MEDIALINE

IT Security

Security Awareness Prozess

Cyberangriffe haben existenzielle Konsequenzen für Unternehmen

Die Mitarbeitenden werden als vermeintlich schwächstes Glied des IT-Sicherheitskonzepts von Unternehmen angesehen. Deswegen sind sie die ersten Opfer von Angriffen und damit die Türöffner in die Unternehmens-IT.

Der Medialine Cyber Security Awareness Prozess wurde für diese Herausforderung entwickelt und konzipiert. Er dient als wirkungsvolle Methode die Security Awareness der Mitarbeitenden zu erhöhen. Er soll außerdem dabei helfen eine nachhaltige Security Awareness Strategie in Unternehmen zu implementieren und bei allen Mitwirkenden das Bewusstsein über verschiedene Sicherheitsrisiken zu verinnerlichen und zu steigern. Denn je höher das Sicherheitsbewusstsein bei den Mitarbeitenden ist, desto besser ist die Tragweite der eigenen Sicherheitsverantwortlichkeit. Durch den Cyber Security Awareness Prozess sind die Mitarbeitenden kein Risiko mehr, sondern werden ein entscheidender Teil des IT-Sicherheitskonzeptes.

Ablauf des Cyber Security Awareness Prozesses

Ist-Analyse

Der Medialine Cyber Security Awareness Prozess wurde für diese Herausforderung entwickelt und konzipiert. Er dient als wirkungsvolle Methode die Security Awareness der Mitarbeitenden zu erhöhen. Er soll außerdem dabei helfen eine nachhaltige Security Awareness Strategie in Unternehmen zu implementieren und bei allen Mitwirkenden das Bewusstsein über verschiedene Sicherheitsrisiken zu verinnerlichen und zu steigern. Denn je höher das Sicherheitsbewusstsein bei den Mitarbeitenden ist, desto besser ist die Tragweite der eigenen Sicherheitsverantwortlichkeit. Durch den Cyber Security Awareness Prozess sind die Mitarbeitenden kein Risiko mehr, sondern werden ein entscheidender Teil des IT-Sicherheitskonzeptes.

Workshops:

Die Workshops dienen dazu, eine erste Sensibilisierung bei den Beteiligten hervorzurufen. Hier werden unterschiedlichste Abteilungen, in allen Geschäftsfeldern und -ebenen über aktuelle Cyber-Risiken aufgeklärt, es werden beispielhaft entstandenen Kosten und Konsequenzen vorgestellt und außerdem unterschiedliche IT-Sicherheitsthemen besprochen.

Grobkonzepterstellung

Auf Basis der Erkenntnisse aus der Analyse-Phase und den Workshops entwickeln unsere Awareness Beauftragten ein Security Awareness Konzept, welches auf die individuellen Gegebenheiten und Bedürfnisse zugeschnitten ist. Darin werden verschiedene Vorgehensweisen, Kampagnen und Maßnahmen vorgestellt, um die Security Awareness im Unternehmen maßgeblich zu steigern und so Sicherheitsrisiken effektiv zu minimieren.

Entscheidung

Nach der Präsentation durch unsere Security Awareness Beauftragten folgt eine gemeinsame Abstimmung, welche Maßnahmen umgesetzt werden sollen. Dazu wird ein Zeitplan erarbeitet, in welchem die Durchführung der ausgewählten Kampagnen und Maßnahmen abgestimmt wird.

Maßnahmen

Die vereinbarten Maßnahmen werden gemeinsam mit unseren Security Experten vorbereitet, durchgeführt und ausgewertet. Die Maßnahmen können beispielsweise sporadische Phishing-E-Mail-Kampagnen oder wiederkehrende E-Learnings sein.

Monatliche wiederkehrende Leistungen

Managed Hornetsecurity SAT-Portal

Mit der Security Awareness Suite erhalten Kunden ein umfassendes Security Awareness Training. Dabei werden zur Trainingssteuerung verschiedene Automatisierungen in Form der Awareness Engine und der Spear Phishing-Engine eingesetzt. Auf diese Weise werden Mitarbeiter bedarfsgerecht trainiert, um Cyber-Angriffe sicher zu erkennen und effektiv abzuwehren – ohne, dass sich Administratoren oder CISOs selbst in die zugrundeliegende Psychologie und Didaktik einarbeiten müssen. Die Grundlage des Awareness Trainings bildet ein patentiertes Verfahren zur Messung des Sicherheitsverhaltens aller am Security Awareness-Training teilnehmenden Gruppen und Benutzer. Auf Basis des gemessenen Sicherheitsverhaltens wird die wissenschaftliche Kennzahl Employee Security Index (ESI®) sowie der Trainings KPI berechnet. Spear-Phishing-E-Mails werden in verschiedenen Schwierigkeitsgraden versandt. Das Managed SAT-Portal setzt eine Nutzung des Mail-Security-Dienstes von Hornetsecurity voraus.

Network Box einmalige Managed Phishing Kampagne Stufen 1+2

In diesem Programm werden Phishing-Attacken in einem vorher definierten Rahmen simuliert. Die Details zum Nutzerverhalten werden ausschließlich für die Auswertung der Kampagne verwendet.

Network Box Awareness eLearning-Modul

In diesem Modul werden Ihre Mitarbeitenden in den Grundlagen der IT-Sicherheit geschult. Themenbereiche sind unter anderem: Clear Desk, Passwortmanagement, sicheres Surfen, Phishing und 2-Faktor-Authentifizierung.

Network Box Managed Phishing Kampagne Stufen 1+2+eLearning

Dieses Modul kombiniert die zwei angebotenen monatlichen Leistungen von Network Box. Kunden bekommen 2 Phishing Kampagnen und jeweils Reportings. Zusätzlich werden Teilnehmende durch das eLearning geschult, müssen Prüfungen ablegen und bekommen bei Erfolg Teilnehmerzertifikate. Kunden können außerdem kostenlos auf das Browser Plug-In „NB Detector“ zugreifen, welches vor Fake-Webseiten warnt.

Einmalige Leistungen

Management Impulse Keynote

Ausgerichtet um über Risiken, Vorfälle und Konsequenzen aufzuklären. Außerdem werden klassische Sicherheitstechniken vermittelt und Herausforderungen und To Do's für das Management festgelegt. Neben einem Schwachstellen-Scan gibt es Handlungsempfehlungen für Kunden.

Workshop Situationsanalyse

Dieses Modul kann für unterschiedliche Unternehmensabteilungen ausgelegt werden. Anhand einer Checkliste wird festgestellt in welcher Situation das Unternehmen hinsichtlich seines Informations-Sicherheits-Bewusstseins ist. Hierbei handelt es sich lediglich um eine Bestandsaufnahme. Anhand der Ergebnisse erhält der Kunden ein Grobkonzept als Handlungsempfehlung.

Workshop Grobkonzept und Handlungsempfehlungen

Hier werden Ergebnisse der Situationsanalyse vorgestellt. Außerdem bekommen beteiligte Abteilungen empfohlene Maßnahmen. Wir unterrichten über Kommunikationsmöglichkeiten im Unternehmen und Starten die erste Kampagne mit einem festgelegten Ziel.

Mitarbeiter Awareness-Workshop

Der Workshop basiert auf einer interaktiven Wissensvermittlung. Die Mitarbeitenden werden über Sicherheitsrisiken bei der Benutzung von Endgeräten aufgeklärt. Wir vermitteln Formen, Arten und Möglichkeiten on Social Engineering und gehen auf Motive der Hacker ein. Gleichzeitig werden den Mitarbeitenden Tipps zur Verteidigung und zur Vermeidung von Angriffen bzw. IT-Ausfällen gegeben. Mit der Feedback-Runde und einer Sammlung und Zusammenfassung des Gelernten bekommen die Teilnehmenden eine Übersicht, damit das Sicherheitsbewusstsein auch nach dem Workshop nicht verloren geht. Der Workshop kann sowohl in Präsenz als auch online stattfinden.

Consulting Hornetsecurity SAT

Diese einmalige Leistung schließt sich an einem „Workshop Grobkonzept und Handlungsempfehlung" an Mit dem Hornetsecurity SAT wird eine Kampagne durch einen Medialine Awareness Experten eingerichtet. Durch dieses Cyber Security Awareness Training wird das Risikobewusstsein der Mitarbeitenden geprüft. Anschließend bekommen Sie einen vollständigen Report der Kampagne aufbereitet präsentiert und können passende Maßnahmen auswählen.

Cyber Security Awareness Beauftragte

Cyber Security und Cyber Security Awareness sind tiefgreifende Themengebiete. Damit Kunden mit den aktuellen Herausforderungen nicht allein fertig werden müssen, stellen wir Cyber Security Beauftragte zur Seite.

Leistungsumfang

- IT-Sicherheit in der Unternehmenskultur verankern
- Kampagnen planen und organisieren
- IT-Sicherheit zum Thema der internen Kommunikation machen
- Bewussten Umgang mit digitaler Kommunikation und Internet-Nutzung trainieren
- Trainings, Kurse, Workshops planen und organisieren
- IT-Sicherheits-Beratung des Managements und Führungskreises
- Angstfreie Kultur beim Melden von Cyberangriffe etablieren
- Mitwirkung und Erfassung bei der Analyse von Sicherheitsvorfällen

Stand: 01/2023