Cyber-Kriminalität und - Security

Was muss ich wissen, was kann ich machen

R. Kříž, System Engineer

Wer ist Fortinet

Fortinet: Global Network Security Leader

Highlights: 2000 - present

FOUNDED IN **2000**
BY KEN XIE

HEADQUARTERED IN
SUNNYVALE CALIFORNIA

100+
OFFICES
ACROSS THE GLOBE

5,700
EMPLOYEES WORLDWIDE

$1.8bn
REVENUE

$1.5bn
IN CASH

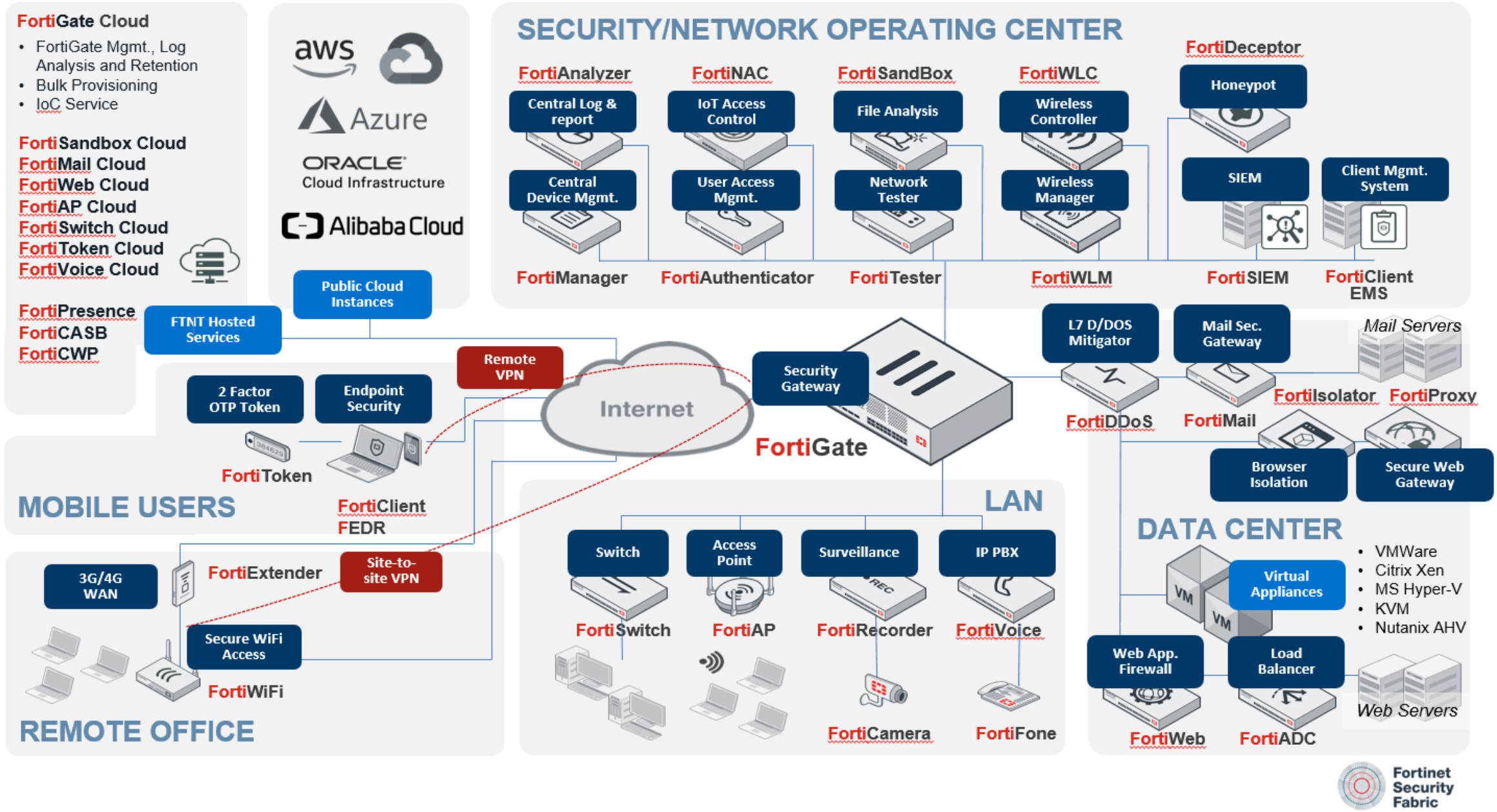
30%
GROWTH
YEAR ON YEAR

4m
SHIPPED SECURITY DEVICES

300K
CUSTOMERS

536
PATENTS ISSUED

240 IN PROCESS



Informationen
Daten

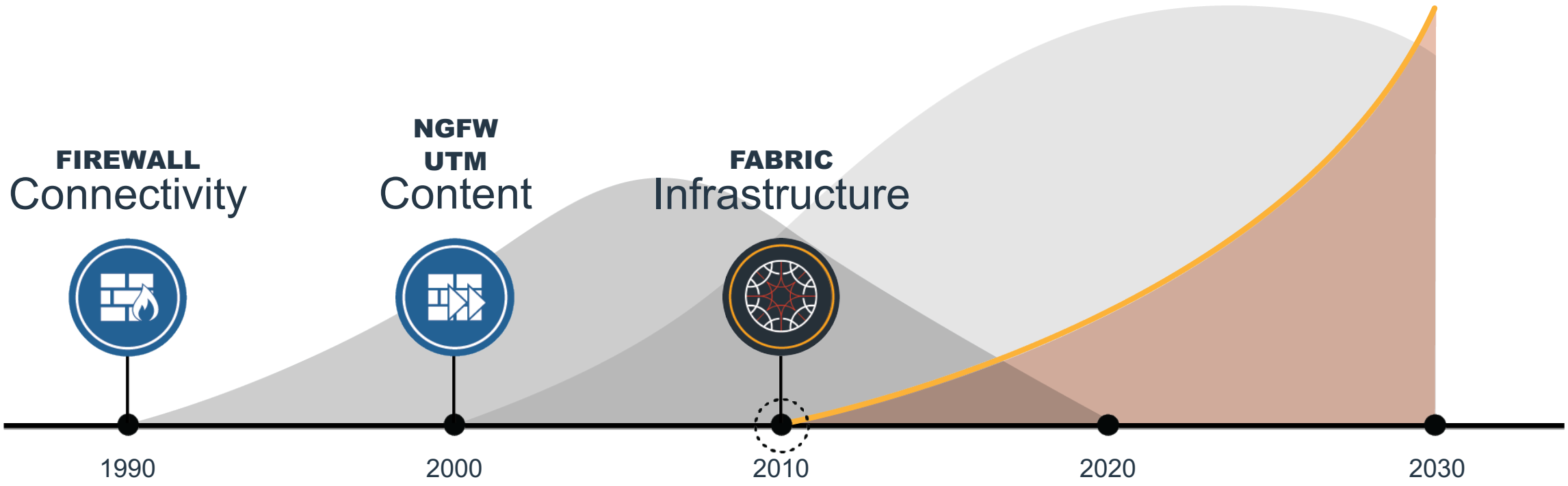
Verlust

Missbrauch

Well-Positioned to Lead the 3rd Evolution of Network Security

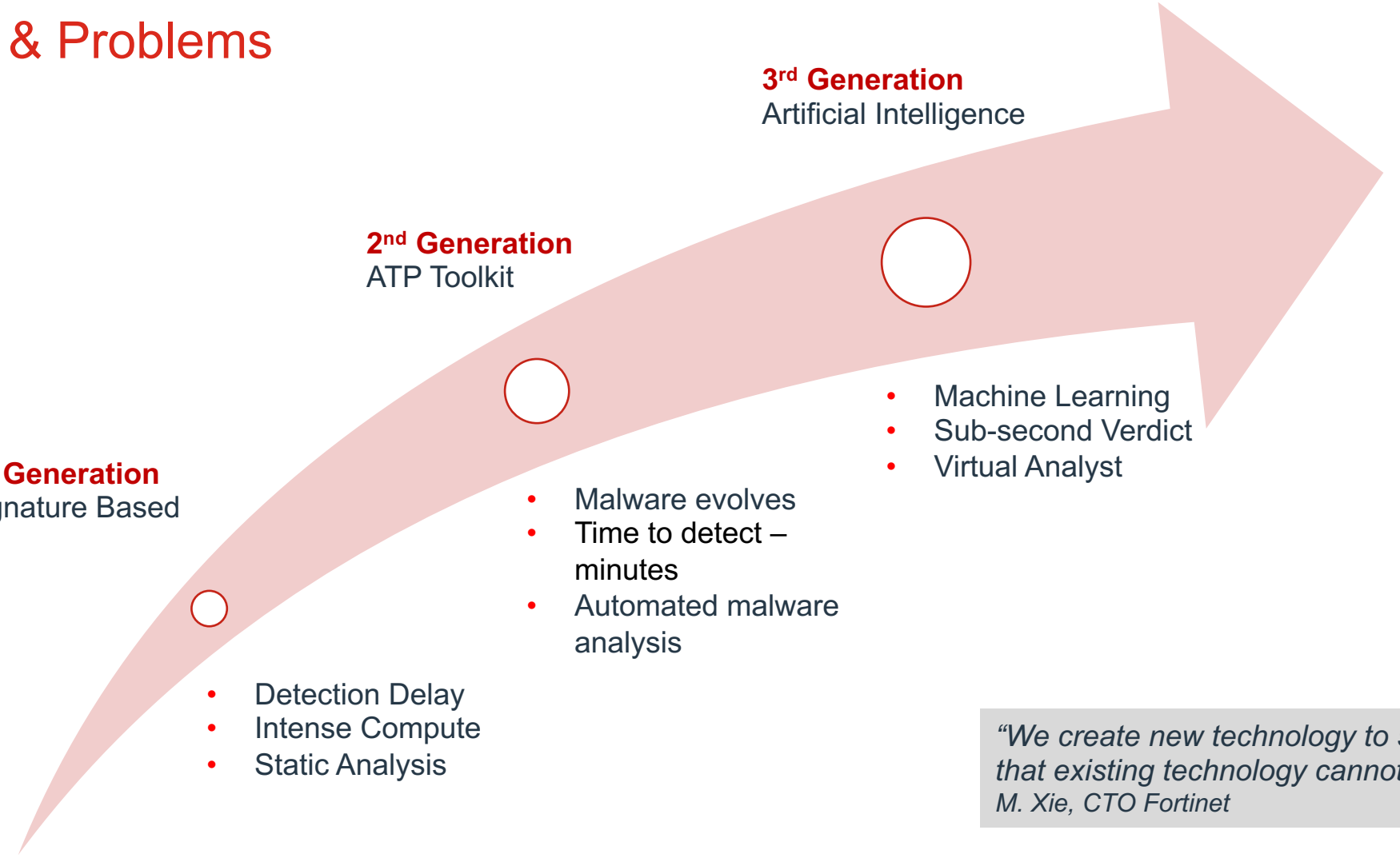
Network Security Evolution

1ST GENERATION → 2ND GENERATION → 3RD GENERATION



Evolution of Malware Detection

Methods & Problems



"We create new technology to solve problems that existing technology cannot solve today"
M. Xie, CTO Fortinet

FORTINET


FORTINET

Helvetia Cyber-Versicherung

helvetia.ch/cyber-versicherung

Cyber-Risiken.
IT gehackt.
Gedeckt.

einfach. klar. helvetia

Ihre Schweizer Versicherung

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

Die Digitalisierung beeinflusst die heutigen Geschäftsprozesse und ist in 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.

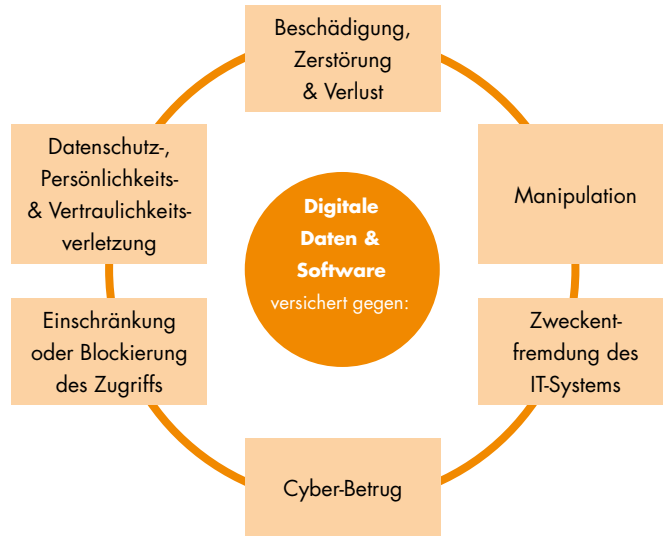
Schutz vor den Folgen von Cyber-Kriminalität und nicht krimineller Ursachen

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 Grippe-Viren 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;
- absichtliche oder unabsichtliche Installation und Ausführung von Schadsoftware;
- unautorisiert eingesetzte Hardware;
- Verwendung von gestohlenen Zugriffsinformationen;
- DoS-Attacken;
- fahrlässige Bedienung durch eigene Mitarbeitende;
- kurzzeitige Störungen.

Risiken vorbeugen und Unternehmen wirksam schützen.

Wie können Sie sich vor Cyber-Risiken schützen?

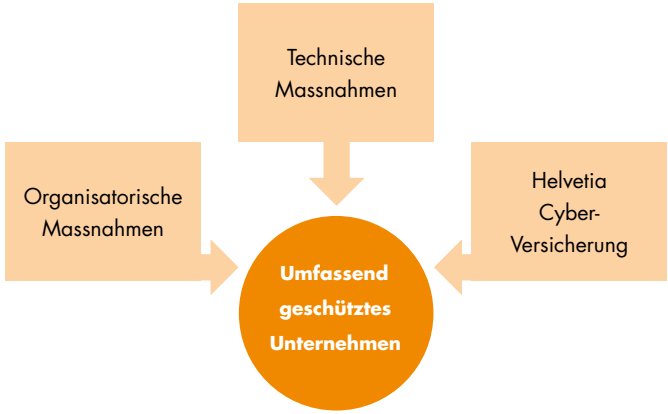
Mittels technischer und organisatorischer Sicherheitsmassnahmen lässt sich das Risiko von Cyber-Schäden beträchtlich einschränken. Die Melde- und Analysestelle Informationssicherung des Bundes (MELANI) publiziert dazu jeweils Empfehlungen für KMU. Auf der Basis dieser Empfehlungen und in Zusammenarbeit mit dem eigenen Expertennetzwerk hat Helvetia einen Sicherheitskatalog entwickelt, den jedes Unternehmen zur eigenen Sicherheit einhalten sollte (siehe Checkliste Seite 4).

Risikominimierung mit 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 den Gefahren an, die über technische und organisatorische Sicherheitsmassnahmen nicht abgedeckt werden können und ergänzt so das Risikomanagement jedes Unternehmens optimal.

Helvetia Cyber-Versicherung
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-Berater, Rechtsberater und Datenschutzspezialisten.



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

- ☐ **Bestimmung eines IT-Verantwortlichen**
- ☐ **Berechtigungsmanagement**
- ☐ **Passwort-Richtlinien**
- ☐ **Abwehrstrategien gegen DoS-Attacken**
- ☐ **Sensibilisierung der Mitarbeitenden und Sicherheits-Trainings zum Thema Cyber-Risiken**
- ☐ **Tägliche Datensicherung (Back-up) sowie deren sichere Aufbewahrung**
- ☐ **Technische Schutzmassnahmen (z.B. Firewalls, Virenscanner, Spam-Filter etc.)**
- ☐ **Physische Sicherungsmassnahmen (z.B. für den Zugang zu Serverräumen)**
- ☐ **Patch- und Update-Management**
- ☐ **Verschlüsselung schützenswerter Daten**
- ☐ **PCI-DSS Regeln bei Kredit- oder Debitkarten-Transaktionen**
- ☐ **Überspannungsschutz**

Besprechen Sie diese Punkte mit Ihrem internen oder externen IT-(Security-)Verantwortlichen.

Falls Sie Unterstützung benötigen, fragen Sie uns. Dank unserer Partnerschaften können wir Ihnen ausgewiesene und spezialisierte Unternehmen zum Thema Schutz vor Cyber-Risiken vermitteln.

Leistungen von Helvetia auf einen Blick.

Übersicht der Leistungen innerhalb der verschiedenen Pakete

Eigenschäden	Light	Standard	Premium
Systemwiederherstellung	✓	✓	✓
Datenrekonstruktion	✓	✓	✓
Mehrkosten zur Aufrechterhaltung des Betriebs	✓	✓	✓
Gewinnausfall infolge Betriebsunterbruch		✓	✓
Schadensanalyse/Forensik		✓	✓
Notifikationsmanagement			✓
Reputationsmanagement			✓
Abwehr von Erpressungen			✓
Vermögensausgleich infolge Cyber-Betrug oder Manipulation			✓
Mangelhafte Produktion		(✓)	(✓)

Haftpflichtschäden	Light	Standard	Premium
Reine Vermögensschäden		✓	✓
Immaterielle Schäden		✓	✓
Schäden durch digitale Kommunikation			✓

Rechtsschutz	Light	Standard	Premium
Juristische Beratung und Erstintervention		✓	✓

Kombination von Eigenschäden, Haftpflichtschäden und Rechtsschutz

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

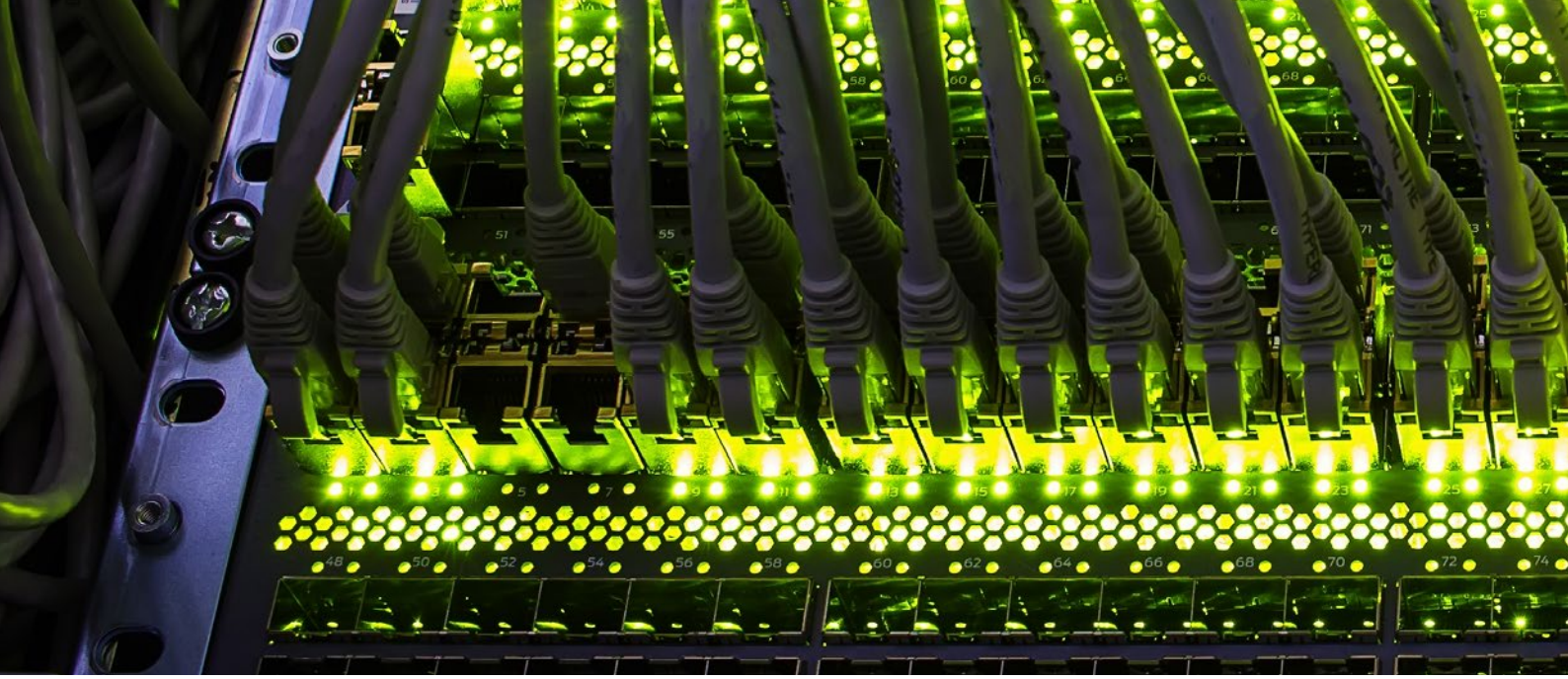
Aufgrund der Komplexität und der Vielfalt möglicher Schadenereignisse hat Helvetia drei Leistungspakete definiert (Light, Standard und Premium), die den unterschiedlichen Bedürfnissen der Unternehmen gerecht werden sollen. Jedes dieser Pakete kombiniert mehrere Leistungen für die Bereiche Eigenschäden,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

www.helvetia.ch/cyber-versicherung



Schadenbeispiele.

Verschlüsselung von Daten auf einer Cloud

Ein Unternehmen speichert alle seine Daten auf einer externen Cloud. Einem Hacker gelingt es, in diese Cloud einzudringen und mittels **Ransomware** alle darauf 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;
- den Mehrkosten zur Aufrechterhaltung des Betriebs;
- dem Gewinnausfall aufgrund des Betriebsunterbruchs;
- der Schadensanalyse inkl. Forensik.

OT-Steuerungen gehackt

Mittels einer betrügerischen E-Mail 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 kommt für folgende Kosten auf

- 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 den Begriff OT-Steuerungen (Operational-Technology-Steuerungen) fallen verschiedenste Steuersysteme (wie bspw. 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.

Firmentelefonanlage manipuliert
Ein Hacker dringt in das Telekommunikationssystem eines Unternehmens ein (**Phreaking**) und manipuliert es so, dass auf Kosten des Unternehmens ständig teuer ins Ausland telefoniert wird. 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.

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
- die Analyse des Schadens und die 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 zu den Patienten wiederhergestellt werden kann;
- mögliche Genugtuungsforderungen der Patienten.

Online-Shop lahmgelegt
Durch eine **DoS-Attacke** auf einen Online-Shop eines Schuhfachgeschäfts können Kundinnen und Kunden nicht mehr auf die Website zugreifen. Die Abwehr des Angriffs benötigt zwei Wochen, wodurch der gesamte Online-Verkauf während der ertragreichen Weihnachtszeit stillsteht.

Helvetia übernimmt folgende Leistungen
- Mehrkosten zur Aufrechterhaltung des Betriebes
- Gewinnausfall aufgrund des blockierten Online-Shops und des daraus resultierenden Verkaufstops
- Schadensanalyse inkl. Forensik
- Übernahme der Kosten für das Reputationsmanagement, damit das Vertrauen zu den Kunden wiederhergestellt werden kann

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

Gedruckt auf 100% Altpapier, das mit dem Blauen Engel ausgezeichnet ist. 120011525 12.18

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

einfach. klar. helvetia
Ihre Schweizer Versicherung