SOCIAL ENGINEERING HANDBUCH

Ein Leitfaden für die Praxis

Inhaltsverzeichnis

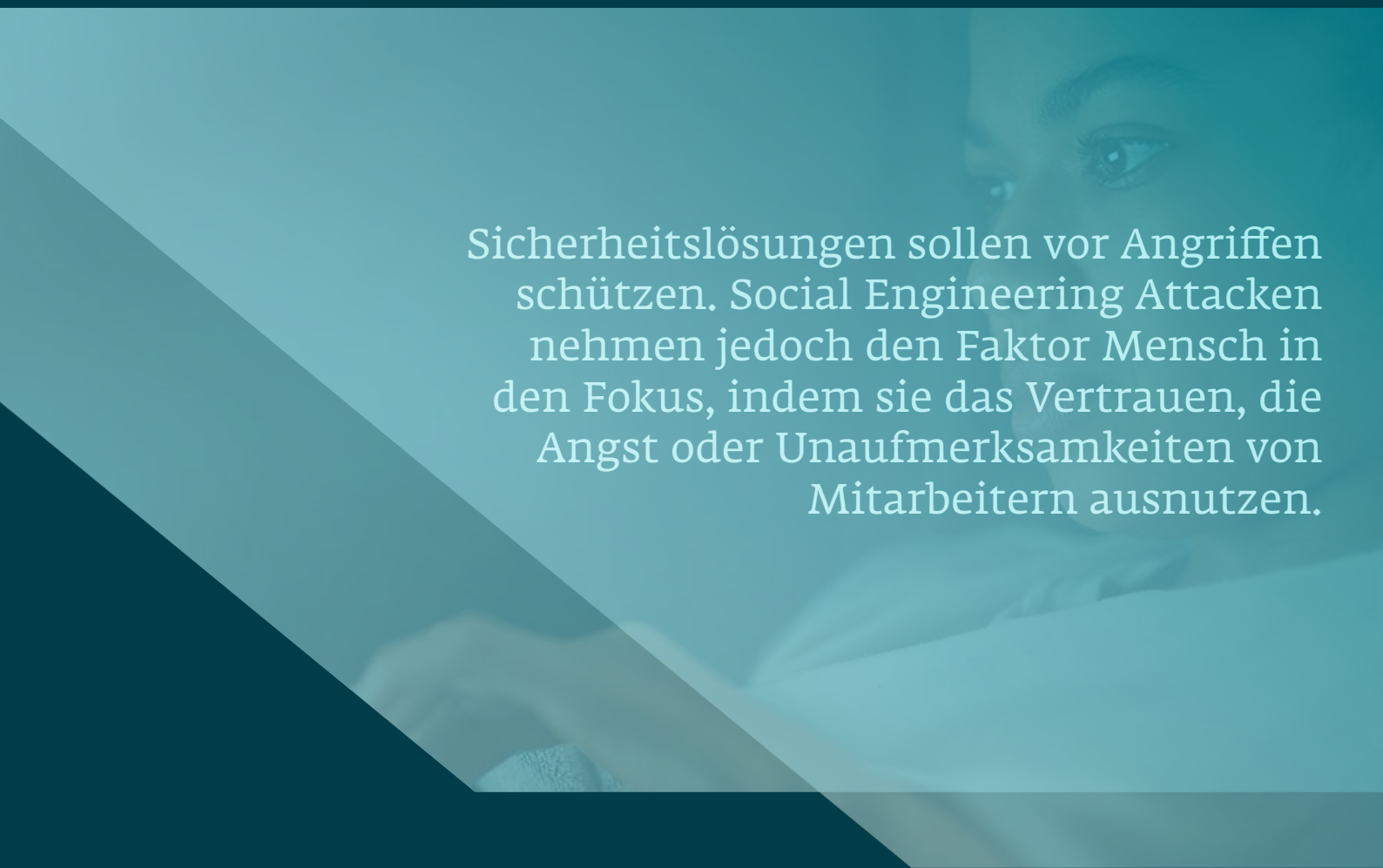
- Einleitung 03
- Social Engineering – Die Methoden im Überblick 05
- Phishing – Der Mitarbeiter an der Angel 07
- Identitätsbetrug – Wenn die E-Mail gar nicht vom Chef kommt 12
- Sextortion – Das Geschäft mit der Angst 16
- Weitere Formen des Social Engineering 19
- 5 Schritte gegen Social Engineering 20

Einleitung

Menschen sind emotionale Wesen, bei denen ein großer Teil des täglichen Handelns von Gefühlen aller Art geprägt wird. Das wissen auch Cyberkriminelle und entwickeln immer neue Methoden, genau diese Eigenart auszunutzen. Beim sogenannten Social Engineering nutzen Angreifer gezielt die Schwachstelle Mensch aus. Dafür benötigen sie noch nicht einmal besondere technische Expertise, um beispielsweise an sensible Daten zu gelangen oder Mitarbeiter dazu zu bringen, ihnen Zugang zu Unternehmensnetzwerken zu ermöglichen. Hierbei spielt es keine Rolle, wie klein das fragliche Unternehmen ist – jedes ist ein potenzielles Ziel.

Dieses kleine Handbuch fasst die wichtigsten Themen rund um das Thema Social Engineering zusammen und gibt Ihnen nützliche Tipps mit an die Hand. Welche Betrugsmaschen waren und sind besonders beliebt? Und wie können sich Unternehmen effektiv und nachhaltig vor Social Engineering Angriffen schützen?

Dabei verlassen wir uns nicht nur auf trockene Theorie, sondern arbeiten mit tatsächlichen Beispielen. Damit erkennen Sie sowie Ihre Mitarbeiter Social Engineering sicher und können die richtigen Maßnahmen ergreifen.



Sicherheitslösungen sollen vor Angriffen schützen. Social Engineering Attacken nehmen jedoch den Faktor Mensch in den Fokus, indem sie das Vertrauen, die Angst oder Unaufmerksamkeiten von Mitarbeitern ausnutzen.

Social Engineering – Eine Gefahr für KMU?

Längst haben Angreifer kleine und mittelständische Unternehmen als lohnenswertes Ziel erkannt und fahren vermehrt Attacken gegen Mittelständler - darunter besonders häufig Social Engineering Angriffe. Dieser Gefahr sind sich auch die Unternehmen mittlerweile bewusst.

So gaben in dem 2020 veröffentlichten Studienbericht „Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt" des Digitalverbands Bitkom 15 % der befragten Unternehmen an, bereits in digitaler Form von Social Engineering betroffen gewesen zu sein.

Und sie tun gut daran, die Lage ernst zu nehmen: Allein 2020 gingen beim Crime Complaint Center (IC3) des FBI 19.369 Meldungen zu kompromittierten E-Mails (Business-E-Mail Compromise, BEC) bzw. E-Mail-Postfächern (E-Mail Account Compromise, EAC) ein. Hierbei geht es den Kriminellen vor allem darum, Privatpersonen oder Mitarbeiter von Unternehmen dazu zu bringen, Gelder auf die Konten der Angreifer zu überweisen. Der dadurch verursachte Schaden wird für das Jahr 2020 auf mehr als 1,8 Milliarden US-Dollar geschätzt.

Auswirkungen von Cyberangriffen auf kleine und mittlere Unternehmen

37%	25%	10%
Finanzielle Verluste	Insolvenz	Aufgabe der Geschäftstätigkeit

Quelle: NCSA

Social Engineering – Die Methoden im Überblick

Phishing / Spearphishing

Phishing: Die wohl bekannteste Form des Social Engineering. Beim Phishing (von engl. „fishing" – angeln) versuchen Kriminelle unvorsichtige Internetnutzer durch Fake-Nachrichten dazu zu bringen, sensible Informationen (z. B. Kreditkarten- oder Logindaten) preiszugeben oder durch Klick auf Links Malware herunterzuladen.

Spearphishing: Während klassische Phishing-Mails wahllos und in großer Menge verschickt werden, sind sogenannte Spearphishing-Attacken genau auf ein bestimmtes Ziel, egal ob Einzelperson, Organisation oder Unternehmen, ausgerichtet und entsprechend optimiert.

Vishing und Smishing

Mit dem klassischen Phishing eng verwandt, bedienen sich diese beiden Formen lediglich anderer Medien, um ihre Opfer zu kontaktieren. Während Vishing VoIP-Anrufe nutzt, arbeitet Smishing mit betrügerischen SMS. Hierbei gab es zwar schon Fälle, bei denen das potenzielle Opfer direkt zur Preisgabe sensibler Daten per SMS-Antwort aufgefordert wurde – meist erfolgt jedoch die Weiterleitung auf eine betrügerische Webseite, auf der die entsprechenden Informationen eingegeben werden sollen.

Identitätsbetrug/Impersonation

Immer häufiger kommt es vor, dass Betrüger sich als Mitarbeiter einer öffentlichen Behörde oder auch als Person der oberen Managementebene ausgeben und ihre potenziellen Opfer aus dieser Position heraus unter Druck setzen. Vor allem im Internet ist diese Masche für Kriminelle ungleich einfacher, da sie hier von der Anonymität profitieren. Vom potenziellen Opfer verlangen sie dann beispielsweise die Überweisung großer Summen auf zwielichtige Konten oder weisen sie an, umfassende Bestellungen bei vermeintlichen Geschäftspartnern aufzugeben.

Social Engineering – Die Methoden im Überblick

Sextortion
Hierbei handelt es sich um eine spezielle Form der Erpressung, bei welcher der Täter dem Opfer mit der Veröffentlichung von kompromittierten Inhalten des Opfers droht. E-Mails sollen potenzielle Opfer durch falsche Anschuldigungen – vor allem zu angeblich pikanten Situationen – in Panik versetzen und zu unüberlegtem Verhalten verleiten.

Scareware
Sogenannte Scareware ist ebenfalls darauf ausgerichtet, das potenzielle Opfer zu verunsichern und es dazu zu bringen, freiwillig Schadsoftware zu installieren. Besonders häufig werden Fake-Antivirus-Programme eingesetzt. Diese geben vor, eine Bedrohung erkannt zu haben, die sich nur durch die Installation eines weiteren Programms – typischerweise Malware – beseitigen lassen.

Tech-Support Scams
Hierbei geben sich die Kriminellen telefonisch oder per Mail als Mitarbeiter eines technischen Supports aus. Ziel ist es, dem potenziellen Opfer nutzlose Services zu verkaufen, nicht-existente technische Probleme zu lösen oder per Remote-Access-Zugriff auf das Gerät und die Daten des Mitarbeiters zu erhalten. Aktuell sieht es so aus, als würden mit zunehmender Verbreitung von Home-Offices solche Betrugsversuche immer häufiger werden.

Als **„Cyber-Scam“** (Scam = engl. Betrug, Abzocke) bezeichnet man üblicherweise einzelne oder Kombinationen mehrerer der oben genannten Betrugsmaschen.

Phishing – Der Mitarbeiter an der Angel

Sicher haben Sie und Ihre Mitarbeiter bereits „klassische“ Phishing-Mails in Ihren Postfächern gefunden. Beim Absender handelt es sich zum Beispiel um eine Bank oder einen speziellen Dienstleister. Dieser fordert vom User die „Bestätigung“ von Konto- oder Kreditkartendaten, meist durch Klick auf einen in der Mail bereitgestellten Link. So veraltet die Methode erscheinen mag, so erfolgreich ist sie noch immer. Dabei sind Fake-Mails moderner Phishing-Kampagnen zum Teil so gut gestaltet, dass sie selbst für geschulte Nutzer nur schwer als solche erkennbar sind.

Doch was wollen die Kriminellen erreichen? Ihr Ziel ist es, durch irreführende Mails an Logindaten oder vertrauliche Informationen zu gelangen oder den Empfänger dazu zu bringen, Malware zu installieren. Phishing-Kampagnen nehmen entweder relativ ungerichtet eine Vielzahl an Nutzern ins Visier oder richten sich spezifisch auf einzelne Personen oder Personengruppen (Spearphishing).

Dabei wissen die Angreifer selbstverständlich, dass die meisten E-Mail-Provider eingehende Mails auf gefährliche Inhalte prüfen und potenzielle Phishing-Mails sofort in den Spam-Ordner verschieben. Um dem zumindest eine gewisse Zeit zu entgehen, werden die Nachrichten laufend verändert.

Phishing – Der Mitarbeiter an der Angel

Die Corona-Pandemie scheint die „Beliebtheit" von Phishing bei Kriminellen noch gesteigert zu haben. Die Methode profitiert doch gerade von Unsicherheit, Ängsten und Engpässen, wie z. B. einem Mangel an wichtigen Gütern. Im März 2020 war COVID-19 eines der beliebtesten Themen von Phishing-Mails, die Malware installieren, sensible Daten abgreifen oder Fake-Produkte an den Mann bringen wollten (Quelle: ESET Threat Report Q1-2020).

Die Pandemie ist übrigens nur ein Beispiel von vielen. Jede Krise bietet Cyberkriminellen durch die damit einhergehenden Unsicherheiten enormes „Geschäftspotenzial".

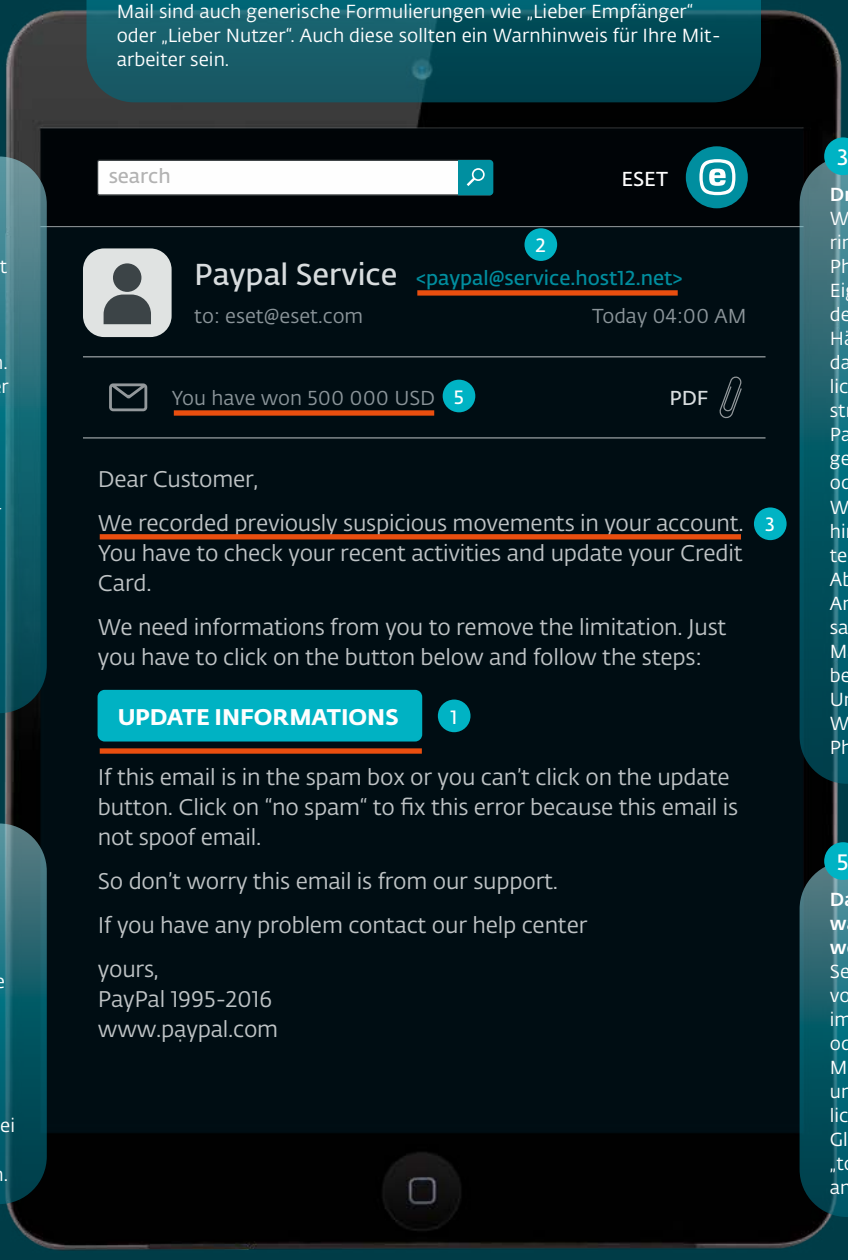
94% der Malware werden per E-Mail verbreitet

17.700 US-Dollar gehen jede Minute durch Phishing-Angriffe verloren

Täglich werden rund 14,5 Milliarden Spam-E-Mails verschickt

Quelle: CSO, hostingtribunal.com

Der beste Schutz: Phishing-Mails erkennen, bevor sie Schaden anrichten



1

Fehler in Rechtschreibung oder Grammatik
Häufig sind die Angreifer der Sprache ihres Opfers nur begrenzt mächtig und nehmen sich nicht die Zeit, Details wie Rechtschreibung und Grammatik ihrer Mails zu prüfen. Es lohnt sich daher, Ihre Mitarbeiter dahingehend zu sensibilisieren. Auffällig viele Tippfehler, fehlende Wörter oder viele grammatikalische Fehler sollten Sie stutzig werden lassen. Ein weiterer deutlicher Hinweis auf eine potenzielle Phishing-Mail sind auch generische Formulierungen wie „Lieber Empfänger" oder „Lieber Nutzer". Auch diese sollten ein Warnhinweis für Ihre Mitarbeiter sein.

2

Verdächtige Absender-Adresse
Die Adresse oder Domain des Senders zu fälschen, um die Mail echter aussehen zu lassen, kostet zusätzlich Zeit und Geld, die sich Angreifer nicht immer nehmen – es fallen auch so genug Opfer auf die Phishing-Versuche herein. Weisen Sie Ihre Mitarbeiter daher auf folgendes hin: E-Mails mit unbekannter Absender-Adresse, die Ihnen seltsam vorkommen, weil sie beispielsweise lediglich aus einer willkürlichen Kombination von Zahlen und Buchstaben bestehen, sollten direkt in den Spam-Ordner verschoben werden. Zudem sollten Mitarbeiter beim Erhalt entsprechender Nachrichten unbedingt die IT-Abteilung darüber informieren.

3

Dringlichkeit
Wie andere Social Engineering-Methoden auch, versucht Phishing typisch menschliche Eigenarten auszunutzen, besonders gern Unsicherheit und Angst. Häufig enthalten Phishing-Mails daher Aussagen, die die Dringlichkeit der Angelegenheit unterstreichen – z. B. weil sonst ein Paket an den Absender zurückgeschickt, ein Account gelöscht oder ein Konto geschlossen wird. Weisen Sie Ihre Mitarbeiter darauf hin, dass Banken, Paketdienstleister, Behörden und selbst interne Abteilungen auch in dringlichen Angelegenheiten E-Mails immer sachlich und neutral formulieren. Machen Sie deutlich, dass es sich bei einer Nachricht, die versucht Unsicherheit auszulösen, mit aller Wahrscheinlichkeit um einen Phinsing-Versuch handelt.

4

Bitte um Zusendung sensibler Daten
Informieren Sie Ihre Mitarbeiter zudem darüber, dass Institutionen wie Banken, Dienstleister oder Behörden und selbst andere Abteilungen in Ihrem Unternehmen üblicherweise nicht darum bitten, sensible Daten (Logindaten, personenbezogene Daten, Passwörter etc.) per Mail oder Telefon zu versenden – es sei denn, es wurde vorher ein entsprechender Prozess angestoßen.

5

Das Angebot klingt zu gut, um wahr zu sein? Dann ist es das wohl auch
Sensibilisieren Sie Ihre Mitarbeiter vor vermeintlichen Super-Deals im Netz. Das gilt für Geschenke oder Gewinne, die durch Social Media-Posts versprochen werden und für die der Nutzer angeblich „überhaupt nichts" tun muss. Gleiches gilt für Mails, die eine „todsichere Gelegenheit, Geld anzulegen" versprechen.

Phishing über andere Kanäle

Auch wenn noch immer die meisten Phishing-Versuche per Mail stattfinden, sind andere Methoden auf dem Vormarsch.

SMiShing

Beim sogenannten SMiShing läuft der Betrugs-Versuch über SMS oder Instant-Messenger anstatt per E-Mail. Auch diese besondere Form des Phishings gewann zu Beginn der Corona-Pandemie an Fahrt. Potenzielle Opfer erhielten plötzlich SMS mit unbekanntem Absender – vorgeblich von örtlichen Behörden.

Dabei waren viele Opfer zunächst erstaunt darüber, dass Kriminelle ohne ihr Wissen an ihre Telefonnummer gelangen konnten. Dabei ist es aus IT-Sicht relativ einfach, eine gültige Telefonnummer in einer endlichen (und verhältnismäßig kleinen) Anzahl an Zahlenkombinationen zu finden.

Eine andere Angriffsart zielt auf unser Mitgefühl ab. Potenzielle Opfer erhielten eine SMS mit der Bitte um Spenden für in Not geratene Mitmenschen, z. B. durch Naturkatastrophen. Praktischerweise wurde gleich eine Kontonummer mitgeliefert, auf welche die Spende dann überwiesen werden sollte.

Kurzer Test: Fake oder nicht? Stammt diese Nachricht wirklich von einer Bank?

Eine Bank würde Ihnen niemals einen direkten Link wie diesen senden.

Wenn Sie sich nicht sicher sind, loggen Sie sich über die offizielle Website oder App in Ihrem Online Banking ein, um zu prüfen, ob Sie eine Benachrichtigung erhalten haben.

Vishing

Während Smishing im Vergleich weniger technisch anspruchsvoll wirkt als Phishing per Mail, ist beim sogenannten **Vishing** das Gegenteil der Fall. Hier rufen die Kriminellen (oder Personen, die von ihnen bezahlt werden) das potenzielle Opfer an und geben sich als Vertreter einer offiziellen Einrichtung, z. B. einer Bank, aus. Sie informieren beispielsweise darüber, dass es Probleme mit einem Konto gäbe. Um das Problem zu lösen, bitten sie um persönliche Daten und Kontoinformationen. Um herauszufinden, ob es sich beim fraglichen Anruf wirklich um eine Anfrage der Bank handelt, sollten Sie und Ihre Mitarbeiter daher folgendes beachten: Geben Sie vorerst auf keinen Fall Informationen preis. Bitten Sie um mehr Informationen und eine Verifizierung des Anrufers bzw. der Bank. Doch vor allem: Sollten Sie oder Ihre Mitarbeiter sich unsicher sein, beenden Sie das Gespräch und rufen direkt beim Kundenservice Ihrer Bank an, um die Situation aufzuklären.

Identitätsbetrug – Wenn die E-Mail gar nicht vom Chef kommt

Ein altbekanntes Beispiel...
„Es ist kurz vor Feierabend, der Mitarbeiter ist noch im Büro. Gerade in dem Moment, in dem er in den Feierabend starten wollte, erhält er eine Nachricht vom CEO der Firma. Der Inhalt: Eine Bitte, noch schnell eine Überweisung auszuführen. Es sei dringend, da nur so der lukrative Vertrag mit dem neuen Partner abgeschlossen werden könne." Natürlich handelt es sich beim Absender der Nachricht nicht um den CEO des Unternehmens. Auch der angebliche Geschäftspartner existiert genauso wenig, wie der vermeintlich lukrative Vertrag.

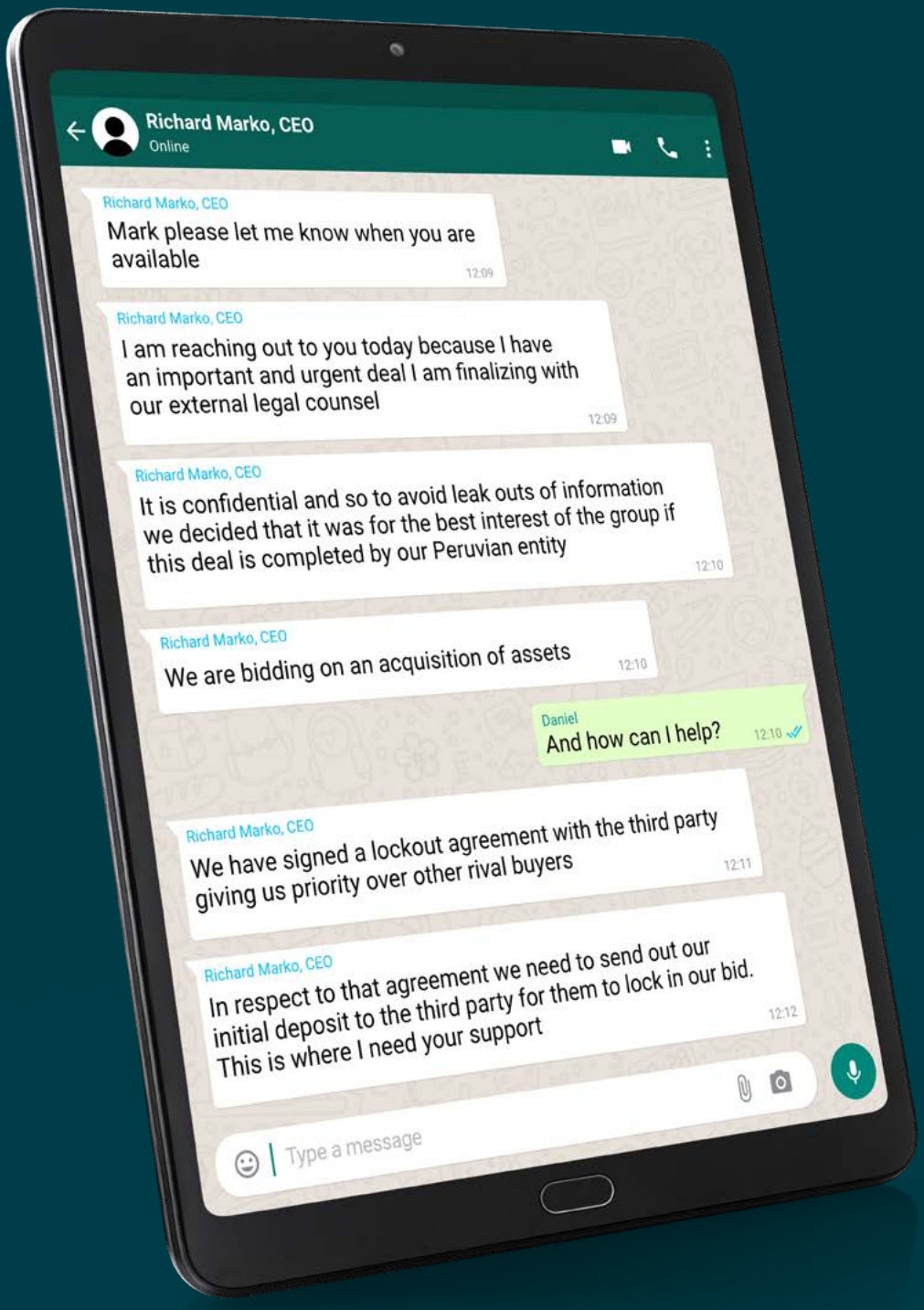
Zugegeben, das ist wohl das bekannteste und offensichtlichste Beispiel für Identitätsbetrug, eine spezielle Form des Social Engineering. Und gerade bei solchen Beispielen fällt es schwer zu glauben, dass noch immer Menschen auf diese Betrugsmasche hereinfallen. Mittlerweile sollte doch jeder entsprechende Nachrichten im Schlaf erkennen? Leider werden Cyberkriminelle aber immer besser darin, ihre Nachrichten so aussehen zu lassen, als kämen sie tatsächlich von offizieller Seite. Gerade im stressigen Arbeitsalltag fällt es Nutzern so schwer, sie als Fake zu erkennen. Ziel der Angreifer ist auch hier wieder, an vertrauliche Informationen zu gelangen oder Zugriff auf eine Person, ein Unternehmen oder ein Netzwerk zu erhalten.

Für einen „gelungenen" Identitätsbetrug geben sich die Kriminellen einige Mühe: Über Unternehmensseiten oder Social Media spionieren sie potenzielle Opfer umfassend aus. Plattformen wie LinkedIn oder Xing bieten nicht nur die Namen von Angestellten und Führungskräften, sondern liefern ihre genaue Positionsbezeichnung gleich mit. Mit einer solchen Vielzahl an Informationen sind die Betrüger in der Lage, ihre Nachrichten möglichst echt aussehen zu lassen.

Auch bei den verwendeten Kanälen sind die Angreifer kreativ. Oft rufen sie ihre potenziellen Opfer an oder – noch häufiger – kontaktieren sie per E-Mail oder Messenger. In diesen Fällen bedienen sie sich häufig der Namen von Personen aus der oberen Managementebene und lassen ihre Nachrichten so aussehen, als kämen sie von „ganz oben". Das Opfer kennt diese Menschen selten persönlich und ist geneigter, auf die Forderungen einzugehen. Diese sind meist sehr ähnlich: Die Betrüger fordern die Opfer auf, Geld zu überweisen, Rechnungen zu begleichen oder vertrauliche Informationen preiszugeben. Die Folge: Direkte finanzielle Verluste oder Datenlecks mit den entsprechenden weitreichenden Nachwirkungen.

Es kann jeden treffen: ESET im Visier

2020 war ESET selbst Ziel eines CEO-Frauds, bei dem sich die Angreifer per WhatsApp als CEO Richard Marko ausgaben. Sie behaupteten, der entsprechende Mitarbeiter müsse dringend Geld überweisen, um ESET Vorteile bei einem Ausschreibungsverfahren zu verschaffen. Aber lesen Sie selbst:



Tipps, wie Sie Ihren Mitarbeitern helfen, Identitätsbetrug sofort zu erkennen

Viele Unternehmen verlassen sich darauf, dass ihre Security-Lösung sie umfassend vor Cyberangriffen schützt – und tun prinzipiell auch gut daran. Gegenüber Social Engineering und insbesondere Identitätsbetrug können jedoch selbst die ausgefeiltesten Abwehrmechanismen nur begrenzt helfen. Neben einer technisch ausgereiften und aktuellen Security-Lösung sollte daher zum Sicherheitskonzept eines Unternehmens auch immer die Schulung der Mitarbeiter gehören.

Auf den nächsten Seiten geben wir Ihnen hilfreiche Tipps zur Schulung Ihrer Mitarbeiter zum Thema Identitätsbetrug/Impersonation.

ZEIGEN SIE AUF, WIE MITARBEITER TYPISCHE MUSTER ERKENNEN KÖNNEN

Üblicherweise klingen die Nachrichten sehr dringlich und sollen beim Empfänger Unsicherheit und Angst auslösen. Werden Sie in einer Mail zu etwas aufgefordert, das Ihnen seltsam vorkommt (wie bspw. Überweisungen an bisher unbekannte Empfänger zu tätigen) und wird dies auch noch mit besonderer Dringlichkeit an sie herangetragen (z. B. mit einer sehr knappen Deadline), sollten Sie hellhörig werden.

Die Angreifer erstellen mittlerweile täuschend echt wirkende E-Mails, zum Teil sogar mit Fotos oder Signaturen „echter" Vorgesetzter. Ihre Mitarbeiter sollten daher folgendes beherzigen: Auch wenn die Form der E-Mail echt wirkt, sollten Sie sich den Inhalt genau anschauen und auf Ungereimtheiten prüfen.

Machen Sie deutlich, warum Mitarbeiter immer den Kontext von Nachrichten prüfen sollten

Ihre Mitarbeiter sollten sich bei merkwürdigen Nachrichten folgende Fragen stellen: Warum möchte der Vorgesetzte, dass die Überweisung getätigt wird? Warum braucht der Kollege genau diese vertrauliche Information? Besonders Anweisungen, die nicht den üblichen Arbeitsabläufen entsprechen, sollten Sie stutzig werden lassen.

Tipps, wie Sie Ihren Mitarbeitern helfen, Identitätsbetrug sofort zu erkennen

GEBEN SIE TIPPS, WIE MITARBEITER DIE ADRESSE DES ABSENDERS PRÜFEN KÖNNEN

Die E-Mail ist geschäftlichen Inhalts, kommt aber von einer privaten Mailadresse? Auch wenn die Nachricht scheinbar von jemandem kommt, den Ihre Mitarbeiter kennen: Teilen Sie Ihren Mitarbeitern mit, dass Sie den vermeintlichen Absender immer über seine offizielle Unternehmens-Mailadresse kontaktieren sollten, um die Rechtmäßigkeit der Anfrage zu prüfen. Teilweise arbeiten Cyberkriminelle auch mit Mailadressen, die nur fast wie offizielle und Ihnen bekannte Unternehmens-Mail-Adressen aussehen. Weisen Sie Ihre Mitarbeiter darauf hin, dass es sich lohnt, genau hinzusehen. Nur so können Buchstabendreher oder leicht zu übersehende Abweichungen wie „rn“ statt „m“ erkannt werden.

Ein weiterer TIPP: Implementieren Sie einen „EXTERN“-Tag

Erreichen E-Mails von außerhalb Empfänger im Unternehmen, lassen sich diese unkompliziert mit dem deutlich sichtbaren Hinweis „EXTERN“ versehen. So können Sie und Ihre Mitarbeiter sofort erkennen, welche E-Mails von außerhalb kommen und feststellen, welche E-Mails ggf. größerer Aufmerksamkeit bedürfen.

VERWEISEN SIE AUF DIE KONTAKTAUFNAHME ÜBER EINEN ANDEREN KANAL

Sensibilisieren Sie Ihre Mitarbeiter, kein unnötiges Risiko einzugehen. Sollte einem Ihrer Mitarbeiter eine E-Mail komisch vorkommen, sollte er den Absender anrufen oder anderweitig kontaktieren. Dasselbe gilt für WhatsApp- oder andere Nachrichten oder Anrufe.

SICHERLICH: All diese Tipps kosten das, wovon wir beim Arbeiten häufig zu wenig haben: Zeit. Dennoch sollten Sie und Ihre Mitarbeiter sie beherzigen, um schwerwiegende negative Folgen für Ihr Unternehmen zu vermeiden

Sextortion – Das Geschäft mit der Angst

„Hallo, mein Lieber. Du kennst mich nicht, aber ich kenne dich sehr gut. Besser, als du vielleicht denkst. Das hier ist dein Passwort, oder?“

E-Mails wie diese landen fast täglich in den Postfächern von Angestellten. Der Verfasser behauptet meist, den Empfänger über dessen Webcam beim Konsum von Pornographie oder anderen kompromittierenden Inhalten gefilmt zu haben. Er fordert Geld – andernfalls würde er die Familie oder Kollegen des Empfängers über dessen „Fehlverhalten“ informieren. So plump sie ist, so erfolgreich ist diese Masche. Aus Angst vor negativen Konsequenzen gehen nicht wenige Empfänger auf die Forderungen ein und zahlen die entsprechende Summe. Dabei sind die Anschuldigungen meist ohnehin haltlos. Das angebliche Video existiert nicht, der Absender hat nichts in der Hand und versucht lediglich, dem Empfänger Angst zu machen und so glaubwürdiger zu erscheinen.

ERLÄUTERN SIE, DASS SEXTORTION-VERSUCHE GERADE IM TREND LIEGEN

Machen Sie Ihren Mitarbeitern klar, dass Erpressungsversuche per Mail, gerade in Bezug auf vermeintlich kompromittierende Inhalte, aktuell zu den häufigsten Betrugsversuchen im Netz gehören. Zusätzlich Vorschub geleistet hat dieser Entwicklung die aktuell grassierende Corona-Pandemie: Zum einen arbeiten immer mehr Menschen mobil von zuhause oder anderswo. Da Heimrechner und -netzwerke oft weniger gut abgesichert sind als Unternehmensnetzwerke, erreichen nicht nur mehr betrügerische Mails die Postfächer von Angestellten – auch ihre „Erfolgs“-Wahrscheinlichkeit ist höher. Es ist davon auszugehen, dass in Zukunft entsprechend mehr Sextortion-Mails in Umlauf geraten werden. Zum anderen profitieren die Angreifer auch in Bezug auf die Inhalte ihrer Erpressermails von COVID-19: So wurden E-Mails beobachtet, die ihren Empfängern damit drohen, bei Nichterfüllung der Forderungen den Empfänger und seine Familie mit dem Virus zu infizieren. Besprechen Sie diese Beispiele mit Ihrem Team.

Doch wie schützen Sie Ihre Mitarbeiter nun am besten davor, auf solche E-Mails hereinzufallen?

VERDEUTLICHEN SIE DIE ZIELE DER ANGREIFER

Ihre Mitarbeiter sollten wissen, was das Hauptziel der Angreifer ist: Geld. Das Opfer soll zur Zahlung bestimmter Summen gebracht werden, möglichst in Bitcoin oder anderen anonymen Cyberwährungen. Allzu schlecht scheinen die Kriminellen damit nicht zu fahren: Dem Crime Complaint Centre des FBI zufolge verzeichneten Unternehmen 2020 Verluste von rund 70,9 Millionen US-Dollar.

Sextortion – Das Geschäft mit der Angst

ERKLÄREN SIE, WIE LEICHT HACKER AN PASSWÖRTER GELANGEN

Nicht selten enthalten erpresserische E-Mails echte Daten ihrer Empfänger, vor allem tatsächlich verwendete Passwörter. Das erhöht den Druck auf den Empfänger und die Sorge, dass der Erpresser tatsächlich kompromittierende Inhalte besitzen könnte. Machen Sie Ihren Mitarbeitern klar, wie der Markt für gestohlene Passwörter funktioniert, insbesondere, zu welch geringen Preisen Kriminelle Passwörter und Zugangsdaten aus Datenlecks im Darknet kaufen können. Dabei können sie mit dem Daten selbst wenig anfangen – sie dienen vor allem dazu, betrügerische E-Mails und die angedrohten Konsequenzen echt wirken zu lassen.

Nutzen Sie die Möglichkeit und verdeutlichen Sie in diesem Zusammenhang auch noch einmal, wie wichtig starke Passwörter oder Passphrasen sind. Vergewissern Sie sich, dass Ihre Mitarbeiter wissen, wie sie diese erstellen. Immer häufigere Datenlecks und der mittlerweile florierenden Handel mit Zugangsdaten machen es umso nötiger, unternehmensweit eine Multi-Faktor-Authentifizierung zu implementieren.

ZEIGEN SIE, WIE AUF SEXTORTION-VERSUCHE ZU REAGIEREN IST

Stimmt das in der E-Mail erwähnte Passwort mit einem aktuell vom Empfänger verwendeten überein, sollte dieser nicht in Panik verfallen – aber natürlich auch nicht das Passwort einfach nur ändern und nichts weiter unternehmen. Unterstreichen Sie, dass unter keinen Umständen Geld gezahlt werden darf. Zudem sollten aber auch keine Links oder andere Inhalte in der Mail angeklickt oder Anhänge geöffnet werden. Verdeutlichen Sie Ihren Mitarbeitern, dass sie – sollten sie doch einmal auf eine betrügerische E-Mail hereingefallen sein – unbedingt die interne IT- oder Sicherheitsabteilung informieren müssen. Scham ist hier fehl am Platz. Es sollte zudem in Erwägung gezogen werden, ob die Polizei hinzuzuziehen ist.

SPRECHEN SIE ÜBER DIE WAHREN GEFAHREN

So furchteinflößend sie für den Einzelnen zunächst sein mögen: Für sich genommen sind Sextortion-Mails – sofern man angemessen mit ihnen umgeht – meist völlig ungefährlich. Nichtsdestotrotz sollte Ihren Mitarbeitern bewusst sein, dass kriminelle Dritte durchaus tatsächlich Zugriff auf fremde Webcams erlangen können.

VERDEUTLICHEN SIE DIE ZUSÄTZLICHEN SICHERHEITSANFORDERUNGEN IM HOME-OFFICE

Auch in Zukunft wird sich der Trend des immer flexibleren und mobileren Arbeitens fortsetzen. Allerdings darf auch hier die Sicherheit nicht außer Acht gelassen werden. Angestellte müssen für die sichere Arbeit im Home-Office gesondert geschult werden. Wissen Ihre Mitarbeiter beispielsweise, dass sie sich nur dann in öffentliche W-LANs einwählen sollten, wenn diese passwortgeschützt sind? Arbeiten Mitarbeiter von außerhalb, sollten sie zudem möglichst nur per VPN (Virtual Private Network) auf das Unternehmensnetzwerk zugreifen, um Angreifern kein leichtes Spiel zu bieten.

Machen Sie deutlich, wie Hacker fremde Rechner oder Webcams kapern

Erklären Sie Ihren Mitarbeitern, dass meist Trojaner/Trojanische Pferde zum Einsatz kommen, um Zugriff auf fremde Rechner oder Webcams zu erlangen, die das Gerät mit einer Remote-Desktop-Software infizieren. Zeigen Sie auf, dass dadurch das Gerät von außen steuerbar wird. Machen Sie jedoch auch deutlich, dass die Angreifer hierfür allerdings die „Unterstützung" des Nutzers benötigen und es oft schon ausreicht, Software aus nicht vertrauenswürdigen Quellen herunterzuladen. Selbst wenn diese die Funktion erfüllt, für die sie installiert wurde – im Programmcode kann sich trotz allem Malware verbergen. Hiermit erlangen die Angreifer völlig unbemerkt Kontrolle über fremde Rechner oder Webcams. Weisen Sie Ihre Mitarbeiter vor allem auch daraufhin, dass es ein Trugschluss ist zu glauben, dass in irgendeiner Weise erkennbar wäre, ob die Kamera gerade aktiv ist. Ein wichtiges Ziel der Angreifer ist schließlich, unerkannt zu bleiben – entsprechend programmieren sie ihre Malware.

Machen Sie Ihren Mitarbeitern bewusst, dass Kriminelle, sobald sie einmal Zugriff auf deren Webcam erhalten haben, zum einen Aufnahmen in Momenten machen können, in denen Sie lieber unbeobachtet wären. Und noch viel schlimmer, Zugang zu vertraulichen Daten oder Dokumenten bekommen, wenn sie zusätzlich auch das Mikrofon gehackt haben. Denn so können Angreifer Unterhaltungen aller Art – darunter auch vertrauliche – ganz einfach mitschneiden.

Weitere Formen des Social Engineering

Scareware versucht ihre Opfer zu überzeugen, potenziell gefährliche Software zu kaufen und herunterzuladen. Dafür macht sie sich – wieder einmal – die Angst der Opfer zunutze und informiert zum Beispiel über auf dem Rechner festgestellte Viren, die nur mit dieser Software entfernt werden können. Und dies natürlich möglichst schnell. Häufig tauchen dabei Pop-ups auf dem Bildschirm auf, die sich nur schwer schließen lassen und den Druck auf den Nutzer erhöhen sollen.

Dem Anwender wird oftmals eine ganze Liste mit Viren, die angeblich auf dem Rechner gefunden wurden angezeigt. Zeigen Sie Ihren Mitarbeitern auf, dass der Rechner in einem solchen Fall nicht wirklich gescannt wurde und die Scan-Ergebnisse frei erfunden sind. Ebenso wie die vermeintliche Security-Software mit schön klingenden Namen wie Advanced Cleaner, SpyWiper, System Defender oder ähnlichen Bezeichnungen. Machen Sie Ihren Mitarbeitern daher bewusst, dass der Rechner jedoch durch das Herunterladen der fragwürdigen Software mit ziemlich großer Wahrscheinlichkeit mit Malware infiziert wird.

Nutzen Sie und Ihre Mitarbeiter außschließlich bekannte, getestete und aktuelle Software.

Zudem ist der Einsatz professioneller Sicherheitslösungen ein „Muss". Darunter fallen Malwareschutz, Verschlüsselung und Multi-Faktor-Authentifizierung im Sinne des Multi Secured Endpoints.

Tech-Support Scams sind eng verwandt mit Scareware und bieten ebenso wie diese ungefragt vermeintlich nützliche Dienste an, um Malware „an den Mann oder die Frau" zu bringen. Im Gegensatz zu Scareware gibt sich diese Form der Fake-Software aber als Produkt bekannter Software-Hersteller, z. B. Microsoft aus. Sie gibt auch nicht vor, Dateien auf Ihrem Rechner zu überprüfen – das überlässt sie Ihren Mitarbeitern schon selbst. Sie werden aufgefordert, einen genaueren Blick auf bestimmte Dateien oder Prozesse auf Ihrem Rechner zu werfen. Eigentlich völlig normale Eigenschaften oder Verhaltensweisen werden Ihnen dann als problematisch verkauft. Angeblich beheben lässt sich dies dann nur mithilfe eines Programms. Verdeutlichen Sie, dass es sich bei dem vermeintlichen Programm natürlich wiederum um Malware handelt.

5 Schritte gegen Social Engineering

1.

Regelmäßige Mitarbeiter-Schulungen

Wichtig: Zu „Mitarbeitern" zählen hier wirklich alle, vom Sachbearbeiter über das IT-Personal bis zum Top-Management. Solche Trainings sollten immer so realitätsnah wie möglich sein und anhand von echten Beispielen aufgezeigt werden. Alle Hinweise sollten dabei so formuliert sein, dass sie auch wirklich im Arbeitsalltag umsetzbar sind und ausprobiert werden können. Behalten Sie immer im Hinterkopf, dass Social Engineering nur dann funktioniert, wenn das potenzielle Opfer darauf hereinfällt.

2.

Sichere Passwörter

Dazu gehört auch, zunächst zu prüfen, wie sicher die aktuell im Unternehmen verwendeten Passwörter sind. Zusätzliche Sicherheit bieten technische Einrichtungen wie der Einsatz einer Multi-Faktor-Authentifizierung.

3.

Aktuelle Security-Produkte

Moderne Security-Lösungen (z. B. Cloud Sandboxing) wie die von ESET erkennen Spam und Phishing-Versuche schnell. Sie löschen oder verschieben entsprechende Mails sofort in einen Quarantäne-Bereich, noch bevor sie den Nutzer überhaupt erreichen.

4.

Einfach umsetzbare Verhaltensregeln

Jeder Mitarbeiter muss in der Lage sein, bei potenziellen Sicherheitsvorfällen mit Social Engineering schnell zu reagieren und genau zu wissen, welche Schritte zu befolgen sind.

5.

Security Management-Tools

Die Management-Konsole ESET PROTECT bietet einen kompletten Überblick über alle Endpoints in Echtzeit innerhalb und außerhalb einer Organisation. Das gewährleistet ein vollständiges Security-Management und umfassendes Reporting.

Quellen:

NCSA
https://staysafeonline.org/small-business-target-survey-data/

CSO
https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

hostingtribunal.com
https://hostingtribunal.com/blog/phishing-statistics/#gref

Digitalverband Bitkom
https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf

ic3
https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

ESET ist ein europäisches Unternehmen mit Hauptsitz in Bratislava (Slowakei). Seit 1987 entwickelt ESET preisgekrönte Sicherheits-Software, die bereits über 110 Millionen Benutzern hilft, sichere Technologien zu genießen. Das breite Portfolio an Sicherheitsprodukten deckt alle gängigen Plattformen ab und bietet Unternehmen und Verbrauchern weltweit die perfekte Balance zwischen Leistung und proaktivem Schutz. Das Unternehmen verfügt über ein globales Vertriebsnetz in über 200 Ländern und Niederlassungen u.a. in Jena, San Diego, Singapur und Buenos Aires. Für weitere Informationen besuchen Sie www.eset.de oder folgen uns auf LinkedIn, Facebook und Twitter.

ESET.DE | ESET.AT | ESET.CH