AWARE7

Servicekatalog

Informationsklassifizierung

SK-0 - PUBLIC
TLP;WHITE

Inhaltsangabe

Über Uns 2
Offensive Services 3
- Penetrationstests 3
- 360 Grad-Analyse 3
- Schwachstellen Scans 4

Awareness 4
- Live Hacking 4
- Phishing 5
- Escape Desk 5

Consulting 6
- Informationssicherheits-Consulting 6
- Informationssicherheitsmanagementsystem 6
- Externer Informationssicherheitsbeauftragter 7

Education 7
- E-Learning 7
- T.I.S.P. - TeleTrusT Information Security Professional 8
- Workshops 8
- Seminare 9
- Schulungen 9

Projektreise Beispiel 10
Kontakt 11

Über Uns

Die AWARE7 GmbH ist ein ISO/IEC 27001 zertifiziertes Unternehmen im Bereich der Informationssicherheit aus Gelsenkirchen, das Technologien und Produkte entwickelt sowie Dienstleistungen anbietet, die zur Förderung, Steigerung und Erhaltung des IT-Sicherheitslevels dienen. Durch die praktische Arbeit und die regelmäßige Veröffentlichung von wissenschaftlichen Artikeln gelingt es uns, komplexe Betrugs- und Angriffsmethoden zu erklären um Unternehmen, Behörden und Personen zu schützen.

IT-Sicherheit funktioniert nur, wenn die Technik sicher und die Menschen sensibilisiert sind. Komplexe Angriffe nutzen menschliche Schwachstellen in Kombination mit technischen Sicherheitslücken aus. Betrachten Sie das IT-Sicherheitsniveau in Ihrem Unternehmen ganzheitlich. Auf menschlicher und technischer Ebene.

Die AWARE7 GmbH hat Ihren Hauptsitz in Gelsenkirchen. Im Wissenschaftspark Gelsenkirchen werden ca. 500qm Bürofläche für die Durchführung von professionellen IT-Sicherheitsdienstleistungen gebracht. Das Unternehmen wurde 2018 von Dr.-Ing. Matteo Große-Kampmann und Chris Wojzechowski gegründet. Mit über 300 Live Hacking Shows im Jahr, mehreren Dutzend Penetrationstests und diversen weiteren Projekten leistet die AWARE7 einen entscheidenden Beitrag für mehr Informationssicherheit in der Region und darüber hinaus.

OFFENSIVE SERVICES

PENETRATIONSTEST

Mit unseren Penetrationstests können unsere Kunden ihr Informationssicherheitsniveau einstufen. Unsere Pentester testen das System oder die Infrastruktur auf Schwachstellen und setzen im Anschluss Maßnahmen, um diese zu schließen. Einen Pentest unterscheiden wir grob von einem externen und einem internen Test. Ein externer Test sollte durchgeführt werden, damit das Unternehmen einen Überblick über die externe Angriffsfläche erhält. Bei dem internen Test geht es primär darum, wie Fremde sich Zugang zum Gebäude verschaffen können und wie Mitarbeiter unbefugte Zugriffe erlangen können. Alle Unternehmen, bei denen ein digitaler Kommunikationsweg besteht und welche Dokumente digital verwalten sollten diese regelmäßig durchführen. Wir führen den Test Remote mit einer konfigurierten Pentest-Box durch oder bei Ihnen vor Ort. Dadurch sind wir flexibel und können Länderübergreifend testen. Wir brauchen vorab Informationen über die zu testenden Systeme, da wir auf Basis dieser ein Angebot erstellen. In dem Erstgespräch nimmt bereits einer unserer Experten teil und schätzt den Aufwand Ihres Angebots mit dem Vertrieb im Abschluss ab. Ein Penetrationstest ist kein einmaliger Vorgang, sondern sollte regelmäßig durchgeführt werden. Die Einschätzung des Sicherheitsniveaus liegt zu dem Zeitpunkt vor, zu dem getestet wurde. Bereits einige Tage später entspricht dies nicht mehr dem aktuellen Stand.

Anzahl Personen Tage (PT)

Unsere Penetrationstest haben einen Umfang von 3 bis zu über 100 Personentagen.
In der Regel wird ein gängiger Test zwischen 3 und 15 PT eingeordnet.

360 GRAD-ANALYSE

Die 360 Grad-Analyse dient als überschaubarer Gesamtüberblick über das Informationssicherheitsniveau eines Unternehmens. Diese sollte durchgeführt werden, wenn das Unternehmen zu einem überschaubaren Festpreis eine Einschätzung über die möglichen Angriffsflächen erhalten möchte. Diese kann sowohl Auskunft über die externe als auch die interne Angriffsfläche bereitstellen. Die Dienstleistung wird remote durchgeführt und kann daher weltweit verkauft werden. Der Bericht erfolgt auf Englisch oder Deutsch. Gerade als Einstieg dient diese Vorgehensweise als sinnvoll und sollte mit einem erweiterten Penetrationstest kontinuierlich durchgeführt werden.

Anzahl Personen Tage (PT)

6 PT

SCHWACHSTELLENSCAN

Bei einem Schwachstellen Scan lassen wir automatisierte Tools über das von Kunden gewünschten System laufen und erstellen aus diesem Scan einen Bericht. Hier wird ebenfalls eine Einschätzung über das Sicherheitsniveau gegeben, allerdings ist diese nicht so verlässlich wie ein tiefgehender Pentest. Ein Schwachstellen Scan sollte durchgeführt werden, um einen groben Überblick über die Sicherheit der Systeme zu erlangen. Zum einen schafft dieser bei sehr großen Systemen einen Überblick, wodurch man sich im Anschluss auf die kritischen Schwachstellen fokussieren kann. Zum anderen ist dieser wesentlich kostengünstiger und daher auch in kleinen Unternehmen angebracht. Die Scans werden ausschließlich Remote durchgeführt und können dadurch weltweit an den Kunden gebracht werden. Oft sind zu große Systeme ein Grund für Schwachstellen Scans, da diese den tatsächlichen Aufwand eines Pentests minimieren können. Da die Systeme des Kunden sich meist in einem stetigen Wandel befinden, sollten diese genau wie die Pentests regelmäßig durchgeführt werden.

Anzahl Personen Tage (PT)
1,5 PT

AWARENESS

LIVE HACKING

Bei einer Live Hacking Show zeigen wir die Vorgehensweise von Angreifern live auf. Die Shows sind informativ und unterhaltsam zugleich. Eine Live Hacking Show öffnet vielen Mitarbeitern oft die Augen, wie schnell ein Angriff tatsächlich stattfinden kann. Jedes Unternehmen, welches seine Mitarbeiter mit dem Thema vertraut machen und Gefahren aufzeigen möchte, sollte eine solche Show durchführen. Die Live Hacking Show kann vor Ort oder Remote stattfinden und ist daher auf der ganzen Welt durchführbar. Die Sprachen sind allerdings auf Deutsch und Englisch begrenzt. Da sich die Angreifer weiterentwickeln und neue Betrugsmaschen zum Vorschein kommen, sollten Live Hacking Shows in regelmäßigen Abständen stattfinden.

Anzahl Personen Tage (PT)
2 PT

Individualisierung
2 PT

PHISHING

Mithilfe unserer Phishing Simulationen können die Mitarbeiter unserer Kunden auf aktuelle Bedrohungen per E-Mail vorbereitet werden. Phishing Mails sind das größte Einfallstor für Hacker, da ca. 77 % der erfolgreichen Angriffe durch eine E-Mail starten. Jedes Unternehmen, welches E-Mails als Kommunikationsweg verwendet, sollte solche Simulationen durchführen. Da die Dienstleistung online stattfindet, können die Simulationen weltweit vertrieben werden. Da diese Angriffe auf aktuellen Begebenheiten beruhen, sollten diese kontinuierlich durchgeführt werden.

Anzahl Personen Tage (PT)

Je nach Mitarbeiteranzahl

ESCAPE DESK

Der Escape Desk funktioniert wie ein Escape Room, ist jedoch auf den Schreibtisch begrenzt. Hier können die Mitarbeiter unserer Kunden Rätsel mit Bezug auf die Informationssicherheit lösen, um das Thema interaktiv und unterhaltsam zu verinnerlichen. Der Escape Desk begeistert in der Regel auch die Mitarbeiter, die sich in dem Thema Informationssicherheit nicht wiederfinden. Gerade auf Messen oder Veranstaltungen ist dieser gut platziert und sorgt aufgrund der außergewöhnlichen Awareness Maßnahme für großes Aufsehen. Die Dienstleistung kann durch uns durchgeführt werden, indem wir mit dem Equipment anreisen, allerdings kann dieses auch per Post versendet werden. Daher ist der Escape Desk in ganz Deutschland, Österreich und der Schweiz einsetzbar. Gerade um Menschen für das Thema zu begeistern, die vorher kein Interesse gezeigt haben, eignet sich die Maßnahme gut, um immer wieder frischen Wind in das Thema zu bringen.

Anzahl Personen Tage (PT)

2 PT

Individualisierung

2 PT

CONSULTING

INFORMATIONSSICHERHEITS-CONSULTING

Wir beraten unsere Kunden bei dem Aufbau eines Informationssicherheitsmanagementsystems und unterstützen auf dem Weg zu Zertifizierungen wie der ISO 27001 und dem BSI Grundschutz. Ein externer ISB kann ohne die Betriebsblindheit vollkommen unabhängig die Informationssicherheit in Ihrem Unternehmen betrachten. Jedes Unternehmen, welches digital aufgestellt ist, sollte wissen, wo die Risiken liegen und wie diese zu bewältigen sind. Über ein bestimmtes Beratungskontingent können wir den Unternehmen monatlich ein gewisses Maß an Unterstützung diesbezüglich bieten. Da das Unternehmen in der Regel wächst und die Infrastruktur sich verändert, sollte dies ein durchgehender Prozess sein, welcher dauerhaft im Einsatz ist. Die Beratung kann auf Deutsch oder Englisch weltweit durchgeführt werden.

Anzahl Personen Tage (PT)

Individuell - je nach Unternehmensgröße und Stand des aktuellen ISMS

INFORMATIONSSICHERHEITSMANAGEMENTSYSTEM (ISMS)

Informationssicherheit planen, organisieren und kontinuierlich erhöhen. Diese Ziele werden mit dem Auf- und Ausbau eines Informationssicherheitsmanagementsystems (ISMS) verfolgt. Ein ISMS verbessert und überwacht die Informationssicherheit in einem Unternehmen in Form von maßgebenden Richtlinien, umfangreichen Methoden und optimierten Prozessabläufen. Unsere Kunden werden zum Beispiel bis zu einer ISO 27001 Zertifizierung und darüber hinaus begleitet. Die permanente Überwachung, Messung und Erhöhung des Reifegrades der Informationssicherheit sind das Ziel, welches mit den Kunden verfolgt und umgesetzt wird.

Anzahl Personen Tage (PT)

Individuelle - je nach Unternehmensgröße und Stand des aktuellen ISMS

EXTERNER INFORMATIONSSICHERHEITSBEAUFTRAGTER (ISB)

Durch die Berufung eines externen Informationssicherheitsbeauftragten (ISB) können Unternehmen aktive Hilfe in Anspruch nehmen, um Risiken zu identifizieren und geeignete Maßnahmen zu ergreifen. Weiterhin können Sie Ihre Daten und Systeme vor Bedrohungen schützen. Die Beratung durch den ISB umfasst dabei nicht nur technische Aspekte wie Netzwerksicherheit oder Datenverschlüsselung, sondern auch die Erstellung von Notfallplänen für den Fall eines Angriffs. Zudem empfiehlt der ISB Schulungen für ihre Mitarbeitenden, um das Sicherheitsbewusstsein zu erweitern. Dazu gehören auch Aktivitäten wie die Identifizierung von Sicherheitsrisiken, die Durchführung von Sicherheitsaudits, die Überwachung von Sicherheitsvorfällen und die Einhaltung von Sicherheitsstandards. Die externen ISB der AWARE7 verfügen über ein vielschichtiges Netzwerk und haben unzählige Verbindungen zu Anbietern und Branchenexperten. Der Einsatz eines externen ISB erfolgt grundsätzlich remote. Bei einem individuell notwendigen Bedarf können auch Termine vor Ort durchgeführt werden. In der Kommunikation wird daher vornehmlich auf E-Mail, Telefonate und Videokonferenzsysteme gesetzt. Somit gestaltet sich eine Zusammenarbeit flexibel und effizient.

Anzahl Personen Tage (PT)

Individuell - je nach Unternehmensgröße und Stand des aktuellen ISMS

EDUCATION

E-LEARNING

Unser Cyberschutzraum ermöglicht den Unternehmen und deren Mitarbeitern durch E-Learning Kurse die Thematik der Informationssicherheit zu verinnerlichen und sich gegen Angriffe sicher aufzustellen. Eine E-Learning Plattform schafft Zugang zur kontinuierlichen Weiterbildung der Mitarbeiter. Alle Unternehmen, welche keinen klaren Überblick über das Informationssicherheitsniveau der Mitarbeiter haben, sollten diese stetig trainieren. Da die Kurse online stattfinden und lediglich Zugangsdaten übermittelt werden, können diese in ganz Deutschland, Österreich und der Schweiz vertrieben werden. Diese Maßnahme ist besonders wichtig, um die Sensibilität der Mitarbeiter langfristig zu steigern und zu trainieren.

Anzahl Personen Tage (PT)

Je nach Mitarbeiteranzahl

T.I.S.P. - TELETRUST INFORMATION SECURITY PORFESSIONAL

Der T.I.S.P. ist ein Personenzertifikat, welches ein hohes Niveau der Informationssicherheit zum Ausdruck bringt. Unsere Kunden erwartet ein breit gefächertes Themenfeld und realitätsnahe Einblicke durch Fachreferenten aus der Praxis und Forschung. Es handelt sich um das einzige deutschsprachige Expertenzertifikat im Bereich der Informationssicherheit und stellt das deutsche Pendant zum Certified Information Systems Security Professional (CISSP) dar. Als anerkannter Schulungsanbieter bieten wir unseren Kunden die T.I.S.P. Vorbereitungsschulung ausschließlich online an.

Anzahl Personen Tage (PT)

2,5 PT

WORKSHOPS

Unsere Workshops bestehen zu einem großen Teil aus der aktiven Mitarbeit der Teilnehmer, einer Gruppenarbeit oder einer praktischen Übung. Das erlernte Wissen umzusetzen steht im Vordergrund. Die Workshops können sowohl remote als auch vor Ort durchgeführt werden. Thematisch bieten wir Workshops zu Themen wie Pentesting oder der Shodan Suchmaschine an. Es besteht aber auch die Möglichkeit die Inhalte an die Bedürfnisse unserer Kunden anzupassen.

Anzahl Personen Tage (PT)

2.5 PT

In den PT sind auch Vor- und Nachbereitung enthalten.

Dauer

3 Stunden

Jede weitere Stunde wird einzeln berechnet.

Stundensatz - 168.75 €

Individualisierung

2 PT

SEMINARE

Bei unseren Seminaren wird eine Weiterbildung auf der Basis von Grundkenntnissen durchgeführt. Hier liegt der Fokus auf dem zu vermittelnden Inhalt, der einer Unterrichts- oder Vorlesungseinheit gleicht. Seminare können intern oder extern absolviert werden. Sie sollen das richtige Handeln der Mitarbeitenden fördern, um beispielsweise einer Cyberattacke richtig begegnen zu können.

Anzahl Personen Tage (PT)

2.5 PT

In den PT sind auch Vor- und Nachbereitung enthalten.

Dauer

3 Stunden

Jede weitere Stunde wird einzeln berechnet.

Stundensatz - 168.75 €

Individualisierung

2 PT

SCHULUNGEN

Um das Sicherheitsbewusstsein eines Mitarbeitenden zu erhöhen sind regelmäßige Mitarbeiterschulungen essenziell. In Schulungen wird standardisiertes Wissen in Form von Frontalunterricht vermittelt. Diese zu Planen und Durchzuführen ist zeitaufwendig. Diesen Zeitaufwand nehmen wir Ihnen gerne ab, indem wir Mitarbeiterschulungen in Abstimmung mit Ihnen durchführen. So kann die Wahrnehmung in Bezug zu Risikofaktoren sowie das Einhalten von Maßnahmen gefördert werden. Je nach Ausmaß und Ziel der Mitarbeiterschulungen können sich diese über mehrere Tage erstrecken. Die Schulungen können sowohl vor Ort als auch remote stattfinden.

Anzahl Personen Tage (PT)

2.5 PT

In den PT sind auch Vor- und Nachbereitung enthalten.

Dauer

3 Stunden

Jede weitere Stunde wird einzeln berechnet.

Stundensatz - 168.75 €

Individualisierung

2 PT

PROJEKTREISE BEISPIEL

LIVE HACKING SHOW

Beginnen Sie Ihre Reise, indem Sie die Grundlagen der Cyber-Sicherheit verstehen. In diesem ersten Schritt geben wir Ihrem Unternehmen einen ersten Eindruck in die faszinierende Welt der Hacker. Durch die Live Hacking Show erfahren Sie, wie ein Angriff entsteht, welche Schwachstellen ausgenutzt werden und wie Sie sich effektiv dagegen schützen können.

PHISHING SIMULATION

Im ersten Schritt haben wir Sie sensibilisiert für Bedrohungen und mit dem Wissen ausgestattet die Gefahren von betrügerischen E-Mails und Websites zu erkennen. Im zweiten Schritt ihrer Reise testen wir das theoretische Wissen mit einer Phishing Simulation. Da Phishing oft der erste Schritt in einem Hackerangriff ist, sollte Sie den Ablauf und die Konsequenzen von Phishing-Angriffen erkennen und verstehen. In der Simulation wird aufgezeigt wie ein Angriff aussieht und was beim Opfer ankommt.

E-LEARNING

Im nächsten Abschnitt Ihrer Servicereise empfehlen wir unsere E-Learning-Plattform. Hier wird Ihren Mitarbeitern die Möglichkeit geboten, ihr Wissen zu festigen, ihren Fähigkeiten im Umgang mit Phishing-Angriffen zu verbessern und sich kontinuierlich weiterzubilden. Auf unserer E-Learning-Plattform bieten wir Ihnen die Werkzeuge und Ressourcen, um sich effektiv vor Cyberbedrohungen zu schützen und Ihre digitale Sicherheit zu stärken.

PENETRATIONSTEST

Schützen Sie sich auch vor potenziellen Angreifern, indem Sie proaktiv handeln, Ihre Verteidigung stärken und Einfallstore für Angreifer eliminieren. Unsere Penetrationstests zielen darauf ab, sowohl menschliche als auch technische Sicherheitslücken aufzudecken und zu schließen. Unsere Experten simulieren realistische Angriffsszenarien, um Schwachstellen in Ihren Systemen aufzudecken und Ihnen konkrete Empfehlungen zur Verbesserung Ihrer Sicherheitsmaßnahmen zu geben.

CONSULTING

Um Ihre Projektreise abzurunden, erhalten Sie regelmäßigs Consulting für die Planung angemessener neuer Maßnahmen. Von der Risikobewertung bis hin zur Implementierung von Sicherheitslösungen, wir unterstützen Sie dabei, die richtigen Entscheidungen zu treffen und Ihre individuelle digitale Infrastruktur zu schützen. Wir beraten Sie, um Ihre Informationssicherheit kontinuierlich zu verbessern und sich gegen aktuelle und zukünftige Bedrohungen zu verteidigen.

KONTAKT

Nehmen Sie jetzt Kontakt mit uns auf!
→ anfrage@aware7.de

Chris Wojzechowski
Geschäftsführender Gesellschafter

+49 209 88306761
+49 170 4113255
chris@aware7.de

Jan Hörnemann
Chief Operating Officer

+49 209 88306762
+49 170 4113255
jan@aware7.de

AWARE7 GmbH
Munscheidstraße 14
45886 Gelsenkirchen
info@aware7.de