Cyber-Risiken

Was ist ein Cyber-Risiko?

Der Begriff Cyber-Risiko umfasst alle Risiken und Gefahren, die mit der Nutzung digitaler Technologien verbunden sind und die Vertraulichkeit, Integrität, Authentizität oder Verfügbarkeit von Daten und Produktionswerkzeugen gefährden können.

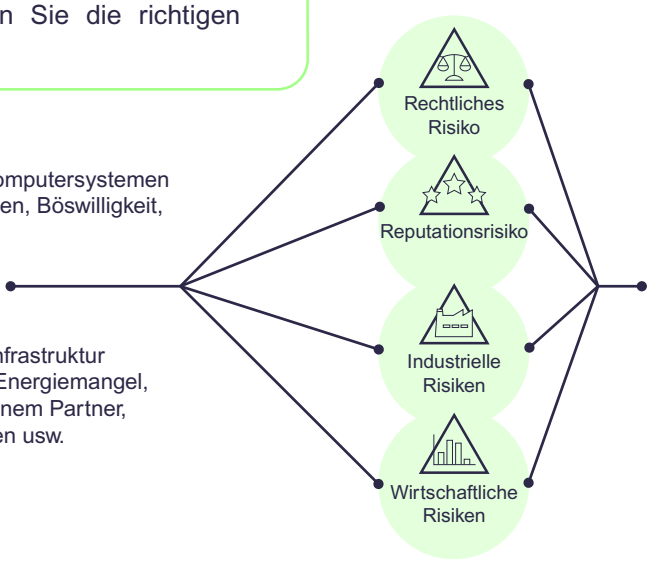
Kein Unternehmen ist davor sicher, unabhängig von seiner Grösse, der Art seiner Tätigkeit oder seiner Branche (Handel, Dienstleistungen, Gesundheitswesen, Finanzwesen, Industrie usw.). Ein einziger Vorfall reicht aus, um die gesamte Geschäftstätigkeit eines Unternehmens zu gefährden. Seien Sie wachsam: Treffen Sie die richtigen Entscheidungen und wenden Sie die richtigen Praktiken an.

Gefahren im Zusammenhang mit Cyber-Risiken

Durch die Gefährdung der Sicherheit sensibler und nicht sensibler Daten können Cyber-Risiken schwerwiegende Folgen wie finanzielle Verluste, Geschäftsunterbrechungen, Betriebsstörungen, Sicherheitsrisiken, Produktionsstopps oder Rufschädigungen nach sich ziehen.

Interne Risiken
Fahrlässigkeit, Missbrauch von Computersystemen oder Daten, menschliches Versagen, Böswilligkeit, mangelnde Schulung usw.

Externe Risiken
Hackerangriffe, Schäden an der Infrastruktur wie Wasser- und Brandschäden, Energiemangel, Mangel an Bauteilen, Brand bei einem Partner, Änderungen der Rechtsvorschriften usw.



Prävention und Risikominderung
Cyber-Risiken können durch verschiedene Massnahmen reduziert werden: Umsetzung von Sicherheitsrichtlinien, Schulung der Mitarbeiter, Einrichtung von Notfall- und Wiederherstellungsverfahren.

„In der vernetzten Welt, in der wir leben, sind Cyberbedrohungen eine unumgängliche Realität. Es ist zwingend erforderlich, alle Massnahmen zu ergreifen, um sein Unternehmen, seine Mitarbeiterinnen und Mitarbeiter bestmöglich zu schützen."

Dimitri Konstantas, Professor und Direktor des Information Science Institute an der Universität Genf

REPUBLIQUE ET CANTON DE GENEVE
POST TENEBRAS LUX

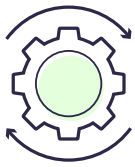
h e g
Haute école de gestion Genève

UNIVERSITÉ DE GENÈVE

Erfahren Sie mehr

Das Unerlässliche

Schützen Sie Ihre Dateien und Geräte

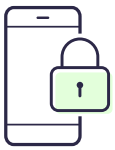


Halten Sie Ihre Software und Systeme auf dem neuesten Stand, indem Sie automatische Updates für Ihre Anwendungen, Webbrowser, Betriebssysteme, Geräte und Ausrüstungen anwenden.

Sperren Sie den Zugriff auf Geräte (Computer, Tablets, Smartphones usw.) mit einem starken Passwort, das Sie selbst oder ein Passwortmanagementservice generiert haben, und lassen Sie sie nicht unbeaufsichtigt an öffentlichen Orten. Gehen Sie bei der Nutzung öffentlicher WLAN-Netzwerke mit Vorsicht vor.

Erzwingen Sie die Multi-Faktor-Authentifizierung für den Zugriff auf Ihr Unternehmensnetzwerk (SMS, E-Mail, Authentifizierungsanwendung usw.).

Sichern Sie wichtige Dateien offline, auf externen Festplatten oder in der Cloud, damit Sie auch bei Verlust, Ausfall oder Diebstahl Ihrer Geräte darauf zugreifen können. Achten Sie auch darauf, dass Sie Ihre Papierakten sicher aufbewahren.



Verwenden Sie einen Verschlüsselungsschlüssel, um sensible und kritische Informationen zu schützen, die sich auf den Geräten Ihres Unternehmens befinden, z. B. Laptops, Tablets, Smartphones, austauschbare Festplatten und USB-Sticks sowie Cloud-Speicherlösungen.

Verwenden Sie Software und/oder Sicherheitssysteme (Antivirenprogramme, Firewalls, Systeme zur Erkennung und Verhinderung von Eindringlingen (IDS/IPS) usw…).

Die Sicherheit Ihres Unternehmens steht an erster Stelle!
Lassen Sie sich von Spezialisten beraten.

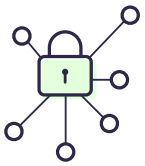
Das Unerlässliche

Schützen Sie Ihre Dateien und Geräte

Aktivieren Sie Ihre Firewall, um den Netzwerkverkehr zu kontrollieren und zu filtern, indem Sie bestimmte Kommunikationstypen und Inhalte nach vordefinierten Regeln zulassen oder blockieren.

Sichern Sie Ihren Router, indem Sie den Standardnamen und das Standardpasswort ändern und die Fernverwaltung deaktivieren. Denken Sie daran, das Passwort in regelmässigen Abständen zu ändern.

Stellen Sie sicher, dass Ihr drahtloses Netzwerk eine WPA2- oder WPA3-Verschlüsselung ermöglicht und diese aktiviert ist, um die Informationen, die über Ihr Netzwerk laufen, vor unbefugten Personen zu schützen.



Legen Sie restriktive Verzeichnisse von Geräten an, die auf das Unternehmensnetzwerk zugreifen dürfen.

Benennen Sie den Standardnamen Ihres WLAN-Netzwerks um, sodass Sie nicht mehr identifiziert werden können. Für mehr Diskretion können Sie diesen ausblenden.

Machen Sie Sicherheit zur Unternehmenskultur

Schaffen Sie eine Sicherheitskultur, indem Sie Ihre Teams regelmässig schulen und sie über neue Risiken und Schwachstellen informieren.

Richten Sie einen **Business Continuity Plan (BCP)** ein. Dieser Plan sollte beschreiben, wie Sie im Falle eines Zwischenfalls, eines Angriffs oder einer Beschädigung Ihre Daten sichern und Ihr Unternehmen am Laufen halten können. Halten Sie diesen Plan schriftlich fest, teilen Sie ihn allen Beteiligten in Ihrem Unternehmen mit und testen Sie ihn in regelmässigen Abständen.

Festlegung einer Strategie

Wie kann man Cyber-Risiken in Unternehmen reduzieren?

Unabhängig von ihrer Grösse sind alle Unternehmen von der Umsetzung der folgenden **fünf Schritte** betroffen.

1 Identifikator

- Erstellen Sie eine Liste aller Geräte, Anwendungen und Dienstleistungen, die das Unternehmen nutzt. Dies gilt für Computer, Smartphones, Tablets, aber auch für Peripheriegeräte wie Drucker oder andere Gegenstände oder Maschinen, die mit dem Netzwerk oder dem Internet verbunden sind.
- Erstellen und teilen Sie eine Richtlinie zur Cybersicherheit für Ihr Unternehmen, die Folgendes berücksichtigt:
  - Die Rollen, Verantwortlichkeiten und Zugänge jeder Mitarbeiterin und jedes Mitarbeiters sowie aller Dritten – Personen oder Unternehmen – die Zugang zu sensiblen Informationen haben könnten.
  - Die Vorgehensweise, um sich vor Angriffen zu schützen und den Schaden zu begrenzen, sollte ein Angriff stattfinden.

2 Schutz

- Kontrollieren Sie, wer auf Ihr Firmennetzwerk zugreifen und Computer und andere Geräte nutzen kann (Mitarbeiterinnen und Mitarbeiter, Kundinnen und Kunden, Partner, Auftragnehmer).
- Verwenden und konfigurieren Sie Sicherheitssoftware, um Ihre Daten zu schützen.
- Verschlüsseln Sie sensible Daten und bewahren Sie die Verschlüsselungsschlüssel an einem sicheren und getrennten Ort auf.
- Definieren Sie einen Plan für die regelmässige und automatisierte Sicherung Ihrer Daten (siehe Seiten 15-16).
- Aktualisieren Sie Ihre gesamte Software regelmässig oder automatisieren Sie die Updates.
- Schulen Sie alle Mitarbeiter, die Ihre Geräte nutzen, in regelmässigen Abständen. Helfen Sie Ihren Mitarbeiterinnen und Mitarbeitern, die Herausforderungen und Risiken für sich selbst und für das Unternehmen zu verstehen.

3 Erkennen

- Richten Sie eine aktive Überwachung Ihrer Geräte ein, um unberechtigten Zugriff durch Personen, Geräte (wie USB-Sticks) und Software zu erkennen.
- Überwachen Sie Ihr Netzwerk auf unerlaubte Verbindungen.
- Führen Sie eine Untersuchung bei verdächtigen Aktivitäten in Ihrem Netzwerk und Ihren Systemen durch.

Festlegung einer Strategie

4 Reagieren

Erstellen Sie einen **Business Continuity Plan (BCP)**, damit Sie im Falle einer Dienstunterbrechung und/oder eines Angriffs:

- Den Angriff erkennen und eindämmen können.
- Den Angriff den zuständigen Behörden melden können.
- Ihre Kundinnen und Kunden, Teams und Partner, deren Daten möglicherweise offengelegt wurden, benachrichtigen können.
- Die Kontinuität Ihres Geschäftsbetriebs sicherstellen können.
- Schwachstellen beheben und den Betrieb wieder aufnehmen können.
- Aktualisieren Sie Ihre Richtlinien für den Umgang mit Cyber-Risiken.
- Antizipieren Sie mögliche unvorhergesehene Szenarien (z. B. Naturereignisse), die Ihre Daten beschädigen könnten.

Testen und aktualisieren Sie regelmäßig Ihren Geschäftskontinuitätsplan

5 Restaurierung

Nach einem Angriff:

- Identifizierung, Auflistung und Analyse von Schäden (beschädigte Geräte, Datenlecks, kompromittierter Zugang usw.).
- Sicherung und Sanierung Ihrer Arbeitsumgebung und der Geräte, die in Mitleidenschaft gezogen wurden.
- Reparatur und Restaurierung von beschädigten Geräten und Teilen Ihres Netzwerks.
- Halten Sie Ihre Teams, Kundinnen und Kunden sowie Partner über die Fortschritte bei der Restaurierung auf dem Laufenden.

Um Ihnen dabei zu helfen, eine Strategie zum Schutz vor Cyber-Risiken zu entwickeln und diese umzusetzen, sollten Sie sich von einem spezialisierten Unternehmen beraten lassen.

Wussten Sie schon?

Bei einem Cyberangriff dauert es durchschnittlich 22 Tage bis zur vollständigen Restaurierung des Geschäftsbetriebs.

Weitere Informationen finden Sie auf der Website des **Bundesamt für Cybersicherheit (BfCS)** des Bundes.

Physische Sicherheit digitaler Ressourcen

Die Vermeidung von Cyber-Risiken beginnt bei der physischen Sicherheit

Lücken in der physischen Sicherheit können dazu führen, dass sensible Daten offengelegt werden.

Zum Beispiel:

- Ein ungesicherter Computer oder ein ungesichertes Mobiltelefon, das im Zug vergessen wurde.
- Archivmaterial, das in einer Abfallsammelstelle entsorgt wird und für jedermann zugänglich ist.
- Bei einem Einbruch werden Akten und Computerausrüstung entwendet.

Digitale Verantwortung der Unternehmen

Die Sensibilisierung von Mitarbeiterinnen und Mitarbeitern für digitale Verantwortung ist von entscheidender Bedeutung, da sie häufig das verwundbarste Glied in der Kette der Cyberbedrohungen sind und ihre Handlungen sich direkt auf die Sicherheit und den Ruf des Unternehmens auswirken können.

Lesen Sie den Leitfaden zur digitalen Verantwortung der Unternehmen

Wie Sie Ihre Geräte und physischen AKTEN schützen können

- Bewahren Sie Papierakten und elektronische Geräte mit sensiblen Informationen sicher in einem feuerfesten Schrank oder einem geschlossenen Raum auf (Kontaktieren Sie ein spezialisiertes Unternehmen).
- Beschränken Sie den Zugriff auf Ihre Archive, Akten oder Geräte auf befugte Personen und führen Sie über alle Zugriffe Buch.
- Vernichten Sie auf sichere Weise veraltete Akten und Daten. Verwenden Sie einen Aktenvernichter oder beauftragen Sie ein spezialisiertes Unternehmen mit der sicheren Vernichtung von Papierdokumenten oder Datenträgern. Werfen Sie sie nicht einfach weg oder recyceln Sie sie.
- Erinnern Sie Ihre Mitarbeiter regelmässig daran, ihre Arbeitsplätze bei Abwesenheit zu sperren und sensible Dokumente, USB-Sticks, Festplatten, Mobiltelefone usw. nicht unbeaufsichtigt zu lassen.
- Bitten Sie Ihre Teams, ihre Smartphones nach bewährten Verfahren zu sichern, wenn sie diese beruflich nutzen.

Physische Sicherheit digitaler Ressourcen

Die Vermeidung von Cyber-Risiken beginnt bei der physischen Sicherheit

Der Verlust, Diebstahl oder Missbrauch eines Geräts kann schwerwiegende Folgen haben.

Sichern Sie die Daten auf diesen Geräten, indem Sie die folgenden bewährten Verfahren anwenden:

- Verwenden Sie starke Passwörter: Ein starkes Passwort ist lang (mindestens 12 Zeichen), komplex und einzigartig (enthält Sonderzeichen wie !?@#%, Gross- und Kleinbuchstaben und Zahlen).
- Stellen Sie sicher, dass diese Passwörter sicher generiert und gespeichert werden, indem Sie einen Passwortmanager verwenden.
- Erstellen Sie für jedes Konto oder jede Anwendung ein anderes Passwort.
- Unterscheiden Sie zwischen privaten und geschäftlichen Passwörtern.
- Geben Sie Ihre Passwörter niemals weiter.
- Ändern Sie Ihre Passwörter in regelmässigen Abständen.
- Sperren Sie Ihre Geräte mithilfe von Codes.
- Setzen Sie die Multifaktor-Authentifizierung (MFA) für den Zugriff auf Ihr Unternehmensnetzwerk und dessen verschiedene Tools durch (z. B. Einmalpasswort und/oder doppelte Authentifizierung).
- Schalten Sie die Bluetooth-Funktion auf Ihren Geräten aus, wenn Sie sie nicht benötigen.
- Beschränken Sie die Anmeldeversuche auf maximal fünf, um sich vor Eindringlingen zu schützen.
- Verschlüsseln Sie Ihre mobilen Geräte, die sensible Informationen enthalten. Verschlüsseln Sie auch den internen oder externen Austausch mit sensiblen Informationen.
- Bewahren Sie Ihre Verschlüsselungsschlüssel an einem sicheren, von Ihrer Infrastruktur getrennten Ort auf.
- Bevor Sie alte Computer, mobile Geräte, Drucker oder andere elektronische Geräte weiterverkaufen oder verschenken, sollten Sie eine Software zur Datenvernichtung verwenden oder ein spezialisiertes Unternehmen beauftragen.
- Löschen Sie die Daten nicht einfach nur.
- Informieren Sie Ihre Teams regelmässig über Cyber-Risiken und schulen Sie sie, indem Sie ihnen geeignetes Material und Weiterbildungsmöglichkeiten zur Verfügung stellen.
- Fördern Sie gute Sicherheitspraktiken, sei es im Büro oder zu Hause.
- Verbreiten Sie Ihren **Business Continuity Plan (BCP)**. Jedes Teammitglied muss wissen, wen es kontaktieren muss und welche Schritte zu unternehmen sind, wenn Ausrüstung oder Akten verloren gehen oder gestohlen werden.

Sichere Fernzugriffe ermöglichen

Ihre Teams und Partner müssen hohe Sicherheitsstandards einhalten, wenn sie aus der Ferne auf Ihr Netzwerk zugreifen, unabhängig davon, ob es sich um Firmengeräte oder private Geräte handelt.

Geräte bei Fernzugriff schützen

- Sichern Sie Ihren Router: Ändern Sie systematisch die Standardeinstellungen Name und Passwort), und halten Sie die Software auf dem neuesten Stand.
- Verschlüsseln Sie standardmässig alle Daten, die über Netzwerke übertragen werden oder sich auf Geräten befinden, die sich von einem entfernten Standort aus mit Ihrem Netzwerk verbinden.
- Nehmen Sie Einstellungen für Smartphones, Tablets und Laptops vor: Ändern Sie die Standardeinstellungen, um automatische Verbindungen zu drahtlosen Netzwerken zu verhindern.
- Halten Sie die Antivirensoftware auf dem neuesten Stand und planen Sie automatische Updates für alle Geräte, die sich aus der Ferne mit Ihrem Netzwerk verbinden können (einschliesslich Computer und mobile Geräte).

Home-Office

Wenn Sie sich ausserhalb des Unternehmens aufhalten, halten Sie sich an die von Ihrem Unternehmen aufgestellten Richtlinien zur Nutzung von Computer- und Sicherheitstools. Setzen Sie auch zu Hause und unterwegs bewährte Methoden zur Internetsicherheit ein.

Stellen Sie den Teams und Partnern Tools zur Verfügung, mit denen sie ein hohes Sicherheitsniveau aufrechterhalten können

- Stellen Sie sicher, dass jeder Zugriff von einem externen Standort über einen Router erfolgt, der die höchsten Standards für die Verschlüsselung von drahtloser Kommunikation (wie WPA2 oder WPA3) anwendet.
- Verwenden Sie ein Unternehmens-VPN, um Ihren Teams den Fernzugriff auf Ihr Netzwerk zu ermöglichen, um den Datenverkehr zwischen den Geräten und dem Internet zu verschlüsseln.
- Führen Sie die Multi-Faktor-Authentifizierung (MFA) und die Nutzung robuster Passwörter ein.
- Stellen Sie sicher, dass das WLAN-Netzwerk für Gäste vom Firmennetzwerk getrennt ist, und stellen Sie eindeutige Anmeldecodes für Gäste bereit.
- Nehmen Sie Sicherheitsklauseln in alle Verträge mit Partnern auf, die sich mit dem Unternehmensnetzwerk verbinden müssen.

Webhosting

Möchten Sie eine Website erstellen oder aktualisieren?

Wenn Sie nicht über die nötigen Fähigkeiten zur Einrichtung einer Website verfügen, wenden Sie sich an einen Experten für die Erstellung und das Hosting von Websites. Es gibt viele verschiedene Optionen für Webhosting, die Sie entsprechend Ihren Bedürfnissen prüfen sollten. Beim Vergleich von Dienstleistungen sollte die Sicherheit ein zentrales Anliegen sein.

Fragen, die Sie Ihrem zukünftigen Anbieter stellen sollten

- ☐ Ist die Website durch ein TLS-Protokoll gesichert und ist dies im Hosting-Vertrag enthalten?
- ☐ Ich möchte meinen Domainnamen für meine geschäftlichen E-Mail-Adressen nutzen. Können Sie einen Sicherheitsmechanismus wie SPF, DKIM oder DMARC einrichten?
- ☐ Wer ist für die Sicherheits-Updates und die Wartung meiner Website verantwortlich und wie oft werden sie durchgeführt?
- ☐ Wenn die Website einmal online ist, wer hat dann die Rechte zur Verwaltung und Bearbeitung?
- ☐ Wird eine Multifaktor-Authentifizierung für die Personen eingerichtet, die Rechte zur Verwaltung und Bearbeitung der Website haben?

Sichern Sie Ihre Website mit Hilfe von TLS

TLS ist ein Sicherheitsprotokoll, das entwickelt wurde, um eine sichere Kommunikation in einem Computernetzwerk zu ermöglichen. Es wird zur Verschlüsselung der über das Netzwerk übertragenen Daten genutzt und gewährleistet so die Vertraulichkeit und Datenintegrität der Informationen, die zwischen zwei Systemen ausgetauscht werden. Wenn TLS auf Ihrer Website korrekt eingerichtet ist, beginnt Ihre URL mit http**s**://.

Authentifizieren Sie Ihre E-Mail-Adressen

Sie können die E-Mail-Adressen Ihres Unternehmens so einrichten, dass sie den Domainnamen Ihrer Website nutzen (z. B.: masociete. ch / nom@masociete.ch). Um sicherzustellen, dass Betrüger keine E-Mails in Ihrem Namen versenden können, indem sie den Domainnamen Ihrer Organisation missbrauchen, müssen Sie die Echtheit der E-Mails zertifizieren. Dabei können Sie sich auf Verifizierungsmechanismen oder -standards wie Sender Policy Framework (SPF), Domaine Keys Identified Mail (DKIM), Domain-based Message Authentification, Reporting & Conformance (DMARC) beziehen.

Sorgen Sie für die Wartung Ihrer Website

Es muss von Anfang an geklärt werden, wer für die Wartung der Website verantwortlich ist. Diese kann intern oder von einem externen Dienstleister durchgeführt werden, je nachdem, über welche Kompetenzen Sie verfügen. Stellen Sie sicher, dass die Komponenten der Website und die Sicherheit regelmässig aktualisiert werden.

Versicherungen und rechtliche Aspekte

Die Bewältigung eines Cybervorfalls und die Wiederherstellung der Funktionsfähigkeit des Unternehmens ist teuer und komplex

In der Schweiz gibt es Angebote für Cyber-Versicherungen für KMU, die technische Unterstützung, Schutz vor finanziellen Verlusten, Deckung der Haftpflicht und Rechtsbeistand umfassen können. Der Abschluss einer Versicherung entlastet Sie nicht und schützt Sie nicht vor einem Cybervorfall.

Checkliste vor Abschluss einer Cyber-Versicherung

- ☐ Ist die Website durch ein TLS-Protokoll gesichert und ist dies im Hosting-Vertrag enthalten?
- ☐ Führen Sie eine Untersuchung der Aktivitäten des Unternehmens durch, um ein Risikoinventar zu erstellen, dem es je nach Auswirkungsgrad am stärksten ausgesetzt ist.
- ☐ Bestimmen Sie den Umfang des Versicherungsschutzes, den das Unternehmen benötigt.
- ☐ Bewerten Sie die verschiedenen Versicherungsoptionen und wählen Sie diejenige aus, die den Bedürfnissen des Unternehmens in Bezug auf seine Geschäftstätigkeit am besten entspricht.
- ☐ Informieren Sie sich über die Deckungen und Ausschlüsse der einzelnen Policen.
- ☐ Informieren Sie sich über die von der Versicherung abgedeckten Risiken, einschliesslich Datenverlust, Datenschutzansprüche, Datenverletzungen und Rechts- und Geschäftskosten, die durch Verletzungen durch Dritte entstehen.
- ☐ Stellen Sie sicher, dass die Versicherungspolice die Risiken, denen das Unternehmen ausgesetzt sein könnte, abdeckt und dass die Entschädigung der Höhe des versicherten Risikos entspricht.

Unterstützung bei der Risikobewertung finden Sie auf der Plattform der **Digitalen Beobachtungsstelle.**

Rechtsrahmen

In der Schweiz ist die Verwaltung von Cyber-Risiken Teil des Rechtsrahmens, der durch das Gesetz über die Informationssicherheit (ISG) und das Datenschutzgesetz (DSG) geregelt wird.

Die rechtlichen Rahmenbedingungen unterscheiden sich je nach Region und der Art der Geschäftstätigkeit der Unternehmen. Es ist unerlässlich, sich über die geltenden Bestimmungen in den Ländern, in denen das Unternehmen tätig ist, zu informieren, um die geltenden Gesetze einzuhalten.

Weitere Informationen finden Sie im **Leitfaden Globale Datenschutzbestimmungen.**

Wussten Sie schon?

Laut Artikel 19 des Bundesgesetzes über den Datenschutz (DSG) sind Sie verpflichtet, Personen zu informieren, wenn Sie Daten über sie erheben.

Phishing

Wie funktioniert das?

Sie erhalten eine E-Mail oder eine Textnachricht

Sie scheint von einer Ihnen bekannten Person oder Firma zu stammen, die Sie auffordert, per E-Mail oder durch Anklicken eines Links zu antworten, um Details zu Ihrer Identität, Ihrem Passwort oder sensible Informationen über das Unternehmen anzugeben.

Sie sieht authentisch aus

Es ist leicht, Logos zu fälschen und falsche E-Mail-Adressen zu erstellen. In der Regel verwenden Betrüger bekannte Firmennamen oder geben sich als Personen aus, die Sie kennen.

Es ist dringend

Der Absender drängt Sie zu schnellem oder übereiltem Handeln und suggeriert, dass negative Folgen eintreten werden, wenn Sie nicht handeln.

Was als Nächstes passiert

Wenn Sie auf einen Link klicken, können Hacker erkennen, dass Sie auf die Nachricht reagiert haben, und die Aufforderung fortsetzen, um Ihnen Informationen zu entlocken oder Sie zu einer Handlung zu bewegen, z. B. zu einer Geldzahlung.

Wenn Sie eine Nachricht erhalten, die Ihnen verdächtig vorkommt

- **Überprüfen Sie die Adresse des Absenders**
- **Fahren Sie mit der Maus darüber, um die wahre URL zu sehen, bevor Sie darauf klicken**
- **Antworten Sie nicht auf diese Nachricht**
- **Geben Sie niemals Ihre Identität preis**
- **Geben Sie niemals Bankdaten weiter**
- **Überweisen Sie niemals Geld**
- **Öffnen Sie keine Anhänge**

Melden Sie betrügerische Nachrichten auf der Plattform des Bundesamts für Cybersicherheit (BfCS): https://www.ncsc.admin.ch/

Melden Sie es!

Wenn Sie eine Phishing-E-Mail erhalten oder eine Phishing-Website entdeckt haben, melden Sie dies unter **https://antiphishing.ch**

Testen Sie Ihre Teams!

Führen Sie regelmässig interne Tests durch, um das Bewusstsein und das Verständnis der Mitarbeiterinnen und Mitarbeiter für Cyber-Risiken und die Herausforderungen für das Unternehmen zu ermitteln, z. B. mithilfe einer Fake-Phishing-Kampagne.

Fallbeispiel

Ein Klick genügt…

Wenn jemand auf einen betrügerischen Link klickt, der die Installation von Ransomware ermöglicht, wird das gesamte Unternehmensnetzwerk blockiert und die Daten werden als Geiseln genommen. Hacker fordern ein Lösegeld in Form einer Banküberweisung oder einer Kryptowährung, um den Zugriff auf die Daten wieder freizugeben.

In der Zwischenzeit ist der Betrieb des Unternehmens blockiert. Die für den Betrieb erforderlichen Daten, sensible Informationen über Kunden, Teams und Geschäftsaktivitäten geraten in die Hände von Hackern.

Nahezu 80% der Cybervorfälle sind auf menschliches Versagen innerhalb des Unternehmens oder im Zusammenhang mit seinen Partnern zurückzuführen.

Das Bundesamt für Cybersicherheit (BfCS) empfiehlt, in jedem Fall eine Strafanzeige zu erstatten. Nehmen Sie Kontakt mit der Kantonspolizei auf. Die nächstgelegene zuständige Polizeistation finden Sie auf der Website ***„Suisse e-Police“.***

Wie funktioniert ein Computervirus?

Es gibt mehrere Möglichkeiten, Malware in ein System einzuschleusen:

- Durch betrügerische E-Mails mit Links oder Anhängen, die Ihre Daten und Ihr Netzwerk gefährden. Diese Phishing-E-Mails (oder Phishing – siehe vorherige Seite) sind die Ursache für die meisten Angriffe mit Lösegeldforderungen (oder Ransomware).
- Durch den Besuch infizierter Websites, das Scannen eines QR-Codes oder das Anklicken von Links, die automatisch Schadsoftware auf Ihren Computer oder Ihr Smartphone herunterladen.
- Durch die Verbindung eines externen Geräts oder Computers des Unternehmens mit Ihrem Netzwerk oder Ihren Computern (USB-Stick, Festplatte, Smartphone usw.).
- Durch das Ausführen ungeprüfter oder nicht genehmigter Anwendungen.
- Indem Sie das Öffnen externer Links oder das Starten von Makros beim Zugriff auf Dokumente erlauben, die Ihnen von einer Person ausserhalb der Organisation übermittelt wurden.

Was tun, wenn eine Lösegeldforderung eingeht?

Das **BfCS** rät davon ab, Lösegeld zu zahlen, da Sie keine Garantie dafür haben, dass Sie Ihre Daten zurückerhalten. Darüber hinaus trägt das Nachgeben gegenüber Erpressungen zur Finanzierung krimineller Aktivitäten bei und ermutigt Kriminelle, ihre Aktivitäten fortzusetzen oder neu zu starten.

Verhindern von Angriffen und deren Folgen

Erstellen Sie einen Kontinuitätsplan

Dieser Plan ermöglicht es Ihnen, Ihr Unternehmen im Falle eines Cyberangriffs oder eines Cybervorfalls am Laufen zu halten. Halten Sie diesen Plan schriftlich fest, kommunizieren Sie ihn intern und testen Sie ihn in regelmässigen Abständen.

Sensibilisieren Sie Ihre Teams für Social Engineering

Schulen und informieren Sie Ihre Teams über die verschiedenen Manipulationstechniken, die genutzt werden können, um eine Person dazu zu bringen, selbst Informationen weiterzugeben, unabhängig davon, ob es sich um sensible Informationen handelt oder nicht. Diese Daten können persönliche Informationen oder vertrauliche Informationen sein, die den Zugang zum Computernetzwerk einer Organisation ermöglichen. Dabei werden Techniken eingesetzt, die den menschlichen Faktor ausnutzen, z. B. durch Identitäts- oder Rollentäuschung einer Person oder einer Organisation.

Bevor Sie auf einen fragwürdigen Link klicken ...

- Überprüfen Sie, ob der Domainname wirklich existiert und ob er zu dem passt, was Sie sich ansehen möchten.
- Überprüfen Sie, ob die Website sicher ist: Die URL muss mit https beginnen (das „s“ in „https “ bedeutet, dass die Informationen verschlüsselt werden), und kontrollieren Sie, ob das Zertifikat nicht abgelaufen oder ungültig ist (das Vorhängeschloss neben der URL darf nicht durchgestrichen sein).
- Vergewissern Sie sich, dass Sie sich an eine echte und vertrauenswürdige Person oder Organisation wenden und dass Sie nicht im Begriff sind, Schadsoftware herunterzuladen oder Ihren Zugang mit einem Betrüger zu teilen.
- Wenn Sie sich unsicher sind, sprechen Sie mit anderen darüber. Dies hilft Ihnen dabei, festzustellen, ob die Anfrage echt ist oder ob es sich um einen Phishing-Versuch handelt.
- Wenn Sie dennoch Zweifel haben, rufen Sie direkt beim betreffenden Anbieter oder bei der Person an, die Ihnen angeblich die E-Mail geschickt hat. Seien Sie misstrauisch gegenüber der Nummer, die in der Nachricht steht, und verwenden Sie stattdessen Ihr Telefonbuch.

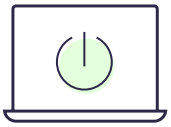
Seien Sie proaktiv!

Wussten Sie schon?

Bei einem Cyberangriff dauert es durchschnittlich 22 Tage bis zur vollständigen Restaurierung des Geschäftsbetriebs.

Vorgehen im Falle eines Angriffs

1 Schadensbegrenzung



- Schalten Sie die internen (WLAN und LAN) und externen (WAN/Internet) Netzwerke ab.
- Identifizieren Sie den infizierten Computer oder die infizierten Geräte und schalten Sie sie aus. Sollten Sie sie nicht schnell identifizieren können, führen Sie diese Schritte für den gesamten Computerbestand durch.
- Ändern Sie alle Passwörter.
- Führen Sie eine Überprüfung aller Geräte (Computer und Server) durch oder lassen Sie diese durchführen, um sicherzustellen, dass sie nicht infiziert sind.

2 Geben Sie eine Warnung aus

- Befolgen Sie die vom Unternehmen eingerichteten Verfahren, um Ihren IT-Manager oder -Dienstleister zu benachrichtigen.
- Warnen Sie Ihre Kollegen und teilen Sie Ihre Erfahrungen mit Phishing-Versuchen, da diese häufig mehr als eine Person in einem Unternehmen betreffen.

3 Melden Sie den Betrug

- Wenn persönliche Daten oder Informationen kompromittiert wurden, benachrichtigen Sie die betroffenen Personen.
- Melden Sie betrügerische Nachrichten auf der Plattform des **Bundesamts für Cybersicherheit (BfCS)**.
- Erstatten Sie im Falle eines Verstosses Anzeige bei der Polizei.

4 Kommunikation

- Halten Sie Ihre Mitarbeiterinnen und Mitarbeiter, Partner, Kunden auf dem Laufenden.

Beziehen Sie sich auf das Bundesgesetz über die Informationssicherheit (ISG)

Artikel 74b listet die Behörden und Organisationen auf, die der Pflicht zur Meldung eines Cyberangriffs unterliegen. Dies betrifft zahlreiche Unternehmen aus verschiedenen Branchen.

Vorschlag für eine Strategie zur Sicherung der Daten

Bei der Datensicherung oder dem Backup werden die Informationen, die für den reibungslosen Betrieb des Unternehmens notwendig sind, auf einem Datenträger und/oder einem externen Speicherplatz dupliziert und so gesichert, dass im Falle eines Cybervorfalls darauf zugegriffen werden kann. Ohne Datensicherung ist es nicht möglich, die Daten eines Unternehmens zu restaurieren.

Einrichten eines Sicherungsplans

1

Kartografieren Sie Ihre Daten

- Machen Sie eine Bestandsaufnahme aller Daten, über die Sie verfügen.
- Beurteilen Sie die Wichtigkeit der Daten für die Geschäftstätigkeit des Unternehmens.
- Organisieren und kategorisieren Sie diese Daten.
- Definieren Sie den Speicherort der Daten: Erfassen Sie, welche Einrichtungen die Daten nutzen und wo sie gespeichert sind.
- Ermitteln Sie, wer und welche Systeme Zugriff auf diese Daten haben.

2

Hierarchisierung der Daten

Ordnen Sie Ihre Daten nach ihrer Wichtigkeit. Stellen Sie sich dazu die folgenden Fragen:

- Welche Dateien und Informationen sind für das Funktionieren der Organisation insgesamt und für jede ihrer Abteilungen oder Bereiche unerlässlich? (Zum Beispiel: Buchhaltung, Kontakte, Kundenkarten, Terminkalender, Personalwesen, Strategie- und Geschäftsdokumente usw.).
- Welche Daten und Dokumente sind unverzichtbar und können bei Verlust, Diebstahl oder Zerstörung der Ausrüstung nicht wiederhergestellt werden?

3

Legen Sie Speicherorte für die Sicherung fest

Für eine gute Backup-Strategie und eine schnelle Restaurierung der Unternehmensdaten sollten Sie Ihre Daten an drei verschiedenen Orten sichern:

- **Speicherung auf einer Backup-Lösung innerhalb der Organisation (z. B. Backup-Server)**
- **Offline-Speicherung auf einer Festplatte innerhalb der Organisation, auf die schnell zugegriffen werden kann (z. B. in einem gesicherten Raum)**
- **Speicherung auf einem Laufwerk, das sich ausserhalb der Organisation befindet (z. B. in einem Bankschliessfach)**

Für mehr Sicherheit und Unabhängigkeit können Sie eine zusätzliche Sicherung auf einem NAS (Mini-Dateiserver), einem SAN (Sicherungslösung, die für mittlere und grosse Unternehmen geeignet ist), in einer Cloud oder einem Rechenzentrum durchführen.

Achten Sie bei der Speicherung in einer Cloud darauf, wo sich die Server befinden, auf denen die Daten gehostet werden, welche rechtlichen Verpflichtungen das Unternehmen in Bezug auf das Hosting der Daten hat und welche Gesetze in den einzelnen Ländern gelten. Die Nutzung einer Cloud, die die Daten im Inland speichert und verarbeitet, wird empfohlen.

Vorschlag für eine Strategie zur Sicherung der Daten

4 Stellen Sie einen Zeitplan für die Datensicherung auf

Es ist wichtig, die Daten in regelmässigen Abständen zu sichern. Legen Sie eine Häufigkeit fest, die zu den Aktivitäten Ihrer Organisation passt.

Sie können beispielsweise eine tägliche Sicherung einrichten, die durch wöchentliche und monatliche Sicherungen ergänzt wird. Überprüfen und testen Sie regelmässig die Sicherungsarchive sowie die Prozesse zur Restaurierung.

Mithilfe dieses Kalenders können Sie Ihre Daten im Falle eines Vorfalls einfach und schnell wiederherstellen und dabei einen minimalen oder gar keinen Verlust erleiden.

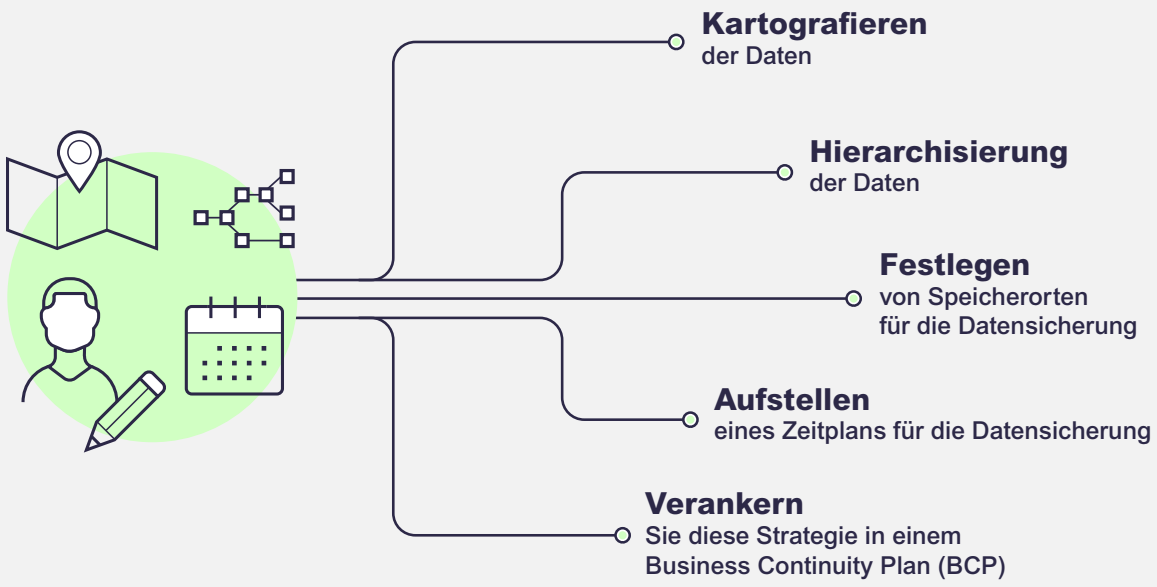
5 Verankern Sie diese Strategie in einem Business Continuity Plan (BCP)

Der BCP beschreibt, wie Sie die Kontinuität Ihres Geschäfts aufrechterhalten können, um Unterbrechungen und Betriebsstörungen zu minimieren (siehe Seite 5).

Darin wird unter anderem festgelegt, wie Daten im Falle eines IT-Vorfalls gesichert und restauriert werden können.

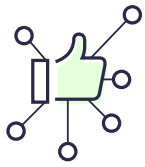
Die Sicherungsstrategie ist daher ein wesentlicher Teil davon, da sie bestimmt, wie die IT-Abteilung wieder in Betrieb genommen werden kann, um die Geschäftsaktivitäten wieder aufzunehmen.

Sicherungsplan



Zusammengefasst

Schlechte Praktiken



- Glauben, dass Cybersicherheit nur ein IT-Problem ist.
- Einführung neuer Technologien und digitaler Praktiken ohne vorherige Analyse der Risiken und Chancen.
- Unterschätzen des Risikos von Auswirkungen oder der Wahrscheinlichkeit eines Cyber-Vorfalls.
- Vernachlässigung der Bedeutung eines Kontinuitätsplans und einer Strategie zur Datensicherung.
- Sammeln und verarbeiten von mehr Informationen als nötig.

Bewährte Praktiken zum Schutz Ihrer Geräte, Ihres Netzwerks und Ihrer Daten

- Halten Sie Ihre Software auf dem neuesten Stand.
- Sichern Sie Ihren WLAN-Router mit einer WPA2- oder WPA3-Verschlüsselung.
- Sichern Sie Ihre Daten regelmässig.
- Fordern Sie starke und eindeutige Passwörter für alle Geräte und Zugänge.
- Aktivieren Sie eine Multi-Faktor-Authentifizierung.

Bewährte Praktiken zum Schutz Ihrer Mitarbeiterinnen und Mitarbeiter, Ihres Unternehmens, Ihrer Kundinnen und Kunden und Ihrer Partner

- Legen Sie eine Richtlinie fest, wonach der Zugriff auf Ressourcen standardmässig eingeschränkt und nur den entsprechenden Personen gestattet wird.
- Beschränken Sie die Informationen, die auf Ihrer Unternehmenswebsite veröffentlicht werden. Vermeiden Sie Informationen, die Rückschlüsse auf Personen und ihre Rolle im Unternehmen zulassen, um Identitätsdiebstahl oder Social-Engineering-Manöver zu verhindern.
- Schulen Sie Ihre Teams, indem Sie ihnen geeignetes Material sowie interne oder externe Weiterbildungsmöglichkeiten zur Verfügung stellen.

Die Sicherheit Ihres Unternehmens steht an erster Stelle!
Lassen Sie sich von Spezialisten beraten.