WWW.EULERHERMES.DE

KRISE FÜR DIE WIRTSCHAFT – KONJUNKTUR FÜR BETRÜGER

Wie sich Unternehmen in Zeiten von Corona vor Cyber- und Täuschungsschäden schützen können

Ein Unternehmen der Allianz

EULER HERMES

CORONAKRISE – BOOMZEITEN FÜR BETRÜGER

Neue Kommunikationswege und neue digitale Geschäftsprozesse halten schon seit einiger Zeit Einzug in das Geschäftsleben. Die Covid-19-Pandemie erhöht an vielen Stellen das Tempo, mit dem diese Umstellung vor sich geht. Dazu birgt die aktuelle Situation viele Unsicherheiten: So manch gewohnter und erprobter Geschäftsprozess muss schneller verändert, neue Kommunikationswege oft von heute auf morgen gefunden werden.

So weicht der Handschlag unter ehrbaren Kaufleuten – oder zumindest das persönliche Treffen mit handschriftlicher Vertragsunterzeichnung – dem elektronischen Versand von Vertragsdokumenten mit gescannten Unterschriften. Die morgendliche Besprechung unter Kollegen findet vielfach nur noch virtuell statt. Die Aufgabenverteilung erfolgt per E-Mail oder Telefon.

Doch funktioniert das immer und überall – und vor allem reibungslos? Gibt es neue, an die ungewohnte Situation angepasste Richtlinien und wer kontrolliert deren Einhaltung? Wer ist eigentlich in Ihrem Büro, wenn Sie von zuhause aus arbeiten? Und wie war das noch mal mit dem Vier-Augen-Prinzip im Homeoffice?

Selbst wenn in Ihrem eigenen Unternehmen alles in Ordnung ist, wer garantiert Ihnen, dass auch bei Ihren Geschäftspartnern alles fehlerfrei funktioniert? Fließen vertrauliche Daten vielleicht jetzt gerade ab – auf indirektem Wege, dafür aber direkt in die Hände von Kriminellen?

Für diese ist die aktuelle Situation ein Eldorado. Mitarbeiter im Homeoffice, die sich in weniger gesicherten IT-Umgebungen bewegen und sich nicht mehr so einfach direkt mit Kollegen austauschen können – das spielt Betrügern in die Hände. Da werden E-Mails gefälscht, vertrauliche Passwörter abgefangen, Identitäten ausgetauscht. Ihre eigenen Mitarbeiter werden getäuscht und sind vollkommen arglos, wenn sie von skrupellosen Kriminellen instrumentalisiert werden. Alles mit dem Ziel, sich auf Ihre Kosten zu bereichern.

Mit welchen immer neuen Tricks Betrüger versuchen, Ihr Firmenkonto zu plündern, was Sie dagegen tun können und wie Sie sich vor finanziellen Schäden schützen können, erfahren Sie auf den folgenden Seiten.

Wir wünschen Ihnen alles Gute und weiterhin viel Erfolg,
Ihr Euler-Hermes-Team

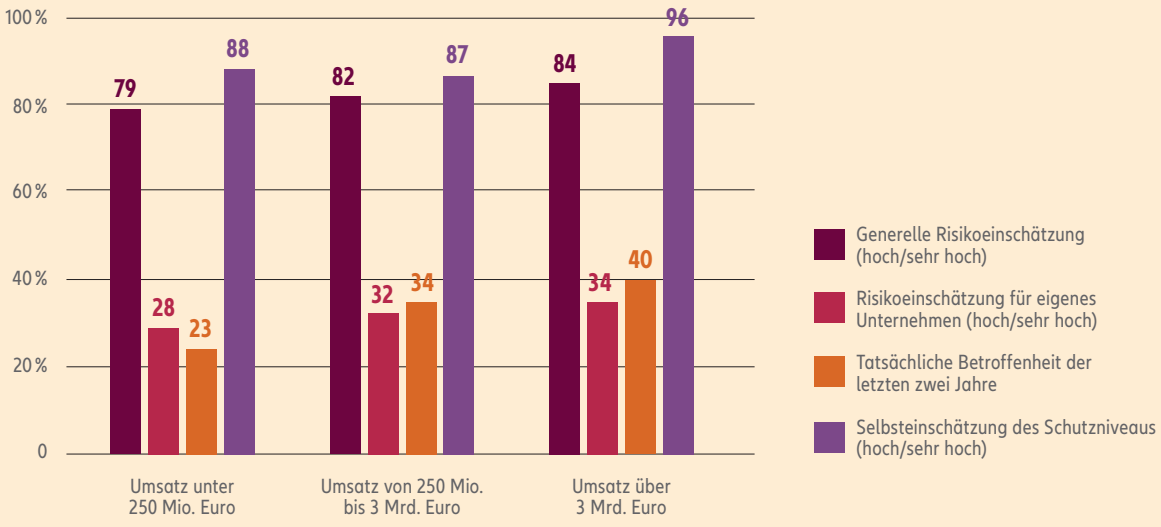
INHALT

WIRTSCHAFTS-KRIMINALITÄT – DIE UNTERSCHÄTZTE GEFAHR

Wirtschaftskriminalität, gar von den eigenen Mitarbeitern im Unternehmen begangen? Keine Spur! Bei uns nicht! Wir haben alles im Griff: Ein ordentliches Betriebsklima, zufriedene Leute, die nicht in Versuchung kommen. Und für den Ernstfall Kontrollen, die funktionieren.

So oder so ähnlich reagieren die meisten Unternehmen, insbesondere Mittelständler, wenn sie auf Wirtschaftskriminalität im Allgemeinen und Vertrauensschäden im Besonderen angesprochen werden. Alles in Ordnung also? Keineswegs, wie sogar Unternehmer und Manager erkennen. Die Gefahr sehen sie nur meistens bei den anderen. Allgemein schätzen sie nämlich die finanziellen Schäden, die der deutschen Wirtschaft durch illegale Machenschaften entstehen, ziemlich hoch ein. Sicher ist, dass die Bedrohung zunimmt, dass Diebstahl, Betrug, Veruntreuung und Unterschlagung durch Mitarbeiter immer häufiger zum betrieblichen Alltag gehören. Die folgenden Zahlen und Analysen zeigen, dass Veruntreuung und Betrug in deutschen Unternehmen längst zu einem enormen Risikofaktor geworden sind.

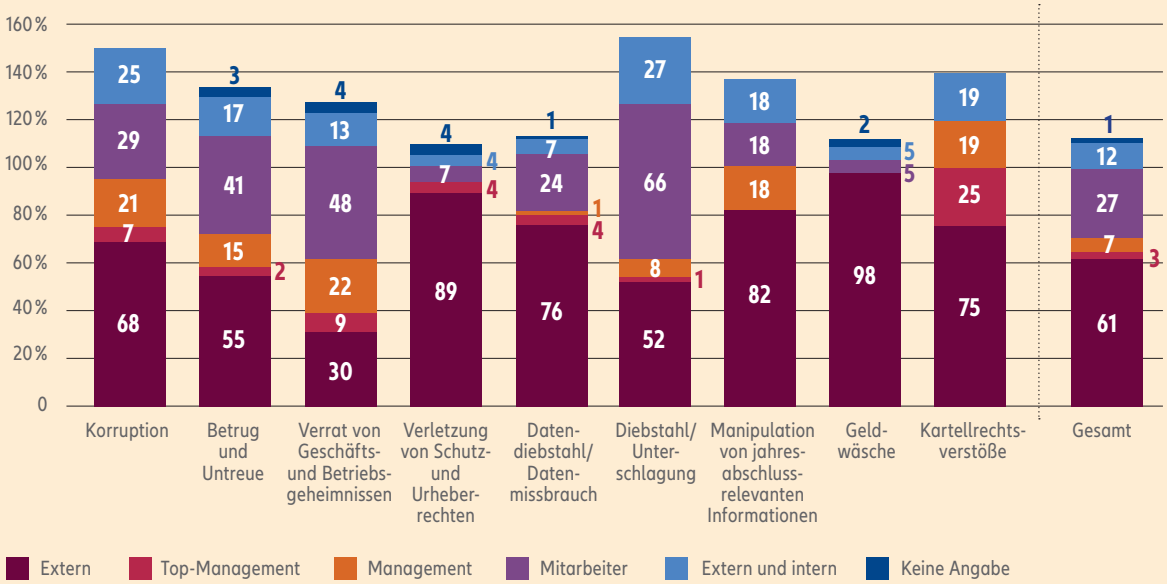
VERGLEICH RISIKOEINSCHÄTZUNG, BETROFFENHEIT UND SELBSTEINSCHÄTZUNG DES SCHUTZES GEGENÜBER WIRTSCHAFTSKRIMINALITÄT



Quelle: KPMG, Deutschland, 2018

Durch alle Unternehmensgrößen hindurch wird das generelle Risiko als sehr hoch eingeschätzt, während man die Gefahr, selbst betroffen zu sein, als eher gering einschätzt.

TÄTERHERKUNFT

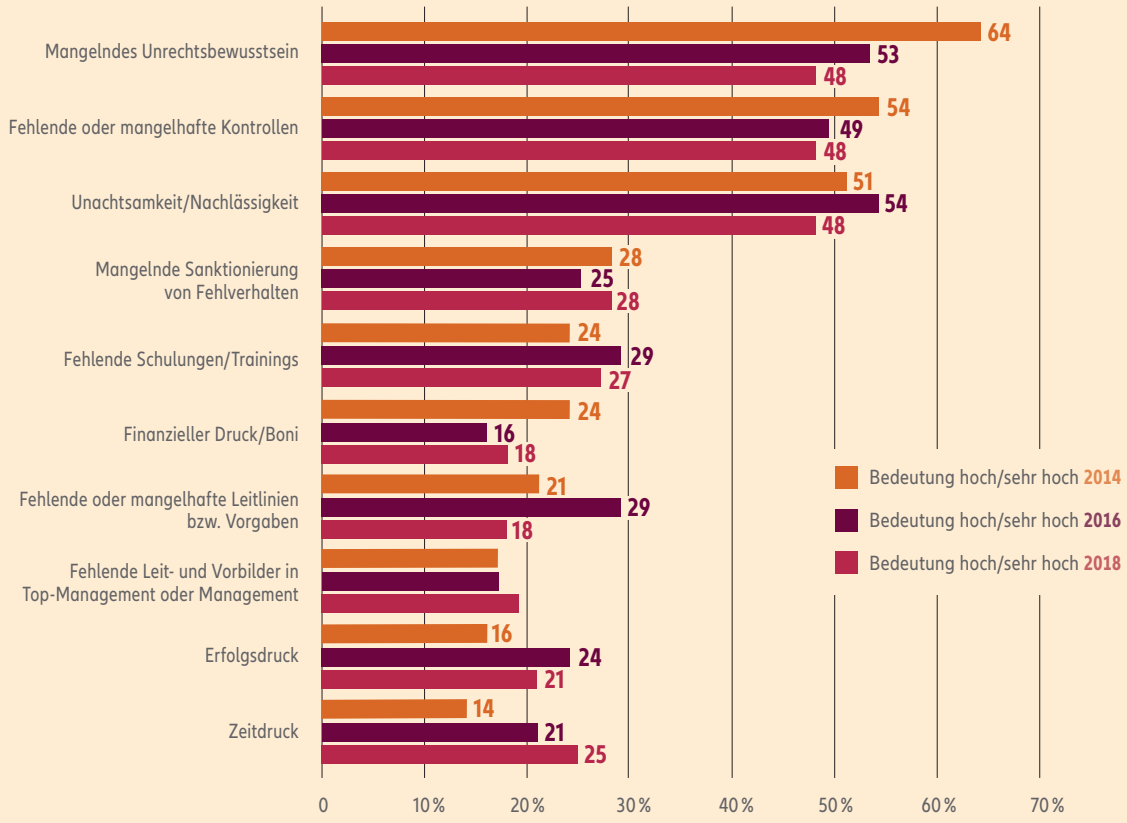


Werte über 100 % ergeben sich daraus, dass auch die Tatbegehung durch ein Zusammenwirken interner und externer Täter abgefragt wurde.

Quelle: KPMG, Deutschland, 2018

Der Anteil der externen Täter an den unterschiedlichen Delikten ist sehr groß.
Bei Verrat und Unterschlagung spielen die eigenen Mitarbeiter die Hauptrolle.

RISIKOFAKTOREN FÜR BEGEHUNG EINER WIRTSCHAFTSKRIMINELLEN HANDLUNG



Quelle: KPMG, Deutschland, 2018

Fragt man nach den Motiven, so spielen vor allem mangelndes Unrechtsbewusstsein, fehlende Kontrollen und Unachtsamkeit die Hauptrollen.

RISIKO HOMEOFFICE

NEW WORK, NEW RISKS

Das Arbeiten im Homeoffice ist in vielen Unternehmen das Gebot der Stunde. Andere haben ihre Belegschaft in Büros und Produktionshallen ausgedünnt, um sie vor der Infektion zu schützen. Allerdings sollten Firmen dringend auch für ihren eigenen Schutz sorgen – vor Cybercrime, Betrug und anderen Vertrauensschäden.

Angela Merkel ist das wohl prominenteste Beispiel für Menschen, die das drohende Coronavirus kurzerhand ins Homeoffice verbannt hat. Dieses Schicksal teilt die Bundeskanzlerin mit hunderttausenden Angestellten. Allein in der Digitalwirtschaft ordneten laut Branchenverband Bitkom zwei Drittel aller Unternehmen die Arbeit in den eigenen vier Wänden an.

Was die einen als Durchbruch von New Work und digitalisiertem Arbeiten feiern, treibt etlichen IT-Profis und Compliance-Experten den Angstschweiß auf die Stirn. Weil Kontaktverbot, Ausgangsbeschränkungen und Produktionsstopps für viele Unternehmen unerwartet kamen, war der Umzug vom Büro ins Homeoffice oft überstürzt und ohne konkrete Planung. „Damit bieten wir derzeit ein Eldorado für Cyberkriminelle", sagt die IT-Beauftragte eines renommierten Medienhauses, das im März über 1.000 Leute binnen einer Woche ins Homeoffice delegierte. *„Unsere Sicherheit ist derzeit nicht so hoch, wie sie sein sollte."* Man habe die hohen Sicherheitsstandards in den ersten beiden Wochen vernachlässigen müssen, *„um große Teams überhaupt remotefähig zu machen"*.

GEFAHREN DURCH ZOOMBOMBING & CO

Teams müssen sich austauschen, weshalb nun in vielen zum Büro umfunktionierten Wohnzimmern fröhlich kostenlose Software für Telefonkonferenzen, Video-Meetings, Datentransfers und Webinare auf Rechner geladen wird. Das Problem: Niemand weiß, ob diese oft sehr einfach zu bedienenden Tools dem deutschen Datenschutz entsprechen, wer eigentlich mithören und mitsehen kann und wo die Daten der Teilnehmer letzten Endes landen.

So ist beispielsweise das Videokonferenz-Tool Zoom – das dank Corona im März bis zu 200 Millionen Nutzerinnen und Nutzer pro Tag zählte – in die Kritik geraten: Beim sogenannten Zoombombing schalten sich wildfremde Leute unbemerkt in die Videokonferenzen, zudem soll Zoom Daten der Teilnehmer an Facebook weitergegeben haben. Das Unternehmen mit Sitz im kalifornischen San José gelobte Besserung – was man glauben kann. Oder auch nicht.

Mindestens so heikel wie der Download von Software ist der Umstand, dass viele Angestellte im Homeoffice mit ihren privaten digitalen Endgeräten arbeiten. Laut der Deloitte-Studie „Mobile Readiness for Work 2019" verfügten nur 20 Prozent der Arbeitnehmer, die im Homeoffice arbeiten, über vom Arbeitgeber bereitgestellte Endgeräte. Mag sein, dass sich die Versorgung der Angestellten mit Firmen-Hardware in der Corona-Krise verbessert hat – 100 Prozent werden es aber kaum sein.

Allein im Büro, während die Kollegen im Homeoffice arbeiten? Neid, Not oder einfach nur Gelegenheit verführen mehr Mitarbeiter zu Vertrauensbrüchen und Straftaten, als mancher Chef vermuten würde.

Dabei warnen Experten eindringlich vor Cybercrime. Die IT-Sicherheitsexperten Markus Schaffrin und Patrick Grihn vom Verband der Internetwirtschaft „eco" schreiben zum Beispiel: *„Nutzen Sie möglichst Ihren Firmen-Laptop, um sich mit den IT-Systemen im Unternehmen zu verbinden. … Umgekehrt sollten Sie Ihre üblichen Unternehmens-Anwendungen auch nicht ohne Zustimmung des Chefs auf einem Privatrechner installieren und nutzen."*

Der laxe Umgang mit Hardware, Daten und Server-Zugängen öffnet findigen Kriminellen gerade Tür und Tor. Ob Diebstahl, Spionage oder Erpressung – die Liste der möglichen Bedrohungen ist lang. Experten warnen vor einem starken Zuwachs an Cybercrime-Delikten. Schon jetzt sorgen diverse Spielarten von Phishing-Mails zum Thema Corona für große Schäden. Selbst in Zeiten, in denen die Wirtschaft nicht unter einem Lockdown leidet, können solche Cybercrime-Attacken für Unternehmen existenzgefährdend sein.

VERTRAUEN IST GUT, ABSICHERN BESSER

Nicht zu vernachlässigen – und das ist kein schönes Thema – sind auch jene Schäden, die Angestellte nicht aus Unwissenheit und Leichtfertigkeit verursachen, sondern mit purer Absicht. Gelegenheit macht bekanntlich Diebe und das Arbeiten im Homeoffice eröffnet viele Möglichkeiten, sensible Unternehmensdaten für eigene Zwecke zu nutzen. Zumal das Vier-Augen-Prinzip derzeit vielerorts außer Kraft gesetzt ist.

Auch denjenigen, die noch in weitgehend verwaisten Produktionsstätten oder nahezu leeren Büros arbeiten, stehen buchstäblich alle Türen offen. Die Marktforscher der GfK haben bereits 2016 in einer repräsentativen Studie herausgefunden, dass jeder vierte Arbeitnehmer schon einmal etwas am Arbeitsplatz gestohlen hat, und da ist Toilettenpapier nur ein ganz kleiner Posten. Insgesamt – das hat Euler Hermes im Rahmen der Vertrauensschadenversicherung errechnet – entstehen deutschen Unternehmen schon in „normalen" Jahren Schäden in Höhe von rund 53 Milliarden Euro durch eigene Mitarbeiter, sei es durch Cybercrime, Datenmissbrauch, Veruntreuung oder andere kriminelle Handlungen.

Fakt ist: Es geht nicht nur um diejenigen, die vielleicht mal einen Kugelschreiber einstecken. Sondern auch um die, die ihrem Chef oder ihrer Chefin immer schon mal eins auswischen wollten und nun – unbeaufsichtigt und unkontrolliert – die Gelegenheit dazu bekommen. Oder um die, die in die Kasse greifen, weil sie wegen der Corona-Pandemie finanziell mit dem Rücken an der Wand stehen, etwa wenn ein Familienmitglied auf Kurzarbeit gesetzt ist. Oder um die, die sich schlicht persönlich bereichern wollen.

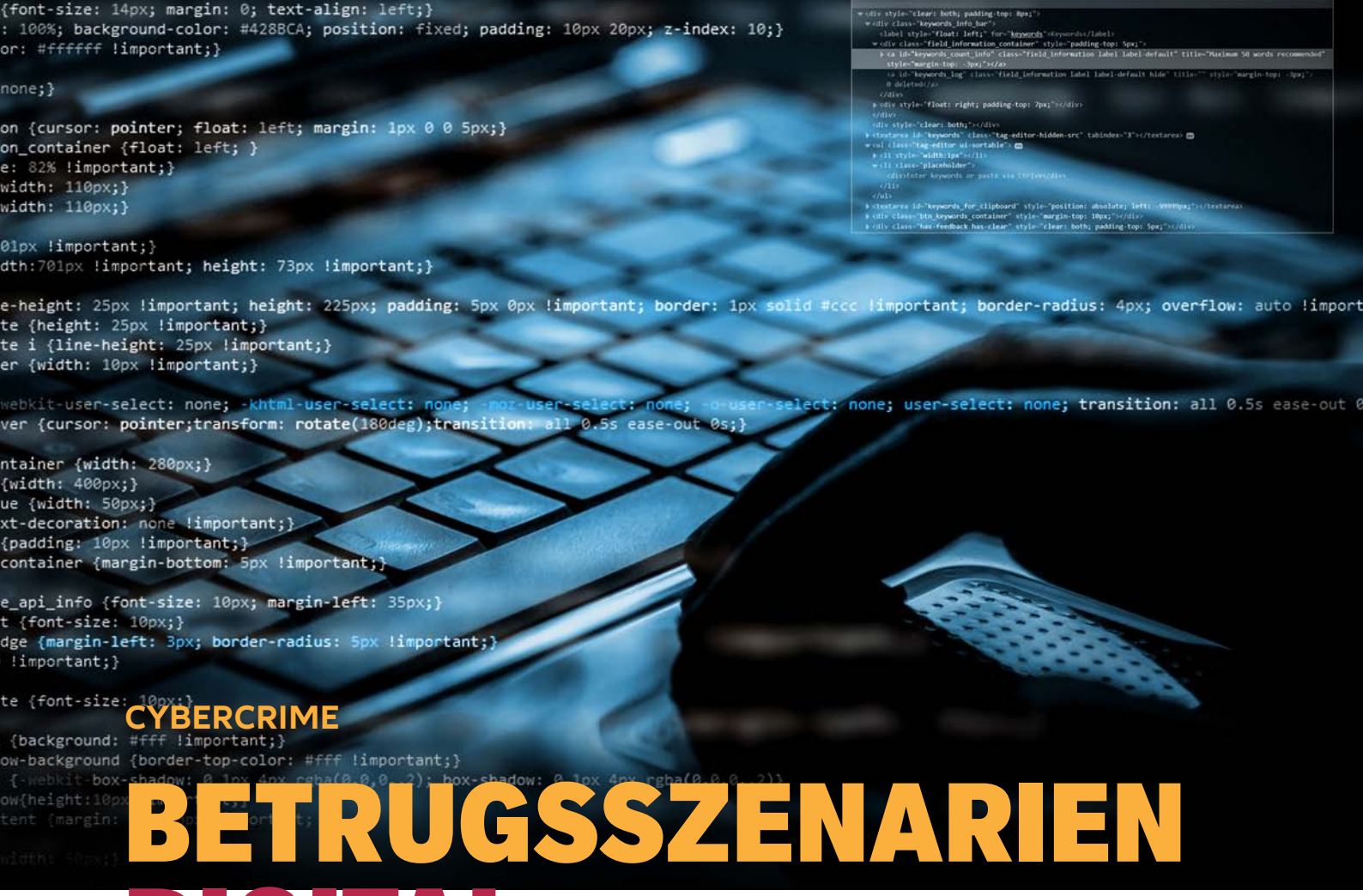
All diese Fälle sind auch unter Compliance-Gesichtspunkten sehr heikel: Vorstände und Geschäftsführer haben eine gesetzlich verankerte Sorgfaltspflicht und tragen ein Haftungsrisiko. Diese Vertrauensdelikte bergen also nicht nur Gefahren für die Firma, sondern auch für jeden Entscheider persönlich.

Die Risiken durch die neue Arbeitssituation sind für Unternehmen und Führungskräfte vielfältig. Es bleibt abzuwarten, wie sich die Schäden durch die Homeoffice-Welle während der Corona-Pandemie entwickeln. Wichtig ist in jedem Fall, sich gut vor ihnen zu schützen.

Mehr Infos online:

Aktuelle Fälle von Cybercrime, Beschreibungen von Betrugsszenarien, Videos, Tipps & Tricks unter https://www.eh-cybercrime.de

Mehr Cybercrime wegen Corona – so schützen Sie sich! Eine Checkliste unter https://www.eulerhermes.de/cybercrime-checkliste-corona



CYBERCRIME

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.

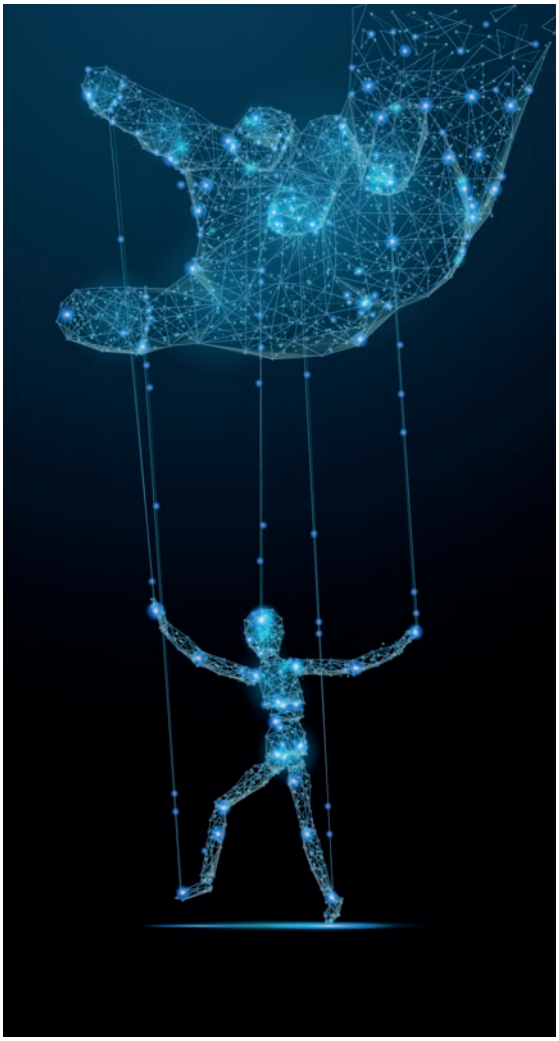
Ziel des Betrugs ist es, mit den erhaltenen Daten beispielsweise Kontoplünderung zu begehen. Eine neuere Variante des Phishing ist Spear-Phishing, worunter ein gezielter E-Mail-Angriff auf eine bestimmte Person oder einen ausgewählten Personenkreis zu verstehen ist – anders als bei herkömmlichem Phishing,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

RISIKOFAKTOREN

SICHERHEITSLÜCKEN JETZT SCHLIESSEN

Die nachfolgende Checkliste soll Ihnen beim Schließen von Sicherheitslücken helfen, schon bevor ein Schaden eingetreten ist. Trotz aller Vorsichtsmaßnahmen lassen sich Betrug und Veruntreuung aber nicht ganz vermeiden. Bei Eintritt eines Schadens ist wichtig, schnell und richtig zu handeln. Die Sicherheitslücke muss konsequent geschlossen werden, damit weitere Schäden vermieden werden. Überprüfen Sie die häufigsten Risikofaktoren am besten regelmäßig.

1. RISIKOFAKTOR UNTERNEHMENSSTRUKTUR

- **a.** Sind die Arbeitsabläufe und -prozesse in Ihrem Unternehmen klar definiert?
- **b.** Gibt es in Ihrem 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 Ihr IT-System ein Sicherheitskonzept?
- **b.** Klassifizieren Sie sämtliche Daten nach ihrer Schutzwürdigkeit und treffen entsprechende Schutzmaßnahmen?
- **c.** Ist Ihre 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 in Ihrem 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.** Haben Sie eine eigene Revisionsabteilung?
- **b.** Prüft diese bzw. ein Wirtschaftsprüfer regelmäßig alle Bereiche Ihres Unternehmens?
- **c.** Ist das 4-Augen-Prinzip durchgehend in Ihrem Unternehmen implementiert?

10 TIPPS,

WIE SICH UNTERNEHMEN IN ZEITEN VON CORONA SCHÜTZEN KÖNNEN

1. **SENSIBILISIERUNG DER MITARBEITER** für spezielle Risiken in Verbindung mit Covid-19 und 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:** Wählen Sie sichere und für unterschiedliche Dienste jeweils andere Passwörter und installieren sie immer umgehend die neuesten Updates für Betriebssysteme und Apps, um Schwachstellen soweit wie möglich zu schließen. 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:** Seien Sie bei E-Mails von unbekannten Absendern mit Anhängen oder Links besonders achtsam. Folgende Domains/ Adressen zum Thema Corona sind beispielsweise bereits als gefährlich identifiziert:

- coronavirusstatus[.]space
- coronavirus-map[.]com
- blogcoronacl.canalcero[.]digital
- - coronavirus[.]zone
- - coronavirus-realtime[.]com
- - coronavirus[.]app
- bgvfr.coronavirusaware[.]xyz
- coronavirusaware[.]xyz

7. **FRAGEN SIE** beim vermeintlichen Auftraggeber/ Absender einer E-Mail nach, wenn Ihnen eine durchzuführende Aktion seltsam vorkommt. Prüfen sie insbesondere Änderungen von Kontoverbindungen, egal ob von Kunden oder von Lieferanten, immer gegen – 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 IN KRISENZEITEN

Es gibt zahlreiche Möglichkeiten, Ihr Unternehmen vor Risiken zu schützen. Hier die wichtigsten Maßnahmen, die auch noch greifen, wenn die Krise schon da ist:

SCHUTZ VOR BETRUG UND CYBERKRIMINALITÄT

- Überprüfen Sie, ob Ihre IT-Systeme vor den neuesten Bedrohungen geschützt sind.
- Beziehen Sie Homeofficelösungen in Ihre Prüfung mit ein.
- Lassen Sie Ihre Mitarbeiter darauf schulen, sensible Informationen zu schützen, betrügerische Versuche abzuwehren und die Gefahren der Verwendung eigener Geräte zu erkennen.
- Eine Vertrauensschadenversicherung kann Sie vor den finanziellen Folgen von Betrug, Veruntreuung und Cyberattacken schützen.

BESTANDSAUFNAHME UND PROGNOSE

- Überprüfen Sie Ihre Kunden auf Anzeichen von Zahlungsverzug wie z. B. unregelmäßige oder nur teilweise Zahlungen.
- Lassen Sie die Bonität Ihrer Geschäftspartner regelmäßig überprüfen.
- Prognostizieren Sie Ihren Cashflow für die nächsten 12 Monate.
- Bilden Sie Liquiditätsreserven, sofern noch nicht ausreichend vorhanden.
- Überprüfen Sie Ihre Verträge und Ihr Debitorenmanagement.
- Versichern Sie sich gegen Insolvenz oder Nichtzahlung mit einer Warenkreditversicherung.

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

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

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