Risiko Mitarbeiter

Der Feind in den eigenen Reihen

Bild: Shutterstock / Immersion Imagery

Viele Unternehmen unterschätzen die Gefahren, die von den eigenen Mitarbeitern ausgehen.

Sicherheit ist im Bewusstsein der allermeisten Unternehmen inzwischen tief verankert: Firewalls, Endpoint-Security, Detection & Response, Access Control und viele weitere Techniken gehören wie selbstverständlich zum Abwehr-Arsenal gegen Cybercrime. Doch nicht wenige Firmen haben einen blinden Fleck – die eigenen Mitarbeiter.

Auch die beste Security-Technik schützt nicht vor der Schwachstelle Mensch. Nicht selten sind die Mitarbeiter ein Einfallstor für Angriffe und Malware. Dabei sind sie in der Regel nicht böswillig, es geschieht eher durch Gutgläubigkeit und Unachtsamkeit. Aktuelle Studien besagen, dass mehr als 80 Prozent der erfolgreichen Cyberangriffe auf menschliches Fehlverhalten zurückzuführen sind. Die Angriffsvektoren sind breit gefächert und reichen von Social Engineering und Phishing über Malware, E-Mails und Drive-by-Downloads bis hin zu zielgerichteten Attacken mit Hilfe von Deepfakes. Wenn es einem Angreifer gelingt, auch nur einen einzigen Mitarbeiter aufs Kreuz zu legen, dann ist die Sicherheit des gesamten Unternehmens gefährdet.

Das muss aber keineswegs passieren: Mit den passenden Trainings und Schulungen wandeln sich die Mitarbeiter im besten Fall vom Sicherheitsrisiko zu einem unschätzbaren Sicherheitsfaktor.

Eine Studie der Personalberatung Rochus Mummert kommt zu dem Ergebnis, dass 60 Prozent der IT-Entscheider mögliches Fehlverhalten der Mitarbeiter als hohes bis sehr hohes Risiko einschätzen. Zum Vergleich: Mängel in der IT-Infrastruktur oder beim Umgang mit Passwörtern halten nur 19 beziehungsweise 34 Prozent der Entscheider für ein hohes oder sehr hohes Sicherheitsrisiko.

Einfallstor Mitarbeiter

Die interne Bedrohung stellt für Unternehmen aller Größenordnungen eine fortwährende Herausforderung dar. Denn der Mitarbeiter von heute setzt viele verschiedene Geräte ein, noch dazu häufig an unterschiedlichen Standorten. Die Aufgabe für die Unternehmen lautet, das ideale Gleichgewicht zu finden zwischen dem notwendigen Mitarbeiterzugriff und der gewünschten Datensicherheit. Dabei gilt der Grundsatz: Je besser die Mitarbeiter darüber Bescheid wissen, wie sie zum Schutz ihres Unternehmens beitragen können, desto sicherer und aufmerksamer verhalten sie sich.

37 %
der deutschen Unternehmen wurden in den vergangenen zwei Jahren mit Hilfe von Social Engineering angegriffen

Quelle: Bitkom Research

Eine zentrale Aufgabe für die IT-Abteilung besteht darin, die Kontrolle darüber zu behalten, wer auf bestimmte Programme, Geräte und vertrauliche Informationen innerhalb des Unternehmens zugreifen kann. Dazu muss sie die verschiedenen Aufgabenbereiche kennen und den Zugriff jeweils auf bestimmte Mitarbeiter beschränken. Einen Sonderfall stellen dabei die nicht immer wohlgesinnten ehemaligen Mitarbeiter dar, die oft noch über weitreichende Zugriffsrechte verfügen. Hier sollte eine automatisierte Access Control für geordnete Verhältnisse sorgen.

Laut Christopher Schmid, SVP und Head of IT Security DACH beim IT-Dienstleister NTT Data, haben die meisten Unternehmen mittlerweile ihre Unternehmensnetzwerke und Systeme auf- und nachgerüstet, sodass es Hackern immer schwerer fällt, unbemerkt in die Firmennetze einzudringen. „Deshalb versuchen sie es über die Mitarbeiter, die aus Sicht der IT-Security in der Tat das größte Risiko darstellen. Hacker wissen um die Schwächen der Mitarbeiter, die häufig Gefahren nicht erkennen, zum Beispiel die zum Teil wirklich gut gemachten Phishing-E-Mails, mit diesen falsch umgehen oder verdächtige Aktionen nicht melden."

Auch für Bogdan Botezatu, Director of Threat Research and Reporting beim Security-Spezialisten Bitdefender, sind die Mitarbeiter oft das schwächste Glied in der Sicherheitskette eines Unternehmens. „Meistens handeln sie in gutem Glauben, aber es fehlen ihnen schlicht die Cybersicherheitskenntnisse. Hin und wieder sind es aber auch verärgerte Mitarbeiter, die wissentlich Vorgaben umgehen. Eine Studie, die wir 2019 durchgeführt haben, zeigt, dass die Mitarbeiter bei den Sicherheitsbedenken von CISOs an erster Stelle stehen." Ein mangelndes Verständnis der Mitarbeiter für die Cybersicherheit bei den täglichen Routinen ist demnach der größte Stressfaktor für die IT-Fachbereiche (36 Prozent), gefolgt von Unterbesetzung der Teams (33 Prozent) und mangelndem Sicherheitsverständnis auf der Führungsebene (30 Prozent).

Jochen Koehler, Regional VP Sales Europe bei Bromium, einem Spezialisten für Mikro-Virtualisierung, sieht es so: „Viele Sicherheitsvorfälle wären zu vermeiden, wenn die Mitarbeiter adäquat für IT-Gefahren sensibilisiert wären. Diese Aussage ist zwar richtig, greift aber zu kurz. Viel wichtiger wäre die Implementierung eines Schutzschildes, der Unachtsamkeiten von Mitarbeitern folgenlos macht." Er betont aber auch: „Natürlich muss bei der Sicherheit der Faktor Mensch Berücksichtigung finden. Mitarbeiter sind die letzte Verteidigungslinie in Sachen Sicherheit und damit auch ein bevorzugtes Angriffsziel. Gerade das Social Engineering, das vor allem in Form von Spear-Phishing-Mails auftritt, stellt eine große Gefahr für jedes Sicherheitssystem dar."

Bild: Bitdefender

„Wenn unsere Büronetzwerke auf Zero-Trust-Sicherheit basieren, dann sind unsere Netzwerke im Homeoffice genau das Gegenteil."

Bogdan Botezatu
Threat Research and Reporting bei Bitdefender
www.bitdefender.de

Typische Fehler

Kaum ein Mitarbeiter will seinem Arbeitgeber vorsätzlich schaden. Aber bei Stress und hohem Arbeitsdruck ist man weniger aufmerksam und klickt vielleicht auf Dateien in E-Mails, die eigentlich sofort in Quarantäne müssten. „Vor allem, wenn eine E-Mail im Namen des CEOs im Postfach liegt, klicken viele automatisch", bestätigt Christopher Schmid von NTT Data. „Und dann gibt es natürlich ausgereifte Social-Engineering-Attacken, bei denen auch typisch menschliche Eigenschaften ausgenutzt werden: Hilfsbereitschaft – etwa einem unbekannten Kollegen mal schnell die Türe öffnen –, Angst vor Konsequenzen und Automatismen."

„Phishing nicht zu erkennen und das Wiederverwenden von Passwörtern gehören zu den häufigsten Problemen", weiß Bogdan Botezatu. Gefährlich sei auch das bewusste Ignorieren von Sicherheitspraktiken, etwa indem Mitarbeiter die Antiviren-Lösung vorübergehend deaktivieren, um eine Einschränkung aufzuheben. „Auch die Installation eines Remote-Support-Clients auf einem Firmencomputer, damit sich die Mitarbeiter von außerhalb des Büros am PC anmelden können, kann die Sicherheit gefährden. Dies führt in der Regel zu Sicherheitslücken, die Angreifer leicht ausnutzen könnten." Wie Mitarbeiter mit Unternehmensdaten umgehen, werde ebenfalls leicht übersehen. So sollten Kunden- oder Firmendaten etwa nicht auf öffentliche Cloud-Sharing-Plattformen kopiert werden.

Die zeitlosen Klassiker sind das gedankenlose Öffnen von E-Mail-Anhängen und das leichtfertige Klicken auf Links. Christian Knothe, Head of Security Sales Germany beim britischen TK-Riesen BT, geht noch weiter: „Dazu kommen aber auch Vorfälle, die nicht auf einen Angriff, sondern auf die unbedachte Nutzung und Konfiguration von Systemen zurückgehen. Besonders im Hinblick auf die Nutzung von Cloud-Diensten ist hier noch einiges zu tun."

Apurba Bhangale ist Senior IT Security Specialist bei Teamviewer. Ihrer Meinung nach gehören schwache Passwörter und die Weitergabe von Passwörtern zu den häufigsten ▶

Bild: Warner Bros. Pictures

Gesichter tauschen: Mit Deepfake-Technik ist es ein Leichtes, Amy Adams durch Nicolas Cage zu ersetzen.

Interview

„E-Mail ist und bleibt der Angriffsvektor Nummer eins“

Stefan Schachinger, Product Manager Network Security beim IT-Unternehmen Barracuda Networks, erklärt, wie Firmen der Sicherheitsgefahren durch die Mitarbeiter Herr werden.

Bild: Barracuda Networks

Stefan Schachinger

Product Manager Network Security bei Barracuda Networks
www.barracuda.com

com! professional: *Reißt Homeoffice zusätzliche Löcher ins Sicherheitsnetz von Firmen?*

Stefan Schachinger: Homeoffice birgt sicher Risiken, insbesondere wenn es schnell und unerwartet eintritt. Die Heimnetze, in denen viele jetzt arbeiten, sind aus Richtliniensicht des Unternehmens nicht vertrauenswürdig. Eine große Gefahrenquelle stellen privat genutzte Geräte im Homeoffice dar. Eine BYOD-Policy muss gut überlegt sein und sollte nicht überstürzt eingeführt werden. Der Trend geht eher wieder davon weg, da die mögliche Kostenersparnis bezüglich der Anschaffung zusätzlicher Geräte das Sicherheitsrisiko nicht rechtfertigt.

Im Unternehmen kommt Perimeter-Security zum Einsatz, die zu Hause wegfällt. Während sich die Firewall um Antivirus, Webfilter, Advanced Threat Protection und dergleichen zuverlässig kümmert, sitzen die Mitarbeiter jetzt oft hinter einfachen Provider-Modems, die keinen Schutz bieten. Der Einsatz von Cloud-Diensten kann diesen Schutz jedoch immerhin bis zum Edge verlängern, auch ohne Eingriffe ins lokale Netzwerk.

> „Während sich die Firewall um Antivirus, Webfilter, Advanced Threat Protection und dergleichen zuverlässig kümmert, sitzen die Mitarbeiter jetzt oft hinter einfachen Provider-Modems, die keinen Schutz bieten.“

Häufig stehen IT-Admins heute vor der zusätzlichen Herausforderung, VPN-Zugänge remote einzurichten, da oft wenig Zeit blieb, geeignete Geräte zu besorgen und sie zu konfigurieren. Neben den klassischen Software-VPN-Clients können auch Hardware-Clients helfen, vor allem wenn mehrere Geräte wie Telefone oder Drucker angebunden werden sollen.

com! professional: *Warum ist E-Mail immer noch so erfolgreich als Einfallstor für Cyberkriminelle?*

Schachinger: E-Mail ist und bleibt der Angriffsvektor Nummer eins, auch in absehbarer Zukunft. Insbesondere durch das momentan situationsbedingt angestiegene Arbeiten von zu Hause ist mit einem weiteren Anstieg des E-Mail-Volumens zu rechnen.

Es bleibt nur ein umfassender Schutz als Ausweg. Dazu gehören neben dem klassischen Spamfilter und der Malware-Erkennung auch Advanced Threat Protection, Tools zur Erkennung von E-Mail-basierten Social-Engineering-Angriffen, Security-Awareness-Trainings sowie Incident Response. Zudem sollte ein Notfallplan vorhanden sein: Was ist zu tun, wenn etwas passiert ist? Ist die Schad-Software erst im eigenen Netz angekommen, kann die Ausbreitung rasant vor sich gehen und es wird fast unmöglich, alle infizierten Systeme zu identifizieren.

com! professional: *Sind Awareness-Schulungen erfolgversprechend?*

Schachinger: Awareness-Trainings speisen sich aus einer Vielzahl von Inhalten. Natürlich müssen die Mitarbeiter darin geschult werden, welche technischen Konzepte die Angreifer einsetzen und wie diese zu erkennen sind. Die größte Gefahr besteht aber darin, technisch fortgeschrittene Mitarbeiter eventuell gar nicht zu erreichen oder die technisch weniger versierten Mitarbeiter irgendwann zu verlieren. Inhalte müssen jeweils an das vorhandene Sicherheitsbewusstsein des Mitarbeiters angepasst sein sowie kontinuierlich angehoben und verändert werden. Auch Sichtweise und Sprache müssen auf die Mitarbeiter ausgerichtet sein. Zudem haben nicht alle Mitarbeiter Zugang zu den gleichen Informationen, auch kann das geforderte Sicherheitslevel variieren. Nur so kann der Prozess zur Awareness-Steigerung über längere Zeit spannend und damit sicher bleiben.

com! professional: *Greift eine klassische Netzwerksegmentierung, um besonders schützenswerte Daten zu trennen?*

Schachinger: Eine Trennung der Netze innerhalb der IT etwa in Server, Clients und Gäste sollte Standard sein. Sind noch nachgelagerte OT-Netze vorhanden, etwa in Produktions- und Industrieunternehmen, aber auch in medizinischen Einrichtungen, dann müssen diese betriebskritischen Netze besonders geschützt sein.

> „Die größte Gefahr besteht darin, technisch fortgeschrittene Mitarbeiter eventuell gar nicht zu erreichen oder die technisch weniger versierten Mitarbeiter irgendwann zu verlieren. “

Auch besonders schützenswerte Daten oder verwundbare Systeme lassen sich durch zusätzliche Segmentierung vor Angreifern oder Schad-Software schützen. Solche Systeme sollten unbedingt netzwerkseitig segmentiert und geschützt sein. Eine Segmentierung ist also grundsätzlich sinnvoll und hilft, Ausbrüche einzudämmen. Zwischen Netzen kann dann nur kommunizieren, was explizit freigeschaltet wurde, und selbst das wird noch inspiziert und auf mögliche schädliche Inhalte geprüft.

Sicherheitsfehlern, die Mitarbeiter machen. Ebenso kritisch sei es, kostenlose Software aus nicht vertrauenswürdigen Quellen zu installieren oder Anwendungen wie Antiviren- oder Endpoint-Security-Tools nicht ernst zu nehmen. Weitere Sicherheitsrisiken könnten durch die Verbindung mit ungesicherten WLAN-Netzwerken entstehen. Dazu kommt: „Viele melden sich nicht beim IT-Sicherheitsteam, wenn sie etwas Verdächtiges bemerken."

Bild: BT

Der Grad der Security-Awareness in Unternehmen ist nicht nur eine Frage von Trainings, sondern spiegelt auch die generelle Unternehmenskultur wider."

Christian Knothe
Head of Security Sales Germany bei BT
www.globalservices.bt.com/de

Social Engineering

Besonders beliebt bei Angreifern ist Social Engineering, also die gezielte Beeinflussung und Manipulation von Mitarbeitern, um sie zur Preisgabe von vertraulichen Informationen zu bewegen. „Social Engineering ist auch deshalb so erfolgreich, weil die Mittel der Angreifer immer besser werden", vermutet Jochen Koehler. „Gerade Entwicklungen wie Deepfakes, also täuschend echte Fakes von Bildern, Videos oder Audiodateien, erhöhen die Gefahren erheblich. Damit können Betrugsversuche per E-Mail oder am Telefon noch besser kaschiert werden, um Zielpersonen zum Öffnen von E-Mail-Anhängen oder zur Preisgabe von Dokumenten zu veranlassen."

Deepfakes sind quasi der letzte Schrei. Sie basieren auf Deep Learning, einer besonderen Art des Machine Learnings. Die den Deepfakes zugrunde liegenden KI-Algorithmen werden mit großen Mengen an Bild- und Videomaterial gefüttert. Je mehr Daten von einer Person vorliegen, desto besser und glaubwürdiger fällt das Ergebnis aus. Schon wenige Hundert Bilder der Zielperson reichen aus, um einen plausiblen Deepfake zu erzeugen. Deepfakes werden bald so gut sein, dass eine Stimme in Echtzeit generiert werden kann. Ein Angreifer kann so direkt mit seinem Opfer interagieren und wie ein Vorgesetzter aussehen oder wie der CEO klingen. Der grundlegende Unterschied zu herkömmlichen Fakes, bei denen etwa der Kopf aus einem Bild in ein anderes Bild eingefügt und retuschiert wird: Deepfakes hantieren nicht mit bestehenden Daten, sondern erzeugen neues Material.

„Wir sind alle Menschen mit Tugenden und Schwächen", sagt Christopher Schmid. „So ist es ein Charakterzug von Menschen, gern zu helfen, auf Druck zu reagieren oder mit Kollegen zu fachsimpeln. Dieses Verhalten machen sich Hacker beim Social Engineering zunutze. Hacker bereiten sich gründlich auf solche Angriffe vor, etwa indem sie Insights im Web oder in Social Networks recherchieren, die sie dann gekonnt im Gespräch oder in der E-Mail einsetzen."

Gefahrenherd Homeoffice

In Zeiten von Corona ziehen viele Mitarbeiter freiwillig oder gezwungenermaßen ins Homeoffice. Das Büro in den eigenen vier Wänden ist aber besonders gefährdet, weil es private und geschäftliche Risiken verbindet. Nun rächt sich, dass viele Firmen Homeoffice bislang ablehnten. Bromium-Manager Koehler führt aus: „Die im Unternehmen getroffenen Sicherheitsmaßnahmen können zu Hause oft nicht uneingeschränkt greifen. Ein Beispiel dafür sind nicht ausreichend gesicherte WLAN-Router." Hinzu kommt, dass Hacker die Ängste und Hoffnungen der Menschen ausnutzen und infizierte Corona-E-Mails mit Horrormeldungen oder Wundermitteln verschicken.

NTT-Experte Christopher Schmid betont, dass viele Mitarbeiter bisher keine Erfahrung mit der Arbeit im Homeoffice haben. „Die wenigsten davon dürften ein gezielt auf ein Arbeiten im Homeoffice abgestimmtes Sicherheitstraining bekommen haben. Einige Firmen dürften nicht einmal Policies haben, mit denen Sicherheitsregeln fürs Homeoffice-Arbeiten festlegt sind." Das Problem, so Schmid: Im Homeoffice kommen private und firmengestützte IT zusammen. „Was wird auf welchen Geräten erledigt? Berufliche Aktivitäten wie Telefon- und Videokonferenzen werden unter Umständen außerhalb des Firmennetzwerks durchgeführt, also auf Privatgeräten oder auf Firmenrechnern ohne aktivierten VPN-Zugang."

Bogdan Botezatu ist ebenfalls besorgt: „Homeoffice birgt grundsätzlich aus mehreren Gründen Risiken. Hier einige Beispiele, über die man nachdenken sollte: Das IT-Sicherheitsteam verfügt vielleicht über Sensoren innerhalb des Unternehmensnetzwerks, um bei Traffic-Anomalien oder verdächtigem Verhalten zu warnen. Da wir jetzt zu Hause in unserem eigenen Netzwerk sind, hat die IT-Sicherheit keine Ahnung, was durch unser Netzwerk geht. Wir könnten eine unangemessene Sicherheitskonfiguration haben oder Router mit veralteter Firmware. Wenn unsere Büronetzwerke auf Zero-Trust-Sicherheit basieren, dann sind unsere Netzwerke im Homeoffice genau das Gegenteil. Wir nutzen vielleicht zudem anfällige IoT-Geräte, die sich von Angreifern dazu verwenden lassen, andere Geräte zu kompromittieren. Zu Hause haben mehr unternehmensfremde Personen Zugriff auf die Geschäftsgeräte wie Laptops oder Smartphones."

BT-Manager Knothe sieht besondere Gefahren vor allem für Unternehmen, die sich in ihren Sicherheitsbemühungen bisher nur innerhalb der Grenzen des eigenen Perimeters bewegt haben. „Wer sich bereits im Vorfeld darum geküm- ▶

Bild: Exabeam

„Cyberkriminelle sind mittlerweile so gut darin, Netzwerke zu infiltrieren, dass es oft eher darum geht, Angriffe möglichst frühzeitig zu erkennen, bevor sie Schaden anrichten können."

Egon Kando
Area Vice President of Sales Central, Southern and Eastern Europe bei Exabeam
www.exabeam.com

mert hat, Mitarbeiter außerhalb des eigenen Netzwerks zu schützen, ist eindeutig im Vorteil."

Gegenmaßnahmen

Unternehmen können verschiedene Strategien verfolgen und Produkte nutzen, um dem Sicherheitsrisiko durch die Mitarbeiter zu begegnen. Bromium etwa setzt mit seiner Lösung auf Isolation statt Detektion. Das technische Fundament bildet eine Mikro-Virtualisierung. Sie kapselt jede riskante Anwenderaktivität wie einen Anhang öffnen, ein Dokument herunterladen oder eine Webseite aufrufen in einer eigenen Micro-Virtual-Machine, die nach jeder Aktion automatisch wieder gelöscht wird. „Eine Infizierung des Endgeräts mit Schad-Software – auch mit neuer, bisher unbekannter – ist damit nahezu ausgeschlossen", erklärt Jochen Koehler.

Teamviewer wiederum, so berichtet Apurba Bhangale, sensibilisiert die Mitarbeiter und ihr Sicherheitsbewusstsein kontinuierlich. Dazu werde in All-hands-Meetings mit der ganzen Belegschaft die Bedeutung von IT-Security besonders betont und es gebe regelmäßige Workshops, in denen auf die geltenden IT-Security-Policies hingewiesen werde. IT-Security-Best-Practices seien außerdem fester Bestandteil des Onboarding-Programms für neue Mitarbeiter und man informiere auch regelmäßig per E-Mail über neue Angriffsmethoden.

In vielen Unternehmen aber befindet sich das Sicherheitsbewusstsein der Mitarbeiter in einem Dornröschenschlaf. „Viele reden drüber, aber wenige Vorstände und Entscheider wollen Security Awareness nachhaltig finanzieren und wenige haben sie ganzheitlich umgesetzt. Teure Tools zu implementieren reicht nicht aus und vermag fehlende Security Awareness nicht zu kompensieren. Vor allem KMUs haben bei dem Thema einen großen Nachholbedarf", konstatiert Christopher Schmid.

Egon Kando, Area VP beim SIEM-Unternehmen Exabeam, sieht sehr große Unterschiede, wie Branchen mit dem Thema Security Awareness umgehen. „Generell kann man sagen, dass Unternehmen mehr in Schulungen investieren, je wichtiger die von ihnen verwalteten Daten sind. Verbesserungspotenzial gibt es vor allem dabei, auch Schulungen zur Auffrischung anzubieten. Die Bedrohungslage und die Angriffsvektoren verändern sich sehr schnell und Mitarbeiter sollten regelmäßig geschult werden, um sie auch für die neuesten Angriffsmuster zu sensibilisieren."

Christian Knothe zufolge hat sich die Lage in den vergangenen Jahren verbessert, sie sei aber noch nicht optimal. „Der Grad der Security Awareness in Unternehmen ist dabei nicht nur eine Frage von Trainings, sondern spiegelt auch die generelle Unternehmenskultur wider. Die Arbeit wird niemals aufhören."

Effizientes Training

Ein Weg zur Sensibilisierung sind firmenspezifische Schulungen, in denen auf mögliche Social-Engineering- und Deepfake-Angriffe eingegangen wird. Allgemeine Awareness-Trainings dagegen werden von den Mitarbeitern oft als lästige Pflichtübung betrachtet und erzielen bestenfalls mäßigen Erfolg. Viele Firmen setzen nach wie vor auf den Angstfaktor. Erfolgversprechender ist es, die positiven Auswirkungen eines korrekten Verhaltens hervorzuheben.

Bild: KnowBe4

Mitarbeiter-Training: Auch Filmserien à la Netflix lassen sich verwenden, um das Sicherheitsbewusstsein von Mitarbeitern zu stärken.

Bei Security-Awareness-Training sollte es nicht einfach darum gehen, Wissen zu vermitteln, sondern Verhalten zu verändern. Das gelingt am besten mit Emotionen. Es muss den Mitarbeitern Spaß machen, sicherheitsbewusstes Verhalten zu erlernen. Die Schulungsplattform KnowBe4 etwa arbeitet auch mit Comics und Netflix-ähnlichen Videoserien. Cliffhanger sorgen dafür, dass die Nutzer von sich aus mehr davon haben wollen. Auch Gamification-Elemente wie zu gewinnende Badges oder Wettkämpfe zwischen mehreren Teams eines Unternehmens sorgen spielerisch für Sensibilisierung.

Bild: NTT Data

„Teure Tools zu implementieren reicht nicht aus und vermag fehlende Security Awareness nicht zu kompensieren. Vor allem KMUs haben bei dem Thema einen großen Nachholbedarf."

Christopher Schmid
Senior Vice President und Head of IT Security DACH bei NTT Data
https://de.nttdata.com

Christopher Schmid teilt eine Awareness-Schulung in drei Teile ein: die Phase des Wachrüttelns, die Phase der Inhaltsvermittlung und die Phase der Einübung, bei der Inhalte, zum Beispiel mit Hilfe von E-Learning, kontinuierlich wiederholt werden. Gutes Training sollte sich Schmid zufolge an einigen Prinzipien orientieren: Augenhöhe statt Bevormundung – also nicht mit Konsequenzen drohen, aber Konsequenzen von falschem Verhalten trotzdem aufzeigen – , dabei aktuelle und verständliche Fallbeispiele nutzen und Handlungsanweisungen in das Training einbauen.

Bitdefender-Mann Botezatu kennt kein allgemeingültiges Patentrezept. „Wir sind der Meinung, dass alle Unternehmen oder Betriebe ihr Bedrohungsmodell evaluieren und ihre Mitarbeiter entsprechend schulen müssen. Wenn Sie zum Beispiel eine Buchhaltungsfirma sind, die von Ransomware betroffen sein könn-

te, dann sollten Sie Ihre Schulung wahrscheinlich so anpassen, dass die Mitarbeiter bösartige Anhänge in E-Mails erkennen. Wenn Sie im Finanzwesen tätig sind und viel mit CEOs oder CFOs zu tun haben, sollten Sie Ihre Mitarbeiter darin schulen, die Finanztransferprotokolle gewissenhaft zu befolgen und nie von den Regeln abzuweichen."

Hoffungsträger KI

Künstliche Intelligenz dringt in immer mehr Bereiche vor. Womöglich ist auch ein Einsatz beim Human Learning denkbar. Christopher Schmid sagt dazu: „Grundsätzlich ja. Wenn aus Daten, ermittelt aus internen Sicherheits-Appliances, sinnvolle Erkenntnisse gewonnen werden können, mag dies ein Unternehmens-Awareness-Programm positiv beeinflussen, aber weniger das Lernverhalten des einzelnen Mitarbeiters. Wenn Mitarbeiterverhalten direkt analysiert wird und eine Machine-Learning-basierte Lösung den Nutzer direkt auf Fehlverhalten aufmerksam macht, würde dies hohen Mehrwert bringen. Aus datenschutz- und betriebsrechtlichen Gründen sollte das Tracking jedoch auf anonymisierte Informationen ausgerichtet sein."

Egon Kando zufolge könnte Machine Learning theoretisch auch beim Lernverhalten der Mitarbeiter etwas bringen. „Sinnvoller wäre es jedoch, Machine Learning so einzusetzen, dass es Mitarbeiter vor unbewussten Fehlern schützt. Cyberkriminelle sind mittlerweile so gut darin, Netzwerke zu infiltrieren, dass es oft eher darum geht, Angriffe möglichst frühzeitig zu erkennen, bevor sie Schaden anrichten können. Hier spielt Machine Learning seine Stärken aus, weil es die Netzwerkaktivität jedes Benutzers und jeder Entität im Netzwerk in Echtzeit analysiert und jede Abweichung vom Normalverhalten sofort erkennt." „Wichtiger als das Lernverhalten ist es, den Lernerfolg nachzuvollziehen", ergänzt Christian Knothe von BT. „Nur so können Maßnahmen optimiert und im richtigen Zyklus wiederholt werden. Künstliche Intelligenz ist dabei eine Möglichkeit, aber sicher kein Wundermittel."

Angriffsvektor E-Mails

E-Mails sind nach wie vor einer der häufigsten Angriffsvektoren. Die Folgen sind neben der Verbreitung von Malware oft Datendiebstahl, Spam, Betrug, aber auch Datenverlust.

Bild: Bromium

„Gerade Entwicklungen wie Deepfakes, also täuschend echte Fakes von Bildern, Videos oder Audiodateien, erhöhen die Gefahren erheblich."

Jochen Koehler
Regional VP Sales Europe bei Bromium
www.bromium.com

Bild: Teamviewer

„Viele melden sich nicht beim IT-Sicherheitsteam, wenn sie etwas Verdächtiges bemerken."

Apurba Bhangale
Senior IT Security Specialist bei Teamviewer
ww.teamviewer.com/de

„Hier muss bei den Mitarbeitern Awareness geschaffen werden", fordert Christopher Schmid. „Parallel müssen technische Lösungen wie Antiviren-Programme oder Spam-Filter sein, um bösartige E-Mails zu erkennen und zu isolieren. Auch gilt es, Backup-Konzepte zu überprüfen."

Apurba Bhangale nennt Möglichkeiten, E-Mail-Infrastrukturen zu schützen, etwa durch die Implementierung einer intelligenten Gateway-Lösung. Über Regelsätze können so Spam- und Viren-E-Mails herausgefiltert werden. Zusätzliche Sicherheit bringen Authentisierungsprüfungen und die Validierung der Legitimität von E-Mails. Keine dieser Ansätze bietet jedoch einen 100-prozentigen Schutz vor Spam oder virenbefallenen E-Mails – deshalb bleibt der Nutzer selbst der entscheidende Faktor. „Bei den Mitarbeitern müssen sofort die Alarmglocken läuten, wenn sie unerwartete Mails mit verdächtigem Inhalt, unbekannten Links oder Attachments erhalten, und sie müssen sich direkt beim IT-Security-Team melden."

Christian Knothe sieht in Sachen E-Mail-Sicherheit viele gute technologische Entwicklungen, warnt aber: „Da E-Mail nach wie vor das wichtigste Kommunikationsmedium in Unternehmen ist, kann rein mengenmäßig nicht alles abgefangen werden. Deswegen ist der Mitarbeiter als menschliche Firewall gefragter denn je."

Fazit & Ausblick

Nachdem die Technik sowohl aufseiten der Angreifer als auch bei der Verteidigung weitgehend ausgereizt zu sein scheint, rückt der Faktor Mensch verstärkt in den Mittelpunkt. Social Engineering wird eine immer größere Rolle bei Cyberattacken spielen. Viele Schutzmaßnahmen lassen sich nach wie vor von den Mitarbeiter aushebeln, die sich wiederum von den Angreifern überlisten lassen.

Das Arsenal der Cyberkriminellen erfährt mit Deepfakes eine signifikante Erweiterung. Auch eine Art Deepfake as a-Service wird früher oder später kommen. Deepfake-Angriffe lassen sich schwer abwehren, auch Vorbeugung ist schwierig. 2020 wird wahrscheinlich das Jahr des Social Engineerings auf Deepfake-Basis, nicht zuletzt wegen der Präsidentschaftswahlen in den USA im November. Unternehmen sind deshalb mehr denn je dazu aufgefordert, ein Bündel an Maßnahmen zu ergreifen, um die für sie wichtigen Daten zuverlässig zu schützen – auch vor dem Fehlverhalten der Mitarbeiter.

Es mag ratsam sein, für kritische Informationen ein Konzept zu erstellen, bei dem die Daten verschlüsselt werden und der Schlüssel in der Kontrolle des Dateneigners bleibt. Netzwerksegmentierung gehört ebenfalls zu den Grundlagen moderner Sicherheitskonzepte und kann stark zur Minimierung von Risiken beitragen. Viele Unternehmen haben hier noch großen Nachholbedarf. ■

Andreas Dumont/kpf
kpf@com-professional.de