LB≡BW Bereit für Neues

Corporate Finance Fokus

Research für Unternehmen | **Strategie** | 20.11.2020

Cyber-Security: Zum Schutz des Unternehmens

Uwe Burkert
Chefvolkswirt und
Leiter des Bereichs Research

LBBWResearch@LBBW.de
LBBW_Research

>> Cyber-Kriminalität ist allgegenwärtig und eine der größten Bedrohungen für Unternehmen. Daher ist Cyber-Security ein Muss für jedes Unternehmen. Doch wer glaubt, dass Cyber-Security mit dem Installieren von Anti-Viren-Software beginnt und endet, ist ignorant. Diese Ignoranz schadet in vielerlei Hinsicht mehr als die Viren selbst. Das Ziel sollte sein, die Menschen für das Thema zu sensibilisieren, denn lediglich Amateure hacken Systeme, Profis aber hacken Personen. <<

Andreas Heinemann

Inhalt

Autor:

Andreas Heinemann
Analyst
+ 49 711 127–43938
andreas.heinemann@LBBW.de

01 I Die Highlights

- Cyber-Kriminalität bedroht Unternehmen. Cyber-Security sollte daher höchste Priorität in einem Unternehmen verdienen und ist daher Leitungsaufgabe des Managements.

- Rund jedes dritte Unternehmen war bereits von Wirtschaftskriminalität betroffen. Die Wirtschaftskriminalität steigt vor allem im Finanz- und Rechnungswesen sowie im IT-Bereich.

- Cyber-Vorfälle stehen im deutschen Ranking der wichtigsten Geschäftsrisiken auf Platz 2.

- Die durchschnittlichen Gesamtkosten für eine Datenpanne in Deutschland betragen 4,45 Mio. USD. Je größer die Organisation, desto höher sind tendenziell die Kosten für eine Datenpanne. Dabei wird die Mehrzahl der Datenpannen durch Cyber-Angriffe verursacht.

- 2019 wurden in Deutschland 100.514 Cyber-Kriminalität Straftaten registriert (+15,4% ggü. dem Vorjahr). Computerbetrug macht dabei drei Viertel aller Cybercrime-Straftaten aus. Cybercrime-Fälle durch Ausspähen / Abfangen von Daten sowie durch Täuschung im Rechtsverkehr bei Datenverarbeitung steigen ebenfalls. Reputations- und Imageschäden sowie weitere Folgeschäden sind jedoch nur schwer bezifferbar.

- Das Abweichen von Regelprozessen, kompromittierte E-Mails und Social Engineering werden als Einfallstore von Hackern benutzt (vor allem im Home-Office), um Zahlungen und Überweisungen durchzuführen (z.B. Fake President-Betrug). Neben dem Fake President-Betrug sind Besteller- („Fake Identity“) und Zahlungsbetrug („Payment Diversion“) auf dem Vormarsch.

- Home-Office ist eine Bewährungsprobe für Cyber-Security. Es bedarf Verhaltensgrundsätzen und Leitbildern, einer IT-Sicherheitskultur, Cyber-Awareness Schulungen und notwendigen Investitionen in den Bereich Cyber-Security.

- Da kein absoluter Schutz vor Cyber-Kriminalität möglich ist, gilt es eine unternehmenseigene Cyber-Resilienz aufzubauen. Cyber-Resilienz ist die Agilität und Schnelligkeit sowohl der Abwehr- als auch der Wiederherstellungskapazitäten, also die Fähigkeit einer Organisation, sich auf schadhafte Cyber-Vorfälle einzustellen und diesen entgegenzuwirken – und das nicht reaktiv, sondern proaktiv. Es geht hierbei um die Aufrechterhaltung von Vertraulichkeit, Integrität, Verfügbarkeit und Wiederherstellung der Daten und Dienste, die für das Unternehmen wichtig sind. Für Unternehmen besteht hier Ausbaupotential.

02 I

Die digitale Ära benötigt Sicherheit

Cyber-Security sollte höchste Priorität in einem Unternehmen verdienen

Der unumkehrbare Megatrend Digitalisierung lässt die Gesellschaft und Wirtschaft umdenken. Unternehmen digitalisieren daher ihre Geschäftsmodelle, Produkte, Dienstleistungen und Prozesse. Damit einhergehend entstehen aber auch neue Risiken und Gefahren. Hierzu zählen Cyber-Attacken, die primär wirtschaftliche Ziele verfolgen. Diese reichen von Hacktivismus und Cyber-Vandalismus, über Cyber-Kriminalität und Cyber-Spionage bis hin zur Cyber-Sabotage (Cyber-Terrorismus und Cyber-Krieg verfolgen hingegen ideologische, politische und militärische Ziele).

Cyber-Kriminalität bedroht Unternehmen

Für die Real- und Finanzwirtschaft nehmen solche Cyber-Bedrohungen von Jahr zu Jahr zu. Kriminelle Hacker sind innovativ und analysieren Unternehmens- und Banksysteme aber auch menschliche Gepflogenheiten, um ihre nächsten betrügerischen Transaktionen zu planen und durchzuführen. Seit dem Corona-bedingten Lockdown im Frühjahr kommt das Arbeiten im Home-Office für viele Unternehmen und ihre Beschäftigten hinzu. Unternehmen und Mitarbeitende müssen sich auf diese Situation einstellen und für das sichere Arbeiten von zu Hause sorgen, sei es beim Teilen sensibler Informationen und Bildschirminhalten oder beim gemeinsamen Arbeiten an Dokumenten. Sie müssen sich der Gefahren bewusst und mit den gängigsten Betrugsmaschen vertraut sein.

Cyber-Bedrohungen nehmen vor allem im Home-Office zu

Bereits vor vier Jahren haben wir auf das Thema E-crime, also Cyber-Kriminalität, aufmerksam gemacht. Cyber-Kriminalität ist jedoch nicht nur ein technisches, sondern eben auch ein unternehmensorganisatorisches und menschliches Problem, da nicht nur IT-Sicherheitslücken ausgenutzt, sondern auch Mitarbeitende im Unternehmen getäuscht werden.

Cyber-Security (Cyber-Sicherheit) ist somit ein strategisches Thema und wird damit eine Leitungsaufgabe für das Topmanagement. Es muss auf Vorstands- und Managementebene sichtbar sein, finanziert und unterstützt werden. Mit dieser Studie möchten wir die Problematik von Cyber-Kriminalität erneut verdeutlichen und zur Sensibilisierung aufrufen, da in der Folge von Cyber-Kriminalität erhebliche Schäden einhergehen können. Die Schäden materialisieren sich in Finanzschäden, Image- und Reputationsverlusten, Produktions- und Betriebsunterbrechungen sowie Lieferausfällen. Daher sollte das Thema bei Unternehmen einer jeden Größenklasse höchste Priorität verdienen und genießen.

Cyber-Kriminalität an sich ist kein Desaster, die Folgen davon schon

Infobox: IT-Sicherheit vs. Cyber-Sicherheit

Sowohl IT-Sicherheit als auch die Cyber-Sicherheit zielt auf den Schutz von Informationen ab.

IT-Sicherheit bezieht sich auf einen breiteren Bereich. Sie konzentriert sich auf den Schutz wichtiger Daten vor jeder Art von Bedrohung. Wesentliche Anliegen der IT-Sicherheit umfassen die Vertraulichkeit, Integrität und Verfügbarkeit der Daten. Darüber hinaus befasst sie sich sowohl mit digitalen als auch mit analogen Informationen. IT-Sicherheit deckt dabei einen weiten Bereich ab, der auch die Cyber-Sicherheit einschließt.

Ähnlich wie die IT-Sicherheit zielt die **Cyber-Sicherheit** darauf ab, Informationen sicher zu halten, aber sie konzentriert sich besonders auf die Daten in digitaler Form: mobile Geräte, Tablets, Computer, Arbeitsstationen, Server, Netzwerke und so weiter. Sie befasst sich aber auch mit anderen Dingen: Cyber-Kriminalität, Cyber-Angriffe und Cyber-Betrug bis hin zur Strafverfolgung. Der Zweck aller Cyber-Sicherheitspraktiken ist es, elektronische Daten vor unbefugtem Zugriff zu schützen. Um dies zu erreichen, entscheiden sich Cyber-Sicherheitsexperten für unterschiedliche Protokolle und Methoden, darunter die Identifizierung sensibler und/oder wertvoller Daten, die Reduzierung von Schwachstellen in der Sicherheitsfassade einer Organisation und die Bewertung von Risiken.

03 I

Von der Wirtschaftskriminalität zur Cyber-Kriminalität

Wirtschaftskriminalität ist keine Seltenheit

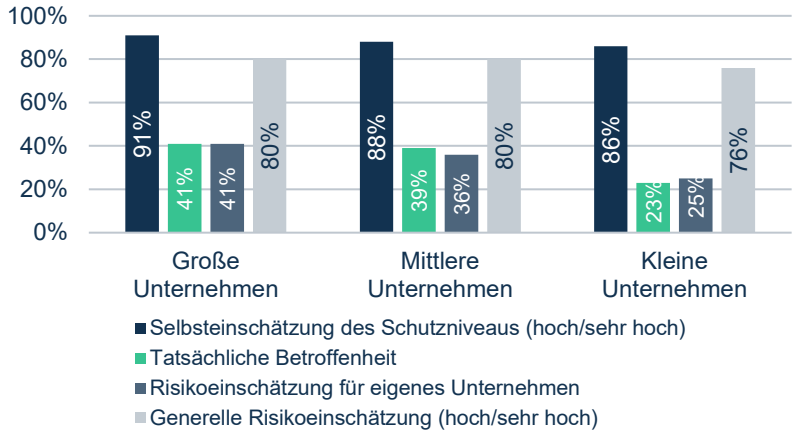
Im Hinblick auf wirtschaftskriminelle Handlungen besteht bei Unternehmen in der Eigen- und Fremdwahrnehmung eine hohe Diskrepanz, die es bereits in der Vergangenheit auch schon gegeben hat. Dass das eigene Unternehmen von Wirtschaftskriminalität betroffen sein könnte, halten 30% der befragten Unternehmen für wahrscheinlich, wohingegen rund drei Viertel der Unternehmen (78%) für andere Unternehmen das generelle Risiko von Wirtschaftskriminalität betroffen zu sein, als hoch oder sehr hoch einschätzen. Dies ist das KPMG-Studienergebnis der Befragung von Vertretern von 1.000 repräsentativ nach Branche, Mitarbeiterzahl und Umsatz ausgewählten Unternehmen in Deutschland zu ihren Erfahrungen im Bereich Wirtschaftskriminalität.

Großer Unterschied bei Selbst- und Fremdwahrnehmung im Hinblick auf das Risiko der Betroffenheit von Wirtschaftskriminalität

Dabei gibt es bei der Risikobewertung zwischen den Unternehmensgrößenklassen kaum Unterschiede. In der Eigenwahrnehmung tendieren kleine Unternehmen jedoch dazu, dass sie die Gefahr selbst von wirtschaftskriminellen Handlungen betroffen zu sein, grundsätzlich geringer einstufen (25%) als mittlere (36%) oder große Unternehmen (41%). Ein weiterer Unterschied zeigt sich in der Selbsteinschätzung des Schutzniveaus: 86% der kleinen Unternehmen schätzen ihr Schutzniveau als hoch oder sehr hoch ein, wohingegen die Einschätzung bei größeren Unternehmen noch optimistischer ausfällt (91%). Somit zeigen Unternehmen insgesamt ein großes Vertrauen in ihr eigenes Schutzniveau. Trotz des hoch wahrgenommenen Schutzniveaus waren 30% der Befragten bereits von Wirtschaftskriminalität betroffen. Dabei steigt mit zunehmender Betriebsgröße die Betroffenheit durch Wirtschaftskriminalität.

Kaum Unterschiede bei Unternehmensgrößenklassen

Wirtschaftskriminalität: Risikoeinschätzung, Betroffenheit und Einschätzung des Schutzes



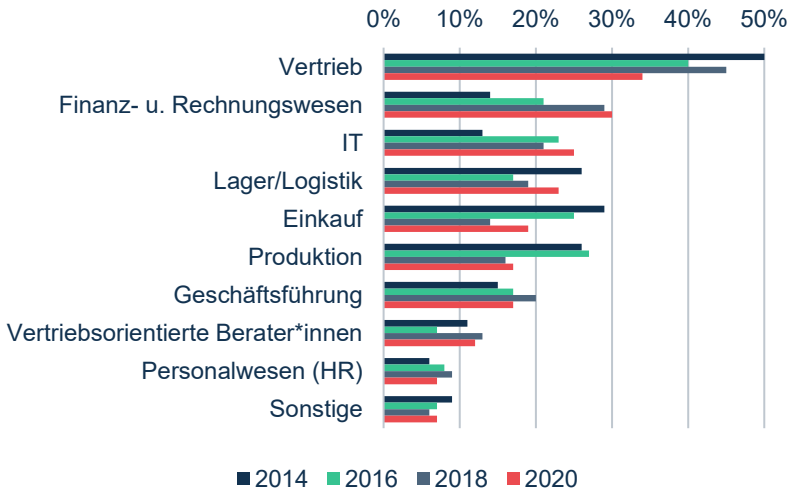
Anmerkung:
Große Unternehmen: Umsatz größer als 3 Mrd. EUR oder Beschäftigtenzahl größer als 500 Mitarbeitende.
Mittlere Unternehmen: Umsatz zwischen 250 Mio. EUR und 3 Mrd. EUR oder Beschäftigtenzahl zwischen 101 bis 500 Mitarbeitende.
Kleine Unternehmen: Umsatz kleiner als 250 Mio. EUR oder Beschäftigtenzahl unter 101 Mitarbeitende.
Quellen: KPMG Deutschland, LBBW Research

Rund jedes dritte Unternehmen bereits von Wirtschaftskriminalität betroffen

Den am häufigsten von Wirtschaftskriminalität betroffenen Unternehmensbereich stellt seit 2014 der Vertrieb dar. Jedoch ist hier zwischen 2014 und 2020 ein nennenswerter Rückgang um 16 Prozentpunkte zu verzeichnen. Es wird allerdings deutlich, dass die Bereiche Finanz- und Rechnungswesen sowie IT zunehmend von Wirtschaftskriminalität betroffen sind und 2020 auf Platz 2 und 3 rangieren. Im Jahr 2014 gaben jeweils 14% und 13% der Unternehmen an, dass das Finanz- und Rechnungswesen sowie die IT die betroffenen Bereiche waren. Sechs Jahre später geben jeweils 30% und 25% der Befragten an, dass es in den jeweiligen Bereichen zu Wirtschaftskriminalität gekommen ist.

Wirtschaftskriminalität steigt im Finanz- und Rechnungswesen sowie im IT-Bereich

Von Wirtschaftskriminalität betroffene Unternehmensbereiche

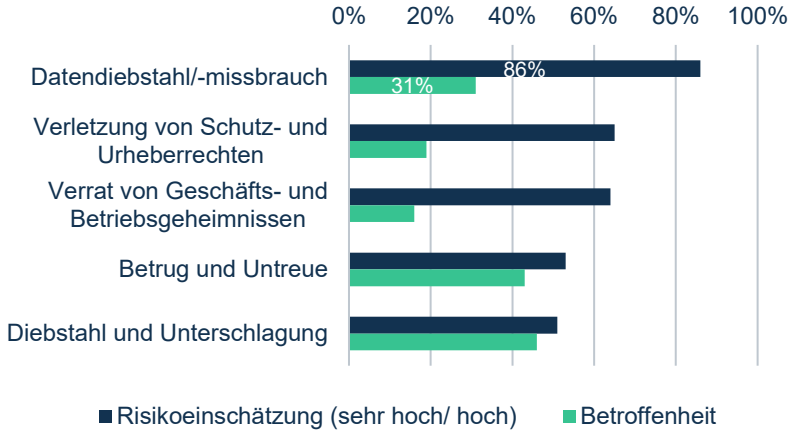


Quellen: KPMG Deutschland, LBBW Research

Vor allem die deliktspezifische Risikowahrnehmung unterstreicht die immense Bedeutung des Themenfelds Datenschutz in Zeiten, in denen für Big Data und Machine Learning enorme Mengen an Daten gesammelt und zunehmend Daten sensibler Kategorien verarbeitet werden. Somit werden mit der fortschreitenden Digitalisierung besondere Schutzvorkehrungen erforderlich. Während knapp ein Drittel der befragten Unternehmen von Datendelikten betroffen war (31%), geben deutlich mehr Unternehmen an (86%), das Risiko eines Datendelikts als sehr hoch einzuschätzen (86%). Die große Divergenz zwischen Betroffenheit und Risikoeinschätzung kann zum einen auf die enorme mediale Präsenz dieser Thematik angesichts der Datenschutz-Grundverordnung (DS-GVO) und zum anderen auf Cyber-Kriminalitätsvorfälle durch Hackerangriffe zurückgeführt werden.

Ein Großteil der Unternehmen schätzt das Risiko von einem Datendelikt betroffen zu sein als hoch ein

Risikoeinschätzung im Vergleich zur tatsächlichen Betroffenheit



Anmerkung:
Ohne die Kategorien Korruption, Geldwäsche, Kartellverstöße und Manipulation von jahresabschlussrelevanten Informationen
Quellen: KPMG Deutschland, LBBW Research

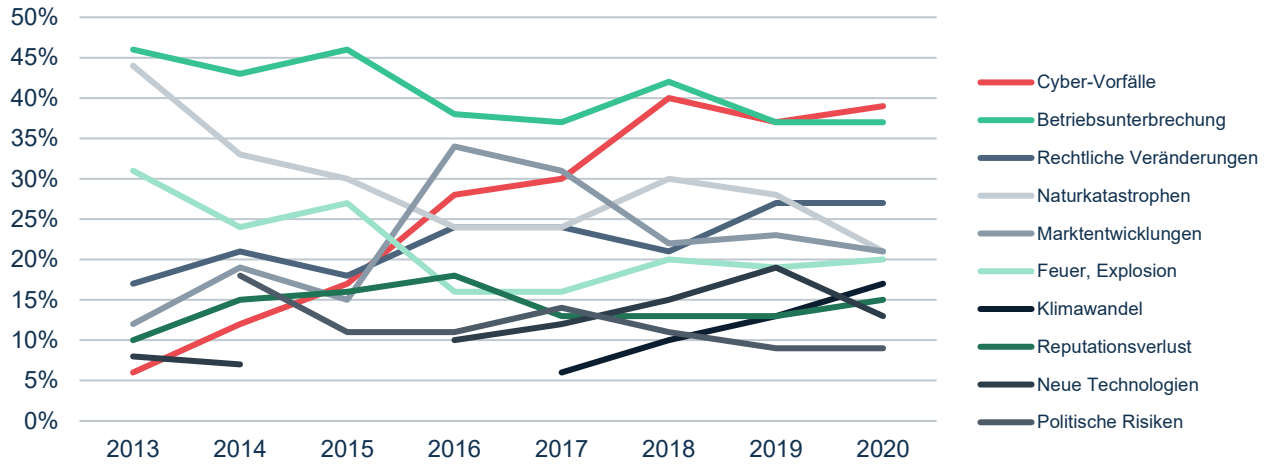
Cyber-Vorfälle als wichtigstes Geschäftsrisiko

Weltweit sind für Unternehmen die Cyber-Vorfälle erstmals das wichtigste Geschäftsrisiko, wie das Allianz Risk Barometer 2020 zeigt, welches die Ergebnisse der jährlichen Umfrage der Allianz Global Corporate & Specialty zu den wichtigsten Unternehmensrisiken unter mehr als 2.700 Risikoexperten (darunter CEOs und Führungskräfte, Risikomanager, Makler und Versicherungsexperten) aus über 100 Ländern zusammenfasst. Bei der Analyse der Allianz Risk Barometer Berichte von 2013 bis 2020 zeigt sich, wie IT-Gefahren (2020: 39% der Antworten) von Jahr zu Jahr ernstzunehmender wurden und letztendlich das Risiko einer Betriebsunterbrechung (2020: 37% der Antworten) auf den zweiten Platz verdrängt hat. Dabei hatten Betriebsunterbrechung seit 2013 den Spitzenplatz im Ranking inne und Cyber-Vorfälle lagen mit lediglich 6% der Antworten auf Platz 15. Obwohl Cyber-Vorfälle weltweit auf Platz eins stehen, belegen sie in Deutschland nur den zweiten Platz (44% der Antworten), weiterhin stehen nämlich Betriebsunterbrechung (55% der Antworten) an der Spitze.

Cyber-Vorfälle im deutschen Risikoranking auf Platz 2

Unter Cyber-Vorfällen versteht man Cyber-Kriminalität (Cybercrime), Datenschutzverletzungen, IT-Ausfälle sowie Geldbußen und Strafen. Im Hinblick auf Datenschutzverletzungen und Geldbußen war es sicherlich die im Mai 2018 europaweit eingeführte DS-GVO, die dem Unternehmensrisiko „Cyber-Vorfälle“ einen Höhenflug beschert hat. Unternehmen müssen jedoch auch in Zukunft mit Datenschutzverletzungen und Geldstrafen rechnen, wenn sie Opfer eines Cyber-Vorfalls werden. Dabei kreisen die wirtschaftlichen Verluste von Unternehmen nach einem Cyber-Vorfall vor allem um den Reputationsverlust, gefolgt von Betriebsunterbrechung und Haftungsansprüchen nach einer Datenschutzverletzung.

Die wichtigsten globalen Geschäftsrisiken



Anmerkung:
Aufgrund fehlender Werte und Unübersichtlichkeit fehlen in der Grafik folgende Kategorien:
Makroökonomische Entwicklungen: z.B. Sparprogramme, Anstieg der Rohstoffpreise, Deflation, Inflation.
Stromausfälle bei kritischer Infrastruktur: z.B. Unterbrechung der Stromleistungen.
Umweltrisiken: z.B. Verschmutzung.
Gesundheitsthemen: z.B. Pandemien.

Quellen: Allianz, LBBW Research

Infobox: Cyber-Kriminalität

Bei der Cyber-Kriminalität agieren Cyber-Kriminelle als Einzeltäter oder in Gruppen, die mehr oder weniger gut organisiert und ausgerüstet sind. Ihre illegalen Aktivitäten im Cyber-Raum sind darauf aus, finanzielle Gewinne zu erzielen. Dabei können sowohl Einzelpersonen als auch Unternehmen geschädigt werden. Die Straftaten weisen eine große Bandbreite auf und umfassen Delikte wie zum Beispiel Kreditkarten- und Warenbetrug, Identitätsdiebstahl und Erpressung.

04 I

Die Fälle und Schäden von Cyber-Bedrohungen steigen

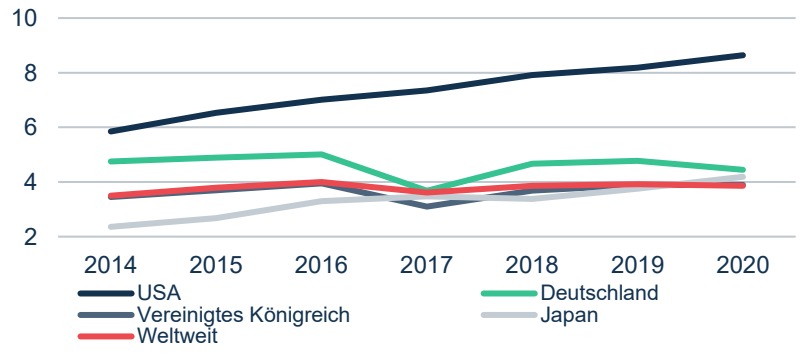
Die Kosten von Datenpannen sind nicht zu unterschätzen

Eine Datenpanne (bzw. ein Datenleck oder Datenverlust) ist ein Vorfall, bei dem Unberechtigte Zugriff auf eine Datensammlung erhalten. Es handelt sich hierbei um eine absichtliche oder unabsichtliche Freigabe (Verlust, Diebstahl oder unberechtigten Zugriff) sicherer oder privater/vertraulicher Informationen an eine nicht vertrauenswürdige Umgebung. Datenpannen sind somit Verstöße gegen die Datensicherheit und den Datenschutz.

Das Ponemon Institut weist darauf hin, dass sich Kosten für Datenpannen zwischen bestimmten Regionen und Branchen unterscheiden können. Die durchschnittlichen Kosten einer Datenpanne variieren und entwickeln sich von Jahr zu Jahr unterschiedlich stark. Auf Basis eines Cyber-Vorfalls nachgelagerten Aktivitäten, die in direkte, indirekte und Opportunitätskosten unterschieden, jedoch leider nicht offengelegt werden, gibt das Institut an, dass weltweit in diesem Jahr die durchschnittlichen Gesamtkosten pro Unternehmen 3,79 Mio. USD betrugen. Gegenüber 2014 (3,5 Mio. USD) ist dies ist ein Anstieg um 8,4%. Dabei sind Vorfälle in US-amerikanischen Unternehmen deutlich teurer (8,64 Mio. USD) als z.B. in Deutschland. Die Kosten in Deutschland betrugen rund 4,45 Mio. USD und entwickeln sich relativ stabil mit einer leicht rückläufigen Tendenz (der Durchschnitt von 2014 bis 2020 liegt bei rund 4,6 Mio. USD). Das zeigt die von IBM Security gesponserte „Cost of a Data Breach"-Studie 2020 des Ponemon Instituts. Hierzu rekrutierte das Ponemon Institute 524 Organisationen, bei denen zwischen August 2019 und April 2020 Datenverstöße aufgetreten sind. Um sicherzustellen, dass die Untersuchung für eine breite Palette von Unternehmen relevant ist, umfassen die in der Studie untersuchten Organisationen verschiedene Größenordnungen und erstrecken sich über 17 Länder und Regionen sowie 17 Branchen. Aus Deutschland haben 37 Unternehmen an der Studie teilgenommen.

Durchschnittliche Gesamtkosten für eine Datenpanne in Deutschland: 4,45 Mio. USD

Durchschnittliche Kosten von Datenpannen

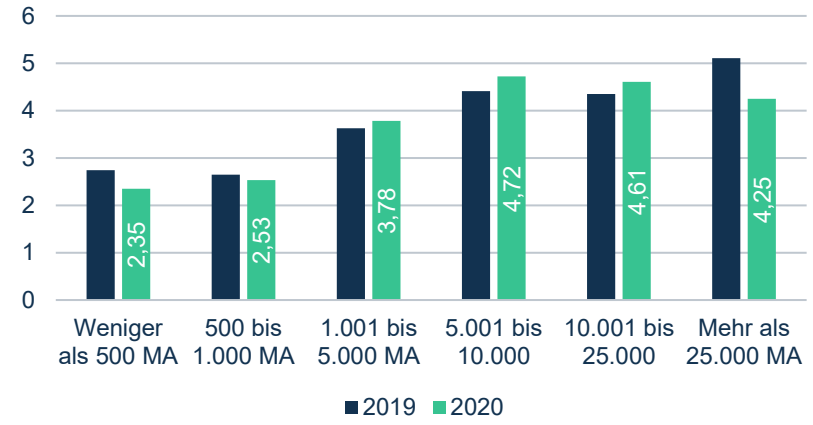


in Mio. USD
Quellen: IBM Security, Ponemon Institute, LBBW Research

Die durchschnittlichen Gesamtkosten einer Datenpanne sanken im Vergleich zum Vorjahr für kleinere Organisationen (1.000 oder weniger Mitarbeitende) und für die größten Organisationen (mehr als 25.000 Mitarbeitende). Organisationen mit mehr als 25.000 Beschäftigten zeigten ein Rückgang der durchschnittlichen Gesamtkosten von 5,11 Millionen Dollar im Jahr 2019 auf 4,25 Millionen Dollar im Jahr 2020, was einem Rückgang von 16,8% entspricht. Für mittelgroße Organisationen (1.001 bis 10.000 Mitarbeitende), stiegen die Kosten einer Datenpanne hingegen leicht an.

Je größer die Organisation, desto höher sind tendenziell die Kosten für eine Datenpanne

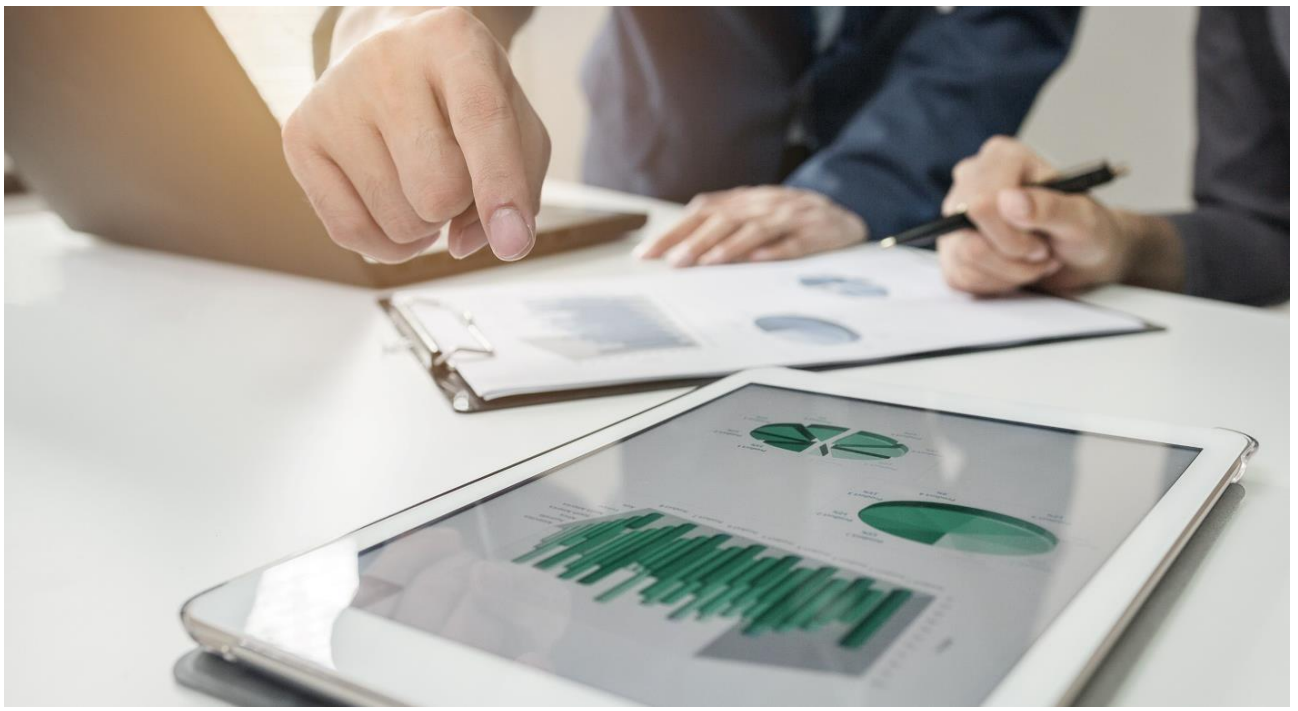
Durchschnittliche Gesamtkosten einer Datenpanne nach Unternehmensgröße (in Mio. USD)



Quellen: IBM Security, Ponemon Institute, LBBW Research

Im Hinblick auf die drei Ursachenkategorien von Datenpannen zeigt sich, dass nach menschlichen Fehlern (23%) und Systemfehlern (25%) vor allem die böswilligen Angriffe (52%) vorherrschen. Bereits seit 2016 werden ebenfalls in Deutschland die allermeisten Datenpannen durch bösartige Angriffe (Malicious attacks) verursacht (2020 waren es 57%).

Die Mehrzahl der Datenpannen werden durch Cyber-Angriffe verursacht



Cyber-Kriminalität in Deutschland steigt

In Deutschland zeigt sich im Hinblick auf Cyber-Kriminalität ein erschreckender Trend. Die Zahl der als Cybercrime im engeren Sinne in der PKS (Polizeiliche Kriminalstatistik) erfassten Straftaten ist im Jahr 2019 gegenüber dem Vorjahr um 15,4% auf 100.514 Straftaten gestiegen (2018: 87.106). Dies zeigen die vom Bundeskriminalamt (BKA) jährlich veröffentlichten Studien zum Bundeslagebild Cybercrime, welche die aktuellen Erkenntnisse zur Lage und Entwicklung im Bereich Internetkriminalität beschreiben.

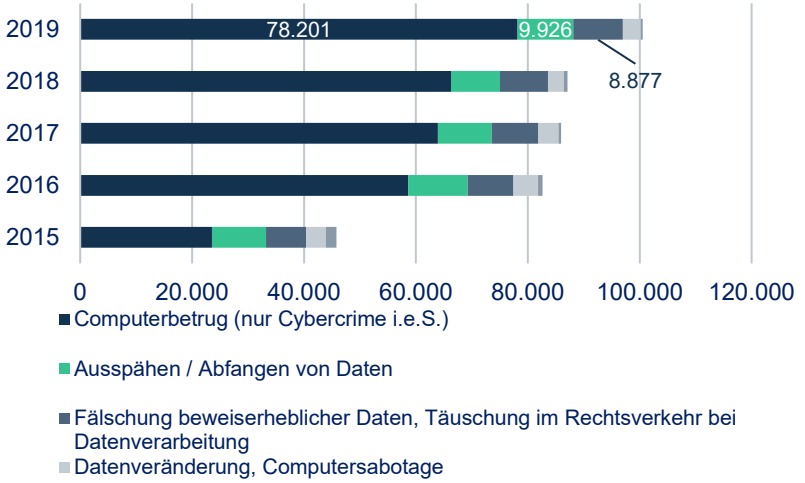
100.514 Straftaten durch Cyber-Kriminalität in 2019: +15,4% ggü. dem Vorjahr

Ganz oben in der Statistik steht der Computerbetrug. Der Computerbetrug (§ 263a StGB) als Cybercrime im engeren Sinne erfasst insbesondere die Verwertungshandlungen des Phishing, Transaktionen unter Nutzung missbräuchlich erlangter Kreditkartendaten und den Einsatz gestohlener oder gefälschter Zahlungskarten am Geldautomaten oder Point-of-Sale (POS)-terminal (daneben umfasst Computerbetrug als Cybercrime i.e.S. weitere Arten des Kreditbetruges, Leistungskreditbetrug und Überweisungsbetrug sowie Abrechnungsbetrug im Gesundheitswesen und das betrügerische Erlangen von Kraftfahrzeugen).

Die Fallzahlen von **Computerbetrug** haben von 2018 (66.284) auf 2019 (78.201) um 18% zugenommen und bilden rund drei Viertel aller Cybercrime-Straftaten (78%). Der starke Anstieg im Bereich des Computerbetrugs von 2015 auf 2016 dürfte insbesondere darauf zurückzuführen sein, dass Delikte, die 2015 noch als (allgemeiner) Betrug, ab 2016 wegen der eindeutigen Zuordnungsmöglichkeiten als Computerbetrug erfasst wurden.

Computerbetrug macht drei Viertel aller Cybercrime-Straftaten aus

Fälle von Cybercrime im engeren Sinne in Deutschland



Quellen: Bundeskriminalamt (BKA), LBBW Research

Um rund 13% sind die Fallzahlen beim Delikt **Ausspähen und Abfangen von Daten** (§§ 202a, 202b, 202c StGB) gestiegen. Dies umfasst den „Diebstahl“ digitaler Identitäten, Kreditkarten-, E-Commerce- oder Kontodaten (z. B. Phishing). Die entwendeten Daten werden in der Re-

gel als Handelsware in der „Underground Economy“ (überregionale Online-Schwarzmärkte, oft im Darknet) zum Kauf angeboten und täterseitig missbräuchlich eingesetzt. Die Verwertung erfolgt damit in zwei Stufen: dem Verkauf der Daten und dem betrügerischen Einsatz erworbener Daten. Auf beiden Ebenen werden erhebliche Gewinne generiert.

Ebenfalls nicht zu vernachlässigen ist der Straftatbestand der **Fälschung beweiserheblicher Daten bzw. der Täuschung im Rechtsverkehr** (§§ 269, 270 StGB), welcher gegenüber dem Vorjahr um rund 4% anstieg. Diese Kategorie erfasst die Täuschung (einer Person) durch die Fälschung von Daten. Durch einen Dateninhaber werden Daten gefälscht bzw. verfälscht und zur Täuschung im Rechtsverkehr genutzt. Dies geschieht z. B. durch die Zusendung von E-Mails unter Vorspiegelung realer Identitäten oder Firmen. Mit überzeugenden Legenden soll das Opfer z. B. zur Preisgabe von Account-Informationen, Kreditkartendaten oder auch zu Zahlungen bewegt werden. Ebenso erfasst ist das Zusenden von als Rechnungen getarnter Schadsoftware in E-Mail-Anhängen.

Cybercrime-Fälle durch Ausspähen / Abfangen von Daten sowie durch Täuschung im Rechtsverkehr bei Datenverarbeitung steigen ebenfalls

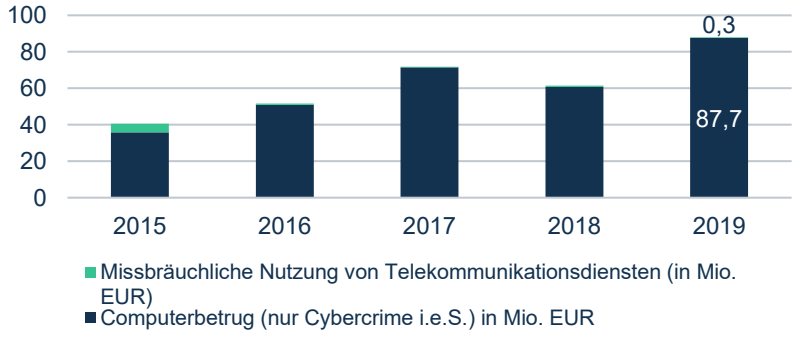
Enorme Schäden durch Cyber-Kriminalität

Anders als bei den Fällen, werden Schäden im Deliktsbereich Cybercrime in polizeilichen Statistiken ausschließlich für Fälle des Computerbetrugs als Cybercrime im engeren Sinne und der missbräuchlichen Nutzung von Telekommunikationsdiensten ausgewiesen/registriert. Die Tatsache, dass zu lediglich zwei Deliktsbereichen eine statistische Schadenserfassung erfolgt, lässt, bedingt durch das hohe Dunkelfeld, keine belastbaren Aussagen zum tatsächlichen monetären (Gesamt-) Schaden durch Cybercrime zu. Neben den statistischen Einschränkungen gilt es zu bedenken, dass finanzielle Schäden eines erfolgreichen Cyber-Angriffs oft nicht gänzlich bekannt oder bezifferbar sind. Reputationsverluste oder Imageschäden lassen sich in finanzieller Hinsicht ebenfalls schwerlich umreißen. Hinzu kommt, dass, je nach Ausgestaltung des Angriffs, oft nicht nur ein einzelnes System für einen bestimmten Zeitraum ausfällt, sondern mitunter komplette Netzwerke und daran gebundene Lieferketten beeinträchtigt werden.

Reputations- und Imageschäden und weitere Folgeschäden nur schwer bezifferbar

Nichtsdestotrotz betrug die für 2019 erfasste Gesamtschadenssumme 88 Mio. EUR. Dies entspricht einer Zunahme um 43% (2018: 61,4 Mio. EUR). Vom erfassten Gesamtschaden entfallen rund 87,7 Mio. EUR auf den Bereich Computerbetrug und nur 0,3 Mio. EUR auf den Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten.

Schäden durch Cyber-Kriminalität in Deutschland



Quellen: Bundeskriminalamt (BKA), LBBW Research

05 I

Vorsicht vor dem Fake President-Betrug

Die Betrugsmasche ist gut geplant

Im Zusammenhang mit Corona und die Verlagerung der Arbeit ins Home-Office, ist die Gefahr sogenannten Fake President-Angriffen zum Opfer zu fallen, gestiegen. Diese Art des Betrugs wird oft von hochgradig organisierten Gruppen von Kriminellen begangen, die ein bestimmtes Unternehmen oder eine Person oder Gruppe von Personen auswählen und den Angriff auf sie ausrichten. Es wird das Abweichen von Regelprozessen ausgenutzt und versucht Personen dazu zu bringen, eine unbefugte Tätigkeit wie zum Beispiel eine Geldüberweisung auf ein ausländisches Konto durchzuführen. In der Regel erfordert ein Fake President-Betrug relativ viel strategische Planung bzw. zeitintensive Vorbereitung. Dabei werden die Aktivitäten des Opfers und die Online-Verhaltensweisen beobachtet, um private Informationen über das Opfer zu sammeln und um eine überzeugende Phishing-Kampagne sowie einen Plan zur Ausführung aufsetzen.

Das Abweichen von Regelprozessen ist ein Einfallstor für Hacker

Der Angriff beginnt oft als Spear-Phishing, was eine Art von Social Engineering darstellt. Beim Spear-Pishing richten sich Betrüger an Nicht-Muttersprachler, die in ausländischen Tochtergesellschaften des Unternehmens beschäftigt sind. Dadurch stellen sie sicher, dass die Wahrscheinlichkeit, dass diese Mitarbeiter den Betrug erkennen, geringer ausfällt. Dies bedeutet auch, dass der betreffende Mitarbeiter mit dem leitenden Angestellten, der eigentlich der Betrüger ist, wenig oder niemals zusammengearbeitet hat.

Es werden Personen gehackt

Letztendlich folgen in den meisten Fällen anhaltende Anrufe, der sogenannte „Vishing“-Angriff. Vishing ist eine Form des Trickbetrugs im Internet. Die Bezeichnung steht für „Voice Phishing“ und ist von dem englischen Begriff für abfischen (fishing) sowie der Methode der eingesetzten VoIP-Telefonie abgeleitet. Dabei wird per automatisierten Telefonanrufen versucht, den Empfänger irrezuführen und zur Herausgabe von Zugangsdaten, Passwörtern, Kreditkartendaten usw. zu bewegen. Der Beschäftigte wird durch Vishing also noch stärker unter Druck gesetzt

Technologien werden zweckentfremdet

Infobox: Betrugsmaschen und Vorgehen

Betrugsmaschen	Vorgehen
Fake President / Chefbetrug / CEO Fraud	Vortäuschung einer falschen Identität: Der Betrüger gibt sich als CEO eines Unternehmens aus und veranlasst mittels „Social Engineering“ (zum Beispiel durch besondere Wertschätzung sowie strenge Geheimhaltung und Druckausübung) Mitarbeiter (meist per E-Mail), Zahlungen zu tätigen, meist für als sehr dringend deklarierte, streng vertrauliche Unternehmenskäufe im Ausland.
Fake Identity / Bestellerbetrug	Vortäuschung einer falschen Identität: Der Betrüger gibt sich als Kunde aus (oft als bestehender) bestellt Waren und lässt diese anschließend an eine abweichende Lieferadresse senden.

Payment Diversion / Zahlungsbetrug	Vortäuschung einer falschen Identität: Der Betrüger gibt sich für einen Lieferanten aus und gibt eine abweichende Kontoverbindung durch für die Bezahlung der bereits erfolgten Lieferung.
Phishing	Der Betrüger versendet gefälschte E-Mails an Mitarbeiter eines Unternehmens zu reellen Themen. Ziel ist es, über den Link in der E-Mail Trojaner oder Keylogger einzuschleusen, um an sensible Unternehmensdaten zu gelangen.
Keylogging	Der Betrüger schleust eine Software ins System ein, die Anmeldedaten und Passwörter aufzeichnet und speichert, zum Beispiel von Kontodaten, Cloud- oder Serverzugängen.
Man in the middle	Der Betrüger hackt sich in die Kommunikation zwischen zwei Kommunikationspartnern ein und besitzt so Zugriff auf den Datenverkehr. Er kann diese Daten einsehen und zu seinen Zwecken beliebig manipulieren.
Man in the cloud	Der Betrüger hackt sich in eine Cloud, in der Unternehmensdaten ausgelagert sind (zum Beispiel durch Keylogging) und kann diese Daten einsehen und beliebig manipulieren oder löschen beziehungsweise Schadsoftware einschleusen.

Quelle: Euler Hermes

Fake President-Fallzahlen und Schadenssummen steigen rasant

Es zeigt sich ein rapider Anstieg der Opferzahlen und der Schadensverluste im Hinblick auf den Fake President-Betrug. Dies zeigt eine Analyse der Studie „Internet Crime Report“ des Federal Bureau of Investigation (FBI, Internet Crime Complaint Center, IC3) der letzten fünf Jahre. Hierbei wurden ausschließlich die Fälle Business E-mail Compromise (BEC) und Email Account Compromise (EAC) betrachtet.

Betrügereien im Zusammenhang mit geschäftlichen E-Mails (BEC-Scams) nutzen die Tatsache aus, dass Personen bei der Abwicklung ihrer privaten und beruflichen Geschäfte auf E-Mail angewiesen sind. BEC ist definiert als ein ausgeklügelter Betrug, der auf Unternehmen abzielt, die mit ausländischen Lieferanten zusammenarbeiten und/oder Unternehmen, die regelmäßig Zahlungen per Überweisung vornehmen. Der Betrug wird durchgeführt, indem legitime geschäftliche E-Mail-Konten durch Social Engineering oder Computereinbruchstechniken kompromittiert werden, um nicht autorisierte Geldtransfers durchzuführen.

Kompromittierte E-Mails und Social Engineering werden benutzt, um Zahlungen und Überweisungen durchzuführen

EAC ist eine verwandte Betrugsmasche des BEC. EAC unterscheidet sich vom BEC dadurch, dass es sich an Einzelpersonen oder einzelne Berufsgruppen richtet und nicht an Unternehmen. EAC ist definiert als ein Betrug, der auf die breite Öffentlichkeit und Fachleute abzielt, die mit Finanz- und Kreditinstituten, Immobiliengesellschaften und Anwaltskanzleien in Verbindung stehen, aber nicht auf diese beschränkt sind. Wie im BEC verwenden die Betreffenden kompromittierte E-Mails, um Zahlungen an betrügerische Orte zu fordern.

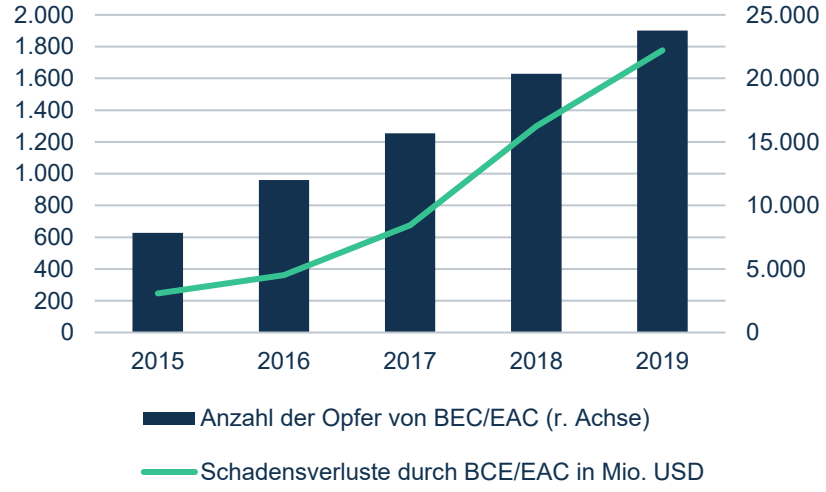
Da sich die Betrugsmaschen BEC und EAC an Personen richten, die regelmäßig Zahlungen per Überweisung durchführen, kann darunter im weitesten Sinne die Fake President-Betrugsmasche verstanden werden.

BEC und EAC können als Fake President-Betrug verstanden werden

Seit ca. 2014 tritt die Fake President-Betrugsmasche in Deutschland vermehrt auf und nahm in den folgenden Jahren stark zu. Exemplarisch zeigt der im Februar 2020 vom FBI veröffentlichte Internet Crime Report

2019 auf, dass es mehr als 23.000 Fake President-Opfer gegeben hat. Laut der Studie haben die Täter mit der Betrugsmasche im vergangenen Jahr weltweit insgesamt 1,7 Mrd. USD erbeutet – Tendenz weiter steigend. Somit ergaben sich zwischen 2015 und 2019 insgesamt Schäden durch Fake President-Scams i.H.v. 4,3 Mrd. USD – und die Dunkelziffer ist weiterhin hoch.

Fake President-Opfer und entstandene Schäden (anhand BEC/EAC)



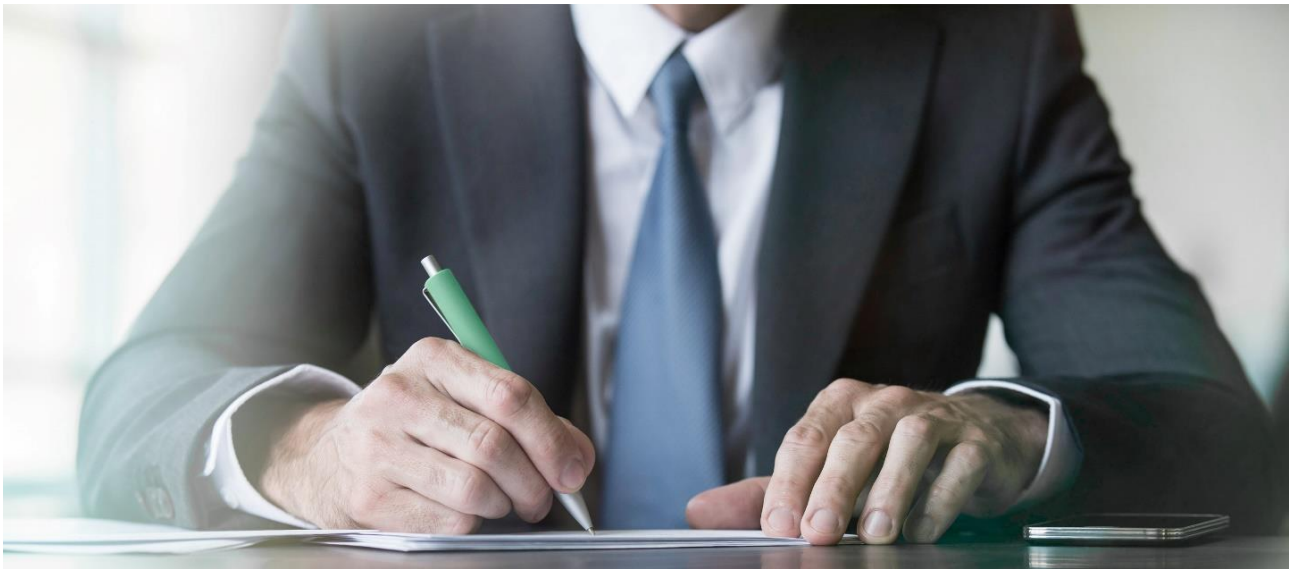
Anmerkung: Die Betrugsmaschen BEC und EAC beinhalten den Fake President-Scam
Quellen: Federal Bureau of Investigation (FBI), LBBW Research

FBI-Statistik als Beispiel für Betrugsfälle und -schäden

23.775 Opfer und 1,7 Mrd. USD Schaden durch den Fake President-Betrug im Jahr 2019

Neben dem Täuschungsdelikt „Fake President“, ist in den letzten Jahren vor allem auch der Besteller- („Fake Identity“) und Zahlungsbetrug („Payment Diversion“) auf dem Vormarsch und macht Unternehmen immer häufiger zu schaffen. Diese drei Täuschungsdelikte haben bei vorwiegend deutschen Unternehmen sowie deren ausländischen Tochtergesellschaften seit 2014 zu Schäden von insgesamt über 190 Mio. EUR geführt. Einen starken Anstieg bei den Fallzahlen gab es 2018 mit +35% im Vergleich zum Vorjahr vor allem beim Bestellerbetrug sowie mit +24% beim Zahlungsbetrug. Dies ergaben Analysen des Kreditversicherers Euler Hermes.

Besteller- („Fake Identity“) und Zahlungsbetrug („Payment Diversion“) auf dem Vormarsch



Infobox: Evolutionsstufen Fake President-Betrug

Evolutionsstufe	Vorgehen
Frühstadium: E-Mail	E-Mail mit z.T. Schreib- und/oder Grammatikfehler, schlecht getarnter Absender, abweichende E-Mail Adresse: Max Mustermann [max@12345.com]
Evolutionsstufe 1: Social Engineering	Korrekte Rechtschreibung, gut getarnte Absender mit z.B. fehlende Buchstaben, Buchstaben- oder Zahlendrehern: Max Mustermann [max.mustermann@musterman.com] Social Engineering – durch Wertschätzung des Mitarbeiters/in und insbesondere durch hohen Druck des falschen externen Anwalts, z.T. müssen die Mitarbeiter alle 1-2 Stunden ihre Vertraulichkeitsvereinbarung erneuern
Evolutionsstufe 2: Gehacktes Intranet	Korrekte, gehackte/gedoppelte Absenderadresse: Max Mustermann [max.mustermann@mustermann.com] Betrüger hacken sich ins Intranet und verweilen dort für einige Tage, spionieren Zuständigkeiten und Gepflogenheiten aus wie z.B. Umgangston, E-Mail Stil (Du/Sie, förmlich/informell), Ansprechpartner Social Engineering durch Interna verbessert – Wissen um interne Informationen schafft Vertrauen
Evolutionsstufe 3: Telefonanruf	Gezieltes Social Engineering: 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	Gezieltes Social Engineering: Kurz nach der E-Mail mit der gefälschten Zahlungsaufforderung ruft ein Fake IT Mitarbeiter in der Buchhaltung an, um dem Mitarbeiter mitzuteilen, dass bei ihm ein Fake President-Versuch 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 aber keine echte Zahlung ausgelöst, weil man mit der Hausbank kooperiere. Der Mitarbeiter überweist – Geld weg.
Evolutionsstufe 5: Stimmimitation	Aktueller Fall mit Stimmimitationssoftware: Software ahmt Sprachmelodie und Akzente nach, so dass der CEO nach dieser telefonischen Bestätigung denkt, die Anweisung per E-Mail käme tatsächlich vom echten Konzern-Chef.
Mögliche zukünftige Evolutionsstufen: Deepfake, Video, Whatsapp	Mit weiterem Fortschritt bei Deepfake-Videos ist diese Technik als nächste Evolutionsstufe denkbar. Aktuell könnten zwar gefälschte Video-Nachrichten per Whatsapp etc. versendet werden, eine „Konversation“ per Video-Fake für Anweisungen des falschen CEO mit eventuellen Rückfragen des Buchhalters ist aktuell noch nicht verbreitet möglich.

Quelle: Euler Hermes

06 I

Die lernende Organisation kann schützen

Home-Office fordert IT- und Cyber-Sicherheit heraus

Um die Beschäftigten vor dem Corona Virus zu schützen haben Unternehmen ihre Mitarbeitenden im Frühjahr – sofern dies möglich war – ins Home-Office geschickt, Team Splitting veranlasst und die Dienstreisetätigkeiten stark beschränkt. Aus einer Notlösung hat sich nun eine Dauerlösung etabliert und es gilt diese neue Arbeitsform für die Zukunft bestmöglich abzusichern. Dies ist für die IT- und Cyber-Sicherheitsstandards einiger Organisationen eine neue Herausforderung. Einhergehend mit der vermehrten Home-Office-Nutzung kann die Häufigkeit von cyber-kriminellen Attacken steigen, denn Internetkriminelle nutzen die mangelnde Vorbereitung der Unternehmen und die Unsicherheiten der Beschäftigten aus und verursachen durch Spam, Phishing, Malware, Identitätsdiebstahl und Datenklau erheblichen Schäden.

Home-Office ist eine Bewährungsprobe für Cyber-Sicherheit

Diesbezüglich müssen nicht nur Unternehmensrichtlinien, Berechtigungskonzepte und Kommunikationswege definiert, sondern auch Prioritäten klar gesetzt werden. Es gilt auch Awareness-Maßnahmen für Mitarbeitende, Absicherungen durch Virtual Private Network (VPN) und Remote Zugriffen (Zwei-Faktor-Authentifizierung) und Regelungen bezüglich Datenverlust und der Nutzung von firmeneigenen Geräten oder BYOD (Bring your own device) anzubieten. Bei der Nutzung von BYOD sollten private Endgeräten über adäquate Antiviren- und Firewall-Software verfügen. Um das Risiko von Schadsoftware zu reduzieren können USB-Laufwerke deaktiviert werden und den Mitarbeitenden stattdessen alternative Datenübertragungsarten angeboten werden. Darüber hinaus soll Vertrauen in die getroffenen Home-Office- und Sicherheitsmaßnahmen geschaffen werden, indem Mitarbeitende bei Unsicherheiten, Bedenken oder Fragen zu Sicherheitsvorkehrung stets einen kompetenten Ansprechpartner erreichen können. Hierfür kann eine Cyber-Security Hotline oder ein Online-Chat mit Sicherheitsexperten eingeführt werden.

Eine IT-Sicherheitskultur kann mehr erreichen als eine Verbotshaltung

Präventionsmaßnahmen gegen Wirtschaftskriminalität treffen

Die am häufigsten ergriffenen Präventionsmaßnahmen gegen Wirtschaftskriminalität sind laut KPMG die Definition von Verhaltensgrundsätzen und Leitbildern sowie die Erfassung und Bewertung besonders schützenswerter Daten bzw. Informationen. Darauf folgt die Integritätsüberprüfung von Geschäftspartnern und/oder Lieferanten, dicht gefolgt von einer sichtbaren Organisationsstruktur mit Compliance-Verantwortung. Des Weiteren gibt es Schulungen zur Vermeidung wirtschaftskrimineller Handlungen und eine regelmäßige Wirksamkeitsprüfung des CMS. Danach kommen die systematische Erfassung und Bewertung von Risiken aus wirtschaftskriminellen Handlungen im Rahmen des Risikomanagements, dem Verbot von privater Nutzung des E-Mail-Systems im Unternehmen, das Einführen von Integritätskriterien als Teil der Zielvereinbarung von Führungskräften und zuletzt die systematische Erfassung von Frühwarnindikatoren (Red Flags).

Verhaltensgrundsätze und Leitbilder definieren

Schulungen anbieten

Schulungen zahlen sich aus

Organisationen, die ihre Mitarbeitenden in den Bereichen Zahlungsbetrug, Kontrollen und Cyber-Betrug schulen, weisen eine geringere Häufigkeit gemeldeter Verluste auf als ihre nicht geschulten Pendants. Darüber hinaus steigen bei ungeschulten Mitarbeitenden die Verluste um den Faktor 1,5 bis 5 je nach Art der Wirtschafts- bzw. Cyber-Kriminalität:

- Faktor 1,5x bei Payment Diversion / Zahlungsbetrug
- Faktor 2x bei Automated Clearing House Betrug (z.B. unter Verwendung von Spear Pishing und Keylogging)
- Faktor 2,5x bei Betrug auf Systemebene (Systemübernahme)
- Faktor 4 bei einem BEC-Betrug (Business Email Compromise und Fake President Betrug) und Bankmandatbetrug
- Faktor 5x bei Malware und Ransomware

Bei ungeschulten Mitarbeitenden können die Verluste bei einem Fake President-Betrug um das 4-Fache steigen

Und auch diejenigen Unternehmen, die über Lösungen für Zahlungsbetrug mit Verbotsfunktionen verfügen, erfahren in der Regel geringere Verluste als Unternehmen ohne solche Systeme. Gerade im Hinblick auf die BEC und Fake President-Betrugsmasche, verzeichnen Unternehmen, die Zahlungsbetrugslösungen nutzen, 75% geringere Verluste als Unternehmen, die nicht über solche Lösungen verfügen. Dies zeigt der Treasury Fraud & Controls Survey Report 2020 von Bottomline und Strategic Treasurer, die mehr als 350 Unternehmensvertreter (darunter CEO/CFO, Cash Manager, Treasurer) befragten.

Fokus auf transparenten Zahlungsverkehr

Neben Schulungen für Beschäftigte im Hinblick auf Cyber-Kriminalität und Risikobewusstsein ist es wichtig interne Prozesse sicher und transparent zu gestalten. Im Hinblick auf den Zahlungsverkehr sollten die Finanzabteilungen im engen Austausch mit IT Abteilungen arbeiten, um ein Treasury System zu entwickeln, das sowohl Zahlungen zentral plant, optimiert und abwickelt als auch Kontosalden und anstehende Zahlungen transparent darlegt. Durch die Implementierung strenger Autorisierungs- und Freigabeprozesse sowie durch die Konfiguration von Benut-

Autorisierungsmechanismen können Sicherheitslücken schließen

zerprofilen, Zeichnungsberechtigungen, Autorisierungsstufen und Zahlungs-Limite kann es möglichen Kriminellen ebenfalls schwergemacht werden. Um die Kontrolle weiter zu steigern könnten ergänzende Überwachungssysteme (beispielsweise Black- und Whitelists von Zahlungsempfängern sowie Limit Monitoring) herangezogen werden. Um Änderungen bei kritischen Daten zu verhindern und Manipulationen sowie Betrugsversuche aufzudecken, können Warnmeldungen durch Anti-Betrugs Software-Systeme generiert werden. Letztendlich sollten zu spezifische Add-on-Sicherheitslösungen vermieden werden, da sie lediglich ein einzelnes Problem lösen und dabei jedoch die Komplexität erhöhen.

Es gilt prinzipiell auf allen Ebenen eine kontinuierliche Verbesserung zu erreichen. Um aus Fehlern zu lernen sollten Cyber-Vorfälle im Unternehmen aufgearbeitet werden. Hierfür kann ein systematischer Fokus auf Feedbackprozesse gelegt werden. Ebenso sollen die Beschäftigten, die Opfer einer Cyber-Attacke geworden sind (z.B. durch das Hereinfallen auf einen Fake President-Betrug), nicht stigmatisiert werden. Stattdessen sollten die Mitarbeitenden, die unter einem Schock stehen, eine psychologische Betreuung und besonderen Schutz erhalten können. Darüber hinaus sollte ein eingetretener Cyber-Vorfall bei Führungskraft und Unternehmensleitung als Chance verstanden werden, um Schwachstellen in Zukunft zu beheben und um Mitarbeitende weiter zu schulen. Andernfalls wird in betroffenen Unternehmen die Bereitschaft der Mitarbeitenden sinken weiterhin elektronische Freigaben zu tätigen, da die Furcht – falsche Zahlungen zu veranlassen – dominieren könnte. Somit wird aus einer Kompetenz, die zunächst erstmal alle haben wollen, durchaus eine erdrückende Last.

Feedback- und Verbesserungskultur pflegen

Infobox: Cyber-Attacken abwehren

Beim **Social Engineering** bauen Betrüger eine Vertrauensbeziehung auf und erbeuten dadurch vertrauliche Informationen, Zahlungsdaten und Passwörter. Was können Sie in einem Verdachtsfall tun? Folgende Punkte geben eine exemplarische Hilfestellung:

- Beenden eines verdächtigen Anrufs: Bei Zweifel an der Echtheit einer Kontaktperson kann das Gespräch abgebrochen werden.
- Echtheit des Anrufers überprüfen: Recherchieren Sie das vermeintliche Unternehmen, rufen Sie dort an und lassen sich zum verdächtigen Anrufer durchstellen (Vorsicht vor gefälschten Unternehmenswebseiten).
- Keine Preisgabe von Informationen: Geben Sie keine Informationen via E-Mail / Telefonat an Personen, die Sie nicht ausreichend überprüft haben (auch nicht an Manager oder IT-Administratoren).
- Informieren Sie den unternehmensinternen IT-Help- oder Service-Desk: Im Verdachtsfalle wenden Sie sich an die Informationssicherheit Ihres Unternehmens und melden den Sicherheitsvorfall.

Hacker versuchen beim **Pishing** an sensible Informationen zu gelangen oder permanenten Zugriff auf IT-Systeme zu erhalten. Oft beginnt alles mit einer E-Mail, die allem Anschein nach von einem vermeintlich vertrauenswürdigen Absender versendet wurde. Durch das Öffnen eines Links oder Anhangs in dieser Pishing E-Mail kann die Unternehmens-IT

Viele einzelne Sicherheitsmaßnahme machen es Cyber-Kriminellen schwer

mit Schadsoftware infiziert werden (die teilweise von Anti-Viren-Software nicht erkannt wird). Was können Sie in einem Verdachtsfall tun? Folgende Punkte können helfen:

- Absender der E-Mail überprüfen: Überprüfen Sie den E-Mail Absender und ob dieser in irgendeiner Weise verdächtig ist. Kennen Sie den vermeintlichen Absender, so können Sie Ihn anrufen und Nachfragen, ob die E-Mail tatsächlich von ihm stammt.
- Kommunikationsstil überprüfen: Werden Sie in der E-Mail mit einer persönlichen (mit Ihrem Namen) oder einer allgemeinen Begrüßung / Anrede angesprochen?
- Dringlichkeit überprüfen: Pishing E-Mails vermitteln oftmals das Gefühl der Dringlichkeit (Öffnen eines Links / Anhangs soll schnellstmöglich geschehen). Öffnen Sie daher solche Links / Anhänge nie, wenn Ihnen die E-Mail verdächtig erscheint. Wenden Sie sich an Ihren IT-Help-Desk und / oder leiten Sie die E-Mail an Ihre IT-Sicherheitsabteilung weiter.

Neben dem Social Engineering und Pishing können einfache und kurze Leitfäden oder Regelwerke für Passwörter (Länge, Sonderzeichen, Groß- und Kleinbuchstaben, kein Wort aus dem Wörterbuch), Umgang mit sensible Information (Klassifizierung von Informationen z.B. öffentlich, nur für den Dienstgebrauch, vertraulich, geheim), Datenaustausch (USB, Cloud), Dienstreise (IT-Geräte Verlust, Firmenfremde Geräte), Arbeitsplatz (Büro oder Home-Office, Clean-Desk Policy, Sperren des PC, Vertraulicher Druck) entwickelt werden.

Cyber-Security Investitionen sollten folgen

Nicht nur bei der Sensibilisierung und Schulung der Mitarbeiter kann und wird es für Unternehmen Nachholbedarf geben, sondern auch bei den Investitionen in Cyber-Security. Gerade die Budgets für IT- und Cyber-Sicherheit stehen im Wettbewerb um die knappen finanziellen Ressourcen eines Unternehmens. Die Konkurrenz um Budgets dürfte bei mittelständischen Unternehmen noch viel ausgeprägter als bei Großunternehmen sein, da die finanziellen Kapazitäten im Mittelstand begrenzter sein dürften. Als Größenordnung für das Cyber-Budget zeigt die Praxiserfahrung, dass ca. zwischen 5% und 20% der IT-Kosten realistisch sind. Die Kosten für Cyber-Security betragen zwischen 0,05% bis 0,2% des Umsatzes (Cyber-Sicherheit Kosten machen ca. 10% der IT-Kosten aus).

Cyber-Security ist ein Kostenfaktor aber auch lebensnotwendig

Beispiel für die Kosten von Cyber-Sicherheit

Umsatz (in Mio. EUR)	Basis	IT-Kosten (in Mio. EUR)	Anteil der IT-Kosten am Umsatz	Cyber-Sicherheit Kosten (in Mio. EUR)	Anteil der Kosten für Cyber-Sicherheit an IT-Kosten	Anteil der Kosten für Cyber-Sicherheit am Umsatz
100	100%	0,5	0,5%	0,05	10%	0,05%
100	100%	1,0	1,0%	0,10	10%	0,10%
100	100%	2,0	2,0%	0,20	10%	0,20%

Quelle: LBBW Research

Das Wirtschaftsprüfungs- und Beratungsunternehmen Deloitte überträgt den Anteil der Kosten für Cyber-Sicherheit auf die Stichprobe ihrer Studie „Cyber Security im Mittelstand“ vom Juni 2020. Die mittelständischen Unternehmen (Umsatzgröße von etwa 50 Mio. EUR und Beschäftigtenzahl ab 300 Personen) in der Stichprobe haben einen Umsatz-Mittelwert von 387 Mio. EUR. Demnach müssten Mittelständler pro Jahr zwischen 193.500 EUR und 774.000 EUR für Cyber-Security ausgeben

Rund 200.000 EUR für Cyber-Security im Jahr ausgeben

Kosten von Cyber-Sicherheit bei mittelständischen Unternehmen

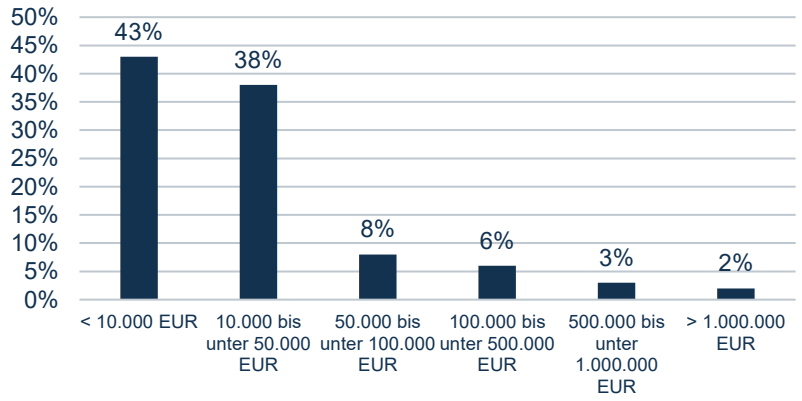
Umsatz (in Mio. EUR)	Basis	IT-Kosten (in Mio. EUR)	Anteil der IT-Kosten am Umsatz	Cyber-Sicherheit Kosten (in Mio. EUR)	Anteil der Kosten für Cyber-Sicherheit an IT-Kosten	Anteil der Kosten für Cyber-Sicherheit am Umsatz
387	100%	1,9	0,5%	**0,1935**	10%	0,05%
387	100%	3,9	1,0%	**0,3870**	10%	0,10%
387	100%	7,7	2,0%	**0,7740**	10%	0,20%

Quelle: Deloitte, LBBW Research

Diese Mittelwertbetrachtung stellt schon fast ein Idealbild dar. Die Studie zeigt nämlich, dass kumuliert 89% der Unternehmen diese Anforderung nicht erfüllen, da sie unter 100.000 EUR für Cyber-Security ausgeben. Nur 11% der befragten Unternehmen geben über 100.000 EUR pro Jahr für Cyber-Security aus.

Lediglich 11% der Unternehmen geben über 100.000 EUR pro Jahr für Cyber-Security aus

Jährliche Ausgaben für Cyber-Security



n=353
Quelle: Deloitte, LBBW Research

Budgets für Cyber-Sicherheit sollte aufgestockt werden

07 I

Fazit: Cyber-Security ist nichts für Passive

Cyber-Resilienz entwickeln

Das Voranschreiten der Digitalisierung führt dazu, dass Cyber-Security keine isolierte Aufgabe einer einzelnen Gruppe, Abteilung, Geschäftseinheit oder Institution mehr ist. Bei einem Großteil aller Cyber-Vorfälle und Datenschutzverletzungen spielt der Faktor Mensch eine Kernrolle. Daher ist es sehr empfehlenswert, wenn Organisationen regelmäßige Trainings und Schulungen hinsichtlich Cyber-Awareness für ihre Belegschaft durchführen. Es bedarf letztendlich einem Prozess der kulturellen Veränderung, in der sich jeder Mitarbeitende als Teil der Verbesserung von Cyber-Security sieht.
Allerdings bieten aber alle Sicherheitskonzepte, -systeme und -maßnahmen sowie Informationssicherheitsschulungen niemals einen absoluten Schutz vor Cyber-Kriminalität. Allerdings erhöhen die Unternehmen damit ihre Widerstandsfähigkeit und verringern das Risiko von Cyber-Kriminalität.

Kein absoluter Schutz vor Cyber-Kriminalität möglich

Es geht darum eine sogenannte Cyber-Resilienz aufzubauen und zu nutzen. Resilienz beschreibt auf psychologischer Ebenen die Widerstandsfähigkeit von Menschen gegen negative Einflüsse. Mit Cyber-Resilienz ist die Agilität und Schnelligkeit sowohl der Abwehr- als auch der Wiederherstellungskapazitäten gemeint, also die Fähigkeit einer Organisation, sich auf schadhafte Cyber-Vorfälle einzustellen und diesen entgegenzuwirken – und das nicht reaktiv, sondern proaktiv. Unabhängig davon, ob Cyber-Vorfälle von Mitarbeitenden oder Fremden mutwillig oder unabsichtlich ausgelöst wurden, erfasst der Resilienz-Grad die Aufrechterhaltung von Vertraulichkeit, Integrität, Verfügbarkeit und Wiederherstellung der Daten und Dienste, die für das Unternehmen wichtig sind.

Cyber-Resilienz aufbauen und nutzen

Cyber-Resilienz ist proaktiv, nicht nur reaktiv

Beim Aufbau von Cyber-Resilienz Fähigkeiten sollten unbedingt die potenziell unterschiedlichen Ansichten von Interessengruppen wie dem Chief Financial Officer, dem Chief Operating Officer, dem Chief Information Officer, dem Chief Technology Officer und anderen Führungskräften (die sich auf Sicherheit, Datenschutz und Risiko konzentrieren), berücksichtigt werden. Entscheider sollten sich hierbei auf die vier Dimensionen der Cyber-Resilienz Bedrohungsschutz (Threat Protection), Anpassungsfähigkeit (Adaptability), Beständigkeit (Durability) und die Fähigkeit zur Wiederherstellung (Recoverbility) fokussieren.

Die Ansichten der C-Suite sind gefragt

Letztendlich ist die proaktive Widerstandsfähigkeit ein Resultat aus der Verzahnung von Unternehmenskultur, strategischer Führungsebene, Informationssicherheit, Risiko- und Notfallmanagement, Desaster Recovery, Business Continuity und weiteren Prozessen.

Unternehmen sind bis dato auf einem guten Weg ihre Cyber-Resilienz auszubauen. So bewerten 53% der befragten Unternehmen die Cyber-Resilienz ihrer Organisation als hoch („hoch“ entspricht einem Wert von

7 und höher, auf einer Skala von 1 = geringe Widerstandsfähigkeit bis 10 = hohe Widerstandsfähigkeit). Im Jahr 2015 waren es lediglich 25% der Unternehmen. Dies zeigt der aktuelle Cyber Resilient Organization Report von IBM Security in Kooperation mit dem Ponemon Institute, der die Antworten von 3.439 IT- und Sicherheitsexperten aus 17 Länder und 18 Branchen zusammenfasst.

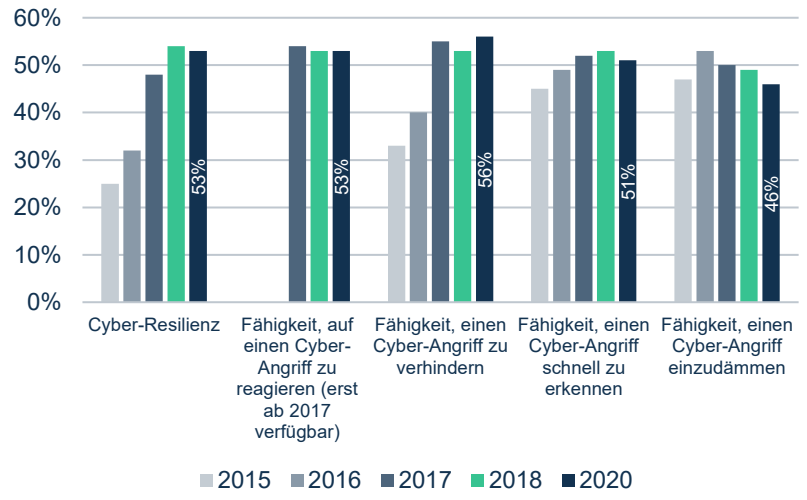
In der Studie ist Cyber-Resilienz definiert als eine Zusammenführung der Präventions-, Erkennungs- und Reaktionsfähigkeiten, um Cyber-Angriffe zu bewältigen, abzuschwächen und zu überwinden. Im Hinblick auf die Prävention, schätzen 56% der Unternehmen ihre Fähigkeit einen Cyber-Angriff zu verhindern, als hoch ein. Die Fähigkeit, Cyber-Angriffe zu erkennen und einzudämmen, wird von 51% bzw. 46% der Befragten ebenfalls hoch eingeschätzt. Die Mehrheit der Befragten (53%) gibt ebenfalls eine hohe Widerstandsfähigkeit an, wenn es um das Reagieren auf einen Cyber-Angriff geht.

Die Cyber-Resilienz von Unternehmen hat sich weltweit im Großen und Ganzen gut entwickelt. Obwohl die Fortschritte nicht zu verkennen sind, dürften Unternehmen, auch in Deutschland, in Zukunft weiterhin an ihrer Widerstandsfähigkeit arbeiten, da die Cyber-Bedrohungen tendenziell nicht weniger werden.

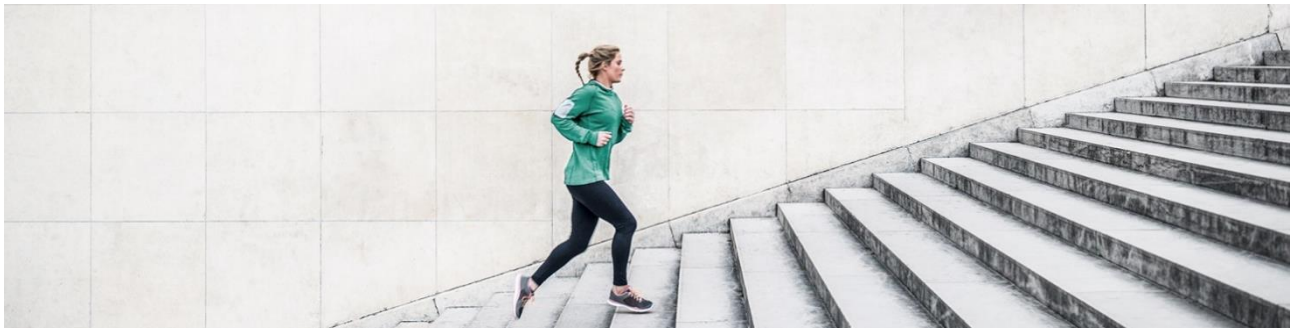
Die Hälfte der Unternehmen schätzt ihre Cyber-Resilienz als relativ hoch ein…

…für die andere Hälfte besteht noch Ausbaupotential

Cyber-Resilienz von Unternehmen



Anteil der Unternehmen, die ihre Cyber-Resilienz als hoch einschätzen („hoch“ entspricht einem Wert von 7 und höher, auf einer Skala von 1 = geringe Widerstandsfähigkeit bis 10 = hohe Widerstandsfähigkeit)
Quellen: IBM Security, Ponemon Institute, LBBW Research



Ansprechpartner Produktlösungen

Corporate Finance Origination
Anleihen, Schuldscheine, Syndizierte Kredite, Eigenkapitalmaßnahmen
+49 711 127-78746

Corporate Finance Spezial
ABS, Akquisitionsfinanzierung
+49 711 127-49379

Zahlungsverkehrslösungen
SEPA, AZV, Cash-Management, Karten, Konten, E-Commerce
+49 711 127-46565

International Business
Trade and Export Finance, Internationales Netzwerk
+49 6131 64-35830

ZWRM
Zins-, Währungs-, Rohstoffmanagement
+49 711 127-75677

SüdLeasing
Mobilienleasing, Vendorleasing, Fördermittel, Mietkauf
+49 711 127-15152

SüdFactoring
Forderungsankauf, Finanzierung, Debitorenmanagement
+49 711 127-78953

Sustainability Advisory
Green Finance, ESG verknüpfte Finanzierungen
+49 711 127-49610

Disclaimer

Diese Publikation richtet sich ausschließlich an Empfänger in der EU, Schweiz und in Liechtenstein.
Diese Publikation wird von der LBBW nicht an Personen in den USA vertrieben und die LBBW beabsichtigt nicht, Personen in den USA anzusprechen.

Aufsichtsbehörden der LBBW: Europäische Zentralbank (EZB), Sonnemannstraße 22, 60314 Frankfurt am Main und Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Graurheindorfer Str. 108, 53117 Bonn / Marie-Curie-Str. 24-28, 60439 Frankfurt.

Diese Publikation beruht auf von uns nicht überprüfbaren, allgemein zugänglichen Quellen, die wir für zuverlässig halten, für deren Richtigkeit und Vollständigkeit wir jedoch keine Gewähr übernehmen können. Sie gibt unsere unverbindliche Auffassung über den Markt und die Produkte zum Zeitpunkt des Redaktionsschlusses wieder, ungeachtet etwaiger Eigenbestände in diesen Produkten. Diese Publikation ersetzt nicht die persönliche Beratung. Sie dient nur Informationszwecken und gilt nicht als Angebot oder Aufforderung zum Kauf oder Verkauf. Für weitere zeitnähere Informationen über konkrete Anlagemöglichkeiten und zum Zwecke einer individuellen Anlageberatung wenden Sie sich bitte an Ihren Anlageberater.

Wir behalten uns vor, unsere hier geäußerte Meinung jederzeit und ohne Vorankündigung zu ändern. Wir behalten uns des Weiteren vor, ohne weitere Vorankündigung Aktualisierungen dieser Information nicht vorzunehmen oder völlig einzustellen.

Die in dieser Ausarbeitung abgebildeten oder beschriebenen früheren Wertentwicklungen, Simulationen oder Prognosen stellen keinen verlässlichen Indikator für die künftige Wertentwicklung dar.

Die Entgegennahme von Research Dienstleistungen durch ein Wertpapierdienstleistungsunternehmen kann aufsichtsrechtlich als Zuwendung qualifiziert werden. In diesen Fällen geht die LBBW davon aus, dass die Zuwendung dazu bestimmt ist, die Qualität der jeweiligen Dienstleistung für den Kunden des Zuwendungsempfängers zu verbessern.

Redaktion:
Landesbank Baden-Württemberg
Strategy Research
Am Hauptbahnhof 2
70173 Stuttgart