Cybersicherheit für den Mittelstand

Was Sie als Unternehmen über Cybersicherheit im Jahr 2022 wissen sollten.

perseus.
Cybersicherheit auf den Punkt

Cyberkriminalität: eines der größten Geschäftsrisiken weltweit

„Die Vorteile der Digitalisierung spielen eine zentrale Rolle und sind heutzutage ebenso ein entscheidender Faktor für den Erfolg sowie die Zukunftssicherheit von Unternehmen, unabhängig von Größe und Branche. Das Internet kann mithin als das leistungsfähigste Werkzeug der modernen Welt angesehen werden. Doch mit den wachsenden Möglichkeiten, steigen auch die Gefahren. Perseus hat sich der digitalen Sicherheit des deutschen Mittelstandes verschrieben. Mit diesem Whitepaper für Cybersicherheit in kleinen und mittleren Unternehmen möchten wir Sie und Ihren Betrieb bei den ersten Schritten in eine cybersichere Zukunft unterstützen. Perseus zeigt Ihnen, welche Bedrohungen lauern und wie Sie sich effektiv und kosteneffizient vor diesen schützen."

Kevin Püster, Geschäftsführer Perseus Technologies GmbH

Das erwartet Sie

Bevor wir Ihnen Maßnahmen und Handlungsempfehlungen mit auf den Weg geben, mit denen Sie Ihr Unternehmen cybersicher gestalten, erhalten Sie einen Überblick über das tatsächliche Ausmaß der Gefahren. Damit möchten wir keineswegs Panik verbreiten. Doch um die Wichtigkeit vieler Maßnahmen richtig einordnen zu können, ist es unserer Meinung nach wichtig, die Gründe für den Handlungsbedarf zu verstehen.

Gefahren verstehen – Cybersicherheit leben

Wir beleuchten die möglichen Kosten, die bei einem Cybervorfall auf Ihr Unternehmen zukommen können sowie die Quellen der Bedrohung. Anschließend kommen wir zu den, aus unserer Sicht wichtigsten Schritten für kleine und mittlere Unternehmen, um eine nachhaltige Cybersicherheit aufzubauen und im Arbeitsalltag zu leben.

Viel Freude beim Lesen wünscht das Perseus Team

Inhalt

Inhalt

01 | Wer ist bedroht?

Zu den großen digitalen Errungenschaften unserer Zeit – für private wie berufliche Belange – gehört die schier unbegrenzte Speicherung von Informationen sowie die einfache und schnelle Kommunikation über das Internet, zum Beispiel per E-Mail und Messenger-Services. Doch mit diesen Vorteilen für unser privates und geschäftliches Leben erhöhen sich auch die Gefahren durch Cyberkriminalität und Sicherheitslücke

Der Mittelstand im Visier von Cyberkriminellen

Cybergefahren wie Phishing-E-Mails und -Websites, Viren oder Trojaner sowie deren erhebliche finanzielle Schäden nehmen jedes Jahr weiter zu[1]. Das gilt sowohl für den privaten als auch für den geschäftlichen Bereich. Besonders der Mittelstand – und das wollen viele Unternehmer nicht wahrhaben – ist enorm bedroht. Denn viele kleine und mittlere Unternehmen glauben, sie seien zu klein und unbedeutend für einen Hacker-Angriff. Weit gefehlt! Gerade diese damit einhergehende Unwissenheit nutzen die Angreifer aus.

„Mein Unternehmen ist zu klein, um für Cyberkriminelle interessant zu sein"
FALSCH!

Die Größe eines Unternehmens ist für Cyberkriminelle zweitrangig. Aktuelle Umfragen zeigen, dass insbesondere kleinere Unternehmen im Fadenkreuz krimineller Hacker stehen. Warum? Weil sie wissen, wie verwundbar Betriebe sind. Zudem sind deutsche Mittelständler als Zulieferer oder Dienstleister oft direkt mit Großunternehmen verbunden. Selbst wenn Cyberkriminelle es also auf die Großen abgesehen haben, schleichen sie sich gerne durch die vermeintlich schwach bewachten Hintertüren kleiner Firmen.

Gefahren werden ignoriert

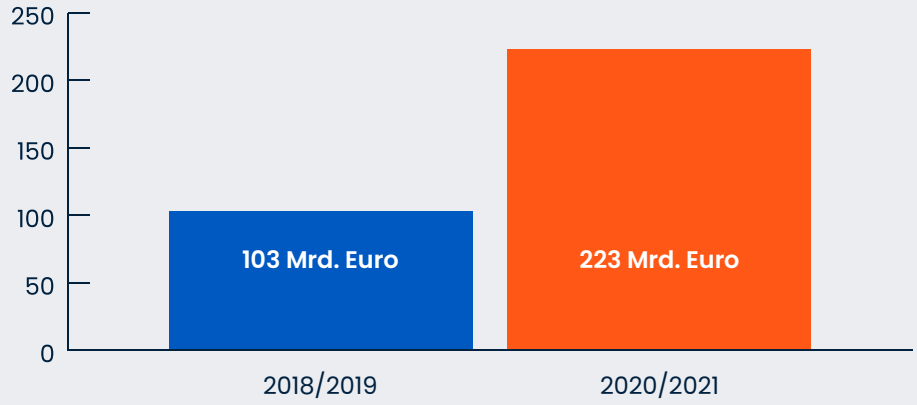
Ein Grund für die Verwundbarkeit von mittelständischen Unternehmen ist die geringe Ernsthaftigkeit, die dem Thema Cybersicherheit in weiten Teilen des Mittelstandes noch entgegengebracht wird.[2] Damit werden schnell am falschen Ende (überschaubare) Kosten eingespart. Clevere Unternehmerinnen und Unternehmer haben schon früh erkannt, dass sie mit geringen Investitionen Cyberrisiken wesentlich verringern und damit das Vertrauen Ihrer Kundinnen und Kunden stärken können.

1 https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr
2 https://www.gdv.de/resource/blob/61466/0456901217b39a5893bc6829b8d7d156/report-cyberrisiken-im-mittelstand-2020-data.pdf

Jedes Unternehmen gerät über kurz oder lang ins Visier der Kriminellen

Das Prinzip Hoffnung rächt sich spätestens dann, wenn ein Cybervorfall eintritt und der Schaden ein Vielfaches der eingesparten Kosten übersteigt.

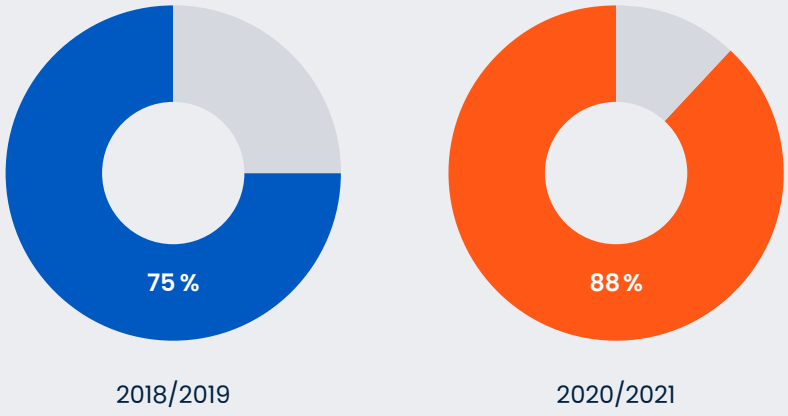
Schadensumme durch Diebstahl, Spionage und Sabotage in Milliarden Euro



Quelle: Bitkom e.V.

Die Schadensumme ist mehr als doppelt so hoch wie in den Jahren 2018/2019, als sie noch 103 Milliarden Euro p.a. betrug.

Anzahl der Unternehmen, die Opfer von Angriffen wurden in Prozent



Quelle: Bitkom e.V.

Neun von zehn Unternehmen (88 Prozent) waren 2020/2021 von Angriffen betroffen. In den Jahren 2018/2019 wurden drei Viertel (75 Prozent) Opfer.

9 von 10 Mittelständlern betroffen
99 % der deutschen Unternehmen gehören zum Mittelstand. Allein 88 % dieser Unternehmen sind im Jahr 2020/2021 Cyber-Attacken zum Opfer gefallen. Davon erlitten 86 % einen finanziellen Schaden. Für den Zeitraum 2018/2019 lag diese Zahl noch bei 70 %.[3]

Unternehmen müssen aktiv werden
Jetzt heißt es, sich zu schützen, um für die Zukunft gewappnet zu sein. Die oben stehenden Zahlen zeigen den Ernst der Lage sehr deutlich: Die Frage ist heute nicht mehr, ob ein Unternehmen Ziel einer Cyber-Attacke wird, sondern wann - unabhängig von Unternehmensgröße und Branche. Umso wichtiger ist es, dass sich die Eigentümer und Mitarbeitende kleiner und mittlerer Unternehmen frühestmöglich mit dem Thema befassen und sich auf mögliche Angriffe von Cyberkriminellen vorbereiten.

02 | Druck vom Gesetzgeber

Die großen Gefahren für das private wie auch wirtschaftliche Leben in Deutschland und Europa hat die EU dazu veranlasst, strengere Vorschriften z. B. beim Datenschutz zu erlassen.

DSGVO - Die Datenschutz-Anforderungen an Unternehmen steigen
Die europäische Datenschutzgrundverordnung (DSGVO) gilt seit dem 25.05.2018 und bringt auch für Unternehmen in Deutschland neue Anforderungen und beeinflusst den Umgang mit personenbezogenen Daten deutscher Unternehmen. Im Grundsatzartikel 5 der DSGVO wird so auch explizit gefordert, geeignete technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten zu treffen, um ein angemessenes Sicherheitsniveau zu gewährleisten.

Bei Missachtung der DSGVO können schließlich auch Sanktionen in Form von hohen Bußgeldern (siehe nächste Seite) folgen. Dies stellt insbesondere den deutschen Mittelstand vor eine doppelte Herausforderung in Sachen Cybersicherheit. Zum einen wächst die Gefahr, selbst ins Visier von Kriminellen zu geraten. Zum anderen kann Unwissenheit beim Thema Datensicherheit zu Sanktionen führen.

Datenschutz als Business-Enabler – Ihr Geschäft lebt von Vertrauen
Doch Datenschutz und Informationssicherheit können mehr sein als lediglich eine rechtliche Verpflichtung. Schaffen Sie Vertrauen und zeigen Sie Haltung, indem Sie Datenschutz aktiv in Ihrem Unternehmen umsetzen. Auf diesem Weg bauen Sie Vertrauen auf, gewinnen neue Kundinnen und Kunden, erhalten langjährige Geschäftsbeziehungen und schützen Ihre Reputation.

3 https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr

03 | Finanzielle Risiken & Sanktionen

Bis heute haben insbesondere die Angst vor hohen Kosten und Unwissenheit beim Thema Cybersicherheit dazu geführt, dass kleine und mittlere Unternehmen immer noch hochgradig ungesichert und anfällig für Cyberangriffe sind. Dabei sind die Kosten für die richtigen Maßnahmen überschaubar – insbesondere im Vergleich zu den möglichen Schäden und Sanktionen, die im Falle eines erfolgreichen Cyberangriffs entstehen können.

Kosten bei DSGVO-Pannen
Verstöße gegen die Datenschutzgrundverordnung können für Unternehmen teuer werden: Mehrere Millionen oder bis zu vier Prozent des Jahresumsatzes für große Unternehmen. Und auch mittelständische Unternehmen wurden bereits mit 20.000 bis 100.000 Euro zur Kasse gebeten, weil sie beispielsweise Kundendaten nicht ausreichend vor Diebstahl geschützt haben.[4]

Solche Forderungen erscheinen vielen Unternehmen als überzogen und absurd. Dabei wird schnell vergessen, dass die direkten Kosten nach einem tatsächlichen Cyberangriff nicht unerheblich sind *(Beispiele auf der nächsten Seite)*.

Unterstützung durch Perseus
Unsere Lösungen unterstützen Sie dabei, rechtskonforme Nachweise über die Schulung Ihrer Mitarbeitenden und Meldungen im Zusammenhang mit Cybersicherheitsvorfällen durchzuführen und damit die Anforderungen der DSGVO zu erfüllen bzw. hohe Strafen zu vermeiden.

4 https://www.spiegel.de/netzwelt/netzpolitik/dsgvo-strafen-fehler-werden-jetzt-teuer-a-1249443.html

01

Finanzielle Beispiele für Risiken Musterszenario 01: Diebstahl

(Quelle: GDV)

Online-Shop/Kreditkartendaten:
Cyberkriminelle attackieren die Datenbank eines mittelständischen Online-Shops und erbeuten die Kreditkarten-Daten von 50.000 Kunden.

Hinweis
Kreditkartenunternehmen weist Shop-Betreiber auf möglichen Datendiebstahl hin.

Security-Initiative & Betriebsunterbrechung
Nach Bestätigung des Angriffs werden die Ursachen gesucht, die Systeme bereinigt und gehärtet. Der Online-Shop bleibt währenddessen geschlossen.
Kosten für IT-Forensik: 40.000 Euro
Kosten der Betriebsunterbrechung: 50.000 Euro

Kundeninformation
Der Shop-Betreiber muss seine Kunden über den Diebstahl ihrer Daten informieren.
Informationskosten: 80.000 Euro

Ersatzkarten
Alle potenziell betroffenen Kunden erhalten neue Kreditkarten.

Aufarbeitung
Die Strafverfolgungsbehörden ermitteln. Das Kreditkartenunternehmen nimmt den Shop-Betreiber für die Ausstellung der Ersatzkarten in Regress.
Vertragsstrafen: 50.000 Euro

Vertrauenskrise
Die Presse berichtet über den Diebstahl der Kreditkartendaten, der Online-Shop verzeichnet einen erheblichen Umsatzrückgang.
Krisenkommunikation: 30.000 Euro

Der Umsatzrückgang ist nicht gedeckt.

02

Finanzielle Beispiele für Risiken Musterszenario 02: Ransomware

(Quelle: GDV)

Maschinenbau
Hacker attackieren mit einem Verschlüsselungs-Trojaner die IT-Systeme eines Maschinenbauers. Sie wollen die blockierten Rechner erst wieder freigeben, wenn sie Lösegeld bekommen

Angriff
Sämtliche Rechner und die vernetzten Produktionssysteme des Maschinenbauers sind ohne Funktion. Auf den Bildschirmen der Steuerungsrechner erscheint lediglich eine Nachricht der Erpresser.

IT-Forensik und Datenwiederherstellung
Nach Rücksprache mit Polizei und Staatsanwaltschaft zahlt das Unternehmen kein Lösegeld. IT-Spezialisten arbeiten mehrere Tage daran, den Trojaner von sämtlichen Systemen zu entfernen; anschließend müssen sie alle Daten aus den Backups wiederherstellen.
Kosten für IT-Forensik und Datenwiederherstellung: 40.000 Euro

Betriebsunterbrechung
Bis die Systeme wieder laufen, kann das Unternehmen nicht produzieren. Die Mitarbeiter aus Fertigung und Verwaltung bleiben zuhause.
Kosten für 5 Tage Betriebsunterbrechung: 45.000 Euro

Information von Kunden und Vertragspartnern
Die IT-Forensiker können nicht ausschließen, dass Daten nicht nur gesperrt, sondern auch entwendet wurden. In diesem Fall wären auch Betriebsgeheimnisse von Vertragspartnern betroffen, die vorsorglich informiert werden müssen.
Informationskosten und Rechtsberatung: 20.000 Euro

Vertrauenskrise
Der bisher tadellose Ruf des Unternehmens nimmt in wichtigen Kundenbranchen Schaden; einige Kunden wenden sich vom Unternehmen ab, der Umsatz sinkt spürbar.
Krisenkommunikation: 30.000 Euro

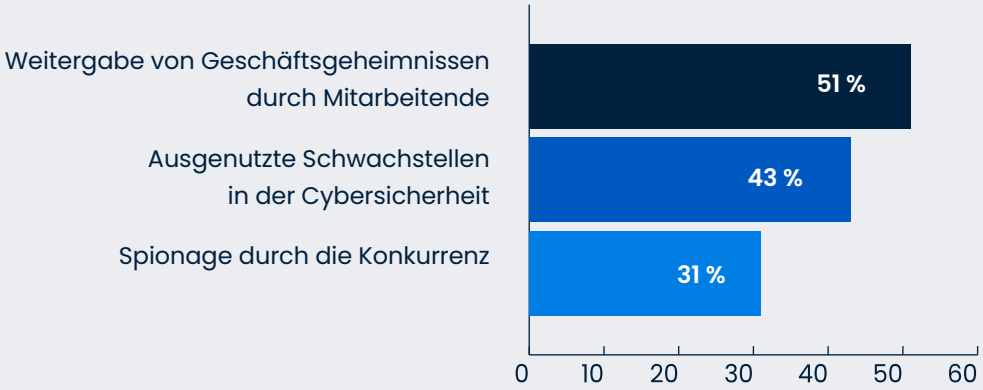
Der Umsatzrückgang ist nicht gedeckt.

Bedrohungslage – die Zahlen sprechen für sich
Cyberattacken und Datendiebstahl gehören zu den Top 5-Risiken der kommenden Jahre.

The Global Risks Report 2021
1. Infektionskrankheiten
2. Existenzkrisen
3. Extremwetterereignisse
4. Cybervorfälle
5. Digitale Kluft

(Quelle: Weltwirtschaftsforum WEF)

Die größten Bedrohungen für die Sicherheit von Geschäftsgeheimnissen in Unternehmen

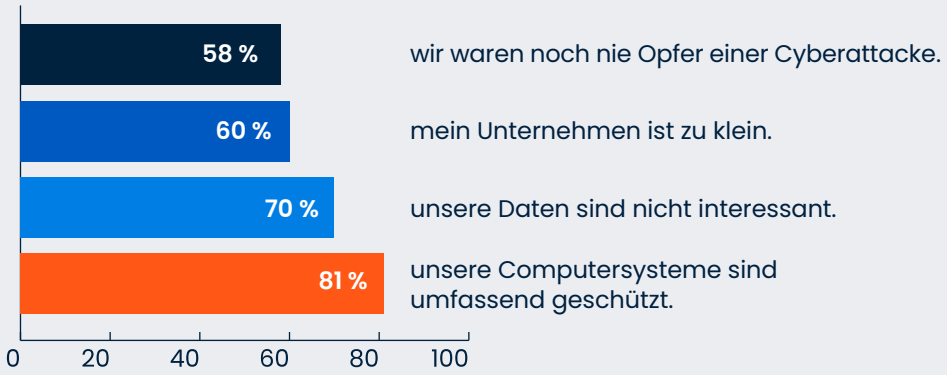


(Quelle: EIU Trade Secrets Survey 2021)

04 | Gefährliche Fehleinschätzung der Unternehmen

Besonders heikel zeigt sich die Selbsteinschätzung des Mittelstands laut einer Forsa Umfrage. Je kleiner das Unternehmen, desto geringer wird das eigene Risiko für einen Angriff eingeschätzt, und desto größer wird der eigene Schutz vor Cyberangriffen bewertet.

Von den Befragten, die nur ein geringes Risiko für das eigene Unternehmen sehen, sagen …



Quelle: Forsa

Wenn Unternehmer aber den eigenen Schutz an der vermuteten und nicht an der tatsächlichen Gefahr ausrichten, empfinden sie sich oft schon mit Virensoftware und Firewall ausreichend geschützt. Eine fatale Fehleinschätzung.

Firewall und Virensoftware sind technische Mindestanforderungen und können Unwissenheit und menschliches Fehlverhalten nicht auffangen. Cyberkriminelle wissen um Schwachstellen vieler kleiner wie mittlerer Unternehmen und greifen sie daher gezielt an.

Firewall und Virenscanner reichen nicht aus!

05 | Urheber von Cybergefahren

Auch für technisch nicht versierte Kriminelle ist es heutzutage einfach, im Netz schnell und günstig an gefährliche Schadsoftware zu gelangen. Der Kreis der Cyberkriminellen besteht also längst nicht mehr nur aus wenigen Profis. Jeder Einzeltäter mit ausreichend krimineller Energie kann mit der Hilfe von von Hard- und Software aus dem Netz Ihr Unternehmen attackieren. Ein Beispiel: Wussten Sie, dass man im Darknet Phishing-Angriffe einkaufen kann? Den sogenannten „Phishing as a Service" kann man zum Teil sogar als Abo erwerben. Um die 140 € monatlich soll der Dienst kosten. [5]

Phishing-Mails als größte Gefahr

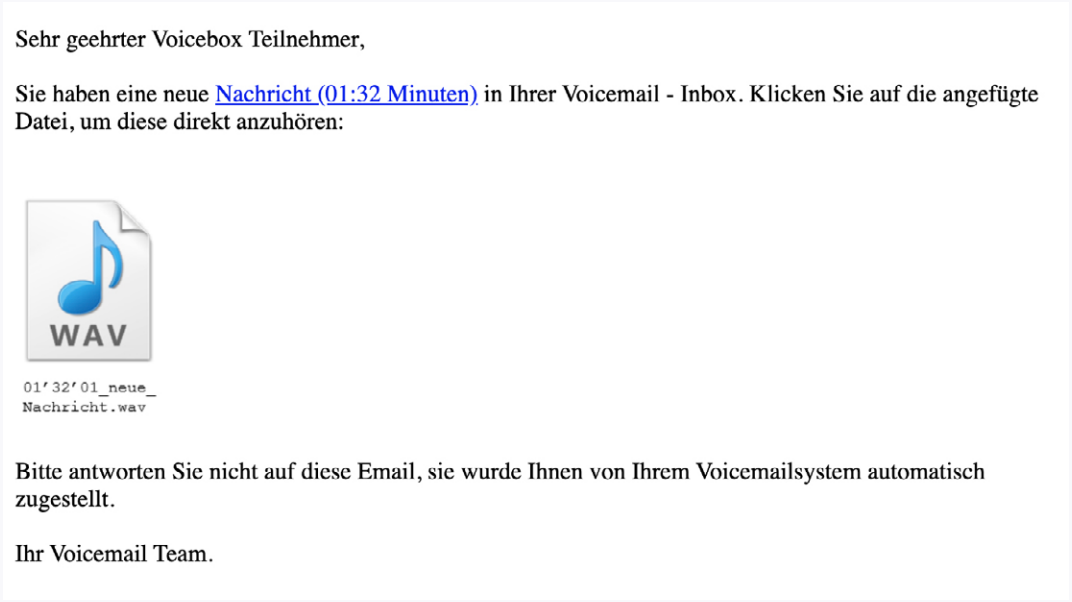
Laut dieverser erhebungen von Bitkom und BSI sind Phishing-E-Mails die gefährlichste und effektivste Form der Hacker ein anvisiertes System zu infiltrieren. Im Rahmen einer Studie des Telekommunikationskonzerns Verizon wurde ermittelt, dass es sich bei 80 % aller Cybervorfälle in Unternehmen um Phishing-Angriffe handelt . Davon erfolgt ein Großteil per E-Mail.[6] So versenden Kriminelle unscheinbare E-Mails an nichtsahnende Mitarbeiter. Kaum sind die E-Mail und der Anhang geöffnet, bzw. wurde einem Link gefolgt, ist der Kollege in die Falle getappt.

Dabei schrecken Betrüger auch nicht vor aufwendigen Angriffsmustern zurück. Sie fälschen ganze Websiten einer Bank oder eines bekannten Online-Shops, um an die Zugangsdaten und Informationen ihrer Opfer zu gelangen.

Typische Phishing-E-Mail-Fallen

- Falsche E-Mails von Kollegen, Vorgesetzten oder Dienstleistern
- Schadsoftware im Anhang einer E-Mail
- Weiterleitung auf gefälschte Unternehmens-Website (Banken, Online-Shops etc.)

Beispiel für eine Phishing-E-Mail


Sehr geehrter Voicebox Teilnehmer,

Sie haben eine neue Nachricht (01:32 Minuten) in Ihrer Voicemail - Inbox. Klicken Sie auf die angefügte Datei, um diese direkt anzuhören:

WAV

01'32'01_neue_Nachricht.wav

Bitte antworten Sie nicht auf diese Email, sie wurde Ihnen von Ihrem Voicemailsystem automatisch zugestellt.

Ihr Voicemail Team.

5 Phishing-Industrie: Erschreckende Details zur Quelle der Angriffe (inside-digital.de)
6 Verizon Data Breach Investigation Rebort 2021

06 | Risikofaktor Mensch

Die Mitarbeitenden sind nach wie vor die größte Sicherheitsrisiko für jedes Unternehmen. Die Studie des Telekommunikations-Riesen von Verizon brachte ebenfalls hervor, dass 85 % aller größeren Cyberangriffe durch die Fahrlässigkeit der Mitarbeitenden verursacht wurden. Beispielsweise durch das Öffnen erwähnter Phishing-E-Mails, die fehlende Installation wichtiger Sofware-Updates, nicht vorhandene Backups oder dem Verwenden unsicherer Passwörter.[7]

Mangele Richtlinien für Cybersicherheit
Umso wichtiger ist es, das gesamte Team beim Thema Cybersicherheit mit einzubeziehen. Stellen Sie sich aus den Vorschlägen auf den kommenden Seiten eine kurze und verständliche Cybersicherheits-Checkliste individuell für Ihr Unternehmen zusammen. Diese können sich all Ihre Mitarbeitenden an den Platz legen und Schritt für Schritt abarbeiten.

Beispiele menschlicher Schwachstellen

07 | Wie Sie ihr Unternehmen schützen können

Trotz aller Gefahren, die im Zuge der Digitalisierung entstehen, sind Mitarbeitende, Managerinnen und Eigentümer kleiner wie auch mittlerer Unternehmen Cyberbedrohungen nicht hilflos ausgeliefert. Es gibt zahlreiche Maßnahmen, die dabei unterstützen, die Sicherheit sensibler, um die Sicherheit sensibler Daten zu gewährleisten sowie Kosten und Schäden durch Attacken zu vermeiden

7 Ebd.

Wichtige Maßnahmen zum Schutz Ihres Unternehmens
- IT-Sicherheitsprüfung
- Schulung der Mitarbeitenden
- Sensibilisierung der Mitarbeitenden
- Regelmäßiges Anlegen von Backups
- Regelmäßiges Update der Firewall
- Endgeräte-Schutz
- Passwort-Hygiene
- Antivirus-Software
- Multi-Faktor-Authentifizierung
- Software-Hygiene
- Finanzielle Absicherung gegenüber Cyberrisiken

IT-Sicherheitsprüfung

Der Sicherheitsstatus Ihres Unternehmens sollte regelmäßig einer eingehenden Prüfung unterzogen werden. Bei einer solchen Prüfung werden die einzelnen wichtigen Faktoren untersucht, die für die Sicherheit Ihres Unternehmens notwendig sind. Dazu gehören unter anderem die Überprüfung der Aktualität der verwendeten Software, des Cybersicherheits-Wissens der Mitarbeiter, dem richtigen Umgang mit Passwörtern und der Schutz von Endgeräten etc.

Notfall-Plan
Kein Netzwerk ist 100%ig sicher. Gerade deswegen ist es besonders wichtig zu wissen, was im Falle eines Cybervorfalls zu tun ist. Je schneller und genauer ein solches Sicherheitsprotokoll umgesetzt wird, desto effizienter kann ein möglicher Schaden verhindert oder minimiert werden.

Bestandteile eines Notfallplans
Ein Notfallmanagement ist in der Regel individuell auf ein Unternehmen, seine Ansprüche und die Position der einzelnen Mitarbeitenden zugeschnitten und kann diese oder ähnliche Punkte enthalten:
- Verzeichnis über alle für Notfälle relevanten Dokumentationen und Informationen
- Checklisten mit Handlungsempfehlungen
- Checklisten zur Fehlereingrenzung und Problemanalyse, mögliche Workarounds und Notbetriebsverfahren
- Verfahren zur Wiederherstellung der Funktion, Kontaktlisten, Zuständigkeiten, Alarmketten und Alarmierungspläne
- Verzeichnis von notfallrelevanten Zugangsdaten und Zugangsinformationen, Vertretungsregelungen etc.

Schulung der Mitarbeitenden

Der Mensch ist und bleibt die größte Schwachstelle für Cybersicherheit. Mitarbeitende eines Unternehmens stehen auf vielfältige Weise in Kontakt mit Kolleginnen, Partnern und Dienstleistungsunternehmen – sei es über E-Mail, Smartphone, Messenger-Services uvm. Cyberkriminelle machen sich dies zunutze und stellen Fallen, um an Daten und in Systeme zu gelangen. Ob Ihre Mitarbeitenden all diese möglichen Gefahren erkennen können, wird zum wichtigsten Faktor Ihrer Cybersicherheit. Gleichzeitig ist Ihr Team auch der beste

Schutzschild vor Cyberangriffen, wenn sie entsprechend geschult sind. Dazu gehört es auch, einen Angriff zu erkennen. Je später ein Angriff erkannt wird, desto höher liegen die Kosten. Mit regelmäßigen Schulungen machen Sie Ihre Mitarbeitenden zu einem essentiellen Teil Ihrer Cybersicherheits-Strategie. Denn nur wissende und aufgeklärte Kolleginnen und Kollegen können sich selbstbewusst und autark in einer digitalen Arbeitswelt bewegen, ohne ein Risiko darzustellen

Sensibilisierung der Mitarbeitenden

Schulungen und Sensibilisierung gehören eng zusammen, letztere muss aber als gesonderter Punkt aufgeführt werden. Denn was bringt eine Schulung, wenn das Wissen im Alltag nicht angewendet werden kann? Besonders da die meisten erfolgreichen Cyber-Attacken auf kleine und mittlere Unternehmen in Deutschland per E-Mail erfolgen, sollten Sie in Erwägung ziehen, Ihre Mitarbeitenden unregelmäßigen Tests mit simulierten Phishing-E-Mails zu unterziehen. Dies sind falsche, also ungefährliche Phishing-E-Mails, über die Ihre Mitarbeitenden in der täglichen Arbeit lernen, Gefahren zu erkennen und sich für tatsächliche Phishing-E-Mails zu wappnen.

Regelmäßiges Anlegen von Backups

Geschäftsinhaberinnen und Unternehmer sollten sicherstellen, dass die Daten des eigenen Betriebs gesichert werden. Geschäftskritische Daten können aus unterschiedlichsten Gründen verloren gehen – von Cyberattacke bis Naturkatastrophe. Backup-Lösungen auf dem Markt sind vielfältig (Desktop, Speichermedien, Cloud). Wir empfehlen die häufig genutzte 3-2-1-Backup-Strategie: Drei Datenkopien, zwei Medien, ein externes Backup.

Regelmäßiges Update der Firewall

Gleichgültig wie klein Ihr Büro-Netzwerk ist, mit falschen Einstellungen kann das Netzwerk dennoch einem erhöhten Sicherheitsrisiko ausgesetzt sein. Firewalls sind mittlerweile ein selbstverständlicher Bestandteil eines Büro-Netzwerks und ein wichtiger Basis-Schutz. Eine Firewall beschränkt den Netzwerkzugriff basierend auf festgelegten Regeln und versucht somit, unerlaubten Zugriff zu unterbinden.

Endgeräte-Schutz

Sowohl die Endgeräte in Ihrem Unternehmen als auch im Home Office (Computer, Smartphones, Tablets, Smartwatches etc.) sind Einfallstore für Cyberkriminelle. Schließlich werden dort sensible Daten durch Mitarbeitende gespeichert und verarbeitet. Stellen Sie unbedingt sicher, dass Sie alle Endgeräte kennen, die mit dem Netzwerk Ihres Unternehmens verbunden sind. Gerade in kleinen und mittleren Firmen und im Home Office neigen Mitarbeitende dazu, mit ihren eigenen privaten Geräten zu arbeiten. Die sogenannte „Bring your own device“-Policy sorgt dafür, dass bestimmte Risiken gar nicht erst entstehen. Häufig sind Sicherheitseinstellungen der Geräte nicht richtig konfiguriert oder die darauf verwendete Software nicht aktuell. Vor allem im Home Office sind die privaten Endgeräte der Mitarbeitenden sowohl mit dem Firmennetzwerk als auch mit öffentlichen und schlecht geschützten Netzwerken verbunden. Legen Sie fest, welche Geräte sich mit dem Firmen-

netzwerk verbinden dürfen. Achten Sie darauf, in der Router-Konfiguration WPA oder besser WPA2 einzustellen, sowie ein sicheres Passwort zu setzen. Router, die im Auslieferungszustand belassen werden, sind oft leicht zu knacken und damit ein hohes Risiko. Selbst wenn Ihr Unternehmen die Nutzung der eigenen Endgeräte erlaubt, sollten sie vorher geprüft und wenn nötig "nachgerüstet" werden. Zum einen sollte sichergestellt sein, dass sich auf den Geräten keine Malware befindet, die Angreifern den Zugang zu Ihrem Unternehmensnetzwerk ermöglicht. Eine aktuelle Antivirensoftware, Firewall, Festplattenverschlüsselung und andere Maßnahmen zur Erhöhung der Cybersicherheit sollten zwingend vorhanden sein. Zum anderen benötigen die Endgeräte vielleicht gewisse Softwarelösungen, wie einen VPN-Client, um sicher auf E-Mails oder die Unternehmens-Cloud zugreifen zu können oder proprietäre Softwarelösungen, die Ihr Unternehmen verwendet. All das können IT-Spezialisten für Sie einrichten, damit Sie und Ihr Team sicher und ohne Einschränkungen weiterarbeiten können, selbst wenn der Rechner im Büro bleiben muss.

Passwort-Hygiene

Viele Mitarbeitende, die ebensoviele Geräte im Büro sowie im Home Office nutzen, erhöhen auch die Wichtigkeit des Endgeräteschutzes durch sichere Passwörter. Ein Großteil von Datenlecks resultieren direkt aus mangelhafter Passwort-Hygiene. Mangelhaft bedeutet an dieser Stelle, dass zu schwache Passwörter gewählt und diese aus Bequemlichkeit dann auch noch für mehrere Geräte und Zugänge verwendet werden. Weisen Sie Ihre Mitarbeitenden darauf hin, starke und lange Passwörter zu wählen, die sowohl Klein- und Großbuchstaben als auch Zahlen und Sonderzeichen beinhalten. Diese sollten mindestens zehn Zeichen lang sein und weder im Duden stehen noch durch Recherche leicht zu erraten sein. Um die Handhabung vieler, komplizierter Passwörter einfacher zu machen, sind Passwort-Manager eine praktische Lösung für den täglichen Einsatz.

Antivirus-Software

Die Bedrohungen aus dem Netz sind vielfältig. Die Cybersicherheits-Schulung Ihrer Mitarbeiter steht hier an erster Stelle. Doch nicht alle Gefahren lassen sich auf diesem Weg vermeiden. Die Anschaffung einer guten Antivirensoftware sowie deren regelmäßige Aktualisierung schützt Ihre Systeme vor vielfältigen Gefahren wie Viren, Trojanern und anderer Malware.

Multi-Faktor-Authentifizierung

Zusätzlich zu einem starken Passwort sollten Sie Accounts und Geräte durch eine Multi-Faktor-Authentifizierung zu schützen. Als schwächster Sicherheitsfaktor neigt der Mensch weiterhin dazu, zu leichte Passwörter zu verwenden oder diese unwissend weiterzugeben - schlimmstenfalls an Cyberkriminelle während einer Phishing-Attacke. Wird ein zweiter Faktor zur Identifizierung verwendet, kann sichergestellt werden, dass Kriminelle allein mit den Zugangsdaten nicht an vertrauliche Informationen gelangen. Bispiele dafür sind ein zusätzlicher Sicherheitscode, der bei Anmeldung auf das Smartphone gesendet wird, oder ein Fingerabdruck.

Software-Hygiene

Es sollte die strikte Anweisung an alle Mitarbeitenden erfolgen, dass Software und Apps ausschließlich
1. nach Rücksprache mit einem Sicherheitsverantwortlichen und
2. aus autorisierten und sicheren Quellen heruntergeladen und installiert werden dürfen.

Hüten Sie sich vor möglicherweise schadhafter Software aus unsicheren Quellen im Netz. Achten Sie bei bestehender Software darauf, diese immer auf dem neuesten Stand zu halten und Updates regelmäßig auszuführen.

Zugänge und Rechte begrenzen
Einzelnen Mitarbeitenden sollte zudem nur begrenzter Zugang und lediglich so viele Rechte für Programme und Konten gegeben werden, wie sie zur Ausübung ihrer Tätigkeit benötigen. Das wahllose Vergeben von Admin-Rechten erhöht die Anfälligkeit Ihres Unternehmens für schadhafte Attacken von außen und innen.

Finanzielle Absicherung gegenüber Cyberrisiken

In Sachen Absicherung gegen Schäden durch Cybervorfälle steht der deutsche Mittelstand hinten an. Nach Umfrage-Ergebnissen des Gesamtverbands der deutschen Versicherungswirtschaft (GDV) zeigt sich: Bei Investitionen in Cybersicherheit erweisen Unternehmen sich nicht gerade als freigiebig. So waren gerade einmal etwas mehr als die Hälfte der Befragten dazu bereit, in den kommenden zwei Jahren in die Sicherheit ihrer Systeme zu investieren. Darüber hinaus fehlt es in vielen Fällen an systemrelevanten Strukturen: Laut eriner Befragung durch Perseues haben 33 Prozent der Erwerbstätigen keinen zuständigen Verantwortlichen, an den sie sich im Cybernotfall wenden können. Weitere 14 Prozent gaben an, dass sie nicht wissen, ob es überhaupt eine verantwortliche Person in ihrem Unternehmen gibt. Das heißt, dass fast die Hälfte der Befragten im Ernstfall auf sich alleine gestellt sind und Cyberkriminelle auf keine aktive Gegenwehr stoßen.

In Anbetracht der Tatsache, dass gerade kleine und mittlere Unternehmen besonders ins Visier der Cyberkriminellen geraten, erschrecken diese Zahlen zur schlechten Absicherung. Denn kommt zu den schlechten bis fehlenden Cybersicherheits-Maßnahmen im Mittelstand auch noch eine fehlende Absicherung, sind teure Cybervorfälle in Zukunft praktisch vorprogrammiert. Wir raten: Investieren Sie in die entsprechende Infrastruktur und in eine Cyberversicherung, die unmittelbare Kosten im Schadensfall abdeckt. Vor allem aber ist es an der Zeit, aus jede Person in Ihrem Unternehmen so zu schulen, dass ein Cybervorfall durch menschliches Versagen ausbleibt. Darüber hinaus ist es sinnvoll, sich einen zuverlässigen Partner für alle Fragen rund um das Thema Cybersicherheit zu suchen, der beratend zur Seite steht und im Notfall alle wichtigen Maßnahmen zur Wiederherstellung des regulären Geschäftsbetriebs einleitet.

08 | Fragen, die Sie sich stellen sollten

Für die Cybersicherheit Ihres Unternehmens

Ihr Unternehmen

- Wie lange könnte Ihr Unternehmen überleben, wenn es zu einem Betriebsstillstand kommt?
- Welche Maßnahmen haben Sie bisher unternommen, um Ihr Unternehmen gegen Cyberrisiken abzusichern?
- Wie schlimm wäre es für Ihr Unternehmen, wenn Sie Kundendaten verlieren würden?
- Was wären die Gesamtkosten eines erfolgreichen Cyberangriffs für Ihr Unternehmen?
- Was wären Sie bereit zu investieren, um Ihr Unternehmen abzusichern?

Ihre IT

- Wie sicher sind Sie, dass Ihre Antivirensoftware alle Viren, Trojaner und sonstige Angriffe abwehrt?
- Sind Sie sicher, dass alle Ihre Mitarbeitenden, verdächtige E-Mails und Dateianhänge erkennen und diese nicht öffnen?
- Führen Sie bereits heute Schulungen zum Thema Cybersicherheit durch?
- Haben Sie Cybersicherheits-Regeln und wissen Sie, wie nachhaltig diese wirken? Wie erfolgt die Schulung neuer Mitarbeitender in Sachen Cybersicherheit?

Ihr Netzwerk

- Wie sehr verlassen Sie sich darauf, dass Sie im Datenaustausch mit Ihren Geschäftspartnerinnen und Kunden keine infizierten Dateien erhalten?
- Wie wichtig ist Ihnen das Vertrauen von Geschäftspartnerinnen und Kunden? Sind deren sensible Daten bei Ihnen absolut sicher?
- Wen würden Sie im Falle eines Cybervorfalls unmittelbar kontaktieren und wie sicher wären Sie, dass Ihnen kompetent geholfen werden würde?

09 | Wie Perseus Ihnen helfen kann.

Perseus verfolgt ein in sich geschlossenes Konzept, das Ihre Mitarbeitenden im Bereich Cybersicherheit fit macht. Bei unserer Lösung steht der Mensch im Mittelpunkt. Er ist der beste Schutzschild zur Abwehr von Cyberangriffen. Der erste Schritt auf dem Weg zu nachhaltiger Cybersicherheit ist die Sensibilisierung gegenüber möglicher Cyberrisiken sowie Schärfung des Gefahrenbewusstseins - kurz gesagt: Awareness. Und hier setzen wir an: Perseus kombiniert Online-Trainings zu Cybersicherheit und Datenschutz mit regelmäßigen Phishing-Simulationen – benutzerfreundlich, nachhaltig und sofort einsatzbereit.

Konkreter:

- Kurzweilige Online-Trainings rund um die Themen Cybersicherheit, Datenschutz, Phishing & Co. geben allen Beteiligten einen Überblick zu Cyberrisiken.

- Verknüpfung von Theorie und Praxis: Regelmäßige Phishing-Simulationen trainieren und schärfen das Gefahrenbewusstsein der Mitarbeitenden nachhaltig.

- Die Perseus Werkzeugbox liefert wertvollen Tools für zusätzliche Cybersicherheit im Arbeitsalltag.

- Auch mit dem besten Schutz kann ein Cybervorfall eintreten. Unsere Notfallhilfe ist rund um die Uhr zur Stelle – bereits beim kleinsten Verdacht auf eine Cyberattacke. Unsere Fachleute für Incident Management und Cyberforensik haben rund 15 Jahre Erfahrung in den Bereichen Netzwerksicherheit, Cyber-Threat-Analyse, Risk-Assessment, Incident-Response und Cyberforensik. Sie nehmen sich dem Notfall an und leiten alle notwendige Maßnahmen ein – von der Analyse des Angriffs bis hin zur Wiederherstellung der Daten. Nach jedem abgewickelten Cybervorfall wird ein vollständiger Bericht erstellt, der den kompletten Ablauf dokumentiert, um Meldepflichten und Versicherungsanforderungen nachzukommen.

Sie haben Fragen, wie Sie Ihr Unternehmen nachhaltig gegen Bedrohungen aus dem Internet schützen können? Wir unterstützen Sie gerne. Auf unserer Website finden Sie hilfreiche Blogbeiträge, Leitfäden und Whitepaper rund um Cybersicherheit. Gerne stehen wir Ihnen auch telefonisch unter +49 30 95 999 8080 oder per E-Mail an info@perseus.de zur Verfügung.

Mit der Lösung von Perseus sensibilisieren Sie Ihre Mitarbeitenden für die Gefahren aus dem Netz, noch bevor Sie ins Visier von Cyberkriminellen geraten. Und das, ohne den Arbeitsalltag und den Erfolg Ihres Unternehmens aus den Augen zu verlieren. Denn am Ende gilt: Cybersicherheit - das sind wir alle.

Impressum

Haftungsausschluss

Haftung für Inhalte
Die Inhalte dieses Whitepapers wurden mit größter Sorgfalt erstellt. Für die Richtigkeit, Vollständigkeit und Aktualität der Inhalte können wir jedoch keine Gewähr übernehmen. Als Diensteanbieter sind wir gemäß § 7 Abs.1 TMG für eigene Inhalte auf diesen Seiten nach den allgemeinen Gesetzen verantwortlich. Nach §§ 8 bis 10 TMG sind wir als Diensteanbieter jedoch nicht verpflichtet, übermittelte oder gespeicherte fremde Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen bleiben hiervon unberührt. Eine diesbezügliche Haftung ist jedoch erst ab dem Zeitpunkt der Kenntnis einer konkreten Rechtsverletzung möglich. Bei Bekanntwerden von entsprechenden Rechtsverletzungen werden wir diese Inhalte umgehend entfernen.

Haftung für Links
Dieses Whitepaper enthält Links zu externen Webseiten Dritter, auf deren Inhalte wir keinen Einfluss haben. Deshalb können wir für diese fremden Inhalte auch keine Gewähr übernehmen. Für die Inhalte der verlinkten Seiten ist stets der jeweilige Anbieter oder Betreiber der Seiten verantwortlich. Die verlinkten Seiten wurden zum Zeitpunkt der Verlinkung auf mögliche Rechtsverstöße überprüft. Rechtswidrige Inhalte waren zum Zeitpunkt der Verlinkung nicht erkennbar. Eine permanente inhaltliche Kontrolle der verlinkten Seiten ist jedoch ohne konkrete Anhaltspunkte einer Rechtsverletzung nicht zumutbar. Bei Bekanntwerden von Rechtsverletzungen werden wir derartige Links umgehend entfernen.

Urheberrecht
Die durch die Seitenbetreiber erstellten Inhalte und Werke auf diesen Seiten unterliegen dem deutschen Urheberrecht. Die Vervielfältigung, Bearbeitung, Verbreitung und jede Art der Verwertung außerhalb der Grenzen des Urheberrechtes bedürfen der schriftlichen Zustimmung des jeweiligen Autors bzw. Erstellers. Downloads und Kopien dieser Seite sind nur für den privaten, nicht kommerziellen Gebrauch gestattet. Soweit die Inhalte auf dieser Seite nicht vom Betreiber erstellt wurden, werden die Urheberrechte Dritter beachtet. Insbesondere werden Inhalte Dritter als solche gekennzeichnet. Sollten Sie trotzdem auf eine Urheberrechtsverletzung aufmerksam werden, bitten wir um einen entsprechenden Hinweis. Bei Bekanntwerden von Rechtsverletzungen werden wir derartige Inhalte umgehend entfernen.

Perseus Technologies GmbH | Hardenbergstraße 32 | 10623 Berlin
Telefon: +49 (30) 959998080 | E-Mail: info@perseus.de
Geschäftsführer: Kevin Püster

Handelsregister: Amtsgericht Charlottenburg HRB 180356 B
USt.-Ident-Nr.: DE308271739
Verantwortlicher gem. § 55 Abs. 2 RStV: Kevin Püster

An wen können Sie sich im Notfall wenden?
Unsere Notfallhilfe steht Perseus-Mitgliedern in Verdachtsfällen zur Seite:
https://www.perseus.de/produkt/notfallhilfe/

Für Nicht-Mitglieder ist diese Notfall-Nummer rund um die Uhr erreichbar:
+49 30 233 2730 95