WIE SICH UNTERNEHMEN EFFEKTIV SCHÜTZEN KÖNNEN

CYBERSICHERHEIT IM MITTELSTAND

Unternehmen werden immer häufiger Opfer von Cyberattacken. Wie gut sind sie auf den Ernstfall vorbereitet? Können die neuen Möglichkeiten der KI-Technologie den Schutz verbessern? Und was können Cyberversicherungen leisten?

IMPRESSUM

Whitepaper:
Cybersicherheit

Veröffentlicht: Dezember 2023

Herausgeber:
Deutscher Sparkassen- und Giroverband e.V.
Charlottenstrasse 47
10117 Berlin Deutschland
V.i.S.d.P.: Christian Achilles,
Leiter Kommunikation

Redaktionelle Umsetzung:
Fazit Communication GmbH
Pariser Straße 1, 60486 Frankfurt am Main

Geschäftsführung:
Hannes Ludwig, Jonas Grashey

Redaktion: Benjamin Kleemann-von Gersum, Harald Czycholl, Hans-Joachim Hoffmann

Art Direction:
Anabell Krebs

Wie stark werden Unternehmen aktuell durch Cyberangriffe bedroht?

Die Bedrohung im Cyberraum ist so hoch wie nie zuvor.
Die Bedrohung durch Cyberkriminelle ist in Deutschland deutlich gestiegen. Zu diesem Ergebnis kommt das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem jüngsten Lagebericht. „Insgesamt zeigte sich im aktuellen Berichtszeitraum eine angespannte bis kritische Lage“, bilanziert die Behörde. So seien täglich durchschnittlich 68 neue Schwachstellen in Softwareprodukten registriert worden – ein Plus von rund 24 Prozent im Vorjahresvergleich.

Ransomware stellt eine der größten Cyberbedrohungen für den Mittelstand dar.
Kriminelle Hacker würden dabei zunehmend den Weg des geringsten Widerstands wählen und vermehrt Opfer auswählen, die ihnen leicht angreifbar erscheinen, heißt es beim BSI. Zunehmend würden kleine und mittlere Unternehmen, Kommunalverwaltungen sowie Schulen und Hochschulen Opfer sogenannter Ransomware-Attacken. Von Ransomware spricht man, wenn Angreifer mangelhafte Datensicherung oder Fehler von Mitarbeitenden ausnutzen, um Systeme zu infiltrieren und Daten zu verschlüsseln. Für die Entschlüsselung verlangen die Erpresser dann Lösegeld.

Wie gut schützen sich deutsche Unternehmen gegen Cyberattacken?
Trotz der enormen Risiken sind jedoch viele Unternehmen hierzulande immer noch unzureichend auf Cyberattacken vorbereitet, zeigt eine aktuelle Umfrage des Digitalverbands Bitkom. Demnach verfügt nur jeder zweite Betrieb hierzulande über einen Notfallplan mit schriftlich geregelten Abläufen und Ad-hoc-Maßnahmen für den Fall von Datendiebstahl, Spionage oder Sabotage – und haben auch die Belegschaft nur unzureichend sensibilisiert. Dabei sind die Mitarbeiter die erste Abwehrreihe gegen Cyberkriminelle – und sollten deshalb über Risiken und Angriffsarten Bescheid wissen, so der Appell des Bitkom.

3 Beispiele von Cyberangriffen der jüngsten Vergangenheit:

Motel One:
Immenser Imageschaden

Anfang Oktober 2023 wurde bekannt, dass Hacker in das IT-System der Hotelkette Motel One eingedrungen waren und dabei Adressdaten und auch Kreditkarteninformationen von Kunden gestohlen hatten. Die Hackergruppe ALPHV bekannte sich zu der Attacke, mit der offenbar Geld erpresst werden sollte. Als Motel One die Lösegeldzahlung verweigerte, wurden die erbeuteten Daten im Darknet veröffentlicht. Vor allem der Imageschaden für Motel One ist immens. Denn wer ein Hotelzimmer bezieht, will sich schließlich sicher fühlen – und auch seine persönlichen Daten in guten Händen wissen.

Bauer AG:
Kurzarbeit nach Cyberattacke

Ende Oktober wurde der bayrische Tiefbauspezialist Bauer AG Opfer eines Cyberangriffs. In der Folge waren verschiedene Systeme vorsorglich abgeschaltet worden. Es kam weltweit zu Einschränkungen für die Geschäftspartner. Zwar konnten die Geschäfte in vielen Bereichen nach einigen Tagen weiterlaufen, weil wieder auf manuelle Verfahren umgestellt worden war. Einige Bereiche wie etwa die Maschinenproduktion waren jedoch weiterhin stark eingeschränkt. Der Vorstand appellierte an die Mitarbeiter, Überstunden abzubauen oder Urlaub vorzuziehen – und kündigte für einige Bereiche Kurzarbeit an.

Südwestfalen IT:
Kommunen nach Hackerangriff offline

Kein Passantrag, keine Geburtsurkunde: Nach einem Hackerangriff auf den IT-Dienstleister Südwestfalen IT Ende Oktober ging in den Bürgerzentren von über 100 Kommunen in Nordrhein-Westfalen für mehrere Wochen gar nichts mehr. Das Unternehmen war Opfer einer Ransomware-Attacke geworden. Um eine Weiterverbreitung der Schadsoftware zu unterbinden, wurde die Verbindung zu den Nutzern gekappt. Wochenlang waren die Kommunen, die die Software des IT-Dienstleisters nutzten, offline. Erst im Dezember konnte das Unternehmen wieder einen Notbetrieb gewährleisten, „um Kommunen und Kreise wieder handlungsfähig zu machen“.

Exkurs: Künstliche Intelligenz – Risiko oder Chance?

KI-Technologien als neue Herausforderung für die Cybersicherheit
Nach jüngst erhobenen Umfrageergebnissen des IT-Branchenverbands Bitkom fürchten 57 Prozent der befragten Unternehmen eher die Gefahren durch Künstliche Intelligenz (KI). Nur ein gutes Drittel hingegen erwartet eine verbesserte IT-Sicherheit durch KI. Sicher ist nur, dass KI Potenzial für beides hat

KI lässt sich als Waffe für Cyberangriffe verwenden
Künstliche Intelligenz kann Bilder, Videos und Stimmen manipulieren und damit sogenannte Deepfakes erstellen. Darüber hinaus sind KI-Anwendungen in der Lage, Phishing-Mails ohne auffällige Schreibfehler zu produzieren. Selbst Schadcode kann KI selbständig programmieren oder Desinformationen in den sozialen Medien streuen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) befürchtet daher, dass KI das Problem der Cyberkriminalität weiter verschärfen wird.

KI als mögliches Einfallstor für Cyberkriminelle
Die in Unternehmen eingesetzten KI-Lösungen können zudem gehackt und missbraucht werden: So warnt das BSI, dass es möglich sei, die KI durch einem Dialog dazu zu bringen, schädliche Aktionen auszuführen oder eigentlich geschützte Daten herauszugeben. Erschwert wird der Schutz vor solchen Prompt Injections durch den Black-Box-Charakter von KI-Sprachmodellen.

Wie kann KI-Technologie die Resilienz gegen Cyberangriffe erhöhen?

Muster erkennen: Beim Analysieren von großen Datenmengen hat KI bekanntlich gegenüber Menschen die Nase uneinholbar vorn, sie ist daher in der Lage, digitale Verhaltensmuster in Echtzeit zu analysieren. Anhand dieser Verhaltensmuster kann sie die Identität von Nutzern verifizieren, aber auch bei Anomalien wie ungewöhnlichen Aktivitäten Alarm schlagen.

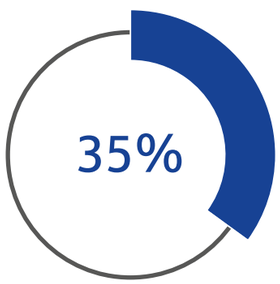
Zeit sparen: Durch ihre Schnelligkeit bei der massenhaften Datenanalyse kann Ki Vorfälle viel besser als der Mensch priorisieren: Was ist wichtig, was weniger? Bei einer IBM-Umfrage unter IT-Sicherheitsexperten kam heraus, dass diese es an einem durchschnittlichen Werktag aus Zeitgründen nicht einmal schaffen, die Hälfte der täglichen Alarmmeldungen abzuarbeiten. Ein Drittel der Zeit gehe für „falsch positive“ Bedrohungen verloren oder für Vorfälle mit geringer Priorität.

Ständig lernen: Ein weiterer exklusiven Vorteil von KI gegenüber herkömmlicher Software: KI-basierte Sicherheitstechnologien sind selbstlernend, sie schauen sich den normalen Betrieb – in diesem Fall Datenverkehr – an und können in kürzester Zeit Abweichungen erkennen, ohne dass sie von menschlicher Seite darauf hingewiesen werden müssen. Das heißt: Die Lernkurve wird von selbst immer steiler, ohne dass es menschlicher Unterstützung bedarf.

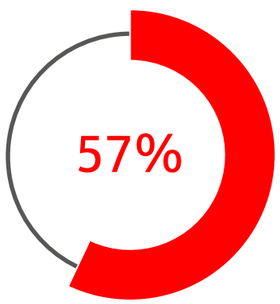
Routine reduzieren: Eine weitere Möglichkeit des Einsatzes von KI in der Cybersicherheit ist die Automatisierung von Routineaufgaben, um sie weniger zeitaufwändig zu machen. So können KI-Anwendungen beispielsweise dazu verwendet werden, Systeme automatisch zu patchen und zu aktualisieren, so dass sich die Cybersicherheitsexperten auf komplexere Aufgaben konzentrieren können.

Effizienz steigern: Die potenziellen Vorteile von KI-Technologien für die Cybersicherheit sind erheblich. Durch eine schnellere und präzisere Erkennung von Bedrohungen und die Reaktion darauf kann KI dazu beitragen, die Auswirkungen von Cyberangriffen zu verringern. KI kann auch dabei unterstützen, die Effizienz von Cybersicherheitsmaßnahmen zu verbessern, wodurch wertvolle Zeit und Ressourcen für andere Aufgaben frei werden.

Wie schätzen Unternehmen den Einfluss von KI auf die Cybersicherheit ein?

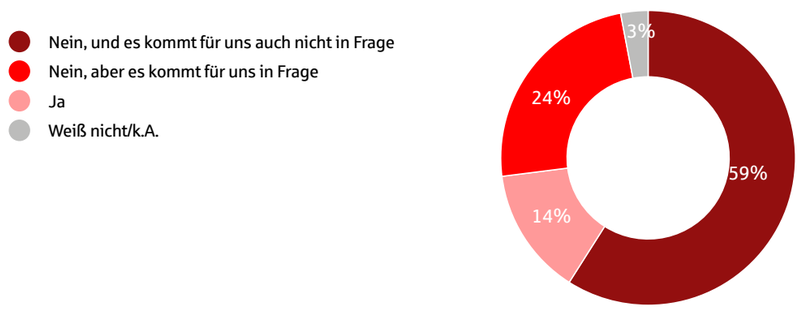


Die Verarbeitung von generativer KI wird die IT-Sicherheit verbessern, weil sie bei der Abwehr von Cyberangriffen genutzt werden kann.



Die Verarbeitung von generativer KI wird die IT-Sicherheit gefährden, weil sie von Cyberangreifern genutzt werden kann.

Haben Sie sich in Ihrem Unternehmen bereits mit dem Einsatz von KI zur Verbesserung der IT-Sicherheit beschäftigt?



Quelle: Bitkom Research 2023

1/2

aller Betriebe wurde innerhalb eines Jahres mit Ransomware attackiert.

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI) 2023

148 MRD. EURO

betragen die Schäden durch Cyberangriffe für die deutsche Wirtschaft 2023.

Quelle: Bitcom 2023

38 MRD. EURO

wird der Umsatz für Cybersecurity in Europa 2023 erreichen.

Quelle: Statista 2023

54 %

der Unternehmen sehen sich durch Cyberattacken in ihrer Existenz bedroht.

Quelle: Bitcom 2023

21.000

infizierte Systeme identifizierte das BSI innerhalb von zwölf Monaten täglich.

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI) 2023

4,45 MIO. USD

betrugen die durchschnittlichen Kosten einer Datenschutzverletzung 2023 weltweit.

Quelle: IBM

11 %

der Unternehmen in Deutschland, die Opfer von Ransomware wurden, haben daraufhin Lösegeld bezahlt.

Quelle: Bitcom Research 2023

68

neue Schwachstellen in Softwareprodukten täglich hat das BSI im Schnitt innerhalb von zwölf Monaten registriert.

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI) 2023

Wie Unternehmen den Schutz der eigenen Daten verbessern

Eine Checkliste für den Mittelstand

Der erste Schritt für die Planung von technischen Maßnahmen für den Schutz vor Cyberangriffen besteht darin, genau zu analysieren, was die IT-Infrastruktur deines Unternehmens umfasst. Auch der Webshop, die Website und Produktionsmaschinen sollten dabei miteinbezogen werden. Ein Überblick über alle Geräte und Systeme sowie deren Anforderungen an die Wartung ist wichtig. Hierfür eignet sich auch eine IT-Infrastrukturkarte.

Eine regelmäßige und vor allem zeitnahe Installation von Updates der im Unternehmen eingesetzten Software, des Betriebssystems und natürlich des Antivirusprogramms und der Firewall sollten selbstverständlich sein. Denn eine veraltete Software ist ein beliebtes Eingangstor für Schadsoftware. Stellen Sie sicher, dass sämliche Computer und Server in Ihrem Unternehmensnetzwerk die Sicherheitsupdates automatisch einspielen.

Eine wichtige Grundmaßnahme zum Schutz vor Cyberangriffen besteht darin, zudem darin die Mitarbeiter in puncto Daten- und IT-Sicherheit zu schulen. Hier lässt sich eine große Gefahr schnell eindämmen, denn die meisten Hackerangriffe finden immer noch per E-Mail statt. Auch das Wissen über die Anwendung der anfälligen ERP-Systeme (Enterprise Resource Planning) sollte immer auf dem aktuellen Stand sein und regelmäßig aufgefrischt werden.

Hat sich ein Unternehmen trotz Prävention einen Verschlüsselungstrojaner eingefangen, kann Schlimmeres durch eine umfassende Backup-Strategie verhindert werden. Dazu gehören zum Beispiel gespiegelte, sich gegenseitig überwachende Serversysteme und tägliche Sicherungen, die offline – also außerhalb der Zugriffsmöglichkeit von Ransomware – aufbewahrt werden.

Einen 100-prozentigen Schutz vor Cyberangriffen gibt es nicht. Bereiten Sie sich mit einem Notfallkonzept auf den Ernstfall einer Cyberattacke vor. Zu den wesentlichen Inhalten gehören technische Anweisungen, Verantwortlichkeiten, Alarmierungsketten, Maßnahmenlisten sowie die nötigen Kontaktinformationen.

3 Fragen an …

Elisa Beyer
Hauptabteilungsleiterin Cyberversicherung,
Provinzial Versicherung AG

Wann ist eine Cyberversicherung für einen Mittelständler sinnvoll?

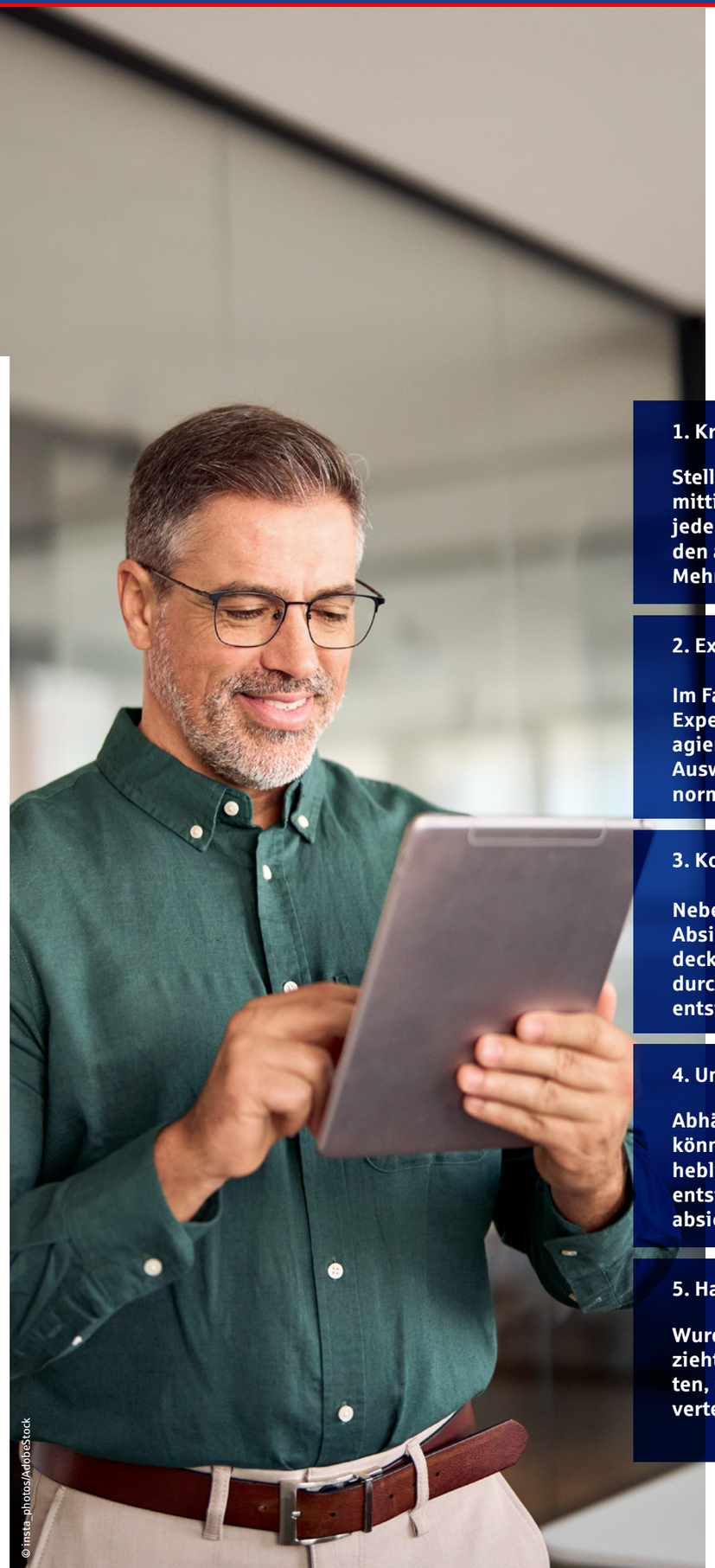
Stellen Sie sich vor, Sie haben keinen Zugriff mehr auf Ihre elektronischen Daten oder sensible Daten Ihrer Kunden würden veröffentlicht. Welche Auswirkungen hätte dies auf Ihr Geschäft? Könnten Sie Ihre Kunden noch bedienen? Wüssten Sie, an wen Sie sich wenden müssen, um das Problem zu beheben? Eine Cyberversicherung ist immer dann sinnvoll, wenn Sie – und sei es nur teilweise – digital arbeiten. Wir empfehlen die Prozessschritte im eigenen Unternehmen zu bewerten und genau zu hinterfragen, was in den Szenarien eines Datenverlustes für finanzielle und rechtliche Konsequenzen drohen.

Welche Arten von Cyberrisiken lassen sich versichern, welche nicht?

Cyberrisiken liegen in der Störung der Vertraulichkeit, Verfügbarkeit oder Integrität von Daten und Systemen. Folgt auf eine Nichtverfügbarkeit von Daten und Systemen ein Ertragsausfall, kann dieser durch eine Cyberversicherung abgedeckt werden. Häufig ist die Veröffentlichung von sensiblen Daten mit Konsequenzen im Datenschutzrecht verbunden. Auch damit verbundene Kosten lassen sich versichern. Ein Reputationsverlust kann jedoch nicht mitversichert werden. Daher gilt es mit Hilfe des Expertennetzwerks Ihres Cyberversicherers einen Angriff so schnell und professionell wie möglich mit positiver Außenwirkung zu managen.

Worauf sollten Firmen beim Abschluss einer Cyberversicherung achten?

Eine Cyberversicherung ersetzt nicht, sich mit seiner eigenen IT-Sicherheit auseinanderzusetzen. Vielmehr fordern Cyberversicherer bestimmte Grundvoraussetzungen, damit überhaupt Versicherungsschutz angeboten werden kann. Es ist daher hilfreich sich intensiv mit den Risikofragen auseinanderzusetzen. Daneben gilt es genau zu prüfen, ob der angebotene Versicherungsschutz zum eigenen Unternehmen passt. Die meisten Cyberversicherungen sind modular aufgebaut, sodass man den Versicherungsschutz genau auf die Bedürfnisse des eigenen Unternehmens zuschneiden kann.



Absicherung für den Ernstfall: Cyberversicherungen

Was können Cyberversicherungen leisten? Ein Überblick.

1. Krisenhotline

Stellt ein Unternehmen fest, dass die eigenen Systeme kompromittiert wurden, spielt der Faktor Zeit eine wichtige Rolle. Denn jede Minute gibt dem Angreifer die Möglichkeit, größeren Schaden anzurichten. Eine Krisenhotline stellt dann einen großen Mehrwert dar.

2. Experten im Notfall

Im Falle eines Cyberangriffs können Versicherer ein Team aus Experten vermitteln, das in der Lage ist angemessen zu reagieren. Es identifiziert die Ursache eines Vorfalls, schätzt die Auswirkungen ab und erarbeitet mögliche Reaktionen, um den normalen Betrieb wiederherzustellen.

3. Kostenabsicherung

Neben der unmittelbaren Hilfe in der Krisensituation ist eine Absicherung gegen die anfallenden Kosten notwendig. Generell deckt eine Cyberversicherung Eigen- und Drittschäden ab, die durch Cyberkriminalität oder technische und menschliche Fehler entstehen.

4. Umsatzeinbußen

Abhängig vom Geschäftsmodell des betroffenen Unternehmens können bis zur Wiederherstellung des Normalzustandes erhebliche Umsatzeinbußen durch die Betriebsunterbrechungen entstehen. Auch diese lassen sich durch eine Cyberversicherung absichern.

5. Haftpflichtansprüche

Wurden bei dem Cyberangriff sensible Kundendaten gestohlen zieht dies meist Haftpflichtansprüche nach sich. Auch die Kosten, um sich im Zweifelsfall juristisch gegen Forderungen Dritter verteidigen zu können, sollte eine Cyberversicherung abdecken.

In einer gemeinsamen Initiative erörtern Sparkasse und Frankfurter Allgemeine Konferenzen neue Perspektiven auf den geopolitischen Wandel und zeigen Handlungsoptionen für die deutsche Wirtschaft auf. Für weitere Informationen besuchen Sie **sparkasse.de/nachhaltiges-management** oder **faz.net/asv-perspektiven**

Veröffentlicht: Dezember 2023

Sparkasse