Helvetia Cyber-Versicherung

helvetia.ch/cyber-versicherung

Cyber-Risiken.
IT gehackt.
Gedeckt.

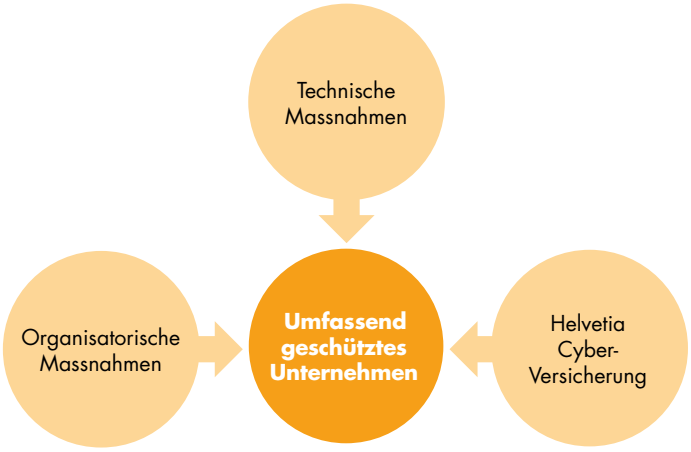
einfach. klar. helvetia

Ihre Schweizer Versicherung

Risiken vorbeugen und Unternehmen wirksam schützen.

Wie können Sie sich vor Cyber-Risiken schützen?
Mittels technischer und organisatorischer Sicherheitsmassnahmen lässt sich das Risiko von Cyber-Schäden beträchtlich einschränken. Das Bundesamt für Cybersicherheit (BACS) publiziert dazu jeweils Empfehlungen für KMU. Auf der Basis dieser Empfehlungen und in Zusammenarbeit mit dem eigenen Expertennetzwerk hat Helvetia einen Sicherheitskatalog entwickelt, den jedes Unternehmen zur eigenen Sicherheit einhalten sollte (siehe Checkliste Seite 4).

Risikominimierung dank der Helvetia Cyber-Versicherung
Auch eine gewissenhafte Einhaltung jeglicher Sicherheitsvorkehrungen garantiert keinen absoluten Schutz vor den vielfältigen Cyber-Risiken. Die Helvetia Cyber-Versicherung nimmt sich der Gefahren an, die über technische und organisatorische Sicherheitsmassnahmen nicht abgedeckt werden können, und ergänzt so das Risikomanagement eines jeden Unternehmens optimal.



Schutz vor Cyber-Risiken dank Prävention
Übersicht der Helvetia Cyber-Security-Services:
- Cyber Security Check
- Cyber-Alert (Warnung vor Cybergefahren)
- Online-Sicherheitstrainings
- Ratgeber
- Kostenlose & vergünstigte Partnerangebote
  helvetia.ch/cyber-prävention

Ihre Vorteile auf einen Blick

- Bedeutende Ergänzung für ein umfassendes Cyber-Security-Management
- Absicherung von ausserordentlichen, nicht kalkulierbaren Kosten
- Schutz vor Gewinnausfall
- Spezialdeckung für digitalisierte Produktionsunternehmen (Industrie 4.0)
- Unterstützung bei Datenschutzverletzungen bzw. Haftpflichtansprüchen Dritter
- Zugang zu einem Expertennetzwerk im Schadenfall, bestehend aus Spezialisten der IT-Security, PR-Beratern, Rechtsberatern und Datenschutzspezialisten
- Schnelle und professionelle Hilfe durch Experten bei einem Cyber-Schadenfall (24/7-Cyber-Schadenhotline)

Helvetia Cyber-Versicherung.
Umfassend geschützt vor Cyber-Risiken.

Die Digitalisierung beeinflusst die heutigen Geschäftsprozesse und ist aus keiner Branche mehr wegzudenken. Mit der damit einhergehenden zunehmenden Vernetzung steigen aber auch die Cyber-Risiken, welchen Ihr IT-System ausgesetzt ist. Für viele Unternehmen gewinnt deshalb der Schutz gegen Cyber-Risiken an Bedeutung.

Schutz vor den Folgen von Cyber-Kriminalität und von nicht kriminellen Ursachen

Als Unternehmen ist es unerlässlich, seine digitalen Daten und Software vor Cyber-Kriminalität zu schützen. Leider gelingt es Kriminellen immer wieder, Lücken auszunutzen. Sie verschaffen sich unautorisierten Zugriff zu vertraulichen Daten, verschlüsseln, zerstören oder stehlen diese, installieren Schadsoftware oder blockieren den Zugriff zum IT-System. Aufgrund von Datenschutz- oder Persönlichkeitsverletzungen können sich für Unternehmen teure Rechtsstreitigkeiten ergeben.

«Da sich Cyber-Risiken ähnlich wie Grippeviren ständig verändern, können auch sehr gute organisatorische und technische Sicherheitsmassnahmen alleine keinen vollständigen Schutz garantieren. Die Cyber-Versicherung bietet die optimale Ergänzung, um diese Lücken zu schliessen.»

Risiken im Cyber-Bereich müssen nicht zwingend krimineller Natur sein. Häufig genügt ein Moment der Unachtsamkeit, und schon geraten heikle Daten unbeabsichtigt in falsche Hände oder gehen verloren. Oder eine kurzzeitige Stromunterbrechung bzw. eine Spannungsschwankung führt zu einem Verlust von Daten. Genau in solchen Fällen sind wir für Sie da.

Wir entschädigen Vermögensschäden und Kosten, die im Zusammenhang mit folgenden Cyber-Risiken entstehen

Diese Gefahren werden verursacht durch

- interne Sabotagen eigener Mitarbeitenden
- Ausnutzung technischer System- oder Sicherheitsschwächen
- Installation und Ausführung von Schadsoftware
- unautorisiert eingesetzte Hardware
- Verwendung von gestohlenen Zugriffsinformationen
- DoS-Attacken
- fahrlässige Bedienung durch eigene Mitarbeitende
- kurzzeitige Störungen

Überprüfen Sie Ihren Sicherheitszustand.
Haben Sie an diese Punkte gedacht?

Gemäss schweizerischem Datenschutzgesetz (DSV, Art. 3) wie auch der EU-Datenschutzverordnung (DSGVO, Art. 32) sind Unternehmen **gesetzlich verpflichtet**, geeignete technische und organisatorische Massnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Helvetia hat in Anlehnung an die Empfehlungen des Bundesamts für Cybersicherheit (BACS) und gemeinsam mit diversen IT-Security- und Datenschutzspezialisten Sicherheitsmassnahmen erstellt, welche jeder Versicherungsnehmer und jede Versicherungsnehmer:in auch zum eigenen Schutz, einhalten soll.

Besprechen Sie mit Ihrer internen oder externen IT-(Security)Verantwortlichen Person, ob die folgenden Punkte für Ihr Unternehmen relevant sind und ob diese bereits umgesetzt wurden beziehungsweise wann dies noch nachgeholt werden wird.

☐ Organisatorische und technische Sicherheitsvorschriften

Als Versicherungsnehmer:in einer Helvetia Cyber-Versicherung sind Sie verpflichtet, gesetzlich geforderte Massnahmen zur Schadenverhütung zu ergreifen.

Zusätzlich sind abhängig von Grösse und Art des Betriebs entsprechend Mindestanforderungen zur Schadenverhütung zu erfüllen.

a. organisatorische Massnahmen

☐ Definition und Implementierung eines Berechtigungsmanagements mit angemessen abgestuften Befugnissen (z.B. funktionsbedingter Zugriff auf Finanz-, Personal- oder Kundendaten)

☐ Definition und Implementierung einer Zugriffsrichtlinie (Access Policy)

☐ Regelmässige Sensibilisierung und Sicherheits-Trainings der versicherten Personen zum Thema Cyber-Risiken

Auf der Website von Helvetia steht Ihnen ein kostenloses Sicherheitstraining für Ihre Mitarbeitenden zur Verfügung.
- helvetia.ch/cyber-prävention

b. technische Massnahmen

☐ Tägliche Datensicherung (Back-up) inkl. automatischem Funktionscheck (Monitoring). Das Back-up darf frühestens nach einer Woche überschrieben werden. Die Qualität der Datensicherung ist mindestens halbjährlich zu prüfen (z.B. Datenmengenvergleich, Datenstichprobe auf Funktionalität). Die Daten auf den Back-ups sind so aufzubewahren, dass sie nicht zusammen mit den Originalen manipuliert, beschädigt, zerstört oder entwendet werden können (z.B. Offline-Back-up, unveränderbare Cloud-Back-ups). Zudem muss jederzeit gewährleistet sein, dass entweder auf die originalen Daten oder die Back-up Daten Zugriff besteht.

☐ Installation aktueller, dem Stand der Technik entsprechender, grundlegender technischer Schutzmassnahmen wie Firewalls, Virenscanner, Spam-Filter, authentisierte Remote-Zugänge (z.B. VPN)

☐ Ein Patch- und Update-Management, welches sicherstellt, dass die aktuellen Sicherheits-Updates/Patches zeitnah installiert werden (d.h. spätestens nach 30 Tagen, ausser die Sicherstellung der Patch-Kompatibilität benötigt einen höheren Zeitaufwand). Software/Systeme für die keine Sicherheits-Updates/Patches verfügbar sind, müssen isoliert werden.

☐ Technische Umsetzung der definierten Zugriffsrichtlinien (Access Policy) und des Berechtigungsmanagements

☐ Der Versand von besonders schützenswerten Daten muss verschlüsselt werden (z.B. mittels VPN, HTTPS, verschlüsselte E-Mail, verschlüsselte Datenträger).

☐ Die Regeln des PCI-DSS sind einzuhalten, sofern Kredit- oder Debitkarten-Transaktionen durchgeführt werden.

☐ Netzwerkübergang zwischen Information Technology (IT) und Operating Technology (OT*)

Falls ein Netzwerkübergang (logische oder physische Schnittstellen) zwischen IT und OT besteht, ist sicherzustellen, dass dieser geschützt ist. Dies hat mittels aktueller und dem Stand der Technik entsprechender technischer Schutzmassnahmen wie Firewalls, Virenscanner und Zugriffsschutzprogramme zu erfolgen. Das Netzwerk soll eine klare Trennung zwischen IT- und OT-Umgebung aufweisen (Netzwerkssegmentierung).

*OT = Maschinen-, Anlagen- und Geräte-Steuerungen, z.B. Steuerungen von medizinischen Geräten, die ans Netzwerk angebunden sind.

☐ Datenschutzerklärung bei eigenen Websites und Anwendungen von Analysetools

Besitzt Ihr Unternehmen eine Website, so sind Sie verpflichtet, auf dieser eine Datenschutzerklärung gemäss anwendbaren datenschutzrechtlichen Vorschriften zu implementieren, wenn durch Ihre Website Personendaten bearbeitet werden (z.B. durch Cookies).
Beim Einsatz von Analysetools (z.B. Google Analytics) ist sicherzustellen, dass die datenschutzrechtlichen Vorgaben (z.B. Anonymisierung von IP-Adressen) eingehalten werden.

☐ Externe Dienstleistende und andere Dritte

Falls Dritte (z.B. Lieferantinnen und Lieferanten) Zugriff auf Ihr IT-System und Ihre digitalen Daten haben und/oder Sie mit externen Dienstleistenden im Zusammenhang mit digitalen Daten zusammenarbeiten, ist sicherzustellen, dass diese die jeweils anzuwendenden Datenschutzgesetze und weitere anwendbare gesetzliche Vorgaben einhalten. Die Zusicherung Ihrer Geschäftspartnerinnen und Geschäftspartner sollte Ihnen schriftlich vorliegen.

Bei der Verwendung von betriebskritischen Cloud-Diensten* muss gewährleistet sein, dass die externen Dienstleister, die diese Dienste anbieten, über einen Notfallplan und einen Business Continuity Plan (BCP) verfügen und damit eine schnelle Wiederaufnahme des Betriebs ermöglichen.

*Cloud-Dienste, die für zentrale Geschäftsprozesse verwendet werden und von derer Verfügbarkeit mehr als 30% des jährlichen Umsatzes/Betriebsertrags abhängen, gelten als betriebskritisch.

☐ Periodische Prüfung

Alle Sicherheitsmassnahmen müssen periodisch überprüft werden. Es ist zwingend, dass die Technik wie auch die organisatorischen Massnahmen stets auf dem aktuellsten Stand sind.

Leistungen von Helvetia auf einen Blick.

Übersicht der Leistungen innerhalb der verschiedenen Pakete

	Light	Standard	Premium
Eigenschäden			
System-, Daten- und Softwarewiederherstellung	✓	✓	✓
Mehrkosten zur Weiterführung der Datenverarbeitung	✓	✓	✓
Gewinnausfall infolge Betriebsunterbruch		✓	✓
Notfallhilfe und Schadensanalyse/Forensik		✓	✓
Notifikationsmanagement			✓
Krisen- und Reputationsmanagement			✓
Unterstützung bei Cyber-Erpressung			✓
Vermögensausgleich infolge Cyber-Betrug oder Manipulation (Kompromittierung)			✓
Mangelhafte Produktion		(✓)	(✓)
Haftpflichtschäden			
Reine Vermögensschäden und immaterielle Schäden		✓	✓
Rechtsschutz		✓	✓

Kombination von Eigenschäden, Haftpflichtschäden und Rechtsschutz
Die Helvetia Cyber-Versicherung deckt im Schadenfall sowohl Eigen- wie auch Haftpflichtschäden und Kosten für den Rechtsschutz.

Aufgrund der Komplexität und der Vielfalt möglicher Schadenereignisse hat Helvetia drei Leistungspakete definiert (Light, Standard und Premium), die den unterschiedlichen Bedürfnissen der Unternehmen gerecht werden sollen. Jedes dieser Pakete kombiniert mehrere Leistungen für die Bereiche Eigenschäden, Haftpflichtschäden und Rechtsschutz.

Die individuelle Auswahl eines Leistungspakets ermöglicht einen optimal auf die Risikosituation und das Schutzbedürfnis eines Unternehmens ausgerichteten Versicherungsschutz.

Im Schadenfall wie auch bei der Risikoberatung können Sie auf unsere Unterstützung und unser kompetentes Expertennetzwerk zählen
- Krisen-/PR-Beratung
- IT-/OT-Security
- Datenschutz-/Rechtsberatung

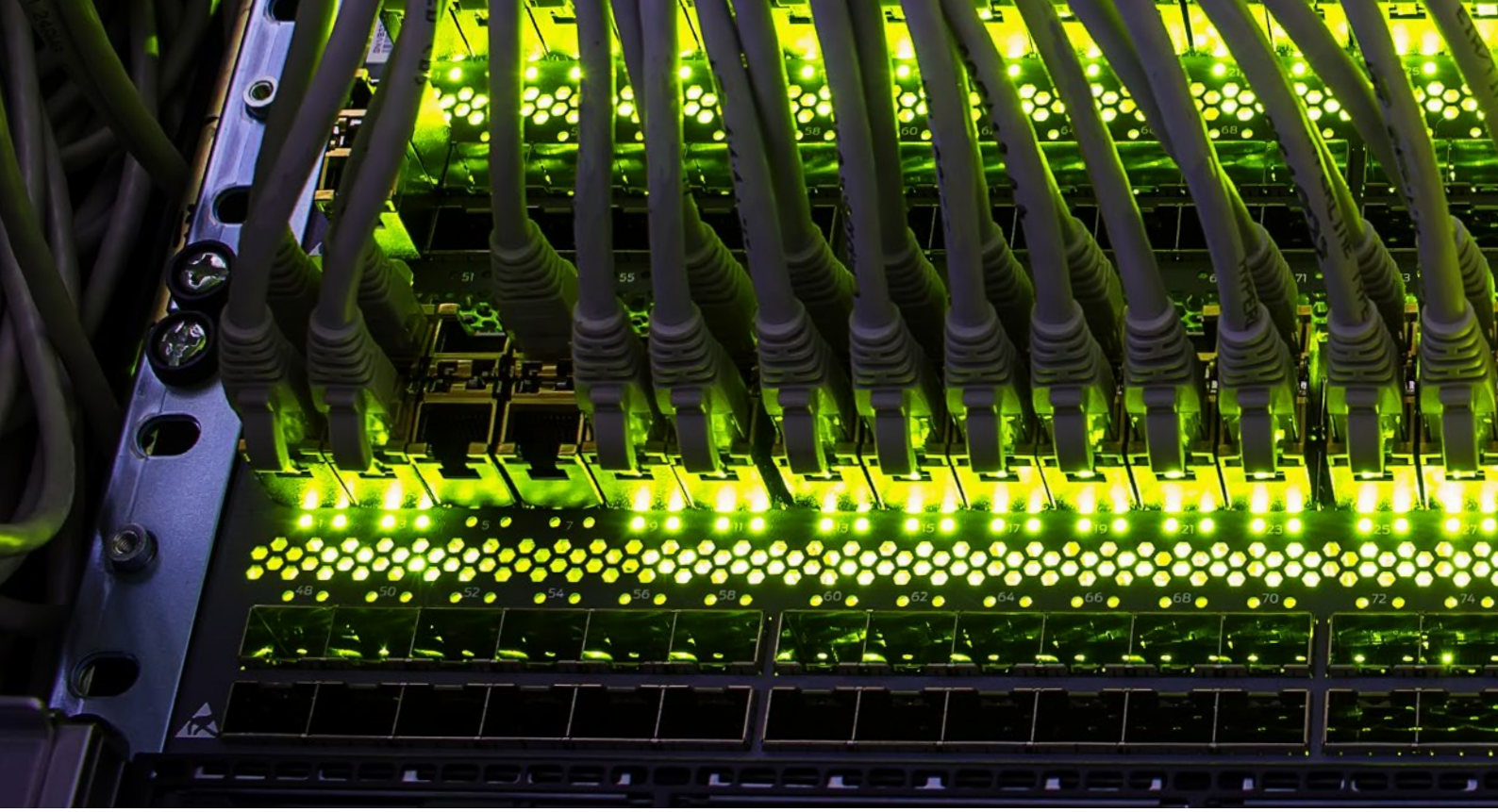
helvetia.ch/cyber-versicherung

Gut zu wissen

Für KMU bietet Helvetia auf ihrer Website einen Cyber Security Check zur Risikobewertung an. Ausserdem finden sich Tipps und Empfehlungen, wie ein Unternehmen den Schutz vor Cybergefahren erhöhen kann.

Ebenso steht ein kostenloses Sicherheits-Training zur Verfügung. Mitarbeitende können dadurch u.a. den korrekten Umgang mit vertraulichen Daten lernen, wie eine betrügerische E-Mail erkennbar ist und worauf beim Arbeiten in der Öffentlichkeit geachtet werden soll.

Und im Schadenfall hilft Ihnen unser kostenloser Schadenservice 24 Stunden/7 Tage die Woche.



Schadenbeispiele.

Verschlüsselung von Daten in einer Cloud

Ein Unternehmen speichert sämtliche Daten in einer externen Cloud. Einem Hacker gelingt es, in diese Cloud einzudringen und mittels **Ransomware** alle darin gespeicherten Daten zu verschlüsseln. Das Unternehmen hat nun keine Möglichkeit mehr, auf seine Daten zuzugreifen und erleidet dadurch einen Produktionsunterbruch.

Weil auch eine externe Cloud zum IT-System eines Unternehmens gehört, übernimmt Helvetia die daraus entstehenden Kosten aus

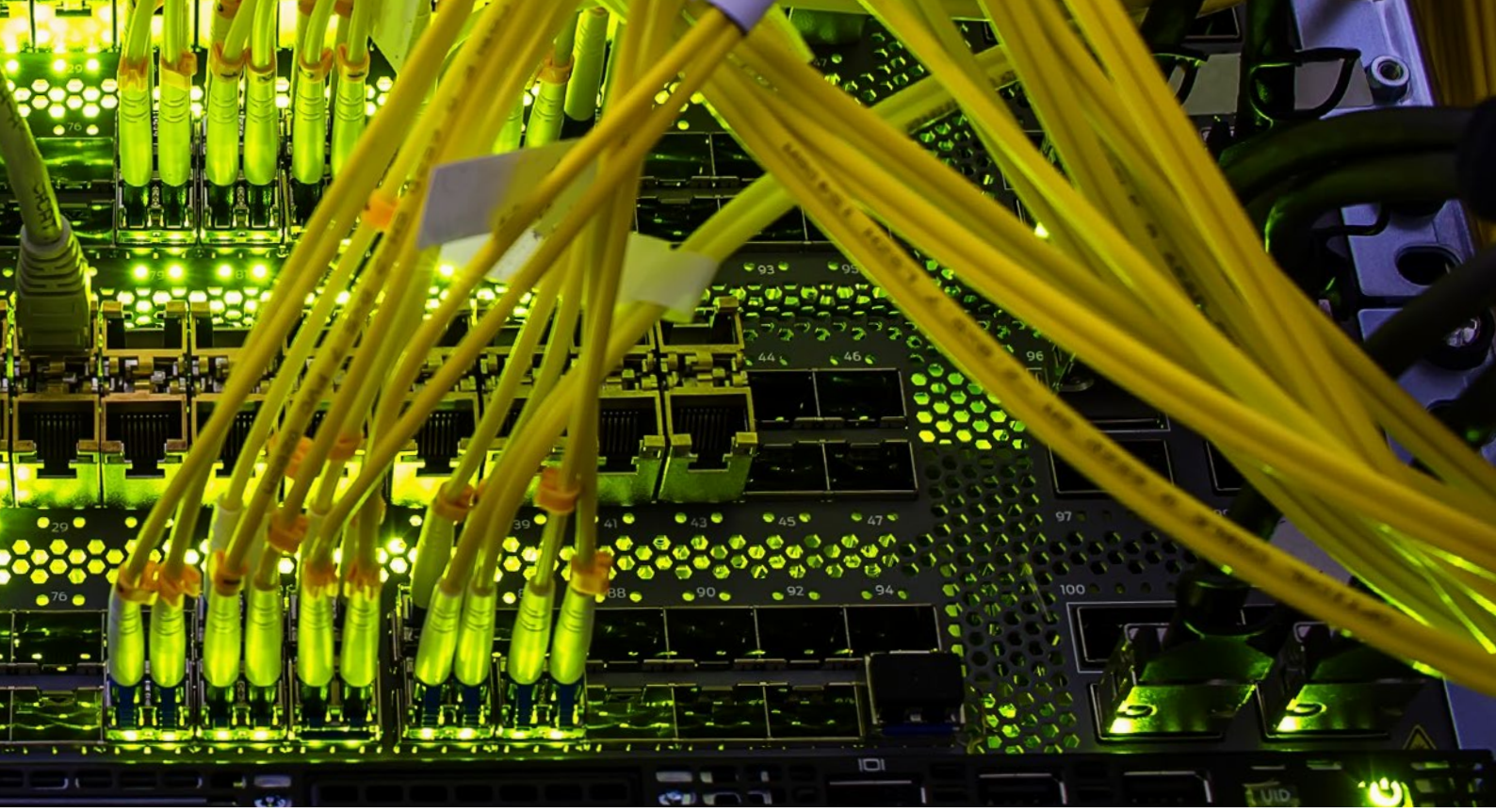
- der Wiederherstellung der Daten aus dem Back-up
- der manuellen Rekonstruktion derjenigen Daten, die technisch nicht mehr über das Back-up hergestellt werden können
- dem Mehraufwand zur Aufrechterhaltung des Betriebs
- dem Gewinnausfall aufgrund des Betriebsunterbruchs
- der Schadensanalyse inkl. Forensik

Firmentelefonanlage manipuliert

Ein Hacker dringt in das Telekommunikationssystem eines Unternehmens ein **(Phreaking)** und manipuliert es so, dass Dritte auf Kosten des Unternehmens ständig teuer ins Ausland telefonieren. Nichtsahnend erhält das Unternehmen am Ende des Monats eine überraschend hohe Telefonrechnung von mehreren Zehntausend Franken.

Helvetia kommt für den Vermögensschaden auf, der aufgrund der manipulierten Telefonanlage verursacht wurde.

Die hier beispielhaft aufgeführten Leistungen im Schadenfall sind abhängig vom gewählten Leistungspaket.



OT-Steuerungen gehackt

Mittels einer betrügerischen E-Mail (Social Engineering) gelangt ein Hacker an die Nutzerdaten von zahlreichen Mitarbeitenden **(Phishing)** eines hochdigitalisierten Produktionsbetriebs. Dadurch gelingt es ihm, in das Maschinennetzwerk der Firma einzudringen und einige Parameter zu verändern. Da die Manipulation nicht sofort bemerkt wird, fällt eine Maschine aus, und es entsteht eine fehlerhafte Produktionsreihe.

Helvetia trägt die

- Kosten für die Analyse des Schadens und die Wiederherstellung der korrekten Parametrisierung
- Mehrkosten zur Aufrechterhaltung des Betriebes
- Vermögenseinbussen aufgrund der mangelhaften Produktionsserie

Was ist mit OT-Steuerungen gemeint?

Unter OT-Steuerungen (Operational-Technology-Steuerungen) fallen verschiedenste Steuersysteme (wie z.B. Steuersysteme der Medizin-, Heiz-, Kühl- und Messtechnik oder Leitsysteme, die für Produktion, Materialbewegung und Manipulation, Verarbeitung usw. eingesetzt werden) sowie elektronische Steuerungen, die integraler Bestandteil einer Maschine oder Anlage sind.

Vertrauliche Patientendaten entwendet

Ein Arzt hat seine Patientendaten auf seinem eigenen Server gespeichert. Trotz einer umfangreichen Sicherheitseinrichtung gelingt es einem Hacker, mittels einer manipulierten E-Mail einen **Trojaner** im System zu platzieren. Da der Vorfall erst nach einigen Wochen bemerkt wird, kann er in aller Ruhe die gesamten vertraulichen Patientendaten kopieren.

Helvetia trägt die anfallenden Aufwendungen für

- Schadenanalyse und Entfernung der Schadsoftware
- Notfallmassnahmen, falls es zu einer Erpressung kommt
- eine rechtliche Notifikation der betroffenen Personen aufgrund einer möglichen Datenschutzverletzung
- das Reputationsmanagement, damit das Vertrauen der Patienten wiederhergestellt werden kann
- mögliche Genugtuungsforderungen der Patienten
- ein behördliches Datenschutzverfahren

Online-Shop lahmgelegt

Durch eine **DoS-Attacke** auf einen Online-Shop eines Schuhfachgeschäfts können Kundinnen und Kunden vorübergehend nicht mehr auf die Website zugreifen. Nach wenigen Tagen kann der Angriff mit Hilfe eines IT-Spezialisten abgewehrt werden. Bis zur Installation der Abwehrmassnahmen entsteht während der ertragsreichen Weihnachtszeit dennoch ein Gewinnausfall für das Schuhfachgeschäft.

Helvetia übernimmt folgende Leistungen

- Mehrkosten zur Aufrechterhaltung des Betriebes (z.B. durch Blackholing, Installation eines Geofilters oder Aufschaltung einer Disaster Recovery Site)
- Gewinnausfall aufgrund des blockierten Online-Shops und des daraus resultierenden Verkaufsunterbruchs
- Schadensanalyse inkl. Forensik
- Kosten für das Reputationsmanagement, damit das Vertrauen der Kunden wiederhergestellt werden kann

Haftpflichtansprüche aus Lieferverzögerungen

Über einen privaten USB-Stick eines Mitarbeitenden eines Architekten wird eine **Malware** auf das IT-System des Unternehmens geladen. Das Schadprogramm verschlüsselt anschliessend sämtliche Daten auf dem Server. Das Architekturbüro kann dadurch die sehr dringend benötigten, neusten Pläne einer Bauleitung nicht mehr termingerecht zustellen, und es entstehen Verzögerungen auf der Baustelle. Mehrere Baubeteiligte machen gegenüber dem Architekturbüro Forderungen (stillstehende Baumaschinen, Mietausfälle etc.) geltend.

Helvetia entschädigt

- begründete Ansprüche bzw. wehrt ungerechtfertigte Forderungen der Vertragspartner des Architekten ab
- Kosten, die im Zusammenhang mit der Systemwiederherstellung (inkl. Entfernung der Malware) entstehen
- Aufwendungen für die manuelle Rekonstruktion jener Daten, die technisch nicht mehr über das Back-up wiederhergestellt werden können

Die hier beispielhaft aufgeführten Leistungen im Schadenfall sind abhängig vom gewählten Leistungspaket.

Helvetia ist eine führende Schweizer Versicherung mit massgeschneiderten Versicherungs- und Vorsorgelösungen für Unternehmen und Privatkundinnen und -kunden – seit 1858. Helvetia unterstützt gesellschaftliche Engagements.

Offizieller Partner von Swiss-Ski seit 2005.

Engagiert für den Schutzwald seit 2011.

120015329 11.25

Helvetia Versicherungen
T +41 58 280 10 00 (24 h), www.helvetia.com

einfach. klar. helvetia
Ihre Schweizer Versicherung