Bild: Shutterstock / nicemonkey

IT-Security

CEO im Fadenkreuz der Cyberkriminellen

Gezielte Angriffe auf Führungskräfte erfordern besondere Schutzmaßnahmen.

Im Frühjahr dieses Jahres meldete sich an einem Freitagnachmittag der deutsche CEO eines Energieunternehmens per Telefon beim Chef der britischen Niederlassung. Er habe den Transaktionszeitraum seiner Bank für eine wichtige Überweisung leider verpasst. Sie müsse aber vor 16 Uhr getätigt werden, damit die Zahlung noch vor dem Wochenende erfolgen könne. Die Überweisung könne nur noch durch die britische Tochter getätigt werden. In Großbritannien war es aufgrund der Zeitverschiebung noch eine Stunde früher.

Der Brite habe sich zwar etwas gewundert, da er die Stimme des CEOs jedoch eindeutig erkannte, habe er den Auftrag trotzdem ausgeführt und 220.000 Euro auf ein ungarisches Konto überwiesen, beschreibt Rüdiger Kirsch den Fall. Er ist Betrugsexperte bei der Kreditversicherungsgesellschaft Euler Hermes.

Dass es ausgerechnet eine britische Tochter des Unternehmens getroffen habe, zum Ziel des Betrugs zu werden, ist Kirsch zufolge kein Zufall – zum einen wegen des genannten Zeitunterschieds, aber auch weil die für den Betrug vermut-

lich verwendete Software zur Imitation von Stimmen momentan lediglich Englisch beherrsche.

Anrufe vom „falschen Johannes“

Solche und vergleichbare Angriffe auf Führungskräfte in Unternehmen oder in ihrem Namen haben verschiedene Bezeichnungen. Sie werden CEO-Betrug, CEO-Fraud oder auch Fake-President-Masche genannt.

Sie gehören zum großen Feld des Social Engineerings. Diese Art von Attacken beschäftigt IT-Sicherheitsspezialisten schon seit einer ganzen Weile. Beim Social Engineering suchen Cyberkriminelle nicht umständlich nach technischen Lücken in den Schutzmaßnahmen von Unternehmen. Stattdessen setzen sie auf den „menschlichen Faktor“, also zum Beispiel auf Mitarbeiter, die mal mehr, mal weniger gezielt adressiert und etwa mit gefälschten Rechnungen zum Ausführen von Schad-Software bewegt werden. Bei Euler Hermes werden diese Betrugsfälle auch als „falscher Johannes“ bezeichnet, weil nicht der „echte Johannes“ einen Mitarbeiter kontaktiert, sondern ein Betrüger.

Technische Abwehrmaßnahmen gelten bei Angriffen via Social Engineering in der Regel als wenig hilfreich. Stattdessen setzen Sicherheitsexperten vor allem auf gezielte und an das jeweilige Umfeld angepasste Security-Awareness-Trainings, in denen die Mitarbeiter auf betrügerische Vorgänge aufmerksam gemacht und auf sie vorbereitet werden.

Im Fall des Energieunternehmens waren die getroffenen Vorkehrungen allerdings vergeblich. Nach Informationen von Euler Hermes war die britische Tochtergesellschaft auf Social Engineering und CEO-Betrug vorbereitet worden. Weil der Mitarbeiter die Stimme des Anrufers aber als echte Stimme seines CEOs einstufte, sei die Täuschung zunächst nicht aufgefallen. Als die Täuschung dann bemerkt wurde, war der Schaden schon nicht mehr gutzumachen: „Das ganze Geld war weg“, so Kirsch.

Bild: NTT Security

„Ist ein Deepfake gut gemacht, wird er mit dem menschlichen Gehör nur sehr schwer oder gar nicht zu erkennen sein.“

David Wollmann
Executive Consultant bei
NTT Security
www.nttsecurity.com/de-de

Misstrauisch sei das Opfer erst geworden, nachdem die versprochene unternehmensinterne Zahlung nicht erfolgte und etwas später eine erneute Zahlung veranlasst werden sollte. „Der Täter wurde nach seinem ersten Erfolg gierig und witterte das große Geld“, kommentiert Rüdiger Kirsch. Dabei sei er aber schlampiger vorgegangen und habe Fehler gemacht. So sei sein zweiter Anruf beispielsweise von einer österreichischen statt einer deutschen Telefonnummer gekommen.

65 Fälle
von CEO-Fraud mit über 165 Mio. Euro Schaden wurden in den vergangenen vier Jahren bekannt

Quelle: Euler Hermes

Steigende Schäden

„In den letzten vier Jahren haben wir 65 Fälle mit einem gemeldeten Schadensvolumen von mehr als 165 Millionen Euro verzeichnet“, beschreibt Rüdiger Kirsch die Situation. Anfangs seien lediglich vereinzelte Attacken zu beobachten gewesen. „Inzwischen sind es durchschnittlich etwa 20 Fälle pro Jahr.“ Die Schadenshöhe variiere zwischen 150.000 und 50 Millionen Euro – mit einer Tendenz nach oben. „Bei den betroffenen Unternehmen waren praktisch alle Branchen und Unternehmensgrößen vertre- ▶

Evolutionsstufen des CEO-Betrugs*

Evolutionsstufe	Methode	Vorgehen
Frühstadium	E-Mail	E-Mail teils mit Schreib- und/oder Grammatikfehlern, schlecht getarntem Absender, abweichenden E-Mail-Adressen
Stufe 1	Social Engineering	Korrekte Rechtschreibung, gut getarnte Absender mit zum Beispiel kleinen Fehlern und Buchstaben- oder Zahlendrehern
Stufe 2	Gehacktes Intranet	Betrüger hacken das Intranet und verweilen dort für einige Tage. Sie spionieren Zuständigkeiten und Gepflogenheiten wie Umgangston und E-Mail-Stil aus
Stufe 3	Telefonanruf	Ein Betrüger ruft einen Mitarbeiter in der Buchhaltung an, um ihm zum zehnjährigen Firmenjubiläum zu gratulieren. Wenige Wochen später ruft er für den CEO-Betrug erneut an – der Mitarbeiter erkennt die Stimme und führt gemäß der Aufforderung per E-Mail eine Überweisung aus
Stufe 4	Falscher IT-Security-Mitarbeiter	Kurz nach der E-Mail mit der Zahlungsaufforderung ruft ein falscher IT-Mitarbeiter in der Buchhaltung an, um dem Kollegen mitzuteilen, dass bei ihm ein CEO-Betrugsversuch entdeckt worden sei. Alles sei unter Kontrolle und der Mitarbeiter solle „zum Schein“ mitspielen, damit man die Betrüger auf frischer Tat ertappen könne. Es werde keine echte Zahlung ausgelöst, weil man mit der Hausbank kooperiere
Stufe 5	Stimm-Imitation	Aktueller Fall mit Stimm-Imitations-Software: Das Programm ahmt Sprachmelodie und Akzent nach, sodass der Mitarbeiter nach dieser telefonischen Bestätigung denkt, die Anweisung per E-Mail käme tatsächlich vom echten Chef
Künftige Stufen	Deepfake, Video, WhatsApp	Weitere technische Fortschritte, etwa beim Machine Learning, machen diese Angriffsvektoren praxistauglich

* nach der Kreditversicherungsgesellschaft Euler Hermes

ten, zunehmend auch kleine und mittelständische Firmen", berichtet Kirsch. Überdurchschnittlich oft seien allerdings Unternehmen mit Tochtergesellschaften im Ausland angegriffen worden.

Komme es erst einmal zu einer Überweisung, dann sei die Zeit knapp: „Die ersten 36 bis maximal 72 Stunden sind entscheidend, ob vielleicht noch ein Teil des Geldes durch schnelles Handeln und einen guten Draht zur Hausbank zurückgeholt werden kann." In den meisten Fällen sei das Geld aber nicht mehr zu retten. Insgesamt nur etwa eine Million Euro habe bei allen 65 Fällen durch rasches Reagieren und einen Rückruf der Überweisungen über die zuständige Bank wiederbeschafft werden können. Auch Ermittlungserfolge seien selten. Nur in einigen wenigen Einzelfällen habe man die Betrüger ausfindig machen und fassen können.

Bild: Euler Hermes

„Das ganze Geld war weg."

Rüdiger Kirsch
Betrugsexperte bei
Euler Hermes
www.eulerhermes.de

KI hilft Kriminellen

Wie in anderen Security-Bereichen auch, wenden die Angreifer immer wieder neue, zuvor unbekannte Tricks an. Das liege daran, dass „die Täter immer professioneller werden", erläutert Kirsch. „Laufend entwickeln sie ihre Methoden weiter." Erst habe man es mit Zahlungs- und Bestellerbetrug, dann mit falschen IT-Mitarbeitern und schließlich mit gefälschten Stimmen zu tun bekommen.

Bei Letzteren greifen die kriminellen Banden auf Techniken aus dem Bereich der Künstlichen Intelligenz (KI) zu. Im Fall des betrogenen Energieunternehmens sei beispielsweise eine Software zum Einsatz gekommen, die mit Hilfe von Machine Learning fremde Stimmen imitieren könne. Ein selbstlernender Algorithmus erfasse innerhalb von Minuten die Stimme eines Menschen und könne sie anschließend täuschend echt nachahmen, inklusive der individuellen Sprachmelodie oder eines landestypischen Akzents. Betrugsfälle mit KI-Unterstützung werde man in Zukunft deswegen „sicher häufiger sehen".

Ron van het Hof bezeichnet den beschriebenen Angriff deswegen auch als „neue Evolutionsstufe". Der CEO von Euler Hermes in Deutschland, Österreich und der Schweiz konstatiert: „Software zur Stimm- oder Handschriftenimitation und Deepfake-Videos eröffnen Betrügern in Zukunft viele neue Möglichkeiten." In ein oder zwei Jahren gebe es vielleicht den ersten CEO-Betrug, bei dem die Zahlungsanweisung per Deepfake-Video und WhatsApp-Nachricht übermittelt werde. Als Deepfake werden Techniken bezeichnet, mit denen etwa Bilder oder komplette Videos täuschend echt nachgemacht werden können.

Der menschliche Faktor

Das Einwirken von Menschen spielt bei der IT-Sicherheit eine nicht zu unterschätzende Rolle. Laut einer Analyse des auf E-Mail-Sicherheit spezialisierten US-Unternehmens Proofpoint nutzten zuletzt weniger als 1 Prozent der von Proofpoint beobachteten Cyberattacken eine technische Schwachstelle aus. Bei allen übrigen Angriffen setzten die Kriminellen dagegen auf den „Human Factor". Die Experten von Proofpoint verstehen darunter eine Mischung aus Neugier und Vertrauen, die Mitarbeiter immer wieder dazu verleiten würde, zum Beispiel auf in E-Mails enthaltene Links zu klicken oder verseuchte Dateien herunterzuladen und auf ihrem Rechner auszuführen.

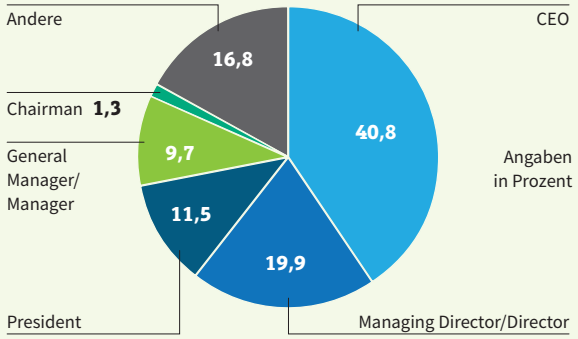
„Wenn es um organisatorische oder institutionelle Sicherheit geht, hat vieles von dem, was wir unternehmen können, um uns besser abzusichern, nichts zu tun mit Technologie, sondern eher mit der Fortbildung der Mitarbeiter", erklärt auch Aaron Zander, Senior IT-Engineer von Hacker One, einer auf Schwachstellen spezialisierten US-Company. „Das Ermuntern der Mitarbeiter, Anfragen anzuzweifeln und sie doppelt zu prüfen, sowie eine gesunde Paranoia sind essenziell, um die allgemeine IT-Sicherheit zu verbessern", so Zander weiter.

Dabei gehe es nicht darum, die Mitarbeiter für schlechte Passwörter oder unerwünschtes Verhalten verantwortlich zu machen. Das Verhindern von Phishing-Attacken habe eher etwas mit den etablierten Vorgehensweisen in den Unternehmen zu tun. „Ist es für die leitenden Angestellten normal, eine Überweisung an einen Anbieter oder einen Kauf von einer unbekannten Webseite ohne weitere Rückfragen zu verlangen? Dann herzlich willkommen im Phishing-Himmel!" Es sei Aufgabe der IT-Abteilung und der Sicherheitsspezialisten im Unternehmen, die Kollegen zu informieren und zu schulen, um auf diese Weise das „schwächste Glied in der Kette zu stärken".

Gefahr durch Deepfakes

Nichtsdestoweniger ist die Erkennung von Angriffen auf Führungskräfte wie dem eingangs beschriebenen keine leichte Aufgabe. Gefährdet sind auch nach Meinung von David Wollmann, Executive Consultant beim Sicherheitsanbieter

Bevorzugte Angriffsziele



Gefälschte E-Mails: Sogenannte Business-E-Mail-Compromise-Attacken (BEC) richten sich vor allem gegen Chief Executive Officers.

com! professional 12/19 Qelle: Trend Micro „2019 Midyear Security Roundup"

NTT Security, vor allem große, international aufgestellte Unternehmen, bei denen die Zielperson die Stimme des Gegenübers nicht 100-prozentig genau kenne. Angriffe mit einer zumindest ähnlich klingenden Stimme seien hier besonders vielversprechend.

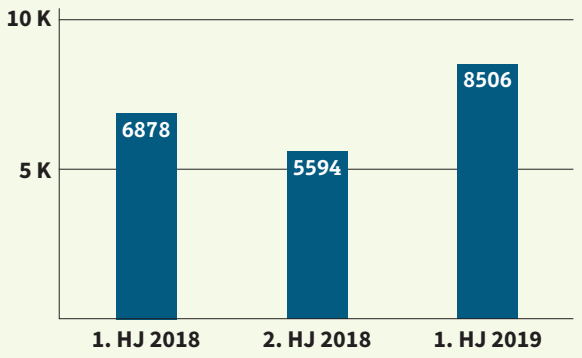
Wollmann rechnet damit, dass die „Anzahl der Social-Engineering-Angriffe mittels Deepfakes, sei es Voice oder auch Video, stark zunehmen" wird. Mit vergleichsweise geringem Aufwand könnten die Angreifer hier relativ gute Ergebnisse erzielen. Bei einer zu schlampigen Vorbereitung könne es jedoch zu Verzögerungen in den Antwortzeiten kommen, die sich als Hinweis auf einen Angriff nutzen ließen. Es gebe aber noch keine technischen Abwehrmaßnahmen, die dafür geeignet seien.

„Ist ein Deepfake gut gemacht, wird er mit dem menschlichen Gehör nur sehr schwer oder gar nicht zu erkennen sein", so Wollmann. „Man könnte höchstens auf komische Geräusche in der Leitung achten, die ein Deepfake-Indiz sein können." Der Experte empfiehlt gefährdeten Unternehmen, einen Prozess aufzusetzen, der bei kritischen Aktivitäten wie einer finanziellen Transaktion oder Übermittlung von Forschungs- und Kundendaten eine telefonische Rückversicherung beinhaltet. Darüber hinaus seien Awareness-Trainings empfehlenswert, die sich speziell mit dem Thema Social Engineering befassen.

Angriffe per E-Mail

Bei all der Aufregung um fortgeschrittene Angriffe auf Führungskräfte darf die Bedrohung durch ganz gewöhnliche gefälschte E-Mails nicht vernachlässigt werden. So hat der japanische Sicherheitsanbieter Trend Micro eine Analyse auf Basis seiner „Smart Protection Network"-Daten veröffentlicht, laut der die Zahl der BEC-Versuche (Business E-Mail Compromise) in der ersten Hälfte dieses Jahres auf über 8500 angestiegen ist. Im Vergleichszeitraum des Vorjahrs lag die Zahl noch bei unter 7000 Attacken. Bei mehr als 40 Prozent dieser Betrugsversuche per E-Mail stand der CEO des jeweiligen Unternehmens im Fokus.

Versuchte Angriffe



Wachsende Gefahr: Nach einem Rückgang im zweiten Halbjahr 2018 hat die Anzahl betrügerischer BEC-Angriffe in diesem Jahr wieder deutlich zugenommen.

com! professional 12/19 Quelle: Trend Micro „2019 Midyear Security Roundup"

Bild: Hacker One

„Ist es für die leitenden Angestellten normal, eine Überweisung ohne weitere Rückfragen zu verlangen? Dann herzlich willkommen im Phishing-Himmel!"

Aaron Zander
Senior IT-Engineer bei Hacker One
www.hackerone.com/de

Nach Angaben von Trend Micro werden inzwischen längst nicht mehr nur Firmen der Privatwirtschaft angegriffen. Bei einer BEC-Attacke gegen eine Kirche im US-Bundesstaat Ohio sei diese um rund 1,75 Millionen Dollar betrogen worden. Zuerst hackten die Angreifer mehrere E-Mail-Accounts von Mitarbeitern der Organisation. Diese wurden dann genutzt, um Kollegen dazu zu bewegen, die genannte Summe auf das Konto eines angeblichen Geschäftspartners zu überweisen.

Dem auf E-Mail-Security spezialisierten Anbieter FireEye zufolge richten sich weitere Angriffe gegen die Lohnbuchhaltung in Unternehmen oder gegen ihre Lieferketten. So werde etwa versucht, die Kontodaten von Mitarbeitern im Auftrag des CEOs zu ändern, um auf diese Weise Gehaltszahlungen auf andere Konten umzuleiten. Oder es werden die E-Mails eines Lieferanten gefälscht, um so ebenfalls illegale Zahlungen auszulösen. Das Problem bei dieser Art von Attacken ist nach Angaben von Ken Bagnall, Vice President of Email Security bei FireEye, dass „nicht jeder Mitarbeiter darauf vorbereitet ist oder nicht über das notwendige Wissen verfügt, dass es sich dabei um einen Angriff handelt".

Sensibilisierung der Mitarbeiter

Aufgrund der zunehmenden Attacken fordert nun auch der E-Commerce-Verband eco, die Mitarbeiter in den Unternehmen besser vorzubereiten. „Viele Mittelständler unterschätzen nach wie vor das Risiko, ins Visier von Cyberkriminellen zu geraten", erklärt Oliver Dehning, Leiter der Kompetenzgruppe Sicherheit im eco-Verband. Nur 41 Prozent der für seine aktuelle IT-Sicherheitsstudie befragten Unternehmen schulen ihre Mitarbeiter laut Dehning regelmäßig, 38 Prozent unregelmäßig, 7 Prozent planen Schulungen und 14 Prozent schulen oder sensibilisieren nie.

„Die Zahlen sind angesichts der wachsenden Bedrohungslage noch immer zu niedrig", kritisiert Dehning. Regelmäßig die Mitarbeiter zu sensibilisieren, sollte in jedem Unternehmen selbstverständlich sein. Zudem fordert er die Einführung von Sicherheits-Notfallplänen. Solche Pläne hätten bislang aber nur 57 Prozent der befragten Firmen. „Jedes Unternehmen sollte früh genug überlegen, wie es bei einem gravierenden Sicherheitsvorfall reagiert, um den Schaden im Fall der Fälle möglichst gering zu halten", so Dehning. Dem ist nichts hinzuzufügen. ■

Andreas Th. Fischer/js
js@com-professional.de