensweise werden auch effektive Empfehlungen zur Abwehr und Härtung solcher Angriffe ausgesprochen. Sämtliche Angriffe des Red Teams werden inklusive Zeitstempel in diesem Bericht dokumentiert. Diese Timeline bietet dem Blue Team einen klaren Überblick über den zeitlichen Verlauf der Angriffe und kann genutzt werden, um das eigene Monitoring nochmals genauer zu untersuchen.

Präsentation

Als Abschluss des Projektes findet mindestens eine Präsentation statt, in der die zentralen Themen und gewonnenen Erkenntnisse aus dem Red Team Assessment gebündelt präsentiert werden.

3.2 Recon (Blick von außen)

Recon beschreibt den Prozess der Informationsbeschaffung über eine Organisation aus öffentlich zugänglichen Quellen mit dem Ziel die Angriffsoberfläche aus Sicht potenzieller Angreifer darzustellen.

Im Zentrum steht dabei nicht die Ausnutzung von Schwachstellen, sondern die Vorbereitung für Angriffe. In diesem Zusammenhang sind Informationen über die Unternehmensstruktur, die IT-Landschaft, die öffentlich zugänglichen Systeme und die Mitarbeiter wichtig, um ein detailliertes Bild der Bedrohungslandschaft zu erhalten. Im Rahmen eines Recon-Assessments werden die folgenden Punkte untersucht:

Unternehmensstruktur

Eine intern vernetzte IT-Landschaft führt häufig dazu, dass ein bösartiger Akteur mehrere Unternehmen angreifen kann, um Zugang zu einem bestimmten Zielunternehmen zu erhalten. Dies ist beispielsweise der Fall, wenn intern Vertrauensstellungen zwischen unterschiedlichen Active Directory Domänen bestehen. Hierbei können Angreifer dann Schwachstellen in den IT-Systemen einer Tochtergesellschaft ausnutzen, um anschließend weitere Zugriffsmöglichkeiten auf die Ressourcen des ursprüngliche Zielunternehmens zu erhalten. Um die Unternehmensverflechtung aufzudecken, werden Plattformen wie Northdata oder das Unternehmensregister verwendet.

Zusätzlich analysiert die Cyfidelity die Firmenwebseiten sowie diverse Online-Enzyklopädie, Annoncen, Pressetexte und Blogbeiträge, um möglichst alle miteinander vernetzten Unternehmen zu identifizieren.

IP-Adressbereiche

Ein wesentlicher Teil eines Recon-Assessments bezieht sich auf die Suche nach IP-Adressbereichen, welche einem Unternehmen zugeordnet sind. Als Quelle werden hierfür die Datenbanken von Internet-Registries verwendet. Internet-Registries sind Organisationen, die für die Registrierung und Verwaltung von IP-Adressen zuständig sind. Ein besonderes Augenmerk liegt auf der RIPE (Réseaux IP Européens) Datenbank. Die RIPE ist eine der fünf großen Regional Internet Registries (RIRs) und deckt Europa, den Nahen Osten und Teile Zentralasiens ab. Durch die Analyse dieser Datenbanken wird die Cyfidelity möglichst alle registrierten IP-Adressbereiche identifizieren.

Domänen und Subdomänen

Zusätzlich gehört die Identifikation von Domänen und Subdomänen zu der Basis eines guten Recon-Assessments. Domänen werden zu IP-Adressen aufgelöst und zur Lokalisierung von Ressourcen im Internet verwendet. Domänen bestehen aus mehreren Bestandteilen, welche durch Punkte getrennt werden. Die höchste Ebene wird als Top-Level-Domain (TLD) bezeichnet, während Subdomänen eine Unterteilung einer Domäne darstellen. Um Informationen über Domänen und Subdomänen zu enumerieren verwendet die Cyfidelity Techniken wie beispielsweise Web-Crawling oder Open Source Intelligence (OSINT) Ressourcen.

Clouddienste

Ein weiterer wichtiger Aspekt ist die Analyse der Cloud-Infrastruktur. Cloud-Anbieter wie Amazon, Microsoft und Google bieten eine Vielzahl an Dienstleistungen an. Dazu gehören beispielsweise virtuelle Server, Applikationen oder Speicherplatz. Immer mehr Unternehmen setzen auf Cloud-Lösungen, da diese Flexibilität, Skalierbarkeit und Kosteneinsparungen bieten. Da diese Dienste immer im Internet zur Verfügung stehen, stellen sie für Angreifer ein interessantes Feld da. Viele Cloud-Lösungen sind so komplex und neu, dass nicht alle für die IT-Sicherheit relevanten Aspekte richtig verstanden und umgesetzt werden. Dabei werden häufig Ressourcen ausgelagert und unwissentlich Angriffsoberfläche exponiert. Die Cyfidelity wird die von dem Kunden verwendeten Cloud-Dienste überprüfen und anschließend aufzeigen, welche Angriffsmöglichkeiten sich hierbei ergeben.

Veröffentlichte Dokumente

Dokumente wie beispielsweise PDF-, Excel- oder Word-Dateien enthalten Metadaten. Häufig ist es möglich interessante Informationen aus den Metadaten von Dokumenten auszulesen. Diese Informationen können zum Beispiel Details zu verwendeten Softwareversionen oder zu der internen IT-Landschaft enthalten. Oftmals ist es auch möglich das Schema der Syntax für Benutzernamen der internen Active Directory Umgebung auszulesen. Auf diese Weise können Angreifer Benutzerlisten für Passwort-Rate-Angriffe erstellen. Die Cyfidelity wird eine Vielzahl an Dokumenten analysieren und die Metadaten auf interessante Informationen hin überprüfen.

Öffentliche Quellcode Repositories

Ein weiterer Bestandteil eines Recon-Assessments besteht in der Analyse von öffentlich zugänglichen Quellcode-Repositories. Ein Repository ist ein digitaler Speicherort, in dem Entwickler ihren Quellcode ablegen und teilen können. Für Angreifer sind solche Repositories interessant, da diese vertraulichen Informationen, wie Passwörter oder API-Keys enthalten können. Es kann beispielsweise vorkommen, dass Mitarbeiter Testdaten oder Konfigurationsdateien mit vertraulichen Informationen erstellen und vergessen, diese vor dem Hochladen in ein Repository wieder zu entfernen. Die Cyfidelity wird nach von dem Kunden verwalteten Repositories suchen und diese anschließend scannen, um somit vertraulichen Daten zu finden.

3.3 Physical Assessment

Das Physical Assessment von Cyfidelity ist eine umfassende Sicherheitsüberprüfung, die physische Schutzmaßnahmen eines Unternehmens analysiert, um potenzielle Schwachstellen zu identifizieren und gezielt zu beheben. Unser Ansatz berücksichtigt sowohl technische als auch organisatorische Aspekte, um eine robuste Sicherheitsinfrastruktur gegen physische Bedrohungen zu gewährleisten.

Zielsetzung des Physical Assessments

- Identifikation von Schwachstellen: Analyse und Aufdeckung von Lücken in den bestehenden physischen Sicherheitsvorkehrungen.
- Bewertung der Schutzmaßnahmen: Untersuchung der Wirksamkeit aktueller Sicherheitsstrategien, Technologien und Prozesse.
- Empfehlung von Verbesserungen: Entwicklung maßgeschneiderter Lösungen zur Optimierung der physischen Sicherheit im Unternehmen.

Vorgehensweise bei einem Physical Assessment

Planung und Vorbereitung

- Definition des Prüfungsumfangs: Festlegung der zu untersuchenden Bereiche, Gebäude und Systeme.
- Informationssammlung: Analyse bestehender Sicherheitsrichtlinien, Zugangskontrollen und technischer Schutzmaßnahmen.

Durchführung der Analyse

- Vor-Ort-Begehung: Inspektion der Räumlichkeiten zur Bewertung physischer Barrieren, Überwachungssysteme und Zugangskontrollen.
- Simulation von Angriffsszenarien: Durchführung von Penetrationstests, Social Engineering und Red-Teaming-Techniken, um die Widerstandsfähigkeit der physischen Sicherheitsmechanismen zu testen.

Auswertung und Berichtserstellung

- Dokumentation der Ergebnisse: Erstellung eines detaillierten Berichts über identifizierte Schwachstellen und Risiken.

- Empfehlungen für Sicherheitsmaßnahmen: Ableitung konkreter Handlungsempfehlungen zur Behebung von Schwachstellen und Optimierung bestehender Sicherheitsvorkehrungen.

Umsetzung der Maßnahmen

- Priorisierung der Sicherheitsmaßnahmen: Einstufung der Schwachstellen nach Kritikalität und Festlegung einer sinnvollen Implementierungsstrategie.
- Schulung des Personals: Sensibilisierung der Mitarbeiter für physische Sicherheitsrisiken und Einführung von Best Practices zur Risikominimierung.

Nachbereitung und kontinuierliche Verbesserung

- Überprüfung der implementierten Maßnahmen: Evaluierung der umgesetzten Sicherheitsoptimierungen und deren Effektivität.
- Regelmäßige Sicherheitsüberprüfungen: Kontinuierliche Anpassung und Aktualisierung der Sicherheitsstrategie an neue Bedrohungsszenarien und technologische Entwicklungen.

Mit dem Physical Assessment von Cyfidelity erhalten Unternehmen eine umfassende Sicherheitsanalyse und gezielte Empfehlungen zur Erhöhung der physischen Resilienz. Unsere Experten begleiten Sie von der Identifikation über die Umsetzung bis hin zur langfristigen Optimierung Ihrer Sicherheitsstrategie. Schützen Sie Ihr Unternehmen effektiv vor physischen Bedrohungen – mit einer maßgeschneiderten Sicherheitslösung von Cyfidelity.

3.4 Schutz Ihrer digitalen Identität: digital footprint

Mit unserer individuellen Analyse ihres "digital footprint" geben wir Ihnen volle Transparenz darüber, welche öffentlich zugänglichen Informationen über Sie im Netz auffindbar sind – und welche potenziellen Risiken sich daraus ergeben könnten.

Zero-Knowledge-Ansatz: Analyse ausschließlich auf Basis Ihres Namens, um die Perspektive eines externen Angreifers ohne Vorwissen zu simulieren.

- Das kompaktes Lagebild Ihrer aktuellen digitalen Sichtbarkeit.

Insider-Ansatz: Erweiterte Analyse unter Einbezug freiwillig bereitgestellter Daten (E-Mail-Adressen, Mobilfunknummern), um die Sicht eines Angreifers mit Vorwissen darzustellen.

- Ihr detailliertes, individualisiertes Risikoprofil.

Invasives Vorgehen: Sowohl der Zero-Knowledge- als auch der Insider-Ansatz lassen sich optional mit einem invasiveren Vorgehen kombinieren, bei dem wir entdeckte Zugangsdaten zum Einbruch in Ihre Accounts nutzen.

- Die Validierung Ihres Schadenspotenzials.

Awareness-Training: Aufbauend auf Ihrem "digital footprint" stärken wir mit individualisierten Phishing-Nachrichten Ihre Awareness für moderne, kontextbasierte Social Engineering-Angriffe.

- Die Stärkung Ihrer persönlichen Cyber-Resilienz.

4 Pentest / Purpleteaming / Devices /Cloud

4.1 IP-Range Test

Im Rahmen eines IP-Range Tests werden ausgewählte IT-Systeme anhand ihrer IP-Adressen aus dem Internet einer gründlichen Schwachstellenanalyse unterzogen. Für alle Feststellungen wird im Anschluss an den Test einer Risikobewertung vorgenommen und in einem Bericht ausführlich dargestellt. Die Cyfidelity wird zunächst exponierte Dienste wie beispielsweise Webserver, Datenbanken, Mailserver etc. identifizieren und anschließend nach Sicherheitslücken suchen. Hierfür werden Netzwerkerkennungs-Werkzeuge eingesetzt, welche aktive Systeme, verwendete Betriebssysteme, offene Ports und darauf laufende Dienste erkennen.

Überprüfung auf Schwachstellen

Auf der Grundlage der gesammelten Informationen über verfügbare Dienste identifiziert die Cyfidelity dann potenzielle Schwachstellen. Dies geschieht sowohl mit automatisierten Scanning-Werkzeugen als auch durch manuelle Überprüfungen. Schwachstellen-Scanner können dabei helfen, bekannte Schwachstellen in den Systemen oder Diensten, die auf den aktiven IT-Systemen laufen, zu identifizieren. Es werden auch manuelle Verfahren eingesetzt, wie beispielsweise die Überprüfung auf Fehlkonfigurationen aktiver Dienste, Standard-Anmeldedaten, veraltete Software, schwache Verschlüsselung, die Preisgabe sensibler Daten und andere potenzielle Sicherheitslücken.

Die Cyfidelity richtet ihr Augenmerk darauf, ein gutes Verständnis der vorhandenen Dienste und ihrer Interaktion untereinander zu erlangen. Dazu verwenden wir die Daten, die wir bereits bei den automatisierten und manuellen Prüfungen erhalten haben. Auf diese Weise können verkettete Schwachstellen identifiziert werden. So können beispielsweise ermittelte sensible Informationen, wie in einem unauthentifizierten Dienst gefundene Zugangsdaten, für andere Dienste genutzt werden. Darüber hinaus können unbeabsichtigt exponierte Dienste, welche umfangreiche Interaktionsmöglichkeiten bieten, zu unbefugtem Zugriff auf ein IT-System führen. So lassen sich auch komplexere Schwachstellen ermitteln, die mit einem automatischen Scanner allein nicht entdeckt werden können.

Validierung von Schwachstellen

Die ermittelten Schwachstellen können nach Rücksprache mit dem Kunden und unter Abwägung von Aufwand und Nutzen durch kontrollierte Ausnutzung validiert werden. Dabei geht es nicht darum, Schaden anzurichten, sondern die Existenz und die potenziellen Auswirkungen der Schwachstellen zu überprüfen. Diese Phase umfasst Schritte wie den unbefugten Zugriff auf Systeme und Daten und die Überprüfung des möglichen Missbrauchs einer Schwachstelle zu kriminellen Zwecken.

4.2 Netzwerk-Sicherheit

Bei einem Test der internen Dienste wird das lokale Netzwerk aus der Perspektive eines Angreifenden betrachtet. Dies bedeutet der Penetrationstest findet im authentifizierten Kontext statt, typischerweise mit Zugangsdaten und aus dem lokalen Netzwerk des Kunden. Innerhalb des Testszenarios sollen mögliche Schwachstellen oder Fehlkonfigurationen ermittelt werden, die ein Risiko für die Unternehmensinfrastruktur darstellen oder gar zu einer vollständigen Kompromittierung führen können. Beispielsweise können die möglichen Auswirkungen eines erfolgreichen Phishing-Angriffs abgeschätzt werden, bei welchem ein Gerät und ein regulärer Benutzer kompromittiert wurden.

Der Test fokussiert sich hierbei auf die Netzwerkkomponenten, die einem authentifizierten Benutzer regulär zur Verfügung stehen oder nicht ausreichend geschützt sind. Im Allgemeinen handelt es sich dabei um Dienste wie Microsoft Active Directory, Dateiablagen, Wissensaustauschplattformen und Client-Plattformen. Die Cyfidelity untersucht in der Regel die aufgeführten Dienste und die darin abgelegten Informationen auf Möglichkeiten der Rechteeskalation. Alternativ können auch andere Ziele, Vorgehensweisen oder Prioritäten vereinbart werden. Innerhalb der einzelnen Bereiche werden unter anderem die folgenden Aspekte untersucht:

Active Directory

In vielen Microsoft geprägten internen Infrastrukturen stellt das Active Directory den zentralen Authentifizierungs- und Autorisierungsanbieter dar. Dieses System stellt die zentrale und kritische Schnittstelle zu vielen (kritischen) Daten und Informationen dar (bspw. E-Mail-Postfächer, Unternehmensgeheimnisse, Personaldaten etc.). Active Directory Strukturen werden selten komplett neugestaltet, so dass in der Regel die Infrastruktur "historisch gewachsen" ist. Dadurch, aber nicht ausschließlich, können sich Konstellationen oder Schwachstellen ergeben, die eine komplette Übernahme des Active Directories ermöglichen. Die Cyfidelity überprüft die Active Directory Infrastruktur auf Schwachstellen, Fehlkonfigurationen oder gefährliche Berechtigungskonstellationen (bspw. mithilfe von Bloodhound Analysen). Zusätzliche werden Szenarien der Rechteausweitung und Impersonierung ebenfalls berücksichtigt, um die möglichen Auswirkungen, Reaktionen und empfohlene Gegenmaßnahmen zu ermitteln. Ausgangspunkt für sämtliche Analysen stellt ein regulärer Benutzer dar.

Dateiablagen

Damit Mitarbeitende Arbeitsergebnisse oder Informationen teilen, einsehen und ablegen können existiert nahezu in allen Infrastrukturen eine zentrale Dateiablage (in der Regel ein oder mehrere Fileserver). Auf diesen werden über Freigaben mit Berechtigungsgruppen Informationen abgelegt und der entsprechenden Zielgruppe zugänglich gemacht. Diese Strukturen können über die Zeit sehr komplexe Ausmaße annehmen und dadurch zu einem Sicherheitsrisiko werden. Beispielsweise können durch fehlerhafte, stark verschachtelte oder zu offene Berechtigungsstrukturen sensible Informationen (wie Personaldaten, Backups, Kennwortspeicher, Systemzugänge, etc.) für einen sehr großen Benutzerkreis einsehbar sein. Innerhalb eines Penetrationstest der Cyfidelity werden die Daten und Freigaben die einem regulären Benutzer zur Verfügung stehen ermittelt. Des Weiteren werden die identifizierten Daten nach technischen Informationen (bspw. Kennwörter, SSH-Schlüsselt, etc.) durchsucht. Dies findet teilweise manuell aber auch automatisiert statt, es soll ein möglichst vollständiger Blick auf die Struktur gewährleistet werden. Im Anschluss werden die identifizierten technischen Daten ausgewertet und für weitere Szenarien wie Rechteausweitung, Impersonierung, etc. verwendet, um die Auswirkungen und Reaktionen innerhalb der Infrastruktur abzuschätzen.

Wissensmanagement

Um Informationen schneller und einfacher darzustellen und zugänglich zu machen, existieren in vielen Unternehmen Systeme für das Wissensmanagement (bspw. ein Wiki). Oftmals sind die Informationen und die Berechtigung dieser durch die Benutzer/Teams selbst organisiert (bspw. innerhalb von Projektteams) - auch hier können sich gefährliche Berechtigungsszenarien ergeben. Falls sensible Informationen (bspw. Systemzugänge) mit einem großen Anwenderkreis geteilt werden kann sich eine Bedrohung für die gesamte Infrastruktur ergeben. Um das Gefahrenpotential und die möglichen Auswirkungen zu überprüfen, wertet die Cyfidelity das Wissensmanagement manuell sowie automatisiert aus und sucht gezielt nach technischen Informationen (Kennwörter, Systemzugänge etc.) für eine mögliche Rechteausweitung.

Interne Dienste und Anwendungen

Innerhalb von Unternehmensinfrastrukturen befinden sich oftmals eine Vielzahl von Anwendungen und Diensten. Teilweise werden diese Anwendungen und Dienste aktiv von Benutzern verwendet, teilweise handelt es sich um Backend Dienste oder auch um ehemalige Testsysteme von geplanten Projekten. Dadurch können sich unterschiedliche Bedrohungsszenarien ergeben. Bei aktiv verwendeten Anwendungen können diese entweder, durch Schwachstellen in veralteten Komponenten oder aber durch bspw. Logikfehler, es Angreifern ermöglichen den Anwenderkreis gezielt zu kompromittieren. Bei Backend Diensten (bspw. SQL-Datenbanken) oder auch bei ehemaligen Testsysteme können sich, durch fehlerhafte Konfigurationen oder zu weit gefasste Rechtevergabe, Konstellationen ergeben, die eine Kompromittierung ermöglichen (bspw. durch die Übernahme von SQL-Servern). Aus diesem Gründen überprüft die Cyfidelity die Dienste und Anwendungen, die innerhalb der Infrastruktur verfügbar sind auf Möglichkeiten zur Rechteeskalation oder Kompromittierung (im Kontext eines internen Tests).

Clientplattformen

Die verwendete Clientplattform stellt für die Nutzer den Hauptinteraktionspunkt mit der Infrastruktur dar. Oft werden für die Verwaltung und Steuerung von Clients Managementsysteme und Softwareverteilungslösungen verwendet. Je nach Konfiguration und Verwendung können diese jedoch auch zur Gefahr innerhalb der Infrastruktur werden - bspw. durch die Streuung hochprivilegierter technischer Benutzer auf Clientsystemen oder unsichere Handhabung von Geheimnissen. Auch unzureichende Härtungsmaßnahmen innerhalb der Clientplattform - bspw. durch Passwortwiederverwendung, fehlende Festplattenverschlüsselung etc. - können zu einem Risiko für die Unternehmensinfrastruktur werden. Die Cyfidelity überprüft die möglichen Risiken und Bedrohungsszenarien für die Gesamtstruktur durch die verwendete Clientplattform (bspw. Rechteausweitung, implementierte Härtungsmaßnahmen etc.) sowie angeschlossene Managementsysteme.

4.3 LAN

Bei einem Test des Local Area Networks (LAN) untersucht die Cyfidelity das lokale Netzwerk des Kunden aus der Perspektive eines unauthentifizierten Angreifers vor Ort. Innerhalb des Testszenarios sollen verfügbare Dienste und Kommunikationsbeziehungen identifiziert werden, mit dem Ziel mögliche Schwachstellen oder Fehlkonfigurationen zu ermitteln, die ein Risiko für die Unternehmensinfrastruktur darstellen.

Identifizierung von Diensten und offensichtlichen Fehlkonfigurationen

Ziel dieser Phase ist es alle von einem gewählten Punkt im Netzwerk erreichbaren Dienste zu ermitteln. Dadurch können insbesondere Dienste identifiziert werden, welche unnötig erreichbar sind, sowie auch Schatten-IT, beispielsweise nicht mehr benötigte Testsysteme. Zusätzlich erfolgt, sofern möglich, eine oberflächliche Analyse der identifizierten Dienste bezüglich der eingesetzten Versionen, Verwendung von Standardpasswörtern und offensichtlichen Fehlkonfigurationen (z.B. Verwendung unsicherer TLS-Konfiguration). Optional kann dieser Schritt durch Kombination mit dem Modul "Interne Dienste" vertieft werden. Analyse der übertragenen Daten

In Absprache mit dem Kunden werden vor Ort von ausgewählten Kommunikationsstrecken die übertragenen Daten ausgewertet. Dazu kann, sofern vorhanden und konfiguriert, die Hardware des Kunden genutzt werden (z.B. Mirroring-Port, Tapping Device, ...) oder aber die Hardware der Cyfidelity. Ziel ist dabei die Identifikation von unverschlüsselter Kommunikation sensitiver Daten und unbeabsichtigten Kommunikationsbeziehungen.

Zonentrennung

Größere Netzwerke sind oft in mehrere unabhängigen Zonen unterteilt, zwischen denen eine Kommunikation nur in einzelnen Ausnahmefällen erwünscht ist. Die Cyfidelity führt daher stichprobenartige Tests durch, um die Effektivität der getroffenen Maßnahmen zur Trennung der unterschiedlichen Zonen zu überprüfen. Dadurch ist es möglich ungewollte interne Kommunikationsmöglichkeiten zu identifizieren, welche beispielweise die Kommunikation zwischen unterschiedlichen Sicherheitsniveaus erlauben oder einem Angreifer die laterale Bewegung erleichtern.

Zusätzlich wird geprüft, ob eine unbeabsichtigte Kommunikationsmöglichkeit mit Diensten aus dem Internet besteht, um Wege für einen potenziellen Datenabfluss sensitivier Informationen zu ermitteln. Sofern das lokale Netzwerk eine Authentifizierung für Endgeräte erfordert, ist die Überprüfung dieses Vorgangs auch Teil der Prüfhandlungen der Cyfidelity.

4.4 Device Security Test

Prüfung der Datensicherheit auf gestohlenen Geräten

Ein Schwerpunkt ist die Analyse der Festplattenverschlüsselung (z. B. BitLocker, FileVault). Hier wird überprüft, ob und unter welchen Umständen Angreifer Zugriff auf gespeicherte Unternehmensdaten erlangen können.

Zusätzlich erfolgt eine Untersuchung der gespeicherten Zugangsdaten und Authentifizierungs-Token auf dem Gerät. Dabei wird geprüft, ob sich Webbrowser-Passwörter, Single-Sign-On-Tokens oder andere Anmeldedaten extrahieren lassen, die einem Angreifer den Zugang zu Unternehmenssystemen ermöglichen könnten. Ebenso wird analysiert, ob lokal gespeicherte Konfigurationsdateien oder API-Keys unzureichend gesichert sind, die für den unbefugten Zugriff auf Cloud-Dienste missbraucht werden könnten.

Prüfung der Umgehung von Schutzmechanismen

Ein zentraler Bestandteil des Tests ist die Überprüfung von Secure Boot-Mechanismen und der Manipulationssicherheit von BIOS/UEFI-Firmware. Hierbei wird getestet, ob Angreifer die Sicherheitsmaßnahmen umgehen können, um ein kompromittiertes oder nicht autorisiertes Betriebssystem zu laden. Dies könnte es ihnen ermöglichen, das Gerät zu übernehmen oder persistente Schadsoftware zu installieren.

Ein weiterer wesentlicher Aspekt ist die Evaluierung der Mobile Device Management (MDM)-Lösung des Unternehmens. Dabei wird geprüft, ob verlorene oder gestohlene Geräte zuverlässig remote gesperrt oder gelöscht werden können, um den unbefugten Zugriff auf Unternehmensdaten zu verhindern. Zusätzlich wird untersucht, ob ein Angreifer in der Lage wäre, MDM-Schutzmechanismen zu deaktivieren oder zu manipulieren.

Die Effektivität der lokalen Authentifizierungsmechanismen wird ebenfalls geprüft, um festzustellen, ob Angreifer Zugriff auf das Gerät erlangen können. Dies umfasst die Analyse von Passwortschutz, biometrischer Authentifizierung und anderen Sicherheitsfunktionen des Betriebssystems. Darüber hinaus wird bewertet, ob ein gestohlenes Gerät möglicherweise für den Zugriff auf das Unternehmensnetzwerk per VPN genutzt werden kann und welche Unternehmensressourcen darüber erreichbar sind.

4.5 Cloud Security Testing

Um das Risiko eines Cloud Breaches zu reduzieren, empfiehlt es sich die Sicherheit der eigenen Cloud-Umgebung regelmäßig von Sicherheitsexperten überprüfen zu lassen. Die Sicherheitsexperten der Cyfidelity unterstützen Sie bei dieser komplexen Thematik. Hinsichtlich der Verantwortung für die Absicherung von Cloud-Infrastruktur, geben Cloud-Anbieter wie Amazon und Microsoft klare Vorgaben: "Für die Sicherheit in der Cloud trägt der Endkunde die Verantwortung". Diese Regelung ist dem jeweiligen Shared Responsibility Model zu entnehmen. Folglich ist der Endkunde selbst für die Absicherung von beispielsweise Identity & Access Management oder Client & End-Point Protection verantwortlich.

Da Cloud Systeme, sich vor allem durch ihre hohe Komplexität, Vielzahl von Services und Systemen, automatischen Deployments, Unterstützung unterschiedlicher Architekturen und beständige Veränderung auszeichnen ist es bei dieser Bandbreite an individuellen Möglichkeiten unvermeidbar substanzielle Sicherheitslücken zu übersehen. Um auf individuelle Anforderungen eingehen zu können stellt allein AWS mittlerweile über 200 verschiedene Services zur Verfügung.

Bei der Cyfidelity gehen wir auf Ihre individuellen Anforderungen für Ihre Cloud-Systeme ein. Unter Verwendung eines passenden Szenarios können wir so zahlreiche unterschiedliche Techniken und Tools einsetzen, um Ihre Schutzmechanismen präzise zu evaluieren, Fehlkonfigurationen aufdecken, um dabei Ihre Cloud-Systeme abzuhärten. Unsere Experten entwickeln dabei die Möglichkeiten für Untersuchungen beständig weiter und reagieren tagesaktuell auf neue Schwachstellen, Fehlkonfigurationen oder brandaktuelle Angriffs-Vektoren.

Vorgehen und Szenarien

Das Vorgehen für das Cloud Assessment richtet sich nach den individuellen Bedürfnissen des Kunden. Generell lassen sich die Anforderungen in folgende Kategorien unterteilen:

- Outsider: Bezeichnet einen Benutzer, der keinen Zugang zum Tenant oder der AWS-Umgebung der Zielorganisation hat. Fokus wird hierbei auf die Information Gathering Bereich gelegt, um Informationen von außen zu erlangen.
- Guest: Bezieht sich auf einen Benutzer, der einen eingeschränkten Gastzugang (externer Benutzer) zum Ziel-Tenant hat. Aufgrund der technischen Architektur ist der Guest nur im Azure-Kontext möglich.
- Insider: Bezieht sich auf die "normalen" Benutzer des Tenants. Sie haben nur Lesezugriff auf praktisch alle Informationen in dem AAD. Bei AWS bezieht sich der "normale" Benutzer auf den Zugriff bei einem AWS-Service mit gültigen AWS-Credentials.

Welches Szenario für einen AWS Pentest herangezogen wird, wird nach Bestimmung des Scopes mit dem Kunden individuell vereinbart.

AWS

Mithilfe eines eigens entwickelten Frameworks zum Penetration Testing von AWS Cloud Umgebungen ist die Cyfidelity in der Lage, alle AWS Services Ihrer AWS Cloud Infrastruktur individuell und detailliert zu analysieren und mögliche Schwachstellen aufzudecken. Folgende Services sind beispielsweise regelmäßig Ziel von Cyber-Attacken:

- S3-Bucket: Stellen eine Art der Datenspeicherung in der AWS-Umgebung dar. Standardmäßig sind diese S3-Buckets nur privat zugänglich. In der Vergangenheit sind immer mehr Konzerne Opfer von S3-Leaks geworden. Durch Fehlkonfiguration ist es möglich unauthentifiziert Daten von S3-Buckets einzusehen.
- EC2-Instanz: Mit Amazon Elastic Compute Cloud (Amazon EC2) bietet AWS Ihnen eine Rechenplattform mit über 600 Instanzen für jeden kundenspezifischen Anwendungsfall. Um Metadaten über eine EC2-Instanz abrufen zu können bietet Amazon mit dem Metadata-Service Ihnen eine Möglichkeit diese Informationen einzusehen. In der Vergangenheit war es unbefugten Angreifern immer wieder möglich, über SSRF-Schwachstellen den Metadata-Service aufzurufen und AWS Credentials auszulesen.

Azure

Ein Penetrationstest einer Azure Cloud Umgebung ist eine sehr umfangreiche Aufgabe. Eine klare Zieldefinition stellt dabei eine essenzielle Grundvoraussetzung dar. Bei der Analyse orientieren sich unsere Sicherheitsexperten an marktüblichen Vorgehensmodellen. Die Sicherheitsexperten der Cyfidelity sind in der Lage alle Services in der Azure-Cloud umfangreich zu testen. Folgende Themen werden u.a. im Rahmen eines Azure Cloud Pentest differenziert analysiert und system-spezifisch eingeordnet:

- Logging: Inwieweit funktioniert das Azure-Logging um unerlaubte Zugriffe zu erkennen und leiten sich daraus die richtigen Responses ab. Typische Pitfalls sind hier beispielsweise fehlendes Logging bei Azure Webapplikation Firewalls und Key Vaults.
- Deployments: Sind Deployments sicher umgesetzt? Werden beispielsweise Runbooks mit ausspähbaren Credentials oder Powershell-Skripte und Storages mit potenziell sensiblen Informationen verwendet?
- Awareness: Welches Phishing oder andere aktuelle Bedrohungsszenarien sind für die jeweilige Infrastruktur am gefährlichsten? Phishing über Onedrive, Cloud Attachments oder externe Unternehmensanwendungen sowie Token Stealer und Admin Illicit Consent Angriffe. Was ist für Sie relevant und wie können Sie sich davor schützen?

4.6 Web Application Pentest

Im Rahmen eines WebApp-Penetrationstests wird eine Webapplikation mit dazugehörigen Webservices/API-Endpunkten auf Sicherheitsschwachstellen und Fehlkonfigurationen überprüft. Das Ziel dabei ist, einen realistischen Einblick auf die Sicherheitslage der Webapplikation aus der Perspektive eines Angreifers aufzuzeigen. Alle Feststellungen werden im Anschluss an den Penetrationstest einer Risikobewertung unterzogen und im Bericht entsprechend dargestellt. Im Zuge eines WebApp-Penetrationstests werden unter anderem die folgenden Prüfungen durchgeführt, welche sich an etablierten Penetrationsstandards für Webapplikationen wie beispielsweise dem OWASP Application Security Verification Standard orientieren.

Ermittlung der Struktur

Im ersten Schritt verschafft sich die Cyfidelity einen Überblick über die zu testende Webapplikation und derer Struktur. Dabei werden aus Sicht eines Angreifers interessante Bereiche und Funktionen,

eingesetzte Software und Servertechnologien ermittelt. Zusätzlich werden die Funktionsabläufe der Webapplikation, wie beispielsweise das Zurücksetzen eines Passworts oder das Freigeben von Vertragsdaten für bestimmte Kunden, näher betrachtet. Am Ende dieser Testphase hat die Cyfidelity einen guten Überblick über die Webapplikation und ihre Business-Logik.

Prüfung der Authentifizierung und Autorisierung

Wenn die Webapplikation eine Benutzeranmeldung verlangt, werden im folgenden Schritt mögliche Angriffe auf Authentifizierung, Autorisierung und Berechtigungskonzept untersucht. Mögliche Schwächen können sowohl auf konzeptionellen als auch auf rein programmatischen Fehlern beruhen. Die Cyfidelity untersucht auch, ob die beabsichtigten Zugriffsbeschränkungen effektiv umgesetzt sind und nicht umgangen werden können.

Prüfung der Eingabevalidierung

Das Ziel dieser Überprüfungsphase ist sicherzustellen, dass alle System- und Benutzerdaten sicher verarbeitet werden. Dies betrifft jeweils die Eingabe, die Verarbeitung und die Ausgabe dieser Daten. Dadurch können Schwachstellen wie Cross-Site-Scripting oder SQL Injection identifiziert werden.

Identifizieren von Datei- und Ressourcenschwachstellen

In diesem Schritt analysiert die Cyfidelity, ob ein unbefugter Zugriff auf sensible Dateien, wie Konfigurationsdateien oder benutzerspezifische Ressourcen, möglich ist. Bekannte Angriffe hierfür sind Directory Traversal und Local/Remote File Inclusion. Zusätzlich werden Angriffsvektoren wie das Überschreiben oder Hochladen von Dateien auf den Server überprüft, mit dem Ziel der Umgehung von Zugriffsbeschränkungen bis hin zur vollständigen Kompromittierung des Servers.

Überprüfung der Business-Logik

Die Cyfidelity legt einen besonderen Fokus darauf, die implementierte Business-Logik der Webapplikation zu verstehen, da viele potenzielle Schwachstellen ohne oder mit wenig Verständnis über die Webapplikation nicht aufgedeckt werden können. Hierfür kommen manuelle Überprüfungen zum Einsatz, da automatisierte Scanner-Werkzeuge hierbei wenig hilfreich sind. So werden beispielsweise bei einer E-Commerce-Webapplikation die Abläufe einer Transaktion manuell überprüft, um sicherzustellen, dass keine Warenkorb- oder Zahlungsmanipulationen möglich sind.

Überprüfung von eingebundenen Webservices/API-Endpunkten

Moderne Webapplikationen kommunizieren mit mehreren Webservices, welche der Webapplikationen mit eingelieferten Daten und Funktionen bedienen. Da diese Webservices feste Bestandteile und in vielen Fällen das Herzstück einer Webapplikation sind, werden sie ebenfalls auf Sicherheitsschwachstellen überprüft. Hierfür untersucht die Cyfidelity die Interaktionen zwischen der Webapplikation und den Webservices, um Sicherheitsschwächen zu identifizieren, wie beispielsweise die übermäßige Preisgabe sensibler Daten an unbefugte Dritte oder Nutzung versteckter Funktionalitäten.

Prüfung der zugrundeliegenden Infrastruktur

Optional kann zusätzlich zu der Webapplikation auch die zugrundeliegende Infrastruktur getestet werden. Dazu gehört die Prüfung der Web-, Datenbank- und Applikationsserver, einschließlich des Patchstands. Außerdem wird untersucht, ob die Anzahl der offenen Ports dem notwendigen Minimum entspricht. Weiterhin analysiert die Cyfidelity die Verschlüsselung der Kommunikation. Da viele Webapplikationen heutzutage in der Cloud gehostet werden, kann es sinnvoll sein, ein separates Assessment der Cloud-Infrastruktur durchzuführen.

4.7 Mobile Application Pentest

Bei einem Mobile Pentest werden Android- und iOS-Apps auf speziell zum Test eingerichteten Smartphones auf Schwachstellen geprüft. Das Vorgehen der Cyfidelity orientiert sich dabei an dem gängigem OWASP Mobile Application Testing Guide (MASTG).

Szenarien

Mobile Tests können in verschiedenen Szenarien durchgeführt werden. Das anzuwendende Szenario wird mit Ihnen individuell in einem Kundengespräch abgestimmt.

Angriffssimulation (Blackbox)

Ein mögliches Szenario wäre die Simulation eines Angriffs auf die App ohne Vorab-Informationen. Hierbei lädt sich die Cyfidelity die App von den gängigen Stores herunter und überprüft sie innerhalb eines festgelegten Zeitraums auf Schwachstellen. Dabei lassen sich Erkenntnisse erzielen, wie weit ein Angreifer mit nur öffentlichen Informationen kommen kann.

Whitebox

Ein weiteres mögliches Szenario wäre ein Whitebox Pentest. Bei einem Whitebox Pentest erhält die Cyfidelity sämtliche Informationen, sowie Daten wie z.B. Source Code und Debug Versionen der App. Diese werden genutzt, um möglichst effizient viele Schwachstellen zu finden.

Scope

Mobile Tests betreffen nicht nur die App selbst, sondern auch die Kommunikation zwischen der App und Servern. Dabei können z.B. API und Cloud Konfigurationen getestet werden. Den genauen Inhalt des Scopes klärt die Cyfidelity zu Beginn des Testes.

Abschluss

Nach Abschluss der Überprüfung erhalten Sie einen detaillierten Bericht mit den identifizierten Sicherheitslücken, sowie Empfehlungen zur Verbesserung der Sicherheit ihrer Anwendung.

Technisches Vorgehen

Im Rahmen eines Mobile Pentests werden unter anderem folgende Punkte untersucht:

Cross-Site Scripting

Cross-Site-Scripting (XSS)-Probleme ermöglichen es Angreifern, clientseitige Skripte in Webseiten einzuschleusen, die von Benutzern aufgerufen werden. Diese Art von Schwachstelle ist in Webanwendungen weit verbreitet. Wenn ein Benutzer eine Webseite samt dem eingeschleusten Skript in einer WebView innerhalb einer App öffnet, kann der Angreifer die same origin policy (SOP) umgehen, was eine Vielzahl von Angriffen ermöglicht (z. B. Stehlen von Sitzungscookies, Protokollieren von Tastendrücken, Ausführen beliebiger Aktionen usw.). Die Cyfidelity prüft die App auf die Nutzung der WebViews und auf potenzielle Angriffe, die aufgrund fehlerhafter Konfiguration der WebView Komponenten und Webseiten auftreten können.

Obfuskation

Bei der Obfuskation werden Code und Daten so umgewandelt, dass sie schwerer zu verstehen (und manchmal sogar schwer zu disassemblieren) sind. Sie ist in der Regel ein integraler Bestandteil des Softwareschutzsystems, sodass Programme auf verschiedene Weise und in unterschiedlichem Maße ganz oder teilweise unverständlich gemacht werden können. Mit unserem Fachwissen bewertet die Cyfidelity die Implementierung der Verschleierung in Ihrer Software gründlich und stellen sicher, dass Logik, Struktur und Absichten Ihres Codes effektiv verschleiert werden.

Root-Detection

Rooting bezieht sich auf den Prozess der Erlangung von privilegiertem Zugriff (Root-Zugriff) auf das Betriebssystem eines mobilen Geräts. Bei der Root-Erkennung wird geprüft, ob ein Gerät gerootet wurde oder nicht. Sie wird eingesetzt, um zu erkennen, ob ein Benutzer das Betriebssystem seines Geräts manipuliert hat. Gerootete Geräte können ein Sicherheitsrisiko darstellen, da bösartige Anwendungen oder Angreifer erweiterte Rechte erlangen und dadurch unbefugten Zugang zu den internen Dateien einer App erhalten. Durch die Implementierung der Root-Detection kann eine Anwendung Maßnahmen ergreifen, um die Funktionalität einzuschränken oder den Zugriff auf gerootete Geräte zu verweigern, wodurch das Risiko eines unbefugten Zugriffs verringert und bestimmte Arten von Angriffen abgewehrt werden. Im Rahmen des mobilen Tests versucht die Cyfidelity diese Funktionalität zu umgehen.

Certificate-Pinning

Das Certificate-Pinning ist eine Technik, die dazu dient, die Authentizität und Integrität des digitalen Zertifikats eines Servers während des Aufbaus einer sicheren Verbindung (HTTPS) zwischen einer mobilen Anwendung und ihrem Backend-Server sicherzustellen. Dabei wird das Zertifikat des Servers oder sein öffentlicher Schlüssel in der Anwendung fest kodiert oder "gepinnt". Dadurch wird verhindert, dass Angreifer Man-in-the-Middle-Angriffe (MitM) durchführen können, indem sie ein anderes Zertifikat ersetzen, da die Anwendung nur das angepinnte Zertifikat akzeptiert. Das Certificate-Pinning dient dem Schutz vor verschiedenen Angriffen wie dem Abhören von Netzwerken, dem Spoofing von Zertifikaten und dem unbefugten Abfangen von Daten. Wie bei der Root-Detection versucht die Cyfidelity im Rahmen des mobilen Tests diese Funktionalität zu umgehen.

4.8 Produkt / Code Review

Ein Produkt Pentest ist, wie bei Web und Mobile Applikationen, geeignet, um Sicherheitslücken in einer Anwendung zu finden und zu minimieren. Dabei versucht die Cyfidelity eine möglichst große Testabdeckung zu erreichen mit dem Ziel Sicherheitslücken und Risiken in Ihrer Anwendung zu identifizieren. Um dies möglichst effizient und vollumfänglich gewährleisten zu können, empfiehlt die Cyfidelity eine Bereitstellung des Source Codes. Bei einer Überprüfung der Anwendungssicherheit kann auch eine dynamische Überprüfung durchgeführt werden. Das Vorgehen von Cyfidelity ist das zu testende Programm bestmöglich zu untersuchen, um eine größtmögliche Testabdeckung zu erreichen.

Fuzzing

Fuzzing ist ein Prozess, um Fehler in Programmen finden zu können. Es hat sich in den letzten Jahren gezeigt, dass Fuzzing sehr effizient ist, um Sicherheitslücken zu finden. Beim Fuzzing werden korrekte Eingaben in ein Programm zufällig mutiert und an das getestete Programm gesendet. Mit verschiedenen Mitteln wird nun das Verhalten des Programms untersucht, deren Eingaben beobachtet und im Fehlerfall genauer überprüft. Fuzzing ermöglicht aufgrund der Geschwindigkeit dieser Vorgehensweise eine große Testabdeckung und somit Risikominimierung für unsere Kunden. Es werden von uns Fuzzer verwendet, um automatisiert das Programm zu verwenden. Diese werden auf das jeweilige Produkt angepasst, um so die Effektivität zu maximieren.

Manuelle Tests

Zusätzlich dazu wird das Programm manuell getestet und mit Hilfe von etwa Debuggern oder Dynamic-Binary-Instrumentation wird das Verhalten überprüft, um bestmöglich unsere Expertise ausnutzen zu können. Gefundene Fehler werden analysiert, um eine genaue Überprüfung möglicher Fehler, Sicherheitslücken sowie ihre Auswirkungen und Risiken geben zu können. Dies beinhaltet - wenn erforderlich - die Erstellung von Proof-of-Concept Exploits.

Vorgehensweise

Bei einer Überprüfung fokussiert Cyfidelity sich normalerweise auf die häufigsten Fehler, welche die Sicherheit des Systems beeinträchtigen können:

- Fehler in Identifikation, Authentifizierung und Zugriffskontrolle
- Datenvalidierung
- unzureichende Fehlerbehandlung
- Session Management
- Security Konfiguration
- Logging
- Verschlüsselung
- potenzielle Offenlegung sensibler Daten
- Injection Flaws (z.B. Buffer Overflows)
- Netzwerk Architektur

Code Review

Ein Secure Code Review ist eine Statische Analyse. Dies ist ein manueller oder automatisierter Prozess, um Fehler und Sicherheitslücken im Source Code von Anwendungen zu finden. Es kann generell zwischen zwei Art von Code Reviews unterschieden werden, automatisiert oder manuell:

- Ein automatisierter Review verwendet Tools, um mit Hilfe von vorher festgelegten Regeln Fehler zu finden. Dieses Vorgehen ist schnell hat aber den Nachteil, dass die Intention des Entwicklers und die Business Logik nicht in Betracht gezogen werden können.
- Ein manueller Review wird von einem Menschen durchgeführt, der Zeile für Zeile den Code durchgeht. Ein Mensch kann dabei auch auf den Kontext eingehen und hat ein Verständnis für etwa die Intention und, falls vorhanden, Spezifikation. Die ermöglicht, eine gründliche Prüfung die strategisch nach spezifischen Problemen suchen kann. Manuelle Reviews können mit Source Code oder in Form eines Binary Review (Reverse Engineering) durchgeführt werden. Ein manueller Review ist sehr zeitaufwendig, hat aber den Vorteil, dass etwa Business Logik Fehler auffindbar sind, die nicht durch automatische Tests gefunden werden können.

Zusätzlich bringt ein Secure Code Review folgende Vorteile:

- Verringerung von Risiken und Eintrittswahrscheinlichkeiten
- Erhöhen von Vertrauen in verwendete Software
- Erhöhen von Sicherheitsbewusstsein von Entwicklern
- Begleitung des Entwicklungsprozesses

4.9 Purple Teaming

Das Purple Teaming der Cyfidelity ist ein moderner, kooperativer Ansatz zur Verbesserung der Cyberabwehr, der die Angriffstechniken eines Red Teams mit den Abwehrstrategien eines Blue Teams kombiniert. Während klassische Red Team Assessments oft eine einseitige Simulation von Angriffen darstellen und das Blue Team lediglich reaktiv auf diese Angriffe reagiert, setzt Purple Teaming auf eine enge Zusammenarbeit beider Teams.

Das Ziel ist es, die Effektivität der Sicherheitsmaßnahmen in Echtzeit zu überprüfen und kontinuierlich zu verbessern. Während des Assessments wird das Blue Team in den Prozess eingebunden und erhält direkte Einblicke in die Angriffsstrategien des Red Teams. Dadurch wird nicht nur die Sicherheitslage des Unternehmens optimiert, sondern es findet auch ein wertvoller Know-how-Transfer statt, der langfristig die Resilienz der IT-Sicherheitsstrukturen stärkt.

Purple Teaming ist besonders sinnvoll für Unternehmen, die ihre Detektions- und Reaktionsmechanismen nicht nur testen, sondern aktiv verbessern wollen. Es ist ein iterativer Prozess, bei dem jede Angriffstechnik sofort analysiert und gemeinsam mit dem Blue Team Gegenmaßnahmen erarbeitet werden. Diese praxisnahe Schulung verbessert die Fähigkeit des Unternehmens, realen Cyberangriffen effektiv entgegenzuwirken.

Ziele des Purple Teaming

Purple Teaming verfolgt mehrere zentrale Ziele, die zur nachhaltigen Stärkung der Cybersecurity-Strategie eines Unternehmens beitragen:

1. Verbesserung der Sicherheitslage

Durch die Simulation realer Angriffsszenarien werden bestehende Sicherheitsmaßnahmen gezielt auf ihre Wirksamkeit getestet. Dabei wird überprüft, ob die vorhandenen Detektions- und Reaktionsmechanismen effektiv greifen oder ob Angriffe unentdeckt bleiben.

2. Förderung der Zusammenarbeit

Die enge Zusammenarbeit zwischen Red und Blue Team fördert den Austausch von Wissen und Best Practices. Anstatt dass das Blue Team nur nachträglich auf Angriffe reagiert, lernt es direkt während des Assessments die Angriffstechniken kennen und kann in Echtzeit Abwehrstrategien entwickeln.

3. Optimierung der Abwehrstrategien

Durch den iterativen Prozess von Angriff und Verteidigung werden die bestehenden Sicherheitsmechanismen analysiert und verbessert. Fehlkonfigurationen, Schwachstellen und ineffektive Schutzmaßnahmen werden identifiziert und optimiert.

4. Erhöhung der Cyber-Resilienz

Die enge Verzahnung von Angriff und Verteidigung bereitet Unternehmen auf reale Bedrohungen vor. Durch praxisnahe Simulationen werden Incident-Response-Prozesse trainiert und die Fähigkeit zur schnellen Reaktion auf Cyberangriffe gestärkt.

Vorgehensweise im Purple Teaming

Ein Purple Team Assessment besteht aus mehreren aufeinander abgestimmten Phasen. Diese sind flexibel und werden an die individuellen Bedürfnisse und technischen Gegebenheiten des Unternehmens angepasst.

1. Zieldefinition & Planung

In einem initialen Workshop werden die spezifischen Ziele des Assessments festgelegt. Dabei wird unter anderem definiert:

- Welche Angriffsvektoren und Szenarien untersucht werden sollen
- Welche Sicherheitsmechanismen getestet und optimiert werden
- Welche Eskalationsinstanzen im Falle kritischer Schwachstellen greifen
- Wie die Zusammenarbeit zwischen Red und Blue Team konkret gestaltet wird

Da Purple Teaming eine enge Kooperation erfordert, wird im Vorfeld ein Kommunikationsrahmen definiert, der regelmäßigen Austausch und die direkte Interaktion zwischen den Teams ermöglicht.

2. Aufklärung & Angriffsoberflächen-Analyse

Bevor Angriffe simuliert werden, sammelt das Red Team Informationen über die Zielumgebung. Diese Phase beinhaltet:

- OSINT (Open Source Intelligence): Analyse öffentlich verfügbarer Daten, um potenzielle Angriffsvektoren zu identifizieren
- Threat Intelligence: Untersuchung aktueller Bedrohungslagen und bekannter Schwachstellen in der Unternehmensinfrastruktur
- Social Engineering: Bewertung der Anfälligkeit der Mitarbeitenden für gezielte Angriffe, wie z. B. Phishing

Diese Erkenntnisse bilden die Grundlage für die anschließenden Angriffssimulationen.

3. Durchführung von Angriffen & Echtzeit-Kollaboration

Das Herzstück des Purple Teamings ist die koordinierte Durchführung von Angriffstechniken und die direkte Zusammenarbeit mit dem Blue Team. Dabei werden verschiedene Angriffsszenarien durchgespielt, unter anderem:

- Initialer Zugang: Simulation realer Angriffsmethoden zur Kompromittierung von Endgeräten oder Benutzerkonten
- Laterale Bewegung: Analyse, wie sich ein Angreifer innerhalb des Netzwerks ausbreiten könnte

- Privilege Escalation: Test, ob es möglich ist, administrative Rechte zu erlangen
- Datendiebstahl-Simulation: Bewertung, wie gut kritische Daten vor unbefugtem Zugriff geschützt sind

Der entscheidende Unterschied zum klassischen Red Teaming liegt darin, dass alle Angriffe in enger Abstimmung mit dem Blue Team erfolgen. Nach jedem durchgeführten Angriff wird das Ergebnis direkt analysiert und gemeinsam mit dem Blue Team Optimierungsmaßnahmen erarbeitet. Dadurch kann das Unternehmen seine Sicherheitsmaßnahmen in Echtzeit verbessern.

4. Dokumentation & Maßnahmenplanung

Während des gesamten Assessments werden die durchgeführten Tests sowie die identifizierten Schwachstellen und Verbesserungspotenziale dokumentiert. Bereits während der Durchführung erhalten die Verantwortlichen regelmäßige Updates zu den Ergebnissen.

Am Ende des Assessments erstellt Cyfidelity einen detaillierten Abschlussbericht, der folgende Inhalte umfasst:

- Eine chronologische Dokumentation der durchgeführten Angriffsszenarien
- Eine Bewertung der Wirksamkeit bestehender Sicherheitsmaßnahmen
- Konkrete Empfehlungen zur Optimierung der Abwehrstrategien
- Eine Priorisierung der identifizierten Risiken und Maßnahmen

Zusätzlich präsentieren unsere Experten die Ergebnisse in einem abschließenden Meeting und stehen dem Unternehmen beratend zur Seite, um die Umsetzung der vorgeschlagenen Maßnahmen zu begleiten.

Purple Teaming bietet einen einzigartigen Ansatz zur Verbesserung der IT-Sicherheit, da es die klassische Trennung zwischen Angriffs- und Verteidigungsstrategien aufbricht. Statt lediglich Schwachstellen aufzuzeigen, wird aktiv an der Verbesserung der Abwehrmechanismen gearbeitet.

Durch den direkten Know-how-Transfer zwischen Red und Blue Team profitieren Unternehmen von einem praxisnahen Training, das nicht nur die Sicherheitslage verbessert, sondern auch das Incident-Response-Team stärkt.

Mit Purple Teaming von Cyfidelity erhalten Unternehmen eine maßgeschneiderte Sicherheitsstrategie, die nicht nur auf dem Papier existiert, sondern aktiv auf realistische Bedrohungen vorbereitet.