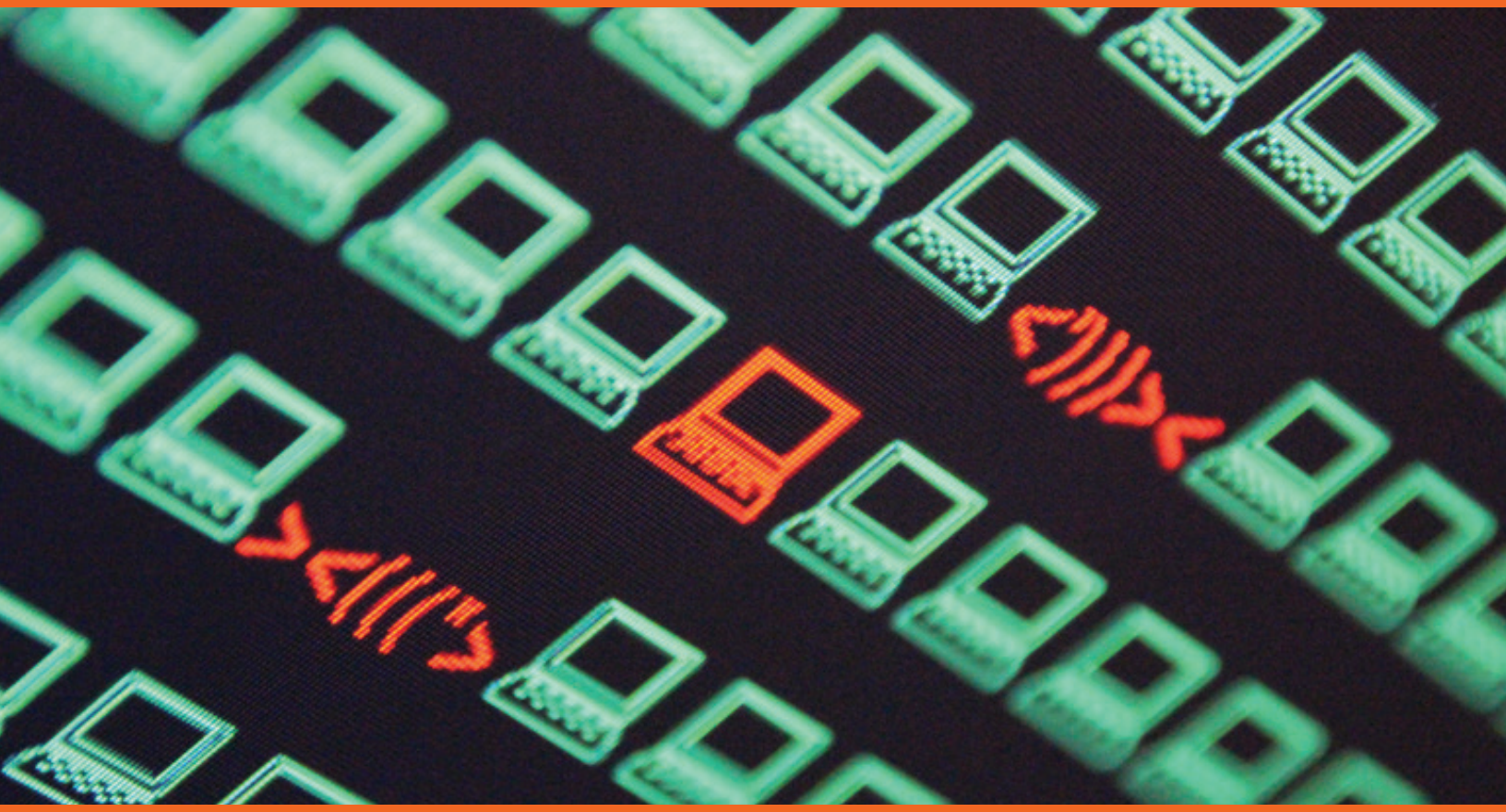
KnowBe4
Human error. Conquered.



CEO Fraud

Schützen Sie Ihr Unternehmen gezielt vor Social Engineering

Cyberkriminelle praktizieren bereits seit Jahren eine lukrative Betrugsmasche: CEO Fraud. Getarnt als Führungskraft eines Unternehmens weisen die Cyberkriminellen dessen Mitarbeiter an, Geldbeträge auf ein Konto unter ihrer Kontrolle zu überweisen oder lukrative Informationen freizugeben und an eines Ihrer E-Mail-Konten zu senden. Die Erfolgsraten und erbeuteten Beträge dieser Betrugsvariante sind erheblich. Nicht ohne Grund befindet sich die Zahl der gemeldeten Fälle von CEO Fraud schon seit Jahren konstant auf Wachstumskurs – weltweit. Längst hat die globale Schadenssumme die Milliardengrenze durchbrochen.

Ein Grund: Die IT-Sicherheit von Unternehmen hat mit dieser Betrugsvariante erheblich zu kämpfen. Denn immer noch wird zu häufig allein auf technische Lösungen gesetzt. Es wird übersehen, dass eine solch komplexe Betrugsmasche, die das Vertrauen der Mitarbeiter zu einem integralen Bestandteil des Angriffs macht, eine ebenso komplexe Antwort erfordert. Mitarbeiter müssen in Sicherheitsfragen geschult, organisatorische Sicherungsmaßnahmen müssen ergriffen werden, um die Cyberkriminellen ihrer zentralen Ansatzpunkte zu berauben.

Ein komplexes Vorhaben, bei dem es Einiges zu beachten gilt. Um Unternehmen bei diesem schwierigen Prozess zu unterstützen, hat KnowBe4 diesen Leitfaden erstellt. Er legt die gängigen Angriffsvektoren eines CEO Fraud offen und liefert grundlegende Hinweise, in welchen Bereichen des Unternehmens zwingend Maßnahmen ergriffen werden müssen. Will man das Risiko, Opfer eines CEO Frauds zu werden, minimieren und das Schadenspotential für das eigene Unternehmen reduzieren, wird man um die Implementierung der hier geschilderten Maßnahmen nicht herumkommen.

“Der Spruch stimmt, dass die Sicherheits-systeme jedes Mal gewinnen müssen, der Angreifer jedoch nur einmal”

Dustin Dykes

I. CEO Fraud – ein Überblick

CEO Fraud, auch bekannt unter dem Namen Business Email Compromise (BEC), ist eine komplexe Betrugsmasche. Der Cyberkriminelle dringt dabei zunächst in die IT-Infrastruktur eines Unternehmens vor, wo er dessen Strukturen, Hierarchien und Prozesse ausspäht. Anschließend verschafft er sich Zugang zum E-Mail-Konto einer Führungskraft. Über dieses sendet er dann – den Stil offizieller Unternehmens-E-Mails nachahmend – E-Mails an rangniedere Mitarbeiter, in denen er diese anweist, Geldbeträge auf ein Konto zu überweisen oder sensible Informationen an eine E-Mail-Adresse weiterzuleiten. Um seine Erfolgschancen zu erhöhen, setzt er die Mitarbeiter dabei häufig psychisch unter Druck, indem er eine möglichst rasche Bearbeitung seiner Anweisung anmahnt. Mit rein technischen Sicherheitslösungen ist diesem Betrugsverfahren für gewöhnlich nicht beizukommen. Hat das Unternehmen den Betrug aufgedeckt, ist es meist schon zu spät. Der Schaden ist entstanden.

Bereits seit 2013 sind auch deutsche Unternehmen zunehmend von CEO Fraud betroffen. In einer Umfrage des Wirtschaftsprüfungs- und Beratungsunternehmens PwC vom Februar 2018 gaben rund 40 Prozent der befragten deutschen Unternehmen zu Protokoll, innerhalb der vergangenen zwei Jahre mindestens einmal Ziel eines solchen Betrugsversuchs geworden zu sein. 5 Prozent berichteten sogar, dass der Angriff auf ihr Unternehmen für die Cyberkriminellen erfolgreich verlaufen sei. Nicht ohne Grund warnt das deutsche Bundesamt für Sicherheit in der Informationstechnik Unternehmen in seinem Bericht zur Lage der IT-Sicherheit in Deutschland 2018 ganz explizit vor dem wachsenden Risiko, Opfer eines CEO Frauds zu werden. Auch Verfassungsschutz, Bundeskriminalamt und Landeskriminalämter haben bereits diesbezügliche Warnhinweise herausgegeben. Und diese Warnungen sind wohlbegründet. Im vergangenen Jahr veröffentlichte das Bundeskriminalamt das Bundeslagebild Wirtschaftskriminalität 2017. In ihm wurden Daten zur damals größten CEO-Fraud-Tätergruppe vorgelegt, die durch eine Sonderermittlung festgestellt worden waren. 175 Millionen Euro tatsächlichen Schaden und 419 Millionen Euro potenziellen Schaden hatte allein diese Tätergruppe der deutschen Wirtschaft zwischen 2014 und 2017 zugefügt.

Techniken und Taktiken

Um einen erfolgreichen CEO Fraud zu begehen, müssen die Cyberkriminellen sich zunächst umfassend über das zu attackierende Unternehmen, seine internen Prozesse und seine Mitarbeiter informieren.
Grundlegende Informationen erhalten die Betrüger für gewöhnlich bereits auf der Webseite des Unternehmens. Weitere Informationen, vor allem zu relevanten Mitarbeitern, können über öffentlich zugängliche Webseiten, wie die Social-Media-Konten der Mitarbeiter, gewonnen werden.

Um nun an tiefergehende Informationen, zum Beispiel über betriebsinterne Prozesse, zu gelangen, werden Mal- und Spyware eingesetzt. Von der IT-Sicherheit unbemerkt speisen die Cyberkriminellen sie ins Netzwerk des Unternehmens ein. Nicht selten operiert die Schadsoftware dort monatelang und liefert den Betrügern Daten über Hierarchien, Strukturen und Betriebsabläufe – beispielsweise den Aufbau einer Überweisungsanordnung und den konkreten Ablauf eines Überweisungsprozesses.

Eine Angriffsmethode, die bei der Übertragung der Mal- und Spyware ins Unternehmensnetz zum Einsatz kommt – aber auch an anderen Stellen des CEO Frauds eine zentrale Rolle spielt – ist das sogenannte Social Engineering. Unter Zuhilfenahme von aus der angewandten Sozialwissenschaft entlehnten Methoden werden Mitarbeiter manipuliert, um diese zur Ausübung einer von den Betrügern gewünschten Handlung zu bewegen. So werden die Mitarbeiter in einer sogenannten Phishing-E-Mail von einer vermeintlichen Autoritätsperson angewiesen, einen Link anzuklicken oder einen Anhang zu öffnen – wodurch dann Mal- und Spyware ins Unternehmensnetz gelangen. Oder sie werden gebeten, vertrauliche Informationen, wie eine E-Mail-Adresse, mitzuteilen, was für die Cyberkriminellen die Erfolgschancen des CEO Frauds erhöht. Schließlich kommt Social Engineering auch beim eigentlichen CEO Fraud zum Einsatz. Nämlich dann, wenn der Cyberkriminelle, getarnt als Führungskraft, einen Mitarbeiter beauftragt, die Überweisung vorzunehmen oder die relevanten Informationen freizugeben.

Dies zeigt: mit der Fähigkeit, Social Engineering-Methoden erfolgreich gegen die Mitarbeiter des Unternehmens zum Einsatz zu bringen, steht und fällt der gesamte CEO Fraud.

Ansatzpunkte

Der Manipulation von Mitarbeitern kommt beim CEO Fraud dementsprechend eine zentrale Bedeutung zu. Für gewöhnlich sind es die Mitarbeiter der Finanzabteilung, die hierbei in den Fokus der Angreifer geraten. Sind sie es doch, die es zu überzeugen gilt, will der Betrüger Geld vom Unternehmenskonto auf eines, das unter seiner Kontrolle steht, transferieren lassen. Doch wird – nicht zuletzt, um die Erfolgschancen zu erhöhen – der Social-Engineering-Angriff meist auf weitere Personenkreise im Unternehmen ausgedehnt. Hierzu zählen:

- Mitarbeiter der IT-Abteilung: Sie kontrollieren die Zugangskontrollen, das Passwortmanagement und die E-Mail-Konten. Hat der Cyberkriminelle sich hier Zugriff verschafft, stehen ihm die Anmeldeinformationen aller Mitarbeiter zur Verfügung.

- Mitarbeiter der Personalabteilung: Sie verwalten alle Mitarbeiterinformationen. Hat der Cyberkriminelle sich hier Zugriff verschafft, kann er seine Social-Engineering-Angriffe stärker individualisieren und so seine Erfolgschancen erhöhen.

- Führungskräfte: Sie sind autorisiert, Überweisungen anzuordnen. Hat der Cyberkriminelle sich hier Zugriff verschafft, kann er E-Mails im Namen der Führungskraft versenden und dessen bisherige Überweisungsanordnungen als Vorlage nutzen.

Dies zeigt, CEO Fraud ist eine Betrugsvariante, die an zahlreichen Stellen im Unternehmen Ansatzpunkte findet. Entsprechend vielfältig gestalten sich auch die Angriffsszenarien.

Angriffsszenarien

Aus der Vielzahl und den Kombinationsmöglichkeiten von Techniken, Taktiken und Ansatzpunkten ergibt sich für die Betrüger ein vielfältiges Spektrum möglicher Angriffsszenarien. Jedoch haben sich in den vergangenen Jahren fünf CEO-Fraud-Szenarien als besonders populär erwiesen. In drei dieser Szenarien versucht der Angreifer, die finanziellen Ressourcen des Unternehmens anzuzapfen:

- Der Angreifer gibt sich als Führungskraft aus: Ein Mitarbeiter oder eine Finanzinstitution wird vom Angreifer – getarnt als Führungskraft – gebeten, Gelder auf ein anderes Konto zu transferieren.

- Der Angreifer gibt sich als Mitarbeiter aus: Ein Unternehmenskontakt erhält vom Angreifer – getarnt als Mitarbeiter – falsche Rechnungen und wird gebeten, Geld auf ein Konto zu überweisen.

- Der Angreifer gibt sich als Zulieferer aus: Ein Mitarbeiter wird vom Angreifer – getarnt als Zulieferer – gebeten, Rechnungsgelder künftig auf ein anderes Konto zu überweisen.

In den übrigen zwei Szenarien versucht der Angreifer, sensible Informationen über das Unternehmen abzugreifen, die nicht zuletzt auch für weitere komplexe Angriffe genutzt werden können:

- Der Angreifer gibt sich als Führungskraft oder Unternehmensanwalt aus: Ein Mitarbeiter wird vom Angreifer – getarnt als Führungskraft oder Rechtsanwalt – gebeten, umgehend vertrauliche Informationen freizugeben.

- Der Angreifer gibt sich als Führungskraft aus: Mitarbeiter der Personal-, Buchhaltungs- oder Prüfungsabteilung erhalten vom Angreifer – getarnt als Führungskraft – die Anfrage, persönliche Informationen zu Mitarbeitern freizugeben.

Die Vielfalt der Ansatzpunkte und Angriffsszenarien zeigt: mit einfachen, herkömmlichen Sicherheitslösungen kommen Unternehmen bei CEO Fraud nicht weiter. Was sie brauchen ist ein komplexes Maßnahmenpaket, das in der Lage ist, die hier vorgestellten Techniken, Taktiken und Ansatzpunkte unbrauchbar zu machen. Nur auf diesem Wege können sie die Bedrohung CEO Fraud nachhaltig in den Griff bekommen.

II. CEO Fraud im Griff

Um sich effektiv vor CEO Fraud abzusichern, bedarf es einer Reihe technischer, personeller und organisatorischer Maßnahmen.

Präventive Maßnahmen

Einige dieser Maßnahmen müssen bereits im Vorfeld eines Angriffs implementiert werden. Sie können das Risiko, Opfer eines CEO Frauds zu werden, deutlich reduzieren. In ihrer konkreten Form können sie sich dabei durchaus von Unternehmen zu Unternehmen unterscheiden und den jeweiligen spezifischen Anforderungen und Bedürfnissen Rechnung tragen. Einige zentrale Bereiche des Unternehmens und der Unternehmenssicherheit müssen jedoch zwingend abgedeckt werden, soll das Maßnahmenpaket tatsächlich größere Erfolge zeitigen.
Diese sollen im Folgenden kurz vorgestellt werden.

Hochrisiko-Nutzer Um sich effektiv vor CEO Fraud zu schützen, müssen die Hochrisiko-Nutzer des Unternehmens ermittelt werden. Hierbei handelt es sich um alle C-Level-Führungskräfte, sowie Mitarbeiter der Finanz-, Personal- und IT-Abteilung. Es muss festgestellt werden, ob unternehmensrelevante Informationen über sie im Netz verfügbar sind, die für die Sicherheit des Unternehmens ein Problem darstellen. Wenn ja, müssen diese entfernt werden. Des Weiteren müssen zusätzliche Schutz- und Kontrollmaßnahmen für die Arbeitsbereiche der Hochrisiko-Nutzer erlassen werden. Bereits mit dieser einfachen Maßnahme lassen sich die Ansatzpunkte eines CEO Frauds deutlich reduzieren.

Technische Sicherheitslösungen Da die Cyberkriminellen bei CEO Fraud für gewöhnlich über E-Mails kommunizieren, Mal- und Spyware zum Einsatz bringen und sich Zugang zu fremden E-Mail-Konten verschaffen, ist es zwingend erforderlich, die diesbezüglichen technischen Kontroll- und Schutzmaßnahmen auszubauen.

Maßnahmen sollten sich zum einen auf die Kommunikation mit externen Gesprächspartnern fokussieren. E-Mail-Filter sind ein guter Anfang. Doch sollten zusätzlich auch Datenverkehrsfilter, ausgestattet mit Black- und White-Lists, implementiert werden. Die Gefahr, dass Mal- und Spyware ins System oder sensible Informationen nach draußen gelangen, lässt sich so deutlich reduzieren.

Zum anderen sollten die Zugangs- und Zugriffskontrollen auf das Unternehmensnetzwerk verstärkt werden. Mit der Implementierung eines effektiven Identity-and-Access-Management-Systems, versehen mit Zugriffsregelungen, welche die Zugriffsrechte der Mitarbeiter auf die für ihre Arbeit notwendigen Bereiche beschränkt, kann hier bereits viel erreicht werden. Der Sicherheitsgrad der Authentifizierungsmaßnahmen kann ebenfalls erhöht werden – beispielsweise durch Einführung einer Zwei-Faktor-Authentifizierung unter Zuhilfenahme eines physischen Tokens. Werden diese Kontrollen dann noch regelmäßig auf etwaige Sicherheitslücken überprüft, wird Cyberkriminellen der Weg ins Unternehmensnetzwerk deutlich erschwert.

Sicherheitstraining Cyberkriminelle sind für einen erfolgreichen CEO Fraud, wie schon im ersten Abschnitt dieses Handbuchs erwähnt, in entscheidendem Umfang auf die Fähigkeit, Mitarbeiter zu manipulieren, angewiesen. Mit ihr steht und fällt der ganze Betrugsversuch. Dementsprechend hat ein Unternehmen hier anzusetzen, will es den Cyberkriminellen seines wichtigsten Ansatzpunktes berauben.
Ein erster Schritt kann dabei die Anfertigung eines Sicherheitshandbuchs sein, in dem Mitarbeitern die Grundlagen von Cyberrisiken und Cybersicherheit vermittelt werden.

An einem nachhaltigen Sicherheitstraining, einem sogenannten „New School Security Awareness Training“, für die gesamte Belegschaft kommt jedoch kein Unternehmen vorbei. Denn hier wird den Mitarbeitern nicht nur einfaches Basiswissen vermittelt, sondern spezifisch auf ihre Funktion und ihre Zugriffsrechte im Betrieb zugeschnittene Kenntnisse. Das Training beinhaltet regelmäßige Praxistests, sogenannte Phishing-Tests, in denen die Mitarbeiter in ihrem Arbeitsalltag am konkreten Beispiel auf die Anwendung des neu erworbenen Wissens hin überprüft werden. Die Testergebnisse werden anschließend ausgewertet und analysiert, um Schwachstellen innerhalb der Belegschaft aufzuspüren und diese gezielt nachzuschulen. Wird dieses Training regelmäßig wiederholt, kann das Sicherheits- und Risikobewusstsein der gesamten Belegschaft spürbar und nachhaltig angehoben werden. Das Risiko, Opfer eines manipulierenden Social-Engineering-Angriffs zu werden, wird so deutlich reduziert.

Sicherheitsregelungen Cyberkriminelle nutzen beim CEO Fraud den Umstand aus, dass bei der Festlegung bestimmter interner Arbeitsprozesse, wie beispielsweise der Durchführung einer Überweisung oder einer Informationsübermittlung, vor allem praktische Gesichtspunkte den Ausschlag gaben. Sicherheitspolitische Bedenken fanden allenfalls am Rande Berücksichtigung. Das Unternehmen fühlte sich vom Grundsatz her sicher, was sich nun rächt.

Im Fall der Überweisung wie der Informationsübermittlung müssen deshalb Sicherheitsregelungen entwickelt und in die Prozesse implementiert werden. Diese Sicherheitsregelungen sollten unter anderem festlegen, dass die Autorisierung eines Prozesses anschließend durch mehrere Personen verifiziert werden muss. Nach Möglichkeit sollten zudem unterschiedliche Kommunikationskanäle (E-Mail, Telefon, Brief, persönlicher Kontakt) genutzt werden. Und schließlich sollte für eine Anfrage eine feste Wartezeit vereinbart werden, bis zu deren Ablauf nicht mit der Abarbeitung der Anfrage begonnen werden kann. Vor allem Letzteres ist von erheblicher Bedeutung. Beraubt es den Cyberkriminellen doch seines wichtigsten psychischen Druckmittels gegenüber dem Mitarbeiter.

Geschäftsführung In vielen Unternehmen zählen Cyberangriffe nach wie vor nicht zu den Bedrohungen, die der Unternehmensführung vorgelegt werden. Bei einem CEO Fraud ist dies nicht mehr möglich, sind doch E-Mail-Konten der Führungskräfte in den Angriff involviert. Auch mussten bereits Führungskräfte aufgrund von signifikanten finanziellen Schäden persönlich die Verantwortung übernehmen und mussten das Unternehmen verlassen. Der CEO und das übrige Management müssen daher die Angriffsvektoren und Risiken der Betrugsmasche ebenso kennen, wie die konkreten Schritte des Unternehmens zur Risikominimierung und den Notfallplan für den Fall, dass den Cyberkriminellen doch ein erfolgreicher Angriff gelingen sollte.

Versicherungsschutz Viele Unternehmen sind gegen Cyberrisiken umfassend versichert. Doch decken nicht alle Cyber-Versicherungen Schäden durch CEO Fraud ab. Sie verorten CEO Fraud in einer Grauzone zwischen E-Mail-Betrug und betrügerischen Finanzinstrumenten. Unternehmen sollten deshalb dringend mit ihrer Versicherung in Kontakt treten und den Versicherungsumfang, wenn nötig, ändern, um sicherzustellen, dass sie größeren Schäden ausreichend abgesichert sind.

Maßnahmen für den Notfall Auch gut umgesetzte Präventivmaßnahmen können keine vollständige Sicherheit garantieren. Ein gewisses Restrisiko bleibt immer bestehen. Um für den Notfall gerüstet zu sein, muss neben den präventiven Maßnahmen deshalb auch ein Katalog mit Sofortmaßnahmen erstellt werden, der im Bedarfsfall augenblicklich greifen kann. Dieser hat folgende Themengebiete abzudecken:

Begrenzung des Schadens Zunächst müssen das zuständige Finanzinstitut selbst, sowie dessen Cybersecurity-Abteilung kontaktiert und über die fragliche Überweisung informiert werden. Es sollte angefragt werden, ob die Überweisung noch zurückgenommen werden kann. Ist dies nicht der Fall, sollte das Finanzinstitut des Betrügers informiert und gebeten werden, die Auszahlung oder Weiterleitung des Geldbetrages zu verhindern.

Informierung aller relevanten Organe Als nächstes müssen alle relevanten internen und externen Organe über den Angriff informiert werden. Eine Notsitzung des Vorstands und der Geschäftsleitung muss einberufen werden, in der diese über den Vorfall, bislang eingeleitete Gegenmaßnahmen und geplante weitere Schritte informiert werden. Des Weiteren sollten das Bundesamt für Sicherheit in der Informationstechnik und die Zentrale Ansprechstelle Cybercrime bei der zuständigen Landespolizei und dem Bundeskriminalamt informiert werden. Rechtsanwälte sollten ebenfalls kontaktiert werden, um etwaige Klagen und Rechtsbeistand in Versicherungsfragen vorzubereiten. Außerdem sollte Anzeige bei der zuständigen Staatsanwaltschaft erstattet werden. Und schließlich sollte die Versicherung kontaktiert und über den Vorfall informiert werden.

Erfassung der Sicherheitslücken Nun muss die hauseigene IT den Einbruch forensisch analysieren, um den Angriffsvektor zu ermitteln. Hierbei sollten auch externe IT-Sicherheitsspezialisten hinzugezogen werden. Nicht immer ist die interne IT in der Lage, alle Schwachstellen der eigenen Verteidigung aufzuspüren.

Beseitigung der Sicherheitslücken Abschließend müssen alle ausgemachten Sicherheitslücken geschlossen werden. Auf Basis der durch die Aufarbeitung des Angriffs gewonnenen Erkenntnisse können dann die Sicherheitstechnologien erweitert, das Wissen und die Wahrnehmung der Mitarbeiter weiter ausgebaut werden. Mitarbeiter, welche die bestehende Sicherheitspolitik nachweislich verletzt haben, müssen im Hinblick auf eine mögliche Kooperation mit den Cyberkriminellen einer eingehenden Überprüfung unterzogen werden. Im Bedarfsfall haben im Anschluss disziplinarische Maßnahmen zu erfolgen.

“Menschen sind daran gewöhnt, eine Technologielösung zu haben [aber] Social Engineering umgeht alle Technologien, einschließlich Firewalls. Technologie ist entscheidend, doch wir müssen uns Menschen und Prozesse ansehen. Social Engineering ist eine Form des Hackens, die Einflusstaktiken verwendet”

Kevin Mitnick

Zusammenfassung

CEO Fraud ist eine komplexe Angriffstechnik von Cyber-Kriminellen, bei der technische, personelle und organistorische Schwachstellen innerhalb eines Unternehmens ausgenutzt werden, um Geldmittel und sensible Informationen zu stehlen. Um sich hiergegen erfolgreich zur Wehr zu setzen, müssen Unternehmen den Cyberkriminellen eine Kombination aus organisatorischen, personellen und technischen Sicherheitslösungen entgegensetzen. Techniken, Taktiken und Ansatzpunkte der Cyberkriminellen können so erfolgreich ausgehebelt werden. Für den Fall, dass Cyberkriminellen dennoch ein CEO Fraud gelingt, sollten Unternehmen stets zusätzlich einen Notfallplan bereithalten.

Um bei der Konzipierung und Umsetzung dieser Maßnahmen keine relevanten Punkte zu übersehen, hat KnowBe4 im Anhang drei Dokumente zusammengestellt, die Unternehmen den Aufbau einer effektiven Abwehr erleichtern sollen:

- eine Checkliste zur Sicherstellung aller erforderlichen präventiven Maßnahmen,
- eine Notfallplan-Checkliste und
- eine Liste mit Beispielen für Verdachtsmomente im täglichen E-Mail-Verkehr, die einen Social-Engineering-Angriff nahelegen.

Halten Unternehmen sich an die hier empfohlenen Maßnahmen, sind sie bestens für den nächsten CEO-Fraud-Betrugsversuch gewappnet. Und der kommt bestimmt.

CEO Fraud – Checkliste zur Vorbeugung

I. Identifizierung aller Hochrisikonutzer

- Stellen Sie fest, ob Außenstehende sich Zugriff auf sensible Informationen (Aufgabenbereiche, E-Mail-Adressen, Telefonnummern, etc.) Ihrer Hochrisiko-Nutzer (Führungskräfte, Mitarbeiter der Finanz-, der IT- und der Personalabteilung, sowie der Buchhaltung) über die Webseite Ihres Unternehmens oder andere öffentlich zugängliche Webseiten (zum Beispiel Social-Media-Kanäle) verschaffen können.
- Sichern Sie die sensiblen Informationen von Hochrisiko-Nutzern vor dem Zugriff Außenstehender ab.

II. Ausbau und Institutionalisierung der technischen Sicherheitslösungen

- Richten Sie E-Mail-Filter ein.
- Sichern Sie die sensiblen Informationen von Hochrisiko-Nutzern vor dem Zugriff Außenstehender ab.
- Erstellen Sie für Ihre Angriffserkennung Systemregeln zum Aufspüren von E-Mails, die Ähnlichkeiten mit den internen E-Mails Ihres Unternehmens aufweisen.
- Richten Sie unter Zuhilfenahme von Black- und White-Lists Datenverkehrsfilter für die ext. Kommunikation ein.
- Richten Sie eine Identity-and-Access-Management-Lösung ein, die mit ihrer Sicherheitspolitik im Einklang steht.
- Statten Sie diese mit einer Zwei-Faktor-Authentifizierung aus, um das Sicherheitsniveau Ihrer Zugangs- und Zugriffskontrollen anzuheben.
- Sichern Sie Ihre Unternehmensdomain durch Domain Spoof Protection-Technologie ab und lassen Sie ähnlich klingende Domains vorsorglich registrieren.

III. Training der Belegschaft in Sicherheitsfragen

- Informieren Sie Ihre Mitarbeiter über die Grundlagen der Cybersicherheit.
- Trainieren Sie sie darin, Social-Engineering-Angriffe selbständig zu identifizieren und zu melden – mit einem „New School Security Awareness Training".
- Stellen Sie sicher, dass dieses Training regelmäßige Phishing-Tests beinhaltet. So kann das Sicherheits- und Risikobewusstsein Ihrer Mitarbeiter kontinuierlich ausgebaut werden.
- Richten Sie für Ihre gesamte Belegschaft ein einfach zu bedienendes Alarmsystem für verdächtige E-Mails ein.

IV. Einrichtung von zusätzlichen Sicherheitsregelungen für Überweisungen

- Lassen Sie die Autorisierung einer Überweisung durch mehrere Führungspersönlichkeiten verifizieren.
- Lassen Sie Autorisierung und Verifizierungen einer Überweisung durch untersch. Kommunikationskanäle laufen.

- Sichern Sie Autorisierung und Verifizierungen durch digitale Signaturen zusätzlich ab.
- Bauen Sie bei Überweisungen ab einem bestimmten Geldbetrag eine zeitl. Verzögerung in die Bearbeitung ein.

V. Einrichtung einer zusätzlichen Sicherheitsregelung für sensible Informationen

- Legen Sie eine ähnliche Sicherheitsregelungen für die Weitergabe sensibler Unternehmensinformationen, wie Finanzdaten, Kunden- und Mitarbeiterberichte, fest.

VI. Implementierung zusätzlicher Prozeduren zur Anhebung des Sicherheitsniveaus

- Identifizieren Sie die relevantesten Informationen Ihres Unternehmens, die um jeden Preis geschützt werden müssen und stellen Sie fest, wo diese Informationen gelagert werden, wer über Zugriffsrechte verfügt und wie sie geschützt werden. Falls erforderlich, erhöhen Sie das Sicherheitsniveau.
- Stellen Sie sicher, dass alle Mitarbeiter des Unternehmens die Sicherheitsregelungen des Unternehmens studieren und durchgängig anwenden.
- Erstellen Sie einen Notfallplan für Cybervorfälle und unterziehen sie diesen regelmäßigen Praxistests.

VII. Einbeziehung der Geschäftsführung

- Stellen Sie sicher, dass Ihre Führungskräfte regelmäßig über aktuelle Cyberbedrohungen und Abwehr maßnahmen informiert werden.
- Integrieren Sie Cyberrisiken in das allgemeine Risikomanagement und die diesbezüglichen Steuerungsprozesse Ihres Unternehmens.

VIII. Sicherstellung einer adäquaten Cyber-Versicherung

- Stellen Sie sicher, dass Sie auch im Fall eines CEO Fraud voll versichert sind.

IX. Nachverfolgung von Hinweisen auf Social-Engineering-Angriffe

- Gehen Sie verstärkt Hinweisen auf Social-Engineering-Angriffe nach. Beispiele möglicher Verdachtsmomente finden Sie im Anhang „Social Engineering – Verdachtsmomente, die einen Phishing-Angriff nahelegen“.

CEO Fraud – Checkliste für den Notfall

I. Kontaktieren Sie Ihre Bank.

- Geben Sie Auskunft über alle Details der Überweisung.
- Wenn möglich, widerrufen Sie die Überweisung.
- Lassen Sie die zum Empfängerkonto gehörende Bank kontaktieren, um den Betrag einfrieren zu lassen.

II. Informieren Sie Ihren Vorstand und Ihre Geschäftsleitung.

- Rufen Sie diese hierzu zu einem Notfallmeeting zusammen, in dem der Vorfall und die Gegenmaßnahmen dargelegt und besprochen werden.

III. Informieren Sie das BSI und die zuständigen Stellen der Polizei.

IV. Kontaktieren Sie Ihre Anwälte.

V. Erstatten Sie Anzeige bei der zuständigen Staatsanwaltschaft.

VI. Informieren Sie Ihre Versicherung.

VII. Lassen Sie den Vorfall IT-forensisch untersuchen.

- Lassen Sie Ihre IT den Vorfall aufarbeiten, um den genauen Angriffsvektor der Cyberkriminellen zu ermitteln.

VIII. Schalten Sie externe IT-Sicherheitsspezialisten ein.

- Ziehen Sie externe IT-Sicherheitsspezialisten hinzu, um sicherzustellen, dass Ihre IT-Experten keine relevanten Details des Angriffs übersehen haben.

VIII. Gehen Sie gegen Missachtungen Ihrer Sicherheitsregelungen durch Ihre Mitarbeiter vor.

- Stellen sie fest, ob Mitarbeiter ihre Sicherheitsregelungen missachtet oder sogar mit den Cyberkriminellen zusammengearbeitet haben. Falls ja, ergreifen Sie die notwendigen disziplinarischen Maßnahmen.

X. Beseitigen Sie die festgestellten Sicherheitsdefizite.

- Schließen Sie die festgestellten Sicherheitslücken.
- Entfernen Sie die aufgespürte Mal- und Spyware.
- Stellen Sie die volle Kontrolle über Ihre E-Mail-Konten wieder her.
- Rüsten Sie die bestehenden Sicherheitstechnologien und -prozeduren auf.
- Erweitern Sie das bestehende Sicherheitstraining für Ihre Belegschaft. Stellen Sie sicher, dass es sich um ein „New School Security Awareness Training“ handelt, das auch regelmäßige Phishing-Tests und eine Analyse des Reaktionsverhaltens ihrer Belegschaft beinhaltet.
  Nur so kann eine langfristige Anhebung des Sicherheitsbewusstseins Ihrer Mitarbeiter gewährleistet werden.

Social Engineering – Verdachtsmomente, die einen Phishing-Angriff nahelegen

Absender:

- Zum Absender der E-Mail bestanden und bestehen bislang keine Kontakte oder Geschäftsbeziehungen.
- Der Absender der E-Mail ist nicht persönlich bekannt.
- Der Absender der E-Mail arbeitet nicht im Unternehmen und hat nichts mit dem eigenen Aufgabenbereich zu tun.
- Der Absender der E-Mail ist zwar bekannt, doch kommt die Nachricht unerwartet.
- Der Absender der E-Mail arbeitet zwar innerhalb des Unternehmens – für einen Kunden, Lieferanten, Partner – doch ist sie für diesen eher untypisch.
- Die E-Mail-Adresse des Absenders ist unbekannt.
- Die E-Mail-Adresse des Absenders stammt von einer verdächtigen Domain.

Betreff:

- Der Betreff der E-Mail ist irrelevant und hängt nicht mit ihrem tatsächlichen Inhalt zusammen.
- Der Betreff der E-Mail weist diese als Antwort auf eine eigene E-Mail aus, die man jedoch nie abgeschickt hat.

Inhalt:

- Im Inhalt kommen auffallend viele Grammatik- und Rechtschreibfehler vor.
- Im Inhalt wird gebeten, einen Link anzuklicken oder einen Anhang zu öffnen.
- Der Inhalt der E-Mail besteht ausschließlich aus Hyperlinks.

Empfänger:

- Als Empfänger der E-Mail wird eine Personengruppe angezeigt, die normalerweise nicht in dieser Zusammensetzung angeschrieben wird.
- Die E-Mail wurde an eine Gruppe von Personen weitergeleitet, die gänzlich unbekannt sind.

Datum:

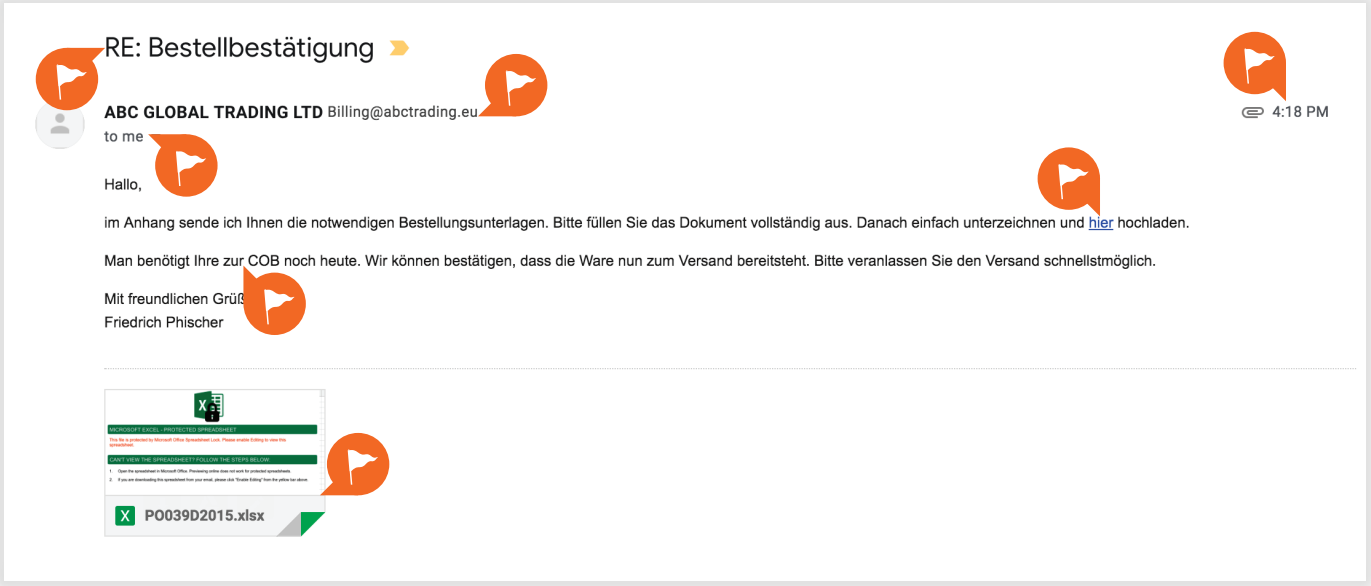
- Die E-Mail wurde zu einem ungewöhnlichen Zeitpunkt abgeschickt.

Hyperlinks:

- Die Anzeige, wenn der Mauszeiger über einem Hyperlink steht, nennt eine andere Zieladresse als der Hyperlink selbst.
- In einem Hyperlink wird die anvisierte Webseite falsch buchstabiert.

Anhänge:

- Der E-Mail ist ein Anhang beigegeben, der nicht erwartet wurde, der normalerweise nicht vom Sender kommt oder nicht mit dem Inhalt der E-Mail in Zusammenhang steht.
- Im Anhang befindet sich ein Dateityp, der ein mögliches Sicherheitsrisiko darstellt.



Über KnowBe4

KnowBe4 ist Anbieter der weltweit größten Plattform für Security Awareness Trainings und Phishing Simulationen. Mehr als 40.000 Unternehmen rund um den Globus setzen KnowBe4 bereits ein.

Das von dem IT- und Data Security-Spezialisten Stu Sjouwerman gegründete Unternehmen hilft Organisationen, den Faktor Mensch in der IT-Security anzugehen, indem das Bewusstsein für Ransomware, CEO-Fraud und andere Social-Engineering-Taktiken durch einen neuartigen Trainings-Ansatz geschärft. wird

Der international bekannte Cybersecurity-Spezialist Kevin Mitnick half als Chief Hacking Officer von KnowBe4 bei der Gestaltung der KnowBe4-Trainings.Zehntausende von Organisationen verlassen sich auf KnowBe4, um ihre Nutzer als letzte Verteidigungslinie zu mobilisieren.

Für mehr Informationen besuchen Sie www.KnowBe4.de

KnowBe4 Germany GmbH | Rheinstraße 45/47 | 12161 Berlin | +49 (0)30 34 64 64 621 | Sales@KnowBe4.com

04C02K01