Security Awareness

Social-Engineering-Angriffe erkennen und verhindern

Phishing, Whaling, CEO-Fraud – die Unternehmens-IT wird zunehmend durch Social-Engineering-Angriffe auf Mitarbeiter attackiert. Wir stellen die beliebtesten Tricks der Angreifer vor und erklären, wie Sie Ihr Unternehmen dagegen schützen können.

› Wie Tiefseeräuber setzen Cyberkriminelle vermehrt auf Täuschung, um die Sicherheitsmaßnahmen ihrer Opfer auszutricksen. (Foto: PedroRamosPhoto, Shutterstock)

„Die Angreifer bewegen sich von der Technologie zu den Menschen, weil es einfacher ist," fasst Lance Spitzner, Leiter des Security Awareness-Programms des Schulungsanbieters SANS Institute, die Lage zusammen. Die technischen Schutzmaßnahmen der Unternehmen würden immer besser und damit hätten es die Angreifer schwerer, sie auf technischem Wege zu überwinden. Könne aber ein Mitarbeiter innerhalb des Netzwerks dazu manipuliert werden, aktiv auf einen schädlichen Link zu klicken, einen infizierten Dateianhang zu öffnen oder sensible Daten preiszugeben, ließen sich die Sicherheitslösungen vergleichsweise einfach umgehen.

Die Mitarbeiter sind ein kritischer Faktor der IT-Sicherheit. Es gilt daher, sie für solche Angriffe zu sensibilisieren und die sogenannte Security Awareness im gesamten Unternehmen zu steigern. Dazu ist es hilfreich, zuerst einen näheren Blick auf die beliebtesten Angriffswege zu werfen.

E-Mail-Betrug

Die E-Mail ist immer noch das verbreitetste Kommunikationsmittel im Unternehmensalltag. Laut Statista steigt die Anzahl der aktiven E-Mail-Accounts sowie täglich verschickten E-Mails weltweit sogar kontinuierlich weiter. Daher ist die elektronische Post laut der Studie „Faktor Mensch 2018" von **Proofpoint** (*www.it-finanzmagazin.de/proofpoint-veroeffentlicht-neue-studie-zum-faktor-mensch-in-der-it-sicherheit-69555/*), Anbieter von E-Mail-Sicherheitslösungen, bei Social-Engineering-Attacken der bevorzugte Angriffsvektor.

Die Angreifer wollen das Opfer dazu bringen, eine bewusste Aktion in der geschickten E-Mail auszuführen – etwa auf einen Link zu klicken oder eine Datei zu öffnen. Dabei gibt es laut Proofpoint zwei verschiedene Muster:

- Es werden einfache Köder, die leicht als Fälschung entlarvt werden können, großflächig versendet – also klassischer Spam. Hier vertrauen die Angreifer darauf, dass trotz großer Streuverluste genügend Empfänger neugierig oder unachtsam genug sind, um die gewollte Aktion auszuführen.
- Die Köder sind aufwändig gestaltet und darauf zugeschnitten, eine relativ kleine Zielgruppe zu überzeugen. Meist sind die Fälschungen sehr nah am Original und nur anhand von kleinen abweichenden Details erkennbar.

Um das Opfer dazu zu bringen, die gewollte Aktion auszulösen, setzen die Mails meist eine oder mehrere der folgenden Taktiken ein:

- Mit Betreffzeilen und Dateinamen wie „Lebenslauf" oder „Neues Konzept" wird die natürliche Neugier der Opfer angesprochen. Vermehrt verwenden Angreifer zudem die „Post vom Anwalt"-Masche, die mit einem rechtlichen Betreff Aufmerksamkeit erregen wollen.
- Im Inhalt wird ein Gefühl der Dringlichkeit erweckt. Der Absender gibt sich beispielsweise als IT-Mitarbeiter aus und verlangt, dass sofort die angehängte Datei geöffnet werden muss, um ein wichtiges Update zu installieren.
- Die Mails imitieren vertrauenswürdige Marken. So könnten die Angreifer zum Beispiel eine Nachricht des Amazon-Supports nachbauen, in der dazu aufgefordert wird, die Bankverbindung über einen Link – der zu einer nachgebauten Phishing-Webseite führt – zu aktualisieren. Die eingegebenen Daten gehen direkt an die Betrüger.

Um die E-Mail darüber hinaus noch authentischer wirken zu lassen, nutzen Angreifer laut der Proofpoint-Studie vermehrt „gefälschte Ketten". Dabei setzen sie „AW:", „Fwd:" oder „WG:" vor den Betreff und fügen manchmal sogar einen gefälschten E-Mail-Verlauf hinzu.

Im deutschsprachigen Raum gilt es seit Mitte 2019 besonders auf eine Malware namens „GermanWiper" zu achten. Sie tarnt sich als E-Mail-Bewerbung auf eine Stellenausschreibung mit einer .zib-Datei im Anhang, die angeblich weitere Unterlagen enthält. Wird sie gestartet, überschreibt der Schädling die Dateien der befallenen Systeme – sie sind nicht mehr wiederherstellbar. Das hält die Betrüger aber nicht davon ab, dennoch eine Lösegeldforderung über 1.500 Euro an die Opfer zu stellen.

CEO-Fraud

Der „Cheftrick" ist laut Spitzner vom SANS Insitute die zweithäufigste Methode der Angreifer. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) schätzt diesen Angriffsvektor als akut gefährlich ein. Im Rahmen eines Ermittlungsverfahrens gegen die organisierte Kriminalität fand die Behörde 2017 eine Liste mit etwa 5.000 potenziellen Zielpersonen in Deutschland.

Die Betrüger konzentrierten sich dem BSI zufolge auf Mitarbeiter aus der Buchhaltung oder dem Rechnungswesen. Sie gäben sich als Führungsperson aus und wiesen die Opfer an, hohe Geldbeträge auf ausländische Konten zu überweisen. Oft werde dabei betont, dass es sich um eine zeitkritische sowie streng vertrauliche Angelegenheit handle, da es vorgeblich um ein geheimes Projekt gehe.

Gefälschte E-Mails sind bei dieser Methode eines der beliebtesten Mittel der Betrüger. Darüber hinaus sind aber auch aufwändig gefälschte Briefe, Telefonanrufe mit imitierter Stimme und Ähnliches bekannt.

Angler-Phishing

Der Begriff Angler-Phishing ist vom Anglerfisch abgeleitet, der mit einem leuchtenden Köder an seinem Kopf die Beute seiner Opfer imitiert und sie so in die Falle lockt. Bei der Social-Engineering-Variante schalten sich Betrüger in die Kommunikation zwischen dem Kunden und einer Marke ein. Sie geben sich als Kundenservice aus und leiten die Konversation auf einen Fake-Account in einem sozialen Netzwerk oder einer gefälschten Web-Präsenz um. Stellt etwa jemand auf Twitter eine Frage an den Support einer Firma, antworten die Betrüger rasch über ein gefälschtes Profil wie etwa „@Service_Firmenname" darauf und starten ein Gespräch. Das Ziel ist oft, die Opfer auf schädliche Internetseiten zu locken oder sich vertrauliche Informationen wie beispielsweise Zugangsdaten zu erschleichen.

Typosquatting

Typosquatting ist eine Abwandlung des Markendiebstahls. Dabei registrieren Betrüger Webdomains, deren URL ähnlich derer bekannter Marken lautet. Meist ersetzen, entfernen oder vertauschen sie Zeichen, fügen eines hinzu oder ergänzen einen Bindestrich. Dort bauen die Betrüger das Original täuschend echt nach und greifen über falsche Log-In-Masken Zugangsdaten ab oder leiten Mitarbeiter auf mit Malware infizierte Seiten weiter.

Das Bewusstsein steigt

Die Maschen der Betrüger sind so vielfältig wie perfide – und sie funktionieren: Im August 2016 teilte der Autozulieferer Leoni der Öffentlichkeit mit, dass er „Opfer betrügerischer Handlungen unter Verwendung gefälschter Dokumente und Identitäten sowie Nutzung elektronischer Kommunikationswege" geworden sei. Die Täter stahlen dem Unternehmen etwa 40 Millionen Euro.

Solche und ähnliche Fälle sorgen dafür, dass die Schwachstelle Mitarbeiter stärker in das Bewusstsein der Verantwortlichen tritt. Auch ein gesteigertes Interesse am Datenschutz durch die DSGVO soll laut SANS dazu beigetragen haben.

Kaspersky Lab führte 2017 eine Umfrage unter 5.000 Unternehmen auf der ganzen Welt durch. Demnach gaben über die Hälfte (52 Prozent) der Befragten an, dass der Faktor Mitarbeiter die größte IT-Sicherheits-Schwachstelle in ihrem Unternehmen sei. Diese Angst scheint nicht unbegründet zu sein. Laut Milos Hrncar, General Manager der DACH-Region bei Kaspersky Lab, sollen bei 80 Prozent der Cybersicherheitsvorfälle unvorsichtige Mitarbeiter beteiligt gewesen sein. „Im Durchschnitt sind sich lediglich etwa ein Zehntel der Mitarbeiter über Regeln und Richtlinien zur IT-Sicherheit in ihrem Unternehmen bewusst," fasst er das Problem aus seiner Sicht zusammen. Um dieser Situation Herr zu werden, gilt es, neben robusten technischen Sicherheitsmaßnahmen, für alle Mitarbeiter ein umfassendes Security Awareness Programm zu implementieren. Dabei sehen sich viele Unternehmen mit einer Reihe von Herausforderungen konfrontiert.

Milos Hrncar von Kaspersky sieht, gerade in kleineren Unternehmen, ein generelles Ressourcenproblem. Für Björn Haan, Geschäftsführer im Geschäftsfeld Cyber-Security bei TÜV Rheinland, stellt das nötige Budget eine große Hürde dar. Zudem wüssten viele Unternehmen nicht, wie sie ein nachhaltiges Programm überhaupt umsetzen sollten. Auch Lars Kroll, Cyber Security Strategist bei Symantec, nennt die Kosten als hemmenden Faktor, betont aber auch das notwendige Zeit-Investment der Mit-

arbeiter. Georgeta Toth, Senior Regional Director CEEMEA bei Proofpoint, nennt die Unterstützung der Führungskräfte als Herausforderung und betont, dass auch die strengeren Datenschutzbestimmungen in Deutschland eine Rolle spielen.

Vorbereitung

Bevor konkret daran gearbeitet werden kann, ein Security Awareness Programm einzuführen, sollten die potenziellen Gegner im Unternehmen identifiziert und mit an Bord geholt werden. Die häufigsten Einwände drehen sich um Geld und Aufwand. Demnach stellen sich laut dem „SANS Security Awareness Report 2018" folgende zwei Abteilungen am wahrscheinlichsten gegen solche Initiativen: Finanzen und Operations.

Um die Finanzabteilung für sich zu gewinnen, sollten im Vorfeld konkrete Zahlen zu den durch Datenlecks, Compliance-Vorfällen etc. verursachten Verlusten eingeholt werden – entweder aus dem eigenen Haus oder von vergleichbaren Unternehmen im Markt. Diese sollten mit den Kosten für unterschiedliche Möglichkeiten, das Programm aufzusetzen (im eigenen Haus oder mit verschiedenen Dienstleistern), verglichen werden. Die Oparations-Abteilung stört sich meist an dem nötigen Zeitaufwand, in dem die Mitarbeiter nicht produktiv sind, und der Komplexität, das Programm im Unternehmen zu koordinieren und umzusetzen. Hier spielt die Art und Weise der Konzeption des Projekts eine wichtige Rolle. Es sollte ein fokussierter, auf die Kernprobleme einzelner Zielgruppen im Unternehmen zugeschnittener Ansatz erarbeitet werden. Damit lässt sich sicherstellen, dass der Aufwand je Mitarbeitergruppe überschaubar bleibt. Zudem werden mögliche „Leerzeiten" vermieden, da Mitarbeiter nur Wissen vermittelt bekommen, das sie auch direkt betrifft. Diese Argumente können auch dabei helfen, die Führungsebene abzuholen. Hier ist es wichtig, dass der CISO, CSO oder IT-Leiter die übergreifenden Vorteile besserer Security Awareness im Unternehmen kommuniziert. Zu viele technische Details sollten vermieden und die konkreten Vorteile für das Geschäft klar dargestellt werden.

Ist das Top-Management an Bord, gilt es laut TÜV Rheinland, so früh wie möglich Stakeholder aus allen Abteilungen mit einzubeziehen. Dadurch ließen sich die individuellen Schwerpunkte, die bei den Schulungsmaßnahmen der einzelnen Zielgruppen fokussiert werden sollten, zeitig konkretisieren. Außerdem wird damit die Basis für ein „Wir"-Gefühl geschaffen, das verhindert, dass sich später Widerstände entwickeln, weil sich Teile der Belegschaft ausgeschlossen fühlen.

Umsetzung

In vielen Unternehmen existieren bereits Sicherheits-Prozesse, die Mitarbeitern helfen sollen, sich gegen Angriffe zu schützen. Laut Lance Spitzner von SANS sind diese aber häufig von IT-Abteilungen aus der technischen Perspektive heraus entwickelt und lassen den Menschen außer Acht. Das macht die Security-Direktiven für die Mitarbeiter oft unverständlich oder umständlich in der Anwendung, sodass sie die Prozesse am Ende nicht einhalten. Es gilt also, diese Abläufe genau zu prüfen und sie im Dialog mit den Anwendern auf die Praktikabilität hin zu optimieren.

In diesem Zusammenhang sind Softskills wichtig. Mitarbeiter aus dem Sicherheits-Team mit technischem Hintergrund stecken meist sehr tief in der Materie. Es fällt ihnen daher manchmal schwer, die Perspektive der anderen Mitarbeiter einzunehmen. Laut den Ergebnissen des „SANS Security Awareness Report 2018" seien Programme schneller erfolgreich, wenn kommunikationsstarke Mitarbeiter mit einem nicht-technischen Hintergrund Teil des Teams sind. Hier eignen sich beispielsweise Kollegen aus den Marketing- oder Kommunikationsabteilungen oder aber ein externer Dienstleister. Die Maßnahmen selbst orientieren sich an einer Mischung aus individuellen Schulungen, Trainings, Simulationen und Tests, die die technischen IT-Sicherheitsmaßnahmen des Unternehmens ergänzen. Je nach Position und Funktion sollten bestimmte Angriffsvektoren eingesetzt und getestet werden. Finanzabteilungen sind beispielsweise begehrte Ziele von CEO-Fraud oder gefälschten E-Mail-Rechnungen und sollten verstärkt dafür sensibilisiert werden. Personalabteilungen sollten über Malware in Email-Anhängen wie Lebensläufen und Phishing-Attacken auf sensible Mitarbeiterinformationen informiert werden. Mitarbeiter in einem Warenlager oder Einzelhandel sollten dagegen eher auf physische Sicherheitsmaßnahmen geschult werden. Auch der richtige Umgang mit genutzten Cloud-Services wird immer wichtiger. So kann eine Unachtsamkeit beim Teilen von Daten über Google Drive dazu führen, dass sensible Daten im gesamten Internet veröffentlicht werden.

Mögliche Schulungs-Formate reichen von regelmäßigen Schulungen über neue Angriffsmethoden über Online-Trainings und Spiele bis hin zu Live-Hacks und Brettspielen. Wichtig ist bei all dem, dass sie kontinuierlich stattfinden. Einstündige Schulungen alle sechs oder zwölf Monate sind laut Proofpoint nicht genug. Toth rät zu praktischen Erfahrungen in simulierten Angriffssituationen oder kurzen, leicht verständlichen Lektionen in hoher Frequenz, die beispielsweise über Comics oder Videos transportiert werden. Björn Haan vom TÜV Rheinland sieht in webbasierten E-Learnings eine gute Möglichkeit, die Security Awareness zu verbessern. Diese sollten auch nachhaltig konzipiert sein, so dass sie in regelmäßigen Abschnitten wiederholt werden können.

Ein Praxis-Beispiel, wie ein internationales Großunternehmen seine Mitarbeiter systematisch in Awareness-Maßnahmen eingebunden hat, ist Henkel. Der Konsumgüterkonzern konzipierte eine breite Kampagne über alle Standorte und Hierarchieebenen hinweg. Das Programms besteht aus freiwilligen E-Learnings und regelmäßigen Informationsveranstaltungen. Zudem veranstaltete Henkel Anfang 2019 eine interne Cyber-Security-Awareness-Messe als Leuchtturmprojekt.

Kontinuierliche Verbesserung

Damit die Sicherheitsmaßnahmen auch Früchte tragen, sind regelmäßige Tests ein wichtiger Bestandteil des Security Awareness Programms. Aus den Ergebnissen können die Verantwortlichen den Erfolg des Programms ableiten und an die Unternehmensführung sowie alle involvierten Stakeholder kommunizieren.

Die gängigste Methode sind regelmäßige Penetrationstests mit fingierten Phishing-E-Mails. Anhand der Auswertung der Klickraten können Erfolge und Mängel im Programm identifiziert und dieses entsprechend angepasst werden. Zudem lassen sich gezielt qualitative Schwachstellen ausmachen, indem erfasst wird, wie oft ein Mitarbeiter den Test nicht besteht. Dabei spielt der Datenschutz natürlich eine große Rolle. Darf ein Unternehmen verfolgen, welcher Mitarbeiter wie oft auf einen Phishing-Test hereinfällt? Christian Kuss, Rechtsanwalt und Partner bei der Luther Rechtsanwaltsgesellschaft, sagt, unter bestimmten Voraussetzungen kann das möglich sein, es müssen im Vorfeld aber einige Details geklärt werden:

„Hier kollidieren die Pflichten der Unternehmen zum Schutz der Daten ihrer Angestellten und die Pflicht zum Schutz der IT-Infrastruktur. Dieser Konflikt lässt sich aber auch im Rahmen der DSGVO lösen. Vorwegschicken muss ich allerdings, dass eine konkrete Lösung dieses Konflikts in der DSGVO nicht vorgesehen ist und somit einige Rechtsunsicherheit verbleibt, wie Unternehmen damit umgehen können. Das Datenschutzrecht erlaubt die Verarbeitung personenbezogener Daten auf Grundlage unterschiedlicher Rechtsgrundlagen. Dies gilt auch im Arbeitsverhältnis."

„Demnach ist eine qualitative Auswertung möglich. Diese Auswertung muss sich im Rahmen der Rechtsgrundlagen bewegen. Dabei stellt sich insbesondere die Frage, zu welchen (weiteren) Zwecken die Daten verwendet werden sollen. Für ein Unternehmen empfiehlt es sich, hier eine Betriebsvereinbarung als Rechtsgrundlage vorzusehen. Da die Auswertungen regelmäßig auch zur Kontrolle der Mitarbeiter geeignet sind, dürfte der Betriebsrat ohnehin ein Mitbestimmungsrecht haben. Alternativ könnte die Datenverarbeitung auch im Rahmen eine Interessensabwägung möglich sein. Hier sollte das Unternehmen aber Selbstbeschränkungen vorsehen, um eine ausufernde Nutzung der Daten zu vermeiden."

Wollen Unternehmen eine qualitative Auswertung nutzen, sollten sie dringend vorher einen Rechtsexperten hinzuziehen und die Gesetzeslage genau klären. Zudem ist es für die Verantwortlichen ratsam, die Implikationen und Konsequenzen einer solchen qualitativen Auswertung sehr genau abzuwägen. Ansonsten könnte der Zweck des Programms, ein höheres Sicherheitsniveau zu erreichen, verfehlt werden.

Kaspersky Labs sagt in der oben erwähnten Studie, dass bei 40 Prozent der weltweit von einem Sicherheitsvorfall betroffenen Unternehmen Mitarbeiter versuchten, einen Vorfall zu verbergen. Oft liege das an strengen aber unklaren Regeln, oder Mitarbeiter befürchteten, ihr Brötchengeber könnte sie bei Nichteinhaltung zur Rechenschaft ziehen. Solche Regeln schürten laut Kaspersky Angst und ließen den Mitarbeitern nur eine Option – Vorfälle vertuschen, um die Bestrafung um jeden Preis zu vermeiden. In solchen Fällen gilt es, die IT-Sicherheitsrichtlinien zu konkretisieren und die Prozesse so in den Arbeitsalltag zu integrieren, dass sie leicht verstanden und verinnerlicht werden könnten. So wird der Belegschaft die Angst genommen, etwas falsch zu machen. Dabei helfe es, in den Abteilungen engagierte Mitarbeiter einzusetzen oder aufzubauen, die als direkter Ansprechpartner bei Unklarheiten dienen und die Schutzmaßnahmen vor Ort gemeinsam mit den Mitarbeitern durchsetzen.

Zum Abschluss darf auch die analoge Welt nicht vergessen werden. Ausgedruckte E-Mails, postalische Korrespondenz, alte Festplatten und dergleichen können natürlich auch sensible Daten enthalten. Es sollten daher auch regelmäßig Müll-Container und Ähnliches dahingehend geprüft werden.

Ein Kraftakt mit Gefühl

Die Schwachstelle Mensch gegen die steigende Flut an Social-Engineering-Attacken abzudichten, ist eine vielschichtige Angelegenheit. Zum einen gilt es, alle Ebenen – von der Geschäftsführung bis zu den einzelnen Abteilungen – zu involvieren, um eventuelle interne Hürden zu überwinden und Security Awareness als strategisches Ziel zu etablieren. Zum anderen sollten die Maßnahmen so gestrickt sein, dass sie das Sicherheitsniveau verbessern und dauerhaft von Mitarbeitern akzeptiert werden.

Dazu ist es wichtig, die Maßnahmen individuell auf die Zielgruppen zuzuschneiden und Mitarbeiter mit starken Softskills in das Programm zu integrieren. Persönliches Engagement in Sachen Sicherheit seitens der Belegschaft ist nicht selbstverständlich und lässt sich nicht erzwingen. Es ist eine kulturelle Entwicklung, die langfristig aktiv gefördert und gelebt werden muss.

Jens Dose