WWW.EULERHERMES.DE

DEEPFAKES, SOCIAL ENGINEERING UND DIE SCHWACHSTELLE MENSCH

Die Betrugsmaschen der Cyberkriminellen von heute und wie sich Unternehmen davor schützen können

Ein Unternehmen der Allianz

EULER HERMES

KREATIV UND KÜNSTLICH INTELLIGENT – DIE NEUEN MASCHEN DER CYBERKRIMINELLEN

Cyberkriminelle sind kreativ und gehen mit der Zeit. Sie nutzen opportunistisch neue Situationen aus. Die Pandemie, Homeoffice und hybride Arbeitswelten öffnen ihnen neue Einfallstore. Aber auch der technologische Fortschritt mit künstlicher Intelligenz (KI) und Deepfakes bietet ihnen neue Spielfelder.

Zuletzt gingen TikTok-Videos von Schauspieler Tom Cruise viral – eine täuschend echte Fälschung, erstellt mit künstlicher Intelligenz. Niederländische Politiker fielen in einem Video-Call auf einen gefälschten Nawalny-Mitarbeiter herein. Betrüger bauten für eine „Fake President"-Attacke ein ganzes Büro nach, um maximales Vertrauen in die Echtheit der Videokonferenz und der erteilten Zahlungsaufträge herzustellen. Und in Hongkong erbeuteten Kriminelle mit einem gefälschten Stimmprofil umgerechnet rund 30 Millionen Euro von einer Bank.

Noch sind es Einzelfälle, noch ist der Aufwand relativ groß – aber die Entwicklung zeigt, was technisch möglich ist. Insofern dürfte es lediglich eine Frage der Zeit sein, bis Deepfakes „massentauglich" werden. Dabei müssen Betrüger gar nicht selbst professionelle Hacker sein: Im Darknet gibt es schon entsprechende „Software-as-a-Service"-Angebote inklusive entsprechender Schulungen.

Und wie können sich Unternehmen schützen? Auch ihnen hilft KI, ebenso wie hohe Sicherheitsstandards, durchdachte Prozesse und Notfallpläne. Den größten Hebel haben sie aber an anderer Stelle: Der Mensch ist weiterhin die größte Schwachstelle im System. Wer hier ansetzt, sensibilisiert und schult, kann Risiken erheblich reduzieren.

Wann die Alarmglocken schrillen sollten, welche Fehler man vermeiden sollte, mit welchen Tricks die Cyberkriminellen arbeiten und welche Tipps es gibt zur Prävention und im „Worst Case", erfahren Sie auf den folgenden Seiten von verschiedenen Betrugs- und Cyberexperten.

Wir wünschen Ihnen viel Erfolg und unterstützen Sie gern,
Ihr Euler-Hermes-Team

INHALT

9 VON 10 UNTERNEHMEN

in Deutschland (88 Prozent) von digitalen Angriffen betroffen.

Bitkom-Umfrage 2020/21

52,5 MILLIARDEN EURO

Schaden durch Cyber-Angriffe alleine im Homeoffice in Deutschland.

Institut für Deutsche Wirtschaft Köln, 2021

JEDER 2.

Cyber-Angriff im Homeoffice ist erfolgreich.

Institut für Deutsche Wirtschaft Köln, 2021

29 %

Anstieg der Cyber-Attacken 2021 weltweit.

„Cyber Attack Trends: 2021 Mid-Year Report", Computerworld

777

Cyber-Angriffe in Europa durchschnittlich pro Woche pro Unternehmen.

„Cyber Attack Trends: 2021 Mid-Year Report", Computerworld

CYBERCRIME UNTERSCHÄTZEN? LIEBER NICHT.

Es ist paradox: Laut Allianz Risk Barometer sehen deutsche Unternehmer Cyber-Vorfälle aktuell als zweitgrößtes Geschäftsrisiko an (nach Betriebsunterbrechung). Doch: Entsprechende Vorsorgemaßnahmen treffen längst nicht alle. Aktuelle Zahlen zeigen, dass Unternehmen gut beraten sind, das Thema ernst zu nehmen.

223 MILLIARDEN EURO

Gesamtschaden im Jahr durch Cyberangriffe in Deutschland. (2018/19: 103 Millarden).

Bitkom-Umfrage 2020/21

80 %

der Cyber-Schäden wegen einfacher Fehler, wie Sicherheitslücken oder veraltete Systeme.

Cyber-Report Allianz Global Corporate & Specialty, 2021

19.369

„Fake President"-Fälle weltweit mit Schäden von 1,9 Mrd. USD.

FBI Internet Crime Report 2020

144 MILLIONEN

Schadprogramme aktuell, täglich kommen 553.000 neue Varianten hinzu.

Bitkom-Umfrage 2020/21

35 %

mehr Payment Diversion Fälle.

Euler Hermes Schadensstatistik

RISIKO HOMEOFFICE

NEW WORK, NEW RISKS

Das Arbeiten im Homeoffice ist in vielen Unternehmen immer noch das Gebot der Stunde, die Pandemie wird die Arbeitswelt voraussichtlich nachhaltig verändern. Das hat viele Vorteile, birgt aber auch erhebliche Risiken. Firmen sollten dabei ihren eigenen Schutz nicht aus den Augen verlieren – vor Cybercrime, Betrug und anderen Vertrauensschäden.

Eine veraltete IT-Infrastruktur, Sicherheitslücken, der laxe Umgang mit Hardware, Daten und Server-Zugängen öffnet findigen Kriminellen Tür und Tor. Ob Diebstahl, Spionage oder Erpressung – die Liste der möglichen Bedrohungen ist lang. Experten warnen vor einem starken Zuwachs an Cybercrime-Delikten. Phishing- und Vishing-Attacken sind gerade im Homeoffice eine nicht zu unterschätzende Gefahr.

Laut einer repräsentativen Befragung von G DATA, brand eins und Statista verursachen beispielsweise Phishing-Mails im Homeoffice deutlich höhere Schäden als im Büro oder auch im Privaten.

KURZ ABGELENKT: MEHR SCHÄDEN IM HOMEOFFICE

Laut der Studie ist jede fünfte Phishing-Mail im Homeoffice so erfolgreich, dass Zugangsdaten oder persönliche Daten in die falschen Hände geraten. Im Büro sind es hingegen „nur" 14,6 Prozent. Schon zu Beginn der Pandemie hatten Experten davor gewarnt, dass Mitarbeitende im Homeoffice teilweise mehr Stress haben und deshalb anfälliger für Angriffe sind. Wenn in der Videokonferenz kurz ein Fenster aufpoppt, die „lieben Kleinen" nerven oder der Paketbote gerade klingelt, ist ein schneller, unachtsamer Klick oft fatal.

Neben der Unachtsamkeit sind aber auch die mangelnde Kommunikation und die fehlenden Kontrollen teilweise ein Problem – in manchen Unternehmen sind nicht alle Compliance-Richtlinien oder Sicherheitsprozesse wie beispielsweise das 4-Augen-Prinzip komplett mit ins Homeoffice gezogen. Die soziale Distanz schafft nahezu perfekte Voraussetzungen für „Social Engineers". So verwundert es wenig, dass Mitarbeiter im Homeoffice ohne große Nachfragen Kontodaten von Lieferanten einfach abändern oder auf „Fake President"-Attacken hereinfallen.

Nicht zu vernachlässigen sind auch jene Schäden, die Angestellte nicht aus Unwissenheit und Leichtfertigkeit verursachen, sondern mit purer Absicht. Gelegenheit macht bekanntlich Diebe und Innentäter verursachen immer noch den größten Teil der Schäden bei Betrugsdelikten – auch hier ist die Dunkelziffer hoch.

PRÄVENTION: SCHULUNGEN UND UNTERNEHMENSKULTUR ENTSCHEIDEND

Fakt ist: Hybride Arbeitswelten werden Unternehmen auch in den kommenden Jahren begleiten. Deshalb sollten sich diese auf die Risiken einstellen, entsprechende Sicherheitsvorkehrungen treffen, in die Infrastruktur investieren und vor allem ihre Mitarbeiter sensibilisieren. Wer wachsam ist und nachfragt, schützt das Unternehmen – gerade bei Social Engineering. Deshalb spielt auch die Unternehmens- und Fehlerkultur eine entscheidende Rolle bei der Prävention von finanziellen Schäden durch Betrug und Cybercrime.

Andreas Dondera
ist Experte für Cyberkriminalität im Landeskriminalamt in Hamburg.

INTERVIEW

„KEIN OPFER WERDEN!“

Cybercrime wird immer arbeitsteiliger, internationaler und ist für die Täter oft hoch lukrativ. Andreas Dondera, Experte für Computerkriminalität im LKA in Hamburg, berichtet über neue Entwicklungen, alte Fehler und wann in jedem Unternehmen die Alarmglocken schrillen sollten.

Herr Dondera, wie sieht’s aus: Steigt die Zahl der Cyber-Kriminellen?
Zumindest registrieren wir eine steigende Zahl von Cybercrime-Delikten. Weil sich ein Teil des gesellschaftlichen Lebens ins Internet verlagert hat, haben sich auch viele Straftaten dorthin verlagert. Und das Internet bietet Tätern die Möglichkeit, international zu agieren, ohne Grenzen überschreiten zu müssen.

Womit macht man denn als Cyber-Krimineller im B-to-B-Segment am meisten Geld?
Wir haben aktuell zwei Schwerpunkte: Business E-Mail Compromise, zu denen auch Payment Diversion Fraud und Fake President gehören, und Ransomware.

Gibt es Trends bei diesen Delikten?
Ja. Die Betrüger werden immer professioneller. Als Ransomware-Delikte 2016 aufkamen, waren sie eher schlicht gehalten, oft in Form einer Bewerber-Mail, die an alle möglichen Unternehmen ging. Meist waren nur lokale Rechner betroffen und vielleicht noch die Netzlaufwerke. Mittlerweile haben die Täter deutlich komplexere Ransomware entwickelt. Seit einigen Monaten geht der Trend außerdem dahin, die betroffenen Daten nicht nur zu verschlüsseln, sondern vorher abzugreifen. Das hat datenschutzrechtlich natürlich Konsequenzen für die Unternehmen, nicht nur was die Verfügbarkeit betrifft, sondern vor allem die Vertraulichkeit. Mit der Drohung, die erlangten Daten zu veröffentlichen, bauen sie somit neben der Verschlüsselung ein zweites Druckmittel auf.

Wie ist die Entwicklung bei Deepfake-Delikten?
Die Entwicklung bei der Technologie schreitet mit künstlicher Intelligenz stark voran, und es tauchen teilweise täuschend echte Deepfakes auf. In Frankreich haben Betrüger sogar ein ganzes Büro nachgestellt, sodass es im Video-Call aussah, als spräche man mit dem echten Geschäftsführer in seinem echten Büro. In Deutschland gab es vereinzelt auch Fälle, bei denen Geschäftsführer mit gefälschten Stimmprofilen ihre Hausbank angerufen haben. Die große Welle an Fällen ist bisher aber ausgeblieben.

Suchen sich die Täter ihre Angriffsziele eigentlich überlegt aus, etwa weil sie mutmaßen, dass dort solche sensiblen Daten liegen oder Geld zu holen ist?
Die initialen Angriffe sind nach unseren Erkenntnissen immer noch eher zufällig. Die Täter scheinen einfach zu gucken, wo sie eine Sicherheitslücke finden. Erst nach dem Einstieg prüfen sie, wo sie eigentlich sind: Bei einem Handwerksbetrieb? In einem Krankenhaus? Oder einer Bank? Je nach Ort können die Täter dann entscheiden, wie sie weiter vorgehen.

Das heißt, dass alle Unternehmen gleichermaßen gefährdet sind?
Erstmal ja. Die Chance auf viel Geld ist für die Täter bei einem großen Unternehmen aber natürlich un-

gleich höher, und deswegen liegt deren Fokus schon dort, wo Geld ist. Vor fünf Jahren hatten wir noch sehr viele Fälle mit Schäden um die 3.000 bis 5.000 Euro. Heute belaufen sich die Schäden auf sechs- und auch siebenstellige Summen.

Welches sind denn die größten Einfallstore in die Computersysteme von Unternehmen?
Das Einfallstor ist eigentlich immer der Mensch. Allerdings werden die Methoden der Täter auch immer ausgefeilter. Ihnen hilft die Menge an Kommunikation, die heutzutage im Netz stattfindet. Fast 90 Prozent der Fälle, die bei uns eingehen, beruhen allerdings auf demselben Problem: Die Menschen erkennen falsche E-Mail-Adressen nicht. Ich hatte gerade einen Fall, in dem eine Mitarbeiterin wegen einer Zahlungsänderung misstrauisch geworden war und deshalb noch eine E-Mail geschickt hat, um sie zu überprüfen – sie hat diese Mail aber an den Fake-Account geschickt. Damit hat sie dem Betrüger leider genau in die Karten gespielt.

Gibt es Unternehmen, die lieber schweigend zahlen, um in der Öffentlichkeit nicht als Cybercrime-Opfer dazustehen?
Da wir das Dunkelfeld nicht kennen, kann ich keine Aussage dazu treffen. Wir hoffen aber, dass möglichst viele Unternehmen die Taten zur Anzeige bringen.

Haben Sie eine Chance, die Täter zu kriegen?
Das Deliktsfeld mit zum Teil international agierenden Tätern bringt es einfach mit sich, dass es schwierig aufzuklären ist. Die Behörden arbeiten natürlich stetig daran, besser zu werden. Wo es erforderlich ist, soll länderübergreifender und internationaler Austausch für eine effektivere Bekämpfung der Cyberkriminellen sorgen. Außerdem hoffen wir auch, durch Präventionskonzepte die Aufmerksamkeit auf die verschiedenen Phänomene lenken und somit Sensibilität bei den Menschen schaffen zu können. Ziel ist natürlich, dass die Täter gar nicht erst zur eigentlichen Tatausführung gelangen.

Was also können die Unternehmen tun?
Das A und O ist es, bei den Mitarbeitern Awareness zu schaffen, und das am besten kontinuierlich. Die Menschen in den IT-Abteilungen sollten ständig beobachten, welche neuen Maschen es gibt und alle Bediensteten regelmäßig darüber informieren, auch Zeitarbeiter und externe Dienstleister. Unternehmen sollten zudem ein durchdachtes Backupkonzept und eine Checkliste für einen IT-Sicherheitsvorfall erstellen. Und sie sollten klare Regelungen schaffen, wie damit umzugehen ist, wenn Zahlungen oder Waren an bislang unbekannte Konten oder Adressen geschickt werden sollen.

Von welchen Schadenssummen reden wir denn da?
Das kommt darauf an. Letztens hat ein Unternehmen gleich zwei Mal eine Zahlung geleistet aufgrund einer Mail mit gefälschten Kontodaten – dadurch kam es zu einer Umlenkung des Zahlungsverkehrs und zu einem Schaden von insgesamt 1,3 Millionen Euro. Viel häufiger bewegen sich die Schäden aber zwischen 30.000 und 100.000 Euro.
Wir haben es aber auch schon gehabt, dass Waren umgeleitet oder fälschlicherweise bestellt wurden.

Wie geht das genau vor sich?
Die Täter wissen, dass die Firma XY bei der Firma Z immer Waren bestellt. Sie schicken eine Fake-Mail mit einer Bestellung und dem Hinweis, die Ware bitte nicht an die gewohnte Lieferadresse, sondern zum neuen Werk zu schicken. Wenn alles plausibel erscheint, wird die Ware geliefert und sie wird auch abgeholt. Der Betrug fällt erst auf, wenn die Zahlung für die Ware ausbleibt. Das Kind ist dann schon in den Brunnen gefallen.

Was meinen Sie: Wie wird sich Cybercrime in Zukunft entwickeln?
Solange die Menschen immer wieder auf solche Sachen reinfallen, wird es weitergehen. Ransomware und Business E-Mail Compromise sind nach wie vor sehr erfolgreich, diese beiden Phänomene werden uns wohl noch lange begleiten. Wobei zum Beispiel Payment Diversion Fraud viel einfacher zu verhindern wäre, wenn man einfach nur ein bisschen mehr aufpasst. Das ist bei Ransomware nicht so einfach. Und es gibt natürlich auch immer besondere Fälle, wie den von einem ehemaligen IT-Administrator, der sich sukzessive eine Hintertür in seine Firma geschaffen hatte und dort alles Mögliche kaputt gemacht hat.

Wer kein Opfer werden will, muss also hochgradig aufmerksam sein und es den Tätern so schwer wie möglich machen – korrekt?
Wenn Unternehmen ihre Sache gut machen und Mitarbeiter sensibilisieren, reduzieren sie das Risiko schon erheblich. Aber die Betrüger sind sehr kreativ, denen fällt ständig was Neues ein – auf solche Ideen würde man selbst erst mal gar nicht kommen.

DIE NEUEN MASCHEN DER KRIMINELLEN

CYBERCRIME & DIE SCHWACHSTELLE MENSCH

Frau Lehmann ist Leiterin der Buchhaltung eines Krankenhauses in Mitteldeutschland. Im Mai 2021 erhält sie eine E-Mail vom CEO der Holdinggesellschaft. Der fragt zunächst, ob sie „erreichbar" sei. Sie bestätigt, dass sie im Homeoffice, aber verfügbar sei. Etwa eine halbe Stunde später folgt die Bitte, eine Zahlung in Höhe von 400.000 Euro auf ein tschechisches Konto zu tätigen für den Kauf von Aktien – natürlich alles streng vertraulich, man zähle auf sie.

Sie ist auf „Autopilot", denkt nicht groß nach, prüft die E-Mail-Adresse nicht näher, fragt nicht nach – obwohl sie die Telefonnummer des CEO hat und dieser erreichbar gewesen wäre. Stattdessen erstellt sie die Zahlungsanweisung und bittet eine Sachbearbeiterin aus ihrem Team per Teams – diese ist ebenfalls im Homeoffice – die notwendige Zweitunterschrift zu leisten. Für sie ist es „business as usual". Sie gibt die Zahlung frei und das Unheil nimmt seinen Lauf.

Am nächsten Morgen meldet sich die Bank, dass eine Überweisung an ein verdächtiges Konto getätigt wurde und fragt nach, ob dies alles seine Richtigkeit habe. Der Finanzchef sieht die Buchung im System und bittet Frau Lehmann um Auskunft und den entsprechenden Schriftwechsel. Schnell ist klar, dass es sich um einen „Fake President"-Betrugsfall handelt. Sowohl Polizei als auch LKA werden eingeschaltet. Die Bank versucht, die Zahlung zurückzuholen, aber leider vergebens.

GEFAHR HOMEOFFICE: GERINGERE SICHERHEITSSTANDARDS & SCHWACHSTELLE MENSCH

Dieser Fall ist nur einer von vielen. Die Methode ist oft die gleiche: Mitarbeiter werden „gehackt" und ihre Gefühle manipuliert: mit Wertschätzung, Angst oder Druck.

Die Pandemie hat den Betrügern zudem in die Karten gespielt. Denn wenn Mitarbeiter im Homeoffice sitzen, sind die IT-Sicherheitsstandards in der Regel wesentlich geringer als im Büro. Ein wahres El Dorado für Cyberkriminelle und Betrüger. Die größte Schwachstelle bleibt dabei der Mensch: Bei rund 90 % aller Cyberattacken dürfte menschliches Versagen oder Fehlverhalten ausschlaggebend sein. Hinzu kommt: Im Homeoffice wird weniger kontrolliert und kommuniziert. Die Hürde, einen Kollegen anzurufen und ihn auf einen Vorgang anzusprechen, ist hier oft viel höher – so auch bei Frau Lehmann und der später hinzugezogenen Sachbearbeiterin.

Die Betrüger gehen dabei mit der Zeit – sowohl thematisch als auch technisch. Sie nutzen neue Rahmenbedingungen wie die Covid-19-Pandemie oder das Homeoffice genauso wie technologischen Fortschritt. Die Möglichkeit von Audio- oder Video-Deepfakes zum Beispiel ist technologisch bereits so ausgereift, dass Konversationen in Echtzeit möglich sind – der falsche Chef hält also Einzug in Video- oder Telefonkonferenzen.

DER FALSCHE JOHANNES: AUDIO DEEPFAKE

2019 erbeuteten Cyberkriminelle im Fall „Der falsche Johannes" 220.000 Euro vom britischen Tochterunternehmen eines deutschen Konzerns: Der falsche deutsche Konzernchef Johannes erteilte per Telefon seine Anweisungen – mit der echten Stimme, Satzmelodie und dem leichten deutschen Akzent im Englischen. Der britische CEO war sicher, den echten Chef in der Leitung zu haben, so gut war das Audioprofil. Bei Euler Hermes blieb dies bisher ein einmaliger Versicherungsfall. Zwar gab es noch weitere ähnliche Schadensfälle, bei denen die Nutzung von Audio Deepfakes nicht ausgeschlossen werden konnte, bei denen die Indizienlage jedoch weitaus weniger eindeutig war. Weltweit sind aber noch wesentlich größere gesicherte Fälle bekannt; der vielleicht spektakulärste ereignete sich 2020 in Hongkong, hier wurde eine Bank um 35 Millionen US-Dollar erleichtert.

NOCH EINZELFÄLLE – ABER DEEPFAKE-BEDROHUNG NIMMT ZU

Bisher blieben solche „Fake President"-Fälle mit Hilfe von Audio Deepfakes erstaunlicherweise Einzelfälle. Allerdings ist es wohl nur eine Frage der Zeit, wann diese Evolutionsstufe der neue Standard werden wird oder mit Video Deepfakes den nächsten Schritt geht: Täuschend echte Deepfake-Videos von Tom Cruise gingen zuletzt auf Tik Tok viral – erstellt von Visual Artist Chris Umé, der mit Hilfe von künstlicher Intelligenz und etwa 6.000 Bildsequenzen des Schauspielers aus allen möglichen Kamerawinkeln einen Algorithmus nahezu perfekt „trainiert" hat. Niederländische Politiker fielen in einer Videokonferenz in Echtzeit auf einen gefälschten Nawalny-Mitarbeiter herein. Auch er sah täuschend echt aus.

35 % ANSTIEG BEI PAYMENT DIVERSION-FÄLLEN

Neben der noch vagen Bedrohung durch Deepfakes in der nahen Zukunft sind neben den „Klassikern" aktuell aber noch andere Maschen auf dem Vormarsch. Insbesondere das Umleiten von Zahlungsströmen hat aktuell Hochkonjunktur: Alleine Euler Hermes verzeichnete im letzten Jahr einen Anstieg der Fallzahlen um 35 % beim Zahlungsbetrug (Payment Diversion) sowie um 25 % beim Bestellerbetrug (Fake Identity). Dabei liegen die Schäden in der Regel zwischen etwa 30.000 EUR und 1 Mio. EUR. Meist sind die Schadenssummen allerdings etwas niedriger als bei „Fake President"-Betrugsfällen. Ausnahmen bestätigen allerdings die Regel und es gab vereinzelt auch Zahlungsbetrugsfälle mit Schäden von bis zu 6 Mio. EUR.

Die Gefahr durch „Fake President" ist ebenfalls weiterhin gegeben, zahlreiche erfolgreiche Angriffe in den letzten Jahren durch praktisch alle Branchen und Unternehmensgrößen belegen das. Zwar blieben die ganz großen Schäden zuletzt aus und Schadenshöhen lagen eher im hohen sechsstelligen oder einstelligen Millionen-Bereich. Die Fallzahlen bewegen sich aber nach wie vor auf hohem Niveau, trotz eines deutlich gestiegenen Problembewusstseins in den Unternehmen.

NEUE MASCHEN BEI „FAKE PRESIDENT"

Zuletzt gab es auch beim „Klassiker" neue Varianten. Neben Betrugsversuchen per Whatsapp-Sprachnachricht oder durch vermeintliche IT-Security-Mitarbeiter traten zuletzt vermehrt falsche Bankmitarbeiter in Erscheinung, die von einem angeblichen Betrugsverdacht bei Transaktionen auf einem Konto berichten und sich so das Vertrauen des Mitarbeiters erschlichen. Die Betrüger hatten dabei Kenntnis über alle Bankbewegungen des Unternehmens und eine Bandbreite an Informationen rund um die Prozesse und Verantwortungen im Finanzbereich.

Bei ihrer Informationsbeschaffung werden die Betrüger immer kreativer: Neben sehr gezieltem Phishing nutzen sie auch zunehmend „Vishing", also die Sammlung von Informationen über gezieltes „Social Engineering" per Telefonanruf. Auch beim Zugriff wird die Palette breiter: Das System einer deutschen Großbank wurde über die Klimaanlage gehackt, weil diese – vermutlich zur Fernwartung – schlecht geschützt online war. Andere Angriffe erfolgten über Funktastaturen oder Smart Home Devices.

Das zeigt: Es gibt nichts, was es nicht gibt. Ein gesunder Menschenverstand, ein gesundes Maß an Misstrauen, eine gute und offene Unternehmens- und Fehlerkultur sowie die Sensibilisierung der Mitarbeiter sind daher weiterhin das schärfste Schwert im Kampf gegen die Cyberkriminellen. Lieber eine Mail zu viel gelöscht als eine zu wenig.

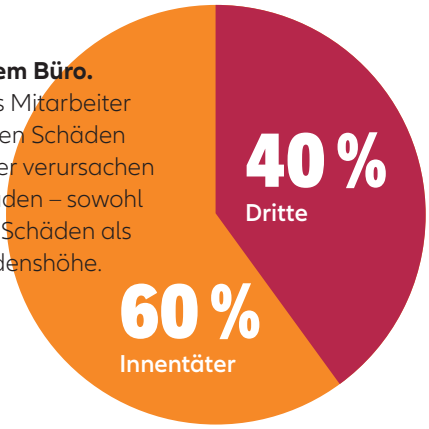
Autor: Rüdiger Kirsch, Global Fidelity Expert, Euler Hermes Deutschland.

ZAHLEN & FAKTEN

AUS DER EULER HERMES SCHADENSSTATISTIK

Eine Vertrauensschadenversicherung (VSV) schützt Unternehmen gegen finanzielle Schäden, die durch zielgerichtete kriminelle Handlungen entstehen – sowohl durch sogenannte „Innentäter" (z. B. Mitarbeiter, Zeitarbeitskräfte) als auch durch externe Dritte (z. B. Hacker).

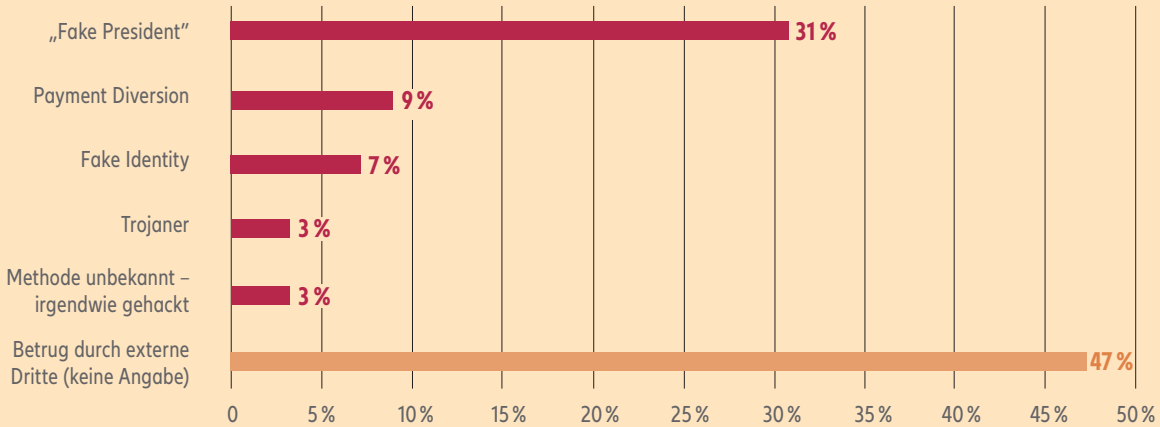
Der Feind in meinem Büro.
Interessant ist, dass Mitarbeiter weiterhin die meisten Schäden verursachen. Hacker verursachen rund 40 % der Schäden – sowohl bei der Anzahl der Schäden als auch bei der Schadenshöhe.



380 MIO. EURO
Schäden durch Dritte seit 2014

225 MIO. EURO
Schäden aus Täuschungsdelikten („Social Engineering") seit 2014

GRÖSSTE HACKERSCHÄDEN WEITER DURCH „FAKE PRESIDENT"

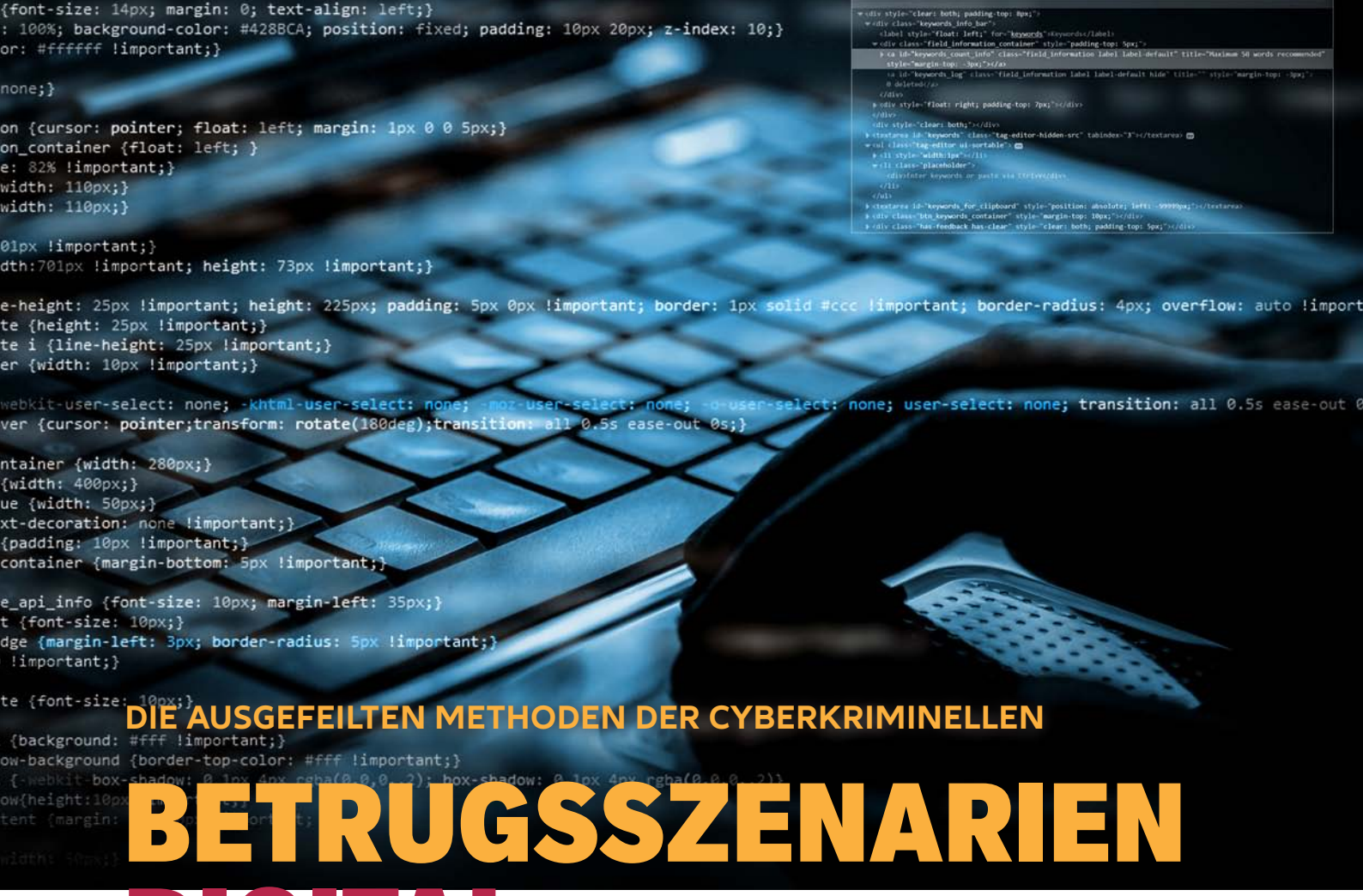


„Fake President" ist noch immer nicht „out":
Beim Betrug mit Hilfe von Social Engineering (Hackerschäden) verursacht der „Fake President"-Betrug weiterhin die größten Schäden – trotz stagnierender Fallzahlen. Die Schadenssummen liegen beim „Fake President"-Betrug inzwischen nur noch im hohen sechsstelligen oder niedrigen einstelligen Millionen-Bereich. Zwischen 2014 und 2017 verursachten die Betrüger häufig noch Schäden zwischen 10 und 50 Mio. EUR.

25 % ANSTIEG
der Schadensfälle bei Bestellerbetrug 2020 vs. 2019 [1]

35 % ANSTIEG
der Schadensfälle bei Zahlungsbetrug 2020 vs. 2019 [1]

[1] Nach den vorläufigen Schadenserfahrungen dürfte sich die Entwicklung beim Anstieg beider Betrugsmaschen auch 2021 in ähnlicher Höhe fortsetzen.



DIE AUSGEFEILTEN METHODEN DER CYBERKRIMINELLEN

BETRUGSSZENARIEN DIGITAL

Eingriffe in die digitale Kommunikation von Unternehmen oder in die Fernsteuerung von Infrastrukturen, Versorgungs- und Produktionsanlagen sind nur ein Einfallstor für Kriminelle. Das digitale Outsourcing von Prozessen und Dienstleistungen ein weiteres. Fast jedes Unternehmen wird heute weitestgehend digital gesteuert.

Unternehmen müssen sich der Risiken bewusst sein. Nur, wenn sie detailliert das unterschiedliche Vorgehen der Betrüger kennen, können sie sich auch effizient schützen. Denn nicht nur die Wege sind vielfältig, sondern auch die Methoden. Die wichtigsten davon stellen wir hier vor:

FAKE PRESIDENT FRAUD

Bei dieser Betrugsmasche geben sich die Täter als ein Organ eines Unternehmens – meist ein Vorstandsmitglied – aus und bitten per E-Mail oder Fax einen Mitarbeiter, der im Unternehmen für die Bankgeschäfte verantwortlich ist, eine dringende Überweisung auszuführen.

Dem Mitarbeiter wird dabei vorgespiegelt, dass es sich um eine höchst geheime und vertrauliche Angelegenheit handelt. Die Betroffenen, die sich einerseits aufgrund des besonderen Vertrauens durch den Vorstand geschmeichelt fühlen, anderseits aufgrund der angeblichen Wichtigkeit der Transaktion erheblich unter Druck stehen, führen diese Überweisungen meist zügig aus.

Fast immer erfolgen die Geldtransfers auf ausländische Konten, vor allem in Asien und Osteuropa. Fliegt der Betrug dann auf, sind die Konten dort meist leergeräumt oder eine Rückholung wird aufgrund des ausländischen Rechtssystems erheblich erschwert.

Häufig werden gezielt Mitarbeiter in ausländischen Niederlassungen des Unternehmens angesprochen. Das erschwert den Mitarbeitern die persönliche Kontaktaufnahme mit den verantwortlichen Organen im Unternehmen, von denen die vermeintlichen Anweisungen kommen.

PAYMENT DIVERSION

In diesen Fällen geben sich die Betrüger als Geschäftspartner oder Lieferanten eines Unternehmens aus und erreichen durch gefälschte Mitteilungen, dass die Bezahlung für Waren oder erbrachte Dienstleistungen auf abweichende Konten erfolgt. Die Umsetzung dieser Form des Betruges wird

ermöglicht durch eine gefälschte Mitteilung an das Unternehmen, dass sich die bisher vereinbarten Bankverbindungen geändert haben und der Zahlungsverkehr nun über die neue Bankverbindung abgewickelt werden soll.

FAKE IDENTITY FRAUD

Bei diesem Betrugsszenario geben sich die Täter als ein bereits existierender Kunde oder als ein Neukunde des Unternehmens aus und ordern schriftlich Waren. Mit plausiblen Erklärungen wird dann die Lieferung an eine abweichende Lieferadresse verlangt.

Da die Identität einer tatsächlich existierenden Firma genutzt wird, schöpfen die Betrugsopfer zunächst keinen Verdacht. Oft fliegt der Betrug erst dann auf, wenn Zahlungsverzug eintritt und die tatsächlich existierende Firma gemahnt wird. Wird dann die Lieferadresse durch die Polizei überprüft, werden die Geschäftsräume verlassen vorgefunden und die Ware ist selbstverständlich längst weiter verschoben worden.

PHISHING

Unter Phishing versteht man Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen. Häufig sind in diesen E-Mails Anhängen enthalten, die beim Öffnen Keylogger oder andere Schadsoftware installieren, die dem Betrüger Zugang zu Dateien und Passwörtern verschaffen können.

Ziel des Betrugs ist es, mit den erhaltenen Daten beispielsweise Kontoplünderung zu begehen. Eine neuere Variante des Phishing ist Spear-Phishing, worunter ein gezielter E-Mail-Angriff auf eine bestimmte Person oder einen ausgewählten Personenkreis zu verstehen ist – anders als bei herkömmlichem Phishing, wo eine große Anzahl an E-Mails an viele Empfänger versendet werden.

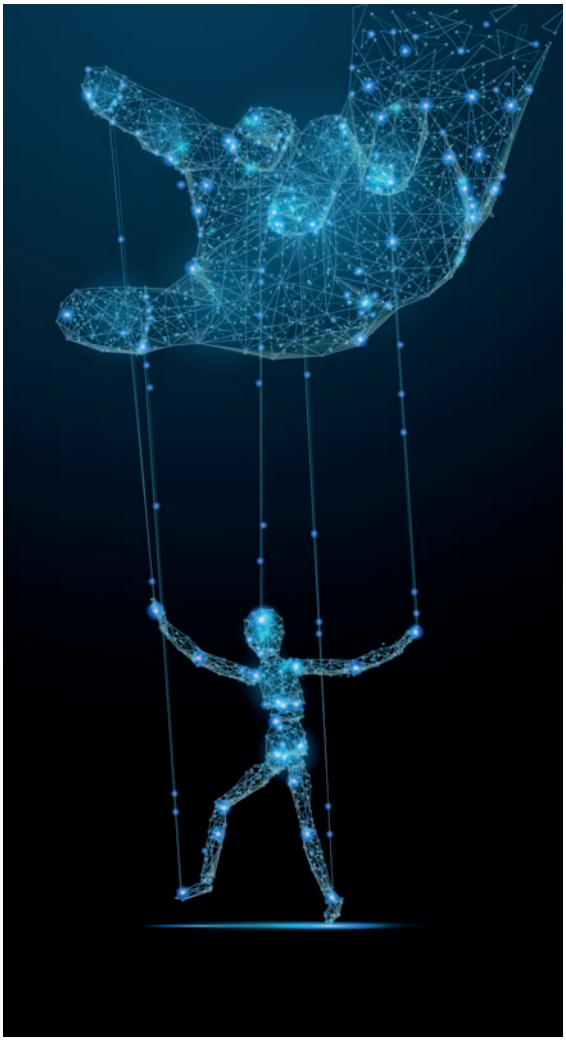
Pharming, eine weiterentwickelte Form des Phishings, basiert auf einer Manipulation der DNS-Anfragen von Webbrowsern, um den Benutzer auf gefälschte Webseiten umzuleiten.

MAN-IN-THE-CLOUD

Unter Cloud Computing versteht man die Ausführung von Programmen, die nicht auf dem lokalen Rechner installiert sind, sondern auf einem anderen Rechner, die über sogenannte Datensynchronisationsdienste i.d.R. über das Internet aufgerufen werden („in der Cloud", z.B. Google Drive, Dropbox oder Microsoft OneDrive).

Für den Diebstahl solcher online gespeicherter Daten benötigt ein Hacker keinen speziellen Zugriff auf den Namen oder das Passwort des jeweiligen Anwenders, sondern lediglich einen Passwort-Token. Dies ist eine kleine Datei auf dem Gerät eines Nutzers, in der die Anmeldedaten hinterlegt sind, damit nicht bei jedem Aufruf des Diensts Benutzername und Passwort erneut eingegeben werden müssen.

Den beispielsweise per Phishing entwendeten Token kann der Angreifer anschließend nutzen, um von einem anderen Rechner aus das Konto des Nutzers zu übernehmen und sich damit Zugriff auf alle online abgelegten Dateien zu verschaffen.



Social Engineering – Schwachstelle Mensch. Viele Betrugsszenarien von Cyberkriminellen nutzen gezielt die Gutgläubigkeit und Loyalität von Mitarbeitern aus.

FALLBEISPIELE CYBERCRIME

Das kann sich doch niemand ausdenken? Diese echten Fälle zeigen, dass gängige Cybercrime-Maschen ziehen – und Unternehmen in große finanzielle Schwierigkeiten bringen können.

FAKE PRESIDENT

AUDIO DEEPFAKE IN HONGKONG: 35 MIO. USD ERBEUTET

Spektakulärer Audio Deepfake Betrug: Der CEO einer bekannten Firma bat den Manager einer Bank in Hongkong um Überweisungen in Höhe von 35 Millionen US-Dollar, um eine Übernahme zu tätigen. Der Bankmanager erkannte die Stimme des CEO sofort. Dieser sagte, ein Rechtsanwalt namens Martin Zelner sei mit der Koordinierung der Verfahren beauftragt worden.

Der Bankmanager konnte in seinem Posteingang E-Mails des Geschäftsführers und von Zelner sehen, in denen bestätigt wurde, welches Geld wohin überwiesen werden musste. Der Bankdirektor glaubte, dass alles rechtmäßig sei, und begann mit den Überweisungen. Nur leider war er Opfer eines Audio Deepfakes geworden – und die Bank um 35 Millionen USD ärmer.
Bekannt wurde der Fall durch ein Gerichtsdokument, in dem Ermittler in den Vereinigten Arabischen Emiraten die USA um Mithilfe baten beim Aufspüren einer Tranche von 400.000 USD, die auf Konten einer amerikanischen Bank eingegangen waren.

BESTELLERBETRUG (FAKE IDENTITY)

ZU SPÄT GING DEM LAMPEN-HERSTELLER EIN LICHT AUF: FAKE-KUNDE ERBEUTET WARE FÜR 400.000 EUR

Es klingt vielversprechend für den Elektrowaren-Produzenten: Eine französische Warenhauskette kündigt Bestellungen im großen Stil an. Die Kreditwürdigkeit der Franzosen wird geprüft, es kommt grünes Licht: Das Geschäft kann beginnen.
Zwar läuft nicht alles rund – mal werden spontan Lieferadressen geändert, mal Teile von Lieferungen umgeordert –, aber innerhalb von zwei Monaten verschickt der Hersteller Leuchten im Wert von über 400.000 EUR an den vermeintlich neuen Kunden. Und natürlich auch die ersten Rechnungen.
Auf die reagiert allerdings die Finanzabteilung der französischen Warenhauskette sehr verwundert: Das müsse ein Irrtum sein, man habe keine Lampen bestellt.
So fliegt der Schwindel auf: Ein Betrüger hatte sich als Mitarbeiter der Warenhauskette ausgegeben, die Waren zu Lieferzentren geordert und von dort auf Nimmerwiedersehen verschwinden lassen. Der Lampen-Hersteller wäre in ernsthafte finanzielle Schwierigkeiten geraten, wäre er nicht gegen Bestellerbetrug versichert gewesen.

ZAHLUNGSBETRUG (PAYMENT DIVERSION)

DAS GROSSE GESCHÄFT MIT DEN MASKEN GING IN DIE HOSE

Das Umleiten von Zahlungsströmen war bei Betrügern in der Pandemie besonders beliebt – auch, weil die Masche ohne großen Aufwand funktioniert und so parallel mehrere Angriffe laufen können. So auch bei einem Unternehmen aus Norddeutschland: Es wittert die Chance, zu Beginn der Corona-Krise mit Schutzmasken das große Geld zu verdienen und bestellt bei einem Produzenten in China einen großen Posten.

Als man sich über Preise und Lieferzeiten einig ist, gibt der Lieferant die Kontoverbindung auf, teilt jedoch kurz darauf mit, dass der Kunde doch auf ein anderes Konto überweisen möge, die Buchhaltung habe dies erbeten. Der Kunde zahlt die vereinbarten 250.000 Euro – doch keine Masken in Sicht. Auf seine Nachfrage zu den Liefermodalitäten bekommt er die Antwort, dass er erstmal bezahlen müsse.
Bei Abgleich der Kontodaten und auch der E-Mail-Adresse stellt sich heraus, dass sich letztere am Ende der Korrespondenz geringfügig im Namen von einem „e“ auf ein „a“ geändert hatte.

TECHNOLOGISCHER FORTSCHRITT & IT-FORENSIK

LEICHTES SPIEL: HACKING AS A SERVICE

Gibt es den typischen Hacker? Und wenn ja, was zeichnet ihn aus, wie und mit wem arbeitet er? Und vor allem: Sind eigentlich alle Hacker böse? Welche Spuren hinterlassen Hacker bei ihrer Tätigkeit im Netz und wie kann man diesen folgen?

Der Begriff „Hacker" ist in der Öffentlichkeit häufig negativ behaftet. Um eine Unterscheidung zwischen vermeintlich gut und vermeintlich böse herauszuarbeiten, haben sich schon vor Jahren Begriffe wie „White hat"- und „Black hat"-Hacker etabliert. Die Kenntnisse und Fähigkeiten beider Lager sind dabei oft vergleichbar – nur der Zweck, für den diese eingesetzt werden, unterscheidet sich.

LÄNGST PASSÉ: COMPUTER-NERDS IM KELLER ODER EINSAMER WOLF

Die Klischees des einsamen Wolfs oder einzelner aus Kellern operierender Computer-Nerds sind jedoch größtenteils überholt. Natürlich mag es auch diese Charaktere noch vereinzelt geben, aber Team-Play wird mittlerweile großgeschrieben und Hacker sehen sich längst als Dienstleister.

Hacken, ob für die „gute" oder die „böse" Seite, braucht Spezialisten. Doch auch „gute" Vorlagen können mit geringem Aufwand für „böse" Zwecke umgemünzt werden. Oft braucht es nur jemanden, der eine mehr oder weniger ausgereifte Anwendungslösung bastelt, die dann auch oft von normalen Kriminellen als Anwender genutzt wird. Über Plattformen in schwer zugänglichen Teilen des Internets, auch unter Begriffen wie „Darkweb" bekannt, kann sich heute theoretisch jeder Otto-Normalbürger ohne großes Vorwissen diese Lösungen kaufen und sie dann anwenden („Software as a Service").

GELEGENHEIT MACHT DIEBE: ANGRIFFE NICHT IMMER ZIELGERICHTET

Dass Angriffe dabei immer zielgerichtet sind, ist ebenfalls ein Irrglaube. Ransomware-Attacken sind in den letzten Monaten stark ansteigend – allerdings in den häufigsten Fällen aufgrund von bestehenden Lücken oder Schwachstellen im System, und nicht aufgrund des bekannten Unternehmensnamens oder finanzieller Stärke. Frei nach dem Motto: „Gelegenheit macht Diebe". Fest steht: Sicherheitslücken laden Hacker ein.

LAIENFREUNDLICH: RANSOMWARE AS A SERVICE

Für Schwachstellen und Informationen, die einen Zugriff ermöglichen, gibt es ebenfalls einen florierenden Schwarzmarkt. Mit den hier erkauften Informationen und den hinzu erworbenen anwenderfreundlichen Lösungen (zum Beispiel „Ransomware as a Service") sind auch weniger qualifizierte Angreifer in der Lage, erfolgreich hohe Lösegeldsummen zu erpressen.

Ähnliches gilt für Stimmsynthese-Software (Audio-Deepfakes) und Software zur Erstellung sogenannter Video-Deepfakes. Bei Deepfakes handelt es sich meist um Bild- oder Tonmanipulation, die mit Hilfe

von lernenden KI-Modellen vorgenommen werden. Täuschend echte Stimmmanipulationen können mittels Video-Tutorials auf öffentlichen Videoplattformen von jedermann erstellt werden. Der Aufwand dafür ist nicht besonders hoch. Diese Stimmprofile können dann beispielsweise verwendet werden, um „Fake-President"-Angriffe zu initiieren oder gezielte Diffamierungskampagnen zu starten.

HEUTE SCHON TECHNISCH MÖGLICH: ECHTZEIT-UNTERHALTUNGEN IN DEEPFAKES

Für den Erfolg eines CEO Fraud ist oft das „Social Engineering" entscheidend. Für diese Manipulation der designierten Opfer ist eine Konversation in Echtzeit notwendig, die Wertschätzung ausdrückt und Bedenken zerstreut, Druck aufbaut oder Fragen beantwortet. Solche Konversationen in Echtzeit sind heute technisch längst möglich – sowohl als Audio- als auch als Video-Deepfake.

Das bedeutet: Auch manipulierte Video-Calls, in denen ein gefälschter CEO mit dem richtigen Aussehen und der richtigen Stimme Anweisungen für Überweisungen gibt, sind möglich. Das schafft ein maximales Vertrauen in die Echtheit des Auftrags, und die Ausführenden dürften in vielen Fällen gar keinen Verdacht schöpfen. Das hebt das Social Engineering – und die Möglichkeiten, die sich Betrügern damit bieten – auf eine ganz neue Ebene.

WAS TUN NACH EINEM ANGRIFF?

Die Gefahr, selbst zum Opfer von Cyberkriminellen zu werden, steigt mit der rasanten Entwicklung der Technologie. Doch was tun, wenn ein Angriff erfolgt ist? Dann müssen Unternehmen vor allem schnell und bewusst handeln. Warum bewusst? Weil zu schnell getroffene Entscheidungen weitreichende Folgen haben können. Unternehmen müssen unbedingt rechtliche Risiken im Auge behalten, unter anderem im Bereich Datenschutz, Arbeitsrecht oder auch im Hinblick auf vertragliche Verpflichtungen. Die zu erwartenden Sanktionen müssen unbedingt in die Überlegungen und Kommunikation einbezogen werden. Dies ist eine Aufgabe, die unternehmensintern oft nur dann abgebildet werden kann, wenn Szenarien bereits zuvor geplant und geprobt wurden. Ansonsten sind Unternehmen gut beraten, auf externe Dienstleister zurückzugreifen, die in dieser oft emotionalen und hektischen Situation mit einem neutralen Blick die Sachlage einschätzen. Schnell ja – aber ein unüberlegter Schnellschuss kann nach hinten losgehen.

72 STUNDEN: DIE UHR TICKT!

Meist spielen bei einem Cyberangriff die ersten 72 Stunden eine absolut kritische Rolle. IT-Forensiker haben kein großes Zeitfenster, um Spuren im Netz nachzugehen und eventuell noch zu retten, was zu retten ist. Die NASA fährt nach kritischen Ereignissen beispielsweise die Schotten runter: „Lock the doors!" Nach diesem Kommando sichern alle am Projekt Beteiligten ihre Daten und schreiben in Gedächtnisprotokollen die letzten Vorgänge und Minuten vor dem Ereignis auf.

Dieses Vorgehen wäre für einen Forensiker nach einem Sicherheitsvorfall jeglicher Art optimal. Gleichzeitig ist das in einem arbeitenden Unternehmen meist illusorisch. Das liegt schon allein daran, dass Sicherheitsvorfälle oft erst mit Verzögerungen festgestellt werden. Es ist daher wichtig, die Situation so weit wie möglich einzufrieren, ohne jedoch den Betriebsablauf weiter unnötig zu schwächen.

Sobald möglichst viele Informationen idealerweise beweissicher festgehalten wurden, muss das Unternehmen diese Informationen in Ruhe sichten und weitere Schritte einleiten. Diese Schritte können aus zivilrechtlichen und strafrechtlichen Maßnahmen bestehen. Je nach Tathergang ist es im Internet jedoch sehr schwer, die Täter hinter den Zugriffen technisch auszumachen. Das Internet ist zwar nicht anonym und technische Spuren lassen sich nicht bis in das letzte Detail verwischen, aber eine internationale Strafverfolgung stößt immer wieder an ihre Grenzen. Hinzu kommt, dass Tätergruppen teilweise auch von ihren Heimatstaaten geschützt oder wissentlich nur schwach verfolgt werden.

Dennoch hilft eine schnelle Reaktion häufig, zumindest einen Teil der erbeuteten Gelder oder Daten wieder zurückzuholen. Eine erfolgreiche Zusammenarbeit mit Banken ist dabei essenziell, um Konten rasch einzufrieren – bevor Geld verschoben und verloren ist.

Autor dieses Beitrags ist Dirk Koch, Rechtsanwalt & Data Protection Risk Manager.

EVOLUTIONSSTUFEN „FAKE PRESIDENT“-BETRUG

FRÜHSTADIUM: E-MAIL

E-Mail mit z. T. Schreib- und/oder Grammatikfehlern, schlecht getarntem Absender oder abweichender E-Mail-Adresse.

EVOLUTIONSSTUFE 1: SOCIAL ENGINEERING

Korrekte Rechtschreibung, gut getarnter Absender mit z. B. fehlenden Buchstaben, leichten Buchstaben- oder Zahlendrehern (Bsp.: max.mustermann@musterman.com). Durch Wertschätzung des Mitarbeiters oder Druckausübung (z. B. angeblicher Zeitdruck) wird hier bereits „Social Engineering“ eingesetzt.

EVOLUTIONSSTUFE 2: GEHACKTES INTRANET

Korrekte, gehackte/gedoppelte Absenderadresse (Bsp.: max.mustermann@mustermann.com). Die Betrüger hacken sich ins Intranet und spionieren dort Zuständigkeiten und Gepflogenheiten aus, wie z. B. Umgangston, E-Mail-Stil (Du/Sie, förmlich/informell) oder Ansprechpartner. So verbessern sie das „Social Engineering“ noch durch Interna und schaffen so Vertrauen.

EVOLUTIONSSTUFE 3: TELEFONANRUF

Fallbeispiel: Der Betrüger ruft eine Mitarbeiterin in der Buchhaltung an, um ihr zum 10-jährigen Firmenjubiläum zu gratulieren. Wenige Wochen später ruft er für den „Fake President“-Betrug erneut an – sie erkennt seine Stimme und führt gemäß der Aufforderung per E-Mail die Überweisungen aus.

EVOLUTIONSSTUFE 4: FAKE IT-SECURITY-MITARBEITER

Fallbeispiel: Kurz nach einer E-Mail mit einer gefälschten Zahlungsaufforderung ruft ein „Fake“-IT-Mitarbeiter in der Buchhaltung an, um dem Mitarbeiter mitzuteilen, dass bei ihm ein „Fake President“-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. Der Mitarbeiter überweist – das Geld ist weg.

EVOLUTIONSSTUFE 5: STIMMIMITATION

Erster Fall mit Stimmimitationssoftware: Die Software ahmt sogar Sprachmelodie und Akzente nach, sodass der Angerufene nach dieser telefonischen Bestätigung denkt, die Anweisung per E-Mail käme tatsächlich vom echten Konzern-Chef.

MÖGLICHE ZUKÜNFTIGE EVOLUTIONSSTUFEN: DEEPFAKE, VIDEO, WHATSAPP

Aktuell sind immer wieder Audio- und Video-Nachrichten von gefälschten CEOs per WhatsApp im Umlauf. Zudem sind Echtzeit-Unterhaltungen via Deepfake-Videos technisch bereits möglich, allerdings noch nicht sehr verbreitet. Dennoch dürfte das die nächste Evolutionsstufe sein. Das echte Aussehen gepaart mit der echten Stimme schafft maximales Vertrauen.

WEITERE UNTERVARIANTEN: GESCHENKKARTEN, BESTELLER- UND ZAHLUNGSBETRUG

Geschenkkarten: Mitarbeiter werden angewiesen, Geschenkkarten oder Gutscheine zu kaufen, für Jubiläumsfeiern oder ähnliche Anlässe.

Bestellerbetrug: Der Betrüger täuscht eine falsche Identität vor und gibt sich als Kunde aus (oft als bestehender), bestellt Waren und lässt diese dann an eine abweichende Lieferadresse senden.

Zahlungsbetrug: Der Betrüger gibt sich als Lieferant aus und gibt für die Bezahlung der bereits erfolgten Lieferung eine abweichende Kontoverbindung durch.

RISIKOFAKTOREN

SICHERHEITSLÜCKEN SCHLIESSEN

Trotz aller Vorsichtsmaßnahmen lassen sich Betrug und Veruntreuung nicht immer vermeiden. Bei Eintritt eines Schadens ist es für Unternehmen wichtig, schnell und richtig zu handeln und die Sicherheitslücken konsequent zu schließen. Zudem sollten Unternehmen die häufigsten Risikofaktoren am besten regelmäßig überprüfen.

1. RISIKOFAKTOR UNTERNEHMENSSTRUKTUR

- **a.** Sind die Arbeitsabläufe und -prozesse im Haus klar definiert?
- **b.** Gibt es im Hause Verantwortliche, die sich über notwendige und mögliche Sicherheitsvorkehrungen auf dem Laufenden halten?
- **c.** Gibt es Katastrophenpläne im Unternehmen?

2. RISIKOFAKTOR PERSONALBESCHAFFUNG

- **a.** Wird bei Bewerbern mit ungewöhnlichen Kündigungsterminen oder häufigem Stellenwechsel die Ursache ergründet?
- **b.** Werden bei Bewerbern für Schlüsselpositionen weitergehende Prüfungen (Referenzen) vorgenommen?
- **c.** Sind sämtliche Mitarbeiter schriftlich zur Geheimhaltung der Firmeninterna verpflichtet?
- **d.** Hat das Management ein Krisenszenario für Vertrauensschadenfälle?

3. RISIKOFAKTOR EDV

- **a.** Gibt es für das IT-System ein Sicherheitskonzept?
- **b.** Werden sämtliche Daten nach ihrer Schutzwürdigkeit klassifiziert und entsprechende Schutzmaßnahmen getroffen?
- **c.** Ist die IT gegen Angriffe von außen geschützt?
- **d.** Ist ein periodischer Passwortwechsel vorgesehen?
- **e.** Gibt es im Unternehmen ungesicherte Internetanschlüsse?
- **f.** Sind Online-Verbindungen zur Hausbank ausreichend geschützt?

4. RISIKOFAKTOR ZAHLUNGSVERKEHR

- **a.** Sind Buchhaltung und Kasse streng getrennt?
- **b.** Werden Scheckvordrucke unter Verschluss gehalten, und werden Nummernkreise kontrolliert?
- **c.** Gibt es im Unternehmen Unterschriftenfaksimiles?
- **d.** Sind dabei vorgelagerte Kontrollen vorgesehen?

5. RISIKOFAKTOR POST

- **a.** Wird die eingehende Post mit einem Eingangsstempel versehen?
- **b.** Werden eingehende Schecks in einem Eingangsbuch notiert?

6. RISIKOFAKTOR EINKAUF/VERKAUF

- **a.** Sind verschiedene Personen jeweils verantwortlich für
  - die Auftragserteilung,
  - die Registrierung eingehender Waren,
  - die Genehmigung der Bezahlung von Waren?
- **b.** Werden regelmäßige Inventuren des Warenbestandes durchgeführt?
- **c.** Werden Retouren gesondert erfasst?
- **d.** Hat das Unternehmen einen Verhaltenskodex für Einkäufer?

7. RISIKOFAKTOR REVISION/KONTROLLEN

- **a.** Gibt es eine eigene Revisionsabteilung?
- **b.** Prüft diese bzw. ein Wirtschaftsprüfer regelmäßig alle Bereiche des Unternehmens?
- **c.** Ist das 4-Augen-Prinzip durchgehend im Unternehmen implementiert? Und wie wird es ggf. im Homeoffice umgesetzt?

MANAGERHAFTUNG

PLÖTZLICH AM PRANGER

Unverhofft kommt oft. Unbewusst auch. Nicht umsonst steigt die Zahl der Fälle, bei denen Unternehmen ihre eigenen Manager in Regress nehmen, in den letzten Jahren stark an. Der Vorwurf: Sorgfaltspflichtverletzungen oder mangelnde Risikoanalyse. Vorsorgemaßnahmen wie Compliance-Systeme, Whistleblowing-Hotlines oder Versicherungen sollen helfen, finanzielle Schäden für das Unternehmen im Worst Case abzufedern.

Eine fatale Falle für Manager: Wie will man nachweisen, dass man bei einem folgenschweren Cyberangriff alles getan hat, um das Unternehmen zu schützen? Genau hier sind Manager im Zweifelsfall aber in der Pflicht: Sie müssen nachweisen, dass sie ausreichende Maßnahmen ergriffen und implementiert haben. Oft genug gelingt das nicht.

Manchmal kommt eines zum anderen: die veraltete Firewall, unzureichende IT-Sicherheit, eine ungenügende Prozess-Dokumentation, ein missachtetes 4-Augen-Prinzip, fehlende Compliance-Schulungen, der unbedachte Klick im Homeoffice und eine damit installierte Ransomware. Oder eine Überweisung an Betrüger nach Anweisungen durch den falschen Chef. Das Unternehmen steht vor ernstzunehmenden finanziellen Schwierigkeiten und Schuldige werden gesucht. Wie soll der Manager jetzt beweisen, dass dem Aufsichtsrat neues IT-Equipment und eine Cyberversicherung zu teuer waren? Hat er solche Entscheidungen nicht schriftlich dokumentiert vorliegen, kann es schnell eng werden. Doch auch Fälle, bei denen Unternehmer vollkommen unbewusst in Haftungsrisiken schlittern, kommen gerade bei kleinen und mittelständischen Unternehmen häufiger vor, als man denkt. Oft hapert es schon an internen Kontrollmechanismen und Compliance-Prozessen.

> **Manager müssen im Zweifelsfall nachweisen, dass sie geeignete Vorsorgemaßnahmen getroffen haben und sie keine Schuld trifft. Ohne entsprechende Beweise ist das jedoch oft schwierig bis unmöglich – gerade bei Cybercrime oder Betrug."** *Jesko Trahms*

Doch welche Verpflichtungen gibt es überhaupt und was können Unternehmen und ihre Manager tun, um sich besser zu schützen? Das erläutert Jesko Trahms, Fachanwalt für Strafrecht und Partner bei BDO Legal Rechtsanwaltsgesellschaft mbH:

Welche Verpflichtungen in der Compliance haben Unternehmen zur Prävention und Bekämpfung der dargestellten Risiken und der damit verbundenen Haftungsszenarien?
Nach gefestigter Rechtsprechung hat die Geschäftsführung eines Unternehmens eine Verpflichtung, ein Compliance Management System im Betrieb zu organisieren und zu implementieren. Dies wird beispielsweise aus der „Sorgfalt einer ordentlichen Geschäftsführung" gefolgert. Das bedeutet: Zunächst muss die Geschäftsführung alle (rechtlichen, tatsächlichen und finanziellen) Risiken identifizieren und geeignet „bekämpfen". Sie muss Verantwortlichkeiten definieren, klare Richtlinien kommunizieren und entsprechende Prozesse implementieren. Wenn die erkannten Risiken auch dadurch nicht ausreichend minimiert werden können,

Jesko Trahms ist Fachanwalt für Strafrecht und Partner bei BDO Legal Rechtsanwaltsgesellschaft mbH

ist eine Absicherung durch eine entsprechende Versicherung eine durchaus adäquate Handlungsoption.

Was passiert, wenn Unternehmen diesen Verpflichtungen nicht nachkommen?
Wird ein Compliance Management System nicht ausreichend organisiert, kann die Rechtsprechung – je nach Einzelfall – hierin eine „Sorgfaltspflichtverletzung" der Geschäftsführung sehen. Diese kann beispielsweise durchaus zu einer persönlichen Haftung für Schäden führen, die dem Unternehmen dadurch kausal entstehen. Wichtig ist dabei, dass nach der Rechtsprechung die Manager in einem Haftungsprozess durch eine sogenannte Beweislastumkehr nachweisen müssen, dass sie keine Sorgfaltspflichtverletzung begangen haben und sie kein Verschulden trifft. Oft ist dieser Nachweis mangels Beweismitteln bzw. fehlender Unterlagen nicht möglich oder schwer zu führen.

> **Gerade beim Thema Compliance haben Unternehmen noch Nachholbedarf. Viele Unternehmer sind sich ihrer Verpflichtungen gar nicht in vollem Umfang bewusst – und laufen so Gefahr, in persönliche Haftungsrisiken zu schlittern."** *Jesko Trahms*

Wie sind Unternehmen aktuell diesbezüglich aufgestellt? Wie gut sind sie vorbereitet? Sind sie sich der Gefahren überhaupt bewusst?
Viele Unternehmen bzw. deren Geschäftsführung haben sich nach meiner Einschätzung mit dem Thema „Compliance" nicht oder nicht ausreichend befasst. Man kann hier die allgemeine Regel aufstellen: Je kleiner die Unternehmung, desto weniger Compliance-Aktivitäten. Sehr oft sind sich dabei die Verantwortlichen der – auch persönlichen – Haftungsrisiken und Gefahren gar nicht bewusst.

Bei der Compliance wird auf eine Früherkennung von Risiken gesetzt. Findet diese nicht statt, können Compliance-Vorfälle gerade kleine und mittlere Unternehmen sehr schnell in existenzielle Schwierigkeiten bis hin zu einer drohenden Insolvenz bringen.

Welche Rolle spielen Whistleblowing-Systeme bei der Aufdeckung von sogenannten „Innentätern"?
Whistleblowing- oder Hinweisgebersysteme haben eine überragende Bedeutung für die Entdeckung von kriminellen Machenschaften, die ein Unternehmen oft über Jahre dauerhaft schädigen. Dies gilt insbesondere für sogenannte „Innentäter", die – oft im gezielt schädlichen Zusammenwirken mit externen Dritten – sprichwörtlich in die Firmenkasse greifen. Sehr oft bekommen andere Mitarbeiter oder das soziale Umfeld der Täter hiervon etwas mit, trauen sich aber aus verschiedenen Motiven heraus nicht, sich mit diesem Wissen „zu outen". Gibt man ihnen mit einem Whistleblowing-System eine Plattform, die Vertraulichkeit und Anonymität garantiert, führt dies sehr oft zum entscheidenden Hinweis, mit dem man Straftaten im Unternehmen entdecken und beenden kann.

SCHEINBAR HARMLOSE WEIHNACHTSGESCHENKE ALS FATALE „TÜRÖFFNER"

In einem Unternehmen hatte ein Mitarbeiter anonym gemeldet, dass Kollegen in einer Abteilung in der Vorweihnachtszeit jeweils ein persönliches Präsent per Paket erhalten hatte. Neben Süßigkeiten umfasste das Geschenk einen USB-Stick und eine Computer-Maus, die von den Mitarbeitern bedenkenlos sofort eingesetzt wurden. Die nach dem Hinweis sofort eingeleitete Untersuchung förderte einen bereits aktiven Cyber-Angriff zutage, bei dem die „Geschenke" als „Türöffner" in das System der Firma genutzt wurden.

Fazit: Hundertprozentige Sicherheit gibt es nicht.
Die „Schwachstelle Mensch" kann niemand schließen: Es gibt immer Fälle, in denen selbst das beste Compliance-System ausgehebelt wird. Die Compliance kann nie einen 100%igen Schutz gewährleisten oder garantieren. Sie sorgt allerdings für eine deutliche Minimierung der Risikopotentiale im Unternehmen, und zwar durch Identifizierung der Risiken verbunden mit internen Vorgaben und Prozessen. Zudem schützt sie die Reputation von Mitarbeitern und Unternehmung. Zur „ordentlichen" Unternehmensführung kann gehören, Restrisiken auf eine Versicherung zu verlagern. Dies betrifft insbesondere die Bereiche Managerhaftung (D&O), Schäden durch Innentäter bzw. Vertrauenspersonen (Vertrauensschadenversicherung) und Cyber-Angriffe (Cyber-Versicherung).

10 TIPPS,

WIE SICH UNTERNEHMEN VOR CYBERCRIME SCHÜTZEN KÖNNEN

1. **SENSIBILISIERUNG DER MITARBEITER** für spezielle Risiken im Homeoffice. Insbesondere Finanzabteilungen (im In- und Ausland) sollten durch virtuelle Schulungen auf aktuelle Betrugsmaschen hingewiesen werden. Unternehmen sollten alle Mitarbeiter ermutigen, verdächtige Inhalte umgehend zu melden.

2. **OFFENE KOMMUNIKATION:** Teams sollten trotz der physischen Distanz versuchen, einen engen Kontakt zu halten (z. B. über virtuelle Meetings, Team-Chats etc.). Der Austausch der wichtigsten Telefonnummern (dienstliche wie auch private Nummern) für Rücksprachen mit Kollegen und Vorgesetzten hilft zudem, Betrugsversuche zu vereiteln.

3. **WEB-ADRESSEN** immer händisch eingeben: Keine Links oder Anhänge anklicken oder auf unerwünschte Nachrichten antworten. Datei-Erweiterungen heruntergeladener Dateien prüfen, Dokumente und Videodateien sollten weder im EXE- noch im LNK-Format erstellt worden sein.

4. **BESCHRÄNKEN DER ZUGRIFFSRECHTE** von Personen, die eine Verbindung zum Unternehmensnetzwerk herstellen. Im Homeoffice sollten – wenn möglich – keine öffentlichen oder privaten Computer für dienstliche Zwecke genutzt werden, da sie manipuliert sein können. Es besteht die Gefahr von Datenabfluss und Manipulation. Sollte es für Mitarbeiter notwendig sein, im Homeoffice ihren privaten Computer zu nutzen, sollte dies nach vorheriger Abstimmung mit der unternehmenseigenen IT und den Vorgesetzten erfolgen.

5. **PASSWÖRTER:** Sichere und für unterschiedliche Dienste jeweils andere Passwörter wählen und immer umgehend die neuesten Updates für Betriebssysteme und Apps installieren, um Schwachstellen soweit wie möglich zu minimieren. Apps sollten dabei lediglich aus vertrauenswürdigen Quellen – etwa Google Play, dem App Store oder durch das eigene Unternehmen zur Verfügung gestellten Anwendungspools – heruntergeladen werden.

6. **EINGEHENDE E-MAILS:** Vorsicht bei E-Mails von unbekannten Absendern mit Anhängen oder Links. Aber auch bei Mails von bekannten Absendern ist Vorsicht angesagt, insbesondere wenn sie Zahlungsaufforderungen oder Konto- und Lieferdaten enthalten. „Mouse over" hilft: In sehr vielen Fällen wird zwar der richtige Absendername angezeigt, die E-Mail-Adresse enthält oft aber kleine Abweichungen. Wer mit der Maus über den Absender fährt, kann leicht die Absenderadresse auf Anomalien prüfen.

7. **NACHFRAGEN** beim vermeintlichen Absender, wenn dem Mitarbeiter ein Auftrag seltsam vorkommt. Insbesondere Änderungen von Kontoverbindungen, egal ob von Kunden oder von Lieferanten, immer gegenprüfen – und zwar unter den bekannten oder im System hinterlegten Kontaktdaten und nicht aus der (möglicherweise gefälschten) Signatur der E-Mail.

8. **STIMMIMITATIONSSOFTWARE:** Mitarbeiter sollten grundsätzlich keine Zahlungsanweisungen oder Änderungen von Bankdaten per Telefon annehmen, weder intern noch extern. Sie sollten die Bitte ihres CEO oder CFO um ihre Mithilfe bei finanziellen Transaktionen kritisch hinterfragen und die Person unter der ihnen bekannten Telefonnummer zurückrufen. Zudem sollten sie unbedingt auf einer schriftlichen Anweisung bestehen und diese an ihren Vorgesetzten weiterleiten.

9. **„WHATSAPP"-SPRACHNACHRICHTEN:** Mitarbeiter sollten grundsätzlich jeder „Whatsapp"-Sprachnachricht misstrauen: Sollten der CEO oder ein Vorgesetzter eine „Whatsapp" mit Zahlungsanweisungen schicken, sollten Mitarbeiter unbedingt den Inhalt durch einen Telefonanruf (kein „Whatsapp"-Anruf und kein FaceTime-Video) mit den betroffenen Kollegen abklären und sich die Anweisung auf jeden Fall schriftlich bestätigen lassen.

10. **WENIGER IST MEHR:** Betrüger nutzen Informationen aus sozialen Netzen. Mitarbeiter sollten deshalb vorsichtig sein bei der Preisgabe von Informationen im Internet.

GUT GERÜSTET GEGEN RISIKEN

Sichern Sie Ihr Unternehmen ab gegen Vermögensschäden durch vorsätzlich unerlaubte Handlungen von sogenannten „Vertrauenspersonen“ und externen Dritten. Wir haben die richtige Lösung für Ihren Bedarf:

SCHUTZ VOR VERUNTREUUNG PREMIUM:

Weitreichende Absicherung gegen Schäden durch eigene Mitarbeiter, zielgerichtete Hackerschäden sowie Schäden durch bestimmte Straftaten Dritter für größere Unternehmen.

SCHUTZ VOR VERUNTREUUNG VSV SMART:

Absicherung gegen Schäden durch Vertrauenspersonen, E-Crime und bestimmte Straftaten Dritter für kleinere Unternehmen.

SCHUTZ VOR BESTELLERBETRUG:

Schutz vor Schäden durch Dritte, die durch „Hacken“ der Datenbank Ihres Unternehmens oder auf anderem Wege an Ihre Kontaktdaten gelangen und diese für betrügerische Bestellungen nutzen.

Stellen Sie Ihr Unternehmen jetzt zukunftssicher auf!
Wir unterstützen und informieren Sie gern:

Tel. + 49 (0) 40 / 88 34 - 35 36
service.de@eulerhermes.com
www.eulerhermes.de/vsv

EULER HERMES

Euler Hermes Deutschland
Niederlassung der Euler Hermes SA
22746 Hamburg
Tel. +49 (0) 40 / 88 34 - 0
Fax +49 (0) 40 / 88 34 - 77 44
info.de@eulerhermes.com
www.eulerhermes.de