Bild: Shutterstock / kentoh

Bewusstsein für Unternehmenssicherheit

Geschulte Mitarbeiter wehren Cyberangriffe ab

Mitarbeiter gelten als Risiko Nummer eins bei Cyberangriffen. Training soll Abhilfe schaffen.

Die E-Mail kam direkt vom Geschäftsführer, mit Ausrufezeichen. Sie war also dringend. Der Betreff: Überweisung von 50.000 Euro auf das Bankkonto eines Dienstleisters in Polen. Der Geldtransfer sei natürlich streng vertraulich und vor allem sehr, sehr eilig, hieß es im Text der E-Mail. Der neue Mitarbeiter, erst seit zwei Wochen in der Buchhaltung des Unternehmens tätig, folgte der Aufforderung und überwies das Geld nach Polen. Das Problem: Die Mail stammte von einem Betrüger, der sich einfach als Geschäftsführer ausgab.

Die Betrugsmethode hinter diesem Szenario ist nicht neu, aber immer öfter anzutreffen und wird von den Kriminellen immer weiter verfeinert. Bekannt ist sie wahlweise unter den Bezeichnungen Chef-Masche, CEO Fraud (Chef-Betrug) oder Business E-Mail Compromise (BEC).

39 %
der Unternehmen in Deutschland wurden bereits Opfer eines Phishing-Angriffs

Quelle: Trend Micro

Die Täter gehen dabei ausgesprochen geschickt vor und nutzen menschliche Eigenschaften wie Hilfsbereitschaft, Empathie oder in diesem Fall Angst vor Autoritäten bewusst aus, um Mitarbeiter zu manipulieren. Um ihr Täuschungsmanöver so glaubwürdig wie möglich zu machen, sammeln sie alles an Informationen über potenzielle Opfer, was sie in die Finger bekommen können.

Fündig werden sie dabei oft über Social Media, wenn sie beispielsweise Meldungen über einen neuen Arbeitgeber auf Facebook oder Twitter auswerten.

Kein Einzelfall

Die Opfer von CEO Fraud sind nicht allein. So wurden in Baden-Württemberg laut Innenminister Thomas Strobl in den letzten vier Jahren 750 Unternehmen mit dieser Masche angegriffen. In rund 90 Fällen waren die Täter erfolgreich und verursachten einen Schaden von rund 50 Millionen Euro. Dem Security-Anbieter Trend Micro zufolge stieg die Zahl dieser heimtückischen und bis ins Detail geplanten Angriffe 2018 um 28 Prozent. Kein Wunder, schließlich verspricht laut Trend Micro jeder CEO-Fraud-Versuch einen Gewinn von durchschnittlich 132.000 Dollar.

Die häufigste Methode für Cyberangriffe auf Unternehmen sind Phishing-Mails, gefälschte E-Mails, mit denen Mitarbeiter hinters Licht geführt werden. Ziel der täuschend echten Mails ist es, die gutgläubigen Opfer dazu zu verleiten, schadhafte Anhänge zu öffnen, auf Links zu Websites mit Schadcode zu klicken oder vertrauliche Informationen preiszugeben.

Im Prinzip geht es um Angriffe auf die Informationssicherheit. Informationen müssen zuverlässig verfügbar sein, da die meisten Geschäftsprozesse mittlerweile digitalisiert sind. Zudem sind sie vor nicht autorisiertem Zugriff (Vertraulichkeit) und ungewollter Veränderung (Integrität) zu schützen.

Die Dimension deutlich macht eine Untersuchung von Trend Micro vom Februar dieses Jahres: Demnach wurden 39 Prozent der befragten Unternehmen aus Deutschland schon einmal Opfer eines Phishing-Angriffs. Und die Anzahl der von Trend Micro geblockten Phishing-URLs stieg im Vergleich zum Vorjahr um 269 Prozent, seit dem Jahr 2015 sogar um fast 2500 Prozent. Für die Studie wurden 1125 IT- und Sicherheitsentscheider im Vereinigten Königreich, den USA, Deutschland, Spanien, Italien, Schweden, Finnland, Frankreich, den Niederlanden, Polen, Belgien und Tschechien befragt.

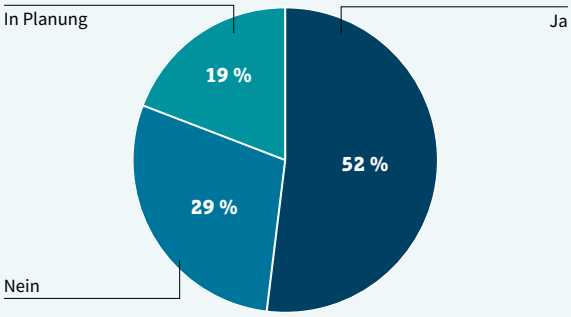
Phishing-Mails haben oft gravierende Folgen für Unternehmen und Organisationen. Wie gravierend, das veranschaulichen zwei Beispiele aus Bayern. Das Krankenhaus Fürstenfeldbruck konnte im November 2018 mehr als eine Woche lang nicht im Normalbetrieb arbeiten und wurde von der integrierten Rettungsstelle abgemeldet. Der Grund: Ein Mitarbeiter infizierte durch einen Klick auf Schad-Software im Mail-Anhang das IT-System und legte alle rund 450 Rechner lahm. Und beim Maschinenbauer KraussMaffei verschlüsselte ein Trojaner Daten, die für die Steuerung einzelner Maschinen in der Fertigung und Montage notwendig sind. Daher konnte das Unternehmen die Maschinen an mehreren Standorten anfangs nicht starten, anschließend liefen sie eine Zeit lang mit gedrosselter Leistung. Auch hier lief der Angriff über eine Phishing-Mail.

Bild: Prof. H. Schmidt

Lernspiele zur Security Awareness: Hier als Beispiel das Spiel „What_The_Hack“, entwickelt an der Hochschule Düsseldorf.

BSI-Lagebericht 2018

„Wird das Personal in regelmäßigen Abständen in Bezug auf die IT-Sicherheit geschult und die Durchführung dieser Schulungen dokumentiert?“



Security Awareness: Gut die Hälfte der deutschen Unternehmen setzt bereits auf entsprechende Schulungen.

com! professional 7/19

Quelle: BSI „Die Lage der IT-Sicherheit in Deutschland 2018“, n = ca. 900

Mitarbeiter als schwächstes Glied

„Phishing-Angriffe können mit relativ wenig Aufwand große Schäden verursachen, da sie auf die Schwachstelle Mitarbeiter zielen. Rund 90 Prozent aller Angriffe haben ihren Ursprung beim Nutzer, da er den einfachsten Angriffspunkt und damit auch das größte Risiko für die IT-Sicherheit darstellt“, erklärt Richard Werner, Business Consultant bei Trend Micro. „Ein einfacher Klick genügt, und die Schad-Software wird im System verbreitet. Oft hilft zwar der gesunde Menschenverstand weiter. Firmen müssen aber zusätzlich ihre Mitarbeiter über Bedrohungen aufklären und ihnen zeigen, wie sie in derartigen Fällen richtig reagieren. Es geht um Sicherheitsbewusstsein, um Security Awareness.“

Das heißt: Technische und IT-Maßnahmen zur Sicherheit können noch so ausgeprägt sein, sie allein helfen nicht. Der Mensch ist das schwächste Glied in der Security-Kette. Er nimmt im Bereich der Informationssicherheit und speziell beim Thema Security Awareness eine Schlüsselrolle ein, da er aus Sicht der Angreifer das wichtigste Einfallstor bildet. Doch andererseits kann jeder Mitarbeiter Phishing-Mails und andere Attacken auch ins Leere laufen lassen, wenn er über genügend Wissen verfügt und deswegen nicht auf einen Anhang mit Schad-Software klickt. „Das Sicherheitsbewusstsein zu sensibilisieren ist ein wichtiger und sich schnell entwickelnder Bereich, insbesondere vor dem Hintergrund immer gezielterer Angriffe, die die Menschen zu einem entscheidenden Glied in der Sicherheitskette machen“, erklärt deshalb William „BJ“ Jenkins, CEO von Barracuda Networks. ▶

Security Awareness

Doch was ist Security Awareness genau? „Security Awareness bedeutet, dass jeder Mitarbeiter mit seiner inneren Einstellung, seinem Wissen um mögliche Angriffstechniken und damit verbundene Folgen sowie seinem Handeln maßgeblich zur Informationssicherheit beiträgt", erklärt Holger Schmidt, Professor für Informatik und IT-Sicherheit am Fachbereich Medien der Hochschule Düsseldorf und freiberuflicher Berater für IT-Sicherheit. Er baut an seinem Lehrstuhl gerade ein Information Security Awareness and Training Lab auf. „Natürlich gibt es keine hundertprozentige Sicherheit, da das menschliche Verhalten unter anderen durch Gefühle beeinflusst ist und sich nicht absolut kontrollieren lässt. Der Mensch soll sich so verhalten, dass er dazu beiträgt, das Restrisiko zu minimieren."

Um das zu gewährleisten und die Mitarbeiter für Sicherheit zu sensibilisieren, setzt rund die Hälfte der deutschen Unternehmen bereits auf Security-Awareness-Schulungen und nimmt Trainingsangebote eines mittlerweile breiten Anbietermarkts wahr. Das zeigt der Lagebericht 2018 des Bundesamts für Sicherheit in der Informationstechnik (BSI). Lediglich für 29 Prozent der Unternehmen kommen derzeit und

Interview

„Awareness-Schulungen erhöhen die Barriere für Angreifer"

Bettina König ist Geschäftsführerin von König Consult und ISO 27001 Lead Auditor für den TÜV Süd. Als Beraterin leitet sie seit Jahren Security-Awareness-Trainings. Im Interview erklärt sie, wie Firmen mit Hilfe von Schulungen das Sicherheitsbewusstsein ihrer Mitarbeiter schärfen können und welche Herausforderungen dabei zu meistern sind.

Bild: König Consult

Bettina König

Geschäftsführerin von König Consult und ISO 27001 Lead Auditor beim TÜV Süd
www.koenig-consult-gmbh.de

com! professional: *Frau König, warum ist Security Awareness in Firmen so wichtig?*

Bettina König: Der Mensch ist und bleibt der größte Risikofaktor für Unternehmen. Wenn Hacker-Angriffe erfolgreich sind, dann liegt das in 70 Prozent der Fälle daran, dass Mitarbeiter aus Unkenntnis etwa auf eine Phishing-Mail hereinfallen oder unbedarft auf Links zu Malware klicken. Damit öffnen sie dem Angreifer die Tür ins Unternehmensnetz. Ich habe auch schon erlebt, dass vergessen wurde, Räume mit Prototypen abzuschließen. Fahrlässigkeit und fehlendes Wissen sind die Hauptursachen für mangelnde Sicherheit. Zudem gibt es frustrierte Mitarbeiter mit sehr guten IT-Kenntnissen, die ihrem Unternehmen bewusst schaden wollen. Sie gelangen an Informationen, die sie eigentlich nicht lesen dürften, und geben diese an Mitbewerber weiter, zum Beispiel Mails von Geschäftsführern mit strategischen Inhalten.

com! professional: *Die Konsequenzen derartigen Fehlverhaltens können dramatisch sein.*

König: Natürlich. Der wirtschaftliche Schaden ist enorm, wenn sensible Daten zur Konkurrenz wandern oder die IT etwa durch Ransomware lahmgelegt wird und Geschäftsprozesse nicht mehr funktionieren.

com! professional: *Können Security-Awareness-Trainings denn bewirken, dass Mitarbeiter eine Phishing-Mail erkennen, und so verhindern, dass sie diese öffnen?*

König: Na ja. Ob ich eine verdächtige Mail öffne oder auf einen Link klicke oder nicht, hat mit Wissen zu tun. Es geht um Information Security Awareness und das Bewusstsein für die eigene Verantwortung im Umfeld Informationssicherheit, ebenso um die Sicherheit der Informationen selbst. Firmen sollten ihre Mitarbeiter dafür sensibilisieren, welche Informationen unternehmenskritisch sind und wie sie diese Informationen entsprechend ihres Schutzbedarfs behandeln. Welche Informationssicherheits-Richtlinien gibt es im Unternehmen?

Mitarbeiter müssen diese Richtlinien kennen und verinnerlichen, wie sie die Vorgaben einhalten können. Auch der Maßregelungsprozess mit Sanktionen bei Nichteinhaltung der Vorgaben muss bekannt sein. Oft hilft hier der gesunde Menschenverstand weiter. Mitarbeiter sollten beispielsweise nie geheime Daten auf USB-Sticks speichern oder offen am Drucker liegen lassen, wenn dies durch Richtlinien gefordert wird.

com! professional: *Gibt es dafür auch technische Möglichkeiten?*

König: Sie können die USB-Ports sperren oder konfigurieren, dass Mitarbeiter ein Dokument am Drucker erst nach der Eingabe einer PIN ausdrucken können. Unterstützend zu umfangreichen

> **„Die Herausforderung besteht daran, die Schulung interessant zu gestalten."**

technischen Maßnahmen müssen Unternehmen ihre Mitarbeiter aber für mögliche Gefahren und Themen rund um Informationssicherheit sensibilisieren.

com! professional: *Wie sind solche Security-Awareness-Trainings aufgebaut? Mit welchen Inhalten müssen sich die Mitarbeiter auseinandersetzen?*

auch in Zukunft keine Security-Awareness-Trainings zum Einsatz. 19 Prozent der befragten Unternehmen planen zumindest ein entsprechendes Schulungsangebot für ihre Mitarbeiter.

Und wie laufen diese Schulungen ab? Wie und mit welchen Inhalten können Firmen ihren Mitarbeitern Sicherheitsbewusstsein vermitteln und ihr Verhalten nachhaltig ändern? Reicht dafür eine eintägige Schulung pro Jahr? Welche Herausforderungen und Fallstricke gibt es bei Security-Awareness-Trainings? Lohnen sich diese Trainings? Fragen über Fragen stellen sich.

König: Zunächst erhalten sie Basiswissen zu Begriffen und Themen rund um Informationssicherheit, sie lernen die Normen und Regeln sowie die Richtlinien des Unternehmens kennen. Neben diesen allgemeinen Themen sind Informationen zu aktuellen

„Fahrlässigkeit und fehlendes Wissen sind die Hauptursachen für mangelnde Sicherheit."

Themen der Cybersecurity Bestandteil der Schulungen. In großen Firmen finden etwa viermal pro Jahr Schulungen mit speziellen Schwerpunkten statt, die zwischen 30 und 40 Minuten dauern, teils online, teils als Präsenzseminar.

com! professional: *Wie sieht es mit Sanktionen bei einem Verstoß gegen die Sicherheitsrichtlinien aus?*

König: Den Maßregelungsprozess gibt die ISO 27001 vor. Die Sanktionen beziehungsweise Maßnahmen hängen von der Schwere und Häufigkeit des Verstoßes ab. Wirkt sich eine Aktion nur sehr gering auf die Informationssicherheit aus, folgen meist ein Gespräch mit dem Information Security Officer und bei Bedarf eine themenbezogene Schulung oder ein Coaching. Bei schweren Verstößen oder wiederholtem Fehlverhalten beziehen Firmen oft den Linien-Vorgesetzten oder die Personalabteilung mit ein, verteilen die Verantwortlichkeiten um oder erwägen arbeitsrechtliche Schritte wie Abmahnungen.

com! professional: *Welche Herausforderungen und Fallstricke gibt es bei Security-Awareness-Trainings?*

König: Viele Mitarbeiter sind zunächst genervt, wenn sie sich mit Richtlinien oder Informationssicherheit auseinandersetzen müssen nach dem Motto „Das macht alles noch komplizierter. Womit soll ich mich denn noch beschäftigen?". Die Herausforderung besteht darin, die Schulung für sie interessant zu gestalten. Der Trainer sollte daher immer einen persönlichen Bezug herstellen und mit Beispielen etwa zu Social Engineering oder Phishing-Mails arbeiten.

Social Engineering

Social Engineering bezeichnet einen Angriffsvektor, bei dem die Schwachstelle Mensch ausgenutzt wird. Die Täter spähen dabei gezielt Mitarbeiter über Facebook, LinkedIn & Co. aus, am besten die, die über privilegierte Accounts verfügen und Zugang zu vertraulichen Daten haben.

Die Kriminellen nutzen Eigenschaften wie Hilfsbereitschaft oder Angst vor Autoritäten aus, um Mitarbeiter zu manipulieren. Über deren Rechner dringen die Angreifer dann in das Unternehmensnetzwerk ein oder gelangen an geheime Informationen. Ein Beispiel dafür sind Phishing-Mails, die Links enthalten, die auf eine kriminelle Fake-Website leiten und dann automatisch Schad-Software laden.

Auch der im Artikel beschriebene CEO Fraud gehört zum Social Engineering. Laut der „2018 Security Awareness Training Deployment and Trends Survey" von KnowBe4, Anbieter einer Trainings- und Phishing-Simulations-Plattform, war Social Engineering im vergangenen Jahr Hauptmethode für Angriffe auf Unternehmen. Das gaben 77 Prozent der Befragten an. Weit dahinter landen Malware (44 Prozent) oder Benutzerfehler (27 Prozent). Für die webbasierte Studie wurden 1100 Unternehmen weltweit befragt.

Kontinuierlich und individuell

Security Awareness ist grundsätzlich ein Thema für Unternehmen jeder Größe. Auch kleine und mittlere Firmen sind Ziel von IT-Angriffen jeder Art, sie haben aber durchaus andere Bedürfnisse als Großunternehmen. Zudem bringen die einzelnen Mitarbeiter unterschiedliches Security-Wissen mit – eine Herausforderung für jede Schulung.

„Viele Awareness-Programme sind standardisiert und zu wenig individualisiert in der Lernmethodik. Jeder bekommt oft das gleiche Thema vorgesetzt, es mangelt an interaktiven Elementen, und speziell global agierende Unternehmen berücksichtigen die kulturellen Unterschiede zwischen ihren Mitarbeitern zu wenig", kritisiert Holger Schmidt. Durch die Einrichtung eines Security-Awareness-Training-Labors will er gemeinsam mit seinem Team die Schulungen über E-Learning individualisieren und mit dem neu entwickelten Serious Game „What_The_Hack" spielerisch nachhaltiges Lernen gewährleisten

„Eintägige Schulungen reichen nicht aus, es geht um kontinuierliche Trainingsmaßnahmen. Security-Themen sollten sich gut in den Alltag integrieren lassen. Eine gute Form sind Lernspiele, die man schnell einschieben kann, weil die einzelnen Abschnitte nur zehn oder 15 Minuten dauern", so Schmidt weiter. Sinnvoll seien auch Kartenspiele und Poster mit Security-Inhalten oder auch Kaffeetassen mit Slogans wie „Lock it, when you leave it" („Sperre Deinen Computer, wenn Du den Raum verlässt"), um das Sicherheitsbewusstsein der Mitarbeiter im Rahmen von Kampagnen anhaltend zu fördern.

Vielfältige Inhalte mit Tests

Auch der Sicherheits-Anbieter Kaspersky Lab setzt bei seiner Automated Security Awareness Platform (ASAP) auf eine ▶

kontinuierliche Wissensvermittlung in kurzen Lerneinheiten mit spielerischen Elementen. „Awareness-Trainings sollen ja auch Spaß machen und regelmäßig über einen längeren Zeitraum erfolgen. Eine Schulung pro Jahr mit Druckbetankung bringt nicht viel, da die Mitarbeiter nach zwei Wochen alles wieder vergessen haben", weiß Peter Neumeier, Head of Channel Sales Germany bei Kaspersky.

Den größten Erfolg bieten Security-Awareness-Schulungen, wenn die Teilnehmer die Inhalte nachvollziehen und einen persönlichen Bezug herstellen können. „Die Trainings sollten mit vielen Beispielen aus dem Unternehmensalltag arbeiten und etwa zeigen, wie einfach Passwörter zu hacken sind. Auch Phishing-Simulationen sind sehr effektiv. Ein Mitarbeiter, der auf eine Fake-E-Mail hereinfällt, wird das nicht so schnell vergessen. Dieses Wissen hilft den Mitarbeitern zudem im privaten Alltag", so Trend-Micro-Business-Consultant Richard Werner.

Bild: Holger Schmidt

„Viele Awareness-Programme sind standardisiert und zu wenig individualisiert in der Lernmethodik. Jeder bekommt oft das gleiche Thema vorgesetzt."

Dr. Holger Schmidt
Professor für Informatik und IT-Sicherheit am Fachbereich Medien der Hochschule Düsseldorf
https://medien.hs-duesseldorf.de/schmidt

Als zentral sieht er an, dass die Mitarbeiter im Fall eines vermeintlichen oder echten Angriffs oder Fehlers ganz genau wissen, was zu tun ist. „Firmen sollten dafür einen Helpdesk als Anlaufstelle einrichten. An ihn können sich die Mitarbeiter auch wenden, wenn sie Fragen haben oder sich unsicher sind, ob eine E-Mail tatsächlich für Phishing oder Ähnliches missbraucht wird. Völlig falsch sind hier Angstmache und die Drohung mit Bestrafung oder negativen Konsequenzen, wenn ein Mitarbeiter einen eigenen Fehler meldet", betont Werner. Stattdessen rät er Firmen, Mitarbeiter für positives Verhalten zu belohnen, zum Beispiel wenn sie einen gefährlichen Angriff erkannt haben.

Ein gutes Beispiel gibt hier Premedia Marketing Solutions aus dem österreichischen Wels. Das Unternehmen, ein Spezialist für softwaregestütztes Marketing, legt bei seinen Mitarbeitern großen Wert auf Security Aware-

Bild: Premedia

„Die Informationssicherheit der Kundendaten ist unser wichtigstes Gut. Daher schulen wir unsere Mitarbeiter monatlich in E-Learning-Kursen zu aktuellen Themen rund um IT-Security."

Werner Stiglbrunner
Marketing Solutions Lead und Prokurist bei Premedia Marketing Solutions
www.premedia.at

Anbieter von Security-Awareness-Trainings (Auswahl)

Anbieter	Beschreibung
Barracuda Networks https://phishline.com	SaaS-Plattform PhishLine für Social-Engineering-Simulation und -Training, mit Datenanalytik und Reporting zur Identifizierung von Risiken
E-SEC www.e-sec.com	Umfangreiches Angebot mit E-Learning-Kursen rund um Informationssicherheit und Security Awareness (größtenteils 3D-animiert)
HvS-Consulting www.hvs-consulting.de	Dienstleistungen rund um Security Awareness; Präsenzschulungen, Social Engineering Assessment, Phishing-Simulationen, E-Learning-Plattform IS-FOX mit unterschiedlichen anpassbaren Modulen
IT-Seal www.it-seal.de	Awareness-Trainings (Präsenz und E-Learning), Employee Security Index (ESI) zum Status der Security Awareness im Unternehmen; Simulation von Phishing-Angriffen; Phishing-Akademie; Sicherheitskultur-Audit
Kaspersky Lab www.kaspersky.de	Security-Awareness-Programme für Unternehmen jeder Größe (auch auf Rollen der Mitarbeiter abgestimmt); E-Learning-Plattformen; Präsenzschulungen und Strategie-Simulationsspiel für Cybersicherheit; läuft vor allem über Partner
Proofpoint www.proofpoint.com	Security-Awareness-Trainings mit mehr als 25 interaktiven Schulungsmodulen in mehr als 30 Sprachen; Phishing-Simulationen
Sophos www.sophos.com	Mehr als 30 Security-Awareness-Trainingsmodule zu Sicherheits- und Compliance-Themen. Tool Sophos Phish Threat für Phishing-Simulationen
SoSafe https://sosafe.de	Awareness-Training vor Ort oder in E-Learning-Modulen aus kurzem Video, praktischen Anleitungen und abschließendem Quiz; simulierte Phishing-Attacken und Reporting-Dashboard
Symantec www.symantec.com	Umfangreiche, webbasierte Security-Awareness-Trainings mit Videos
Trend Micro https://phishinsight.trendmicro.com	Kostenloses Tool Trend Micro Phish Insight zur Simulation von Phishing-Angriffen mit Templates, die sich an die häufigsten Phishing-Kampagnen anlehnen
usd www.usd.de	Security-Awareness-Plattform mit webbasierten Trainingsmodulen, Weiterbildungs- und Sensibilisierungsmaßnahmen wie Live Hacking, Phishing-Simulationen und Security Day mit Präsenzschulungen

Security-Awareness-Trainings: Inhalte und Themen

Awareness-Schulungen vermitteln das notwendige Wissen für den Umgang mit verschiedenen Sicherheitsbedrohungen während der täglichen Arbeit. Die wichtigsten Schwerpunkte von Awareness-Schulungen sind:

- Grundlegende Informationen zur Informations- und Datensicherheit
- Sicherheitsrichtlinien des Unternehmens
- Verhalten bei sicherheitsrelevanten Ereignissen (Informationspflicht bei erkannten Gefahren)
- Sicherer Umgang mit E-Mails
- Gefahren durch Social Engineering und Phishing (mit Informationen über den Ablauf einer Phishing-Attacke)
- Sicherer Umgang mit Passwörtern
- Bedrohung durch Schad-Software
- Risiken beim Einsatz mobiler Geräte und mobiler Datenspeicher
- Gefahren durch soziale Netzwerke und Internetnutzung

ness. „Die Informationssicherheit der Kundendaten ist unser wichtigstes Gut. Daher schulen wir unsere Mitarbeiter monatlich in E-Learning-Kursen zu aktuellen Themen rund um IT-Security, um sie für Sicherheitsgefahren zu sensibilisieren", erklärt Werner Stiglbrunner, Marketing Solutions Lead und Prokurist bei Premedia. Das Unternehmen hat die Meldewege für erkannte Angriffe genau festgelegt und veranstaltet jährlich ein Quiz rund um das Thema Security Awareness. Der Sieger erhält als Belohnung ein neues iPhone.

Bild: Trend Micro

„Firmen sollten einen Helpdesk als Anlaufstelle einrichten, an den sich die Mitarbeiter wenden können. Völlig falsch sind hier Angstmache und die Drohung mit Bestrafung, wenn ein Mitarbeiter einen eigenen Fehler meldet."

Richard Werner
Business Consultant bei Trend Micro
www.trendmicro.de

Security Awareness messen

Ziel der Awareness-Schulungen ist es nicht allein, Wissen zu vermitteln, sondern Gewohnheiten zu ändern und neue Verhaltensmuster zu entwickeln. Doch wie kann man den Erfolg dieser Maßnahmen messen? Einen interessanten Ansatz hat das Sicherheitsunternehmen IT-Seal entwickelt. Es erhielt 2018 für sein Security-Awareness-Programm auf der Security-Fachmesse „it-sa" den Award UP18@it-sa als „Bestes Cybersecurity-Start-up 2018" der DACH-Region.

Ziel oder Kernidee des Unternehmens ist es, eine objektive Methode für das Messen von Security Awareness zu finden. Ergebnis ist der Employee Security Index (ESI). „Über den ESI lässt sich Awareness standardisiert und vergleichbar messen. Für die Ermittlung dieser Kennzahl simulieren wir Phishing-Angriffe, in denen das Öffnen eines Links oder Dateianhangs provoziert wird. Das Ergebnis zeigt, wie verwundbar einzelne Mitarbeitergruppen gegenüber Phishing-Angriffen sind – und macht weitere Maßnahmen planbar", erklärt Yannic Ambach, Geschäftsführer bei IT-Seal.

Vor den Phishing-Angriffen prüft IT-Seal bei Bedarf die Sicherheitsrichtlinien des jeweiligen Unternehmens und ihre Konformität mit Standards wie der DSGVO oder der Norm ISO 27001, die den Aufbau von Information-Security-Management-Systemen beschreibt. Hinzu kommen Umfragen, inwieweit diese Sicherheitsrichtlinien den Mitarbeitern bekannt sind. Oft folgen noch Schulungen durch IT-Seal zu den grundlegenden Schutzzielen und Angriffsformen, vor Ort und/oder via E-Learning: Wie erkenne ich Angriffe? Wie verhalte ich mich richtig?

Fazit & Ausblick

Informationssicherheit steht und fällt mit dem wachsamen Anwender. Awareness sollte daher ein wichtiges Thema in allen Unternehmen darstellen. Ziel muss es sein, die Mitarbeiter über Sicherheitsrichtlinien, aktuelle Bedrohungen und den Umgang mit diesen Bedrohungen aufzuklären. Über eines aber müssen sich Geschäftsleitung und Mitarbeiter im Klaren sein: Um eine nachhaltige Verhaltensänderung zu bewirken, reichen eintägige Schulungen nicht aus. Security Awareness ist als permanenter Prozess zu verstehen, der jeden Mitarbeiter einbezieht und im Alltag immer wieder Situationen schafft, in denen sicheres Verhalten eine Rolle spielt.

Unternehmen sollten daher Security-Awareness-Trainings möglichst individuell, unterhaltsam und praxisnah gestalten und gezielt auf die jeweilige Rolle des Mitarbeiters ausrichten. Als sehr hilfreich erwiesen haben sich beispielsweise Phishing-Simulationen, die Erfolge und Schwächen von Sicherheits-Awareness-Programmen aufzeigen können. Grundsätzlich sollten Firmen positive Anreize für ihre Mitarbeiter schaffen, Sicherheitsvorfälle oder eigene Fehler zu melden. Das kann beispielsweise ein Belohnungssystem oder ein Gamification-Ansatz sein. Die Drohung mit Bestrafung oder negativen Konsequenzen ist hier kontraproduktiv. Dann kann man den menschlichen Faktor in den Griff bekommen und das Sicherheitsniveau im Unternehmen erheblich steigern. ■

Jürgen Mauerer/kpf
kpf@com-professional.de