Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

- Was ist CEO Fraud?
- Schützen Sie sich

CEO Fraud

Was ist CEO Fraud?

Cyberkriminelle sind raffiniert – sie entwickeln ständig neue Wege um an das zu kommen, was sie wollen. Eine ihrer effektivsten Methoden ist es, gezielt Menschen wie Sie ins Visier zu nehmen. Cyberangreifer haben gelernt, dass unwissende Personen das schwächste Glied jedes Unternehmens sind, sie haben aber übersehen, dass sachkundige Mitarbeiter wie Sie als OUCH! Leser die beste Verteidigung eines Unternehmens sein können.

Gastautor

Angela Pappas ist Leiterin des Informationssicherheits- und –bewusst seinstrainings bei Thomson Reuters. In ihrer Rolle ist sie verantwortlich für das Botschafter-Programm, elektronisches Lernen und die Aufklärung der Mitarbeiter über Phishing.

Cyberkriminelle haben eine neue Angriffsform entwickelt, die CEO Fraud genannt wird, auch bekannt als Business Email Compromise (BEC, „Geschäfts-E-Mail-Gefährdung“). Bei diesen Angriffen gibt ein Cyberkrimineller vor, ein leitender Angestellter oder Vorstand Ihrer Organisation zu sein. Die Kriminellen senden eine E-Mail an Mitarbeiter wie Sie, mit der sie versuchen Sie zu einer Handlung verleiten. Diese Art des Angriffs ist extrem effektiv, weil die Kriminellen viel Aufwand in die Vorbereitung stecken. Sie durchsuchen die Webseite Ihrer Organisation nach Informationen über den Geschäftssitz, die Führungskräfte und Vorstände, sowie Organisationen mit denen eine enge Zusammenarbeit besteht. Zudem werten Sie die Verbindungen von Mitarbeitern untereinander in Netzwerken wie LinkedIn, Facebook und Twitter aus. Sobald sie die Struktur Ihrer Organisation kennen, beginnen Sie damit gezielt einzelne Mitarbeiter auszuwählen und auszuforschen. Sie wählen die Ziele passend zu ihrer jeweiligen Absicht – wenn sie auf Geld aus sind, würden sie wahrscheinlich auf einen Mitarbeiter der Lohnabteilung abzielen; wenn sie nach Steuerinformationen suchen, auf jemanden aus der Finanz- oder HR Abteilung. Wenn sie Zugriff auf Datenbanken erlangen wollen, wäre hingegen ein Mitarbeiter der IT-Abteilung ihr Ziel.

Sobald sie festgelegt haben worauf sie aus sind und wer ihr Ziel sein wird, beginnt die Erstellung des eigentlichen Angriffs. Meist wird hierfür das sog. Spear-Phishing genutzt. Als Phishing bezeichnet man einen Angriff, bei dem Angreifer eine E-Mail an Millionen Empfänger senden mit dem Ziel, viele davon zu einer Handlung zu verleiten, wie z.B. dem Öffnen eines infizierten E-Mail-Anhangs oder dem Aufruf einer manipulierten Webseite. Spear-Phishing ist im Prinzip vergleichbar, jedoch wird statt einer generischen E-Mail an Millionen von Empfängern eine sehr spezifische E-Mail an nur wenige, ausgewählte Adressaten verschickt. Diese Spear-Phishing E-Mails sehen meist völlig echt aus und sind daher schwer als solche zu

CEO Fraud

erkennen. Sie scheinen oft von jemandem zu kommen, den Sie kennen oder mit dem Sie zusammenarbeiten, wie z.B. ein Kollege oder gar Ihr Vorgesetzter. Die E-Mails nutzen vielleicht Ihr Firmenlogo, die offizielle E-Mail-Signatur und sind im gewohnten Umgangston geschrieben. Oft erzeugen sie einen starken Zeitdruck und fordern unmittelbare Handlungen, gleichzeitig soll aber auch komplettes Stillschweigen bewahrt werden. Das Ziel der Angreifer ist es, Sie durch die Eile zu Fehlern zu verleiten. Hier sind 3 gängige Szenarien:

CEO Fraud ist eine mächtige Angriffsform, die die meisten Verteidigungsmaßnahmen umgeht. Letztendlich sind SIE der beste Schutz dagegen.

- **Banküberweisung**: Der Angreifer ist auf Geld aus, daher forscht er aus wer in der Lohnabteilung oder dem Finanzbereich Ihrer Organisation arbeitet. Er erstellt dann eine E-Mail die vorgibt vom Leiter der Abteilung zu stammen und berichtet von einem Notfall aufgrund dessen dringend Geld auf ein angegebenes Konto überwiesen werden muss.

- **Steuerbetrug**: Cyberkriminelle wollen Informationen über Sie und Ihre Kollegen stehlen, um in ihrem Namen Steuerbetrug begehen zu können. Sie forschen Ihre Organisation aus und finden heraus, wer Mitarbeiterdaten verarbeitet, wie z.B. die Personalabteilung. Darauf aufbauend senden die Kriminellen E-Mails die vorgeben, von einem leitenden Angestellten oder jemandem aus der Rechtsabteilung zu stammen, und fordern bestimmte Dokumente mit personenbezogenen Inhalten an, die sofort bereitgestellt werden müssen.

- **Anwalts-Nachahmung**: Nicht alle CEO Fraud Angriffe bauen nur auf E-Mail, andere Methoden wie z.B. Anrufe können auch genutzt werden. In diesem Szenario senden die Angreifer zunächst eine E-Mail, die scheinbar von einer Führungskraft stammt. Darin wird angekündigt, dass in Kürze ein Anwalt in einer dringenden Angelegenheit anrufen wird. Ein Krimineller ruft dann tatsächlich an und gibt vor der angekündigte Anwalt zu sein. Er erzeugt eine große Dringlichkeit und spricht über zeitkritische, sehr sensible Themen. Diese Dringlichkeit soll Sie dazu bringen, ohne lange nachzudenken direkt zu handeln.

Schützen Sie sich

Was können Sie tun, um sich und Ihre Organisation bestmöglich zu schützen? Gesunder Menschenverstand ist Ihre beste Verteidigung. Wenn Sie eine Nachricht von Ihrem Vorgesetzten oder einem Kollegen erhalten, mit der einfach

CEO Fraud

irgend etwas nicht zu stimmen scheint, könnte es ein Angriff sein. Indikatoren könnten sein, dass eine große Dringlichkeit erzeugt wird, eine ungewöhnliche E-Mail-Signatur verwendet wird oder ein Ton angeschlagen wird, der sehr ungewöhnlich ist. Oft wird auch einfach eine Anrede für Sie genutzt, die der vermeintliche Absender sonst nie nutzen würde. Oder es wird eine E-Mail-Adresse oder Telefonnummer vom Angreifer genutzt, die Sie vorher nie gesehen haben oder die der Ihres Kollegen oder Vorgesetzten nur gleicht, aber nicht exakt übereinstimmt. Wenn Sie Zweifel haben, rufen Sie zur Absicherung die Person über eine Ihnen bekannte Rufnummer an oder treffen Sie sich mit ihr persönlich – antworten Sie aber nie auf zweifelhafte E-Mails! Umgehen Sie nie die Sicherheitsleitlinien und –prozesse Ihrer Organisation! Oft gibt es Richtlinien, die den Ablauf von Überweisungen oder die Herausgabe von Informationen regulieren, einschließlich eines Freigabeprozesses mit mehreren Beteiligten. Forderungen, die versuchen diese Richtlinien zu umgehen, sollten sofort als verdächtig eingestuft werden, unabhängig von ihrer vermeintlichen Quelle, und ganz genau nachgeprüft werden bevor eine Aktion erfolgt. Wenn Sie eine solche Forderung erhalten und nicht sicher sind, wie Sie damit umgehen sollen, kontaktieren Sie umgehend Ihren Vorgesetzten, den Helpdesk oder das Informationssicherheitsteam.

Weiterführende Informationen

Social Engineering:	https://securingthehuman.sans.org/ouch/2014#november2014
Phishing:	https://securingthehuman.sans.org//ouch/2015#december2015
Schadprogramme:	https://securingthehuman.sans.org/ouch/2016#march2016
Zwei-Faktor-Authentifizierung:	https://securingthehuman.sans.org/ouch/2015#september2015
Tip des Tages (engl.):	https://www.sans.org/tip-of-the-day

Informieren Sie Sich

Abonnieren Sie den monatlichen OUCH! Security Awareness Newsletter, greifen Sie auf die OUCH! Archive zu und lernen Sie mehr über SANS Security Awareness Angebote unter securingthehuman.sans.org/ouch/archives.

Deutsche Ausgabe

Diese OUCH! Ausgabe wurde von Marek Kreul und René Wiedewilt aus dem Englischen übersetzt. Beide arbeiten für das CERT eines DAX-Konzerns und haben sich auf IT-Forensik spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

Redaktionsleitung: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley