xelon

Cyber-Security

Wie ihr euch vor der verschärften Bedrohungslage schützt

Whitepaper 2025

Inhalt

Einleitung 3

Wird die (Cyber-)Welt immer gefährlicher? 4

Diese Cyber-Bedrohungen lauern 2025 6

Warum Disaster Recovery 2025 unerlässlich ist 8

Wann der richtige Zeitpunkt für IT-Notfallplanung ist 10

Worauf IT-Teams bei Backups achten müssen 12

Einleitung

Cyber-Attacken sorgen weltweit immer wieder für Schlagzeilen und auch viele Schweizer Unternehmen fürchten um ihre Daten, die Verfügbarkeit ihrer Systeme oder die Erreichbarkeit ihrer Websites.

Im Laufe des Jahres 2025 dürfte sich die Cyber-Bedrohungslage weiter zuspitzen. Cyber-Kriminelle verfeinern nämlich kontinuierlich ihre Angriffsvektoren, indem sie technologische Fortschritte und ein tieferes Verständnis von typischen Unternehmensschwachstellen nutzen.

Technologien wie Künstliche Intelligenz (KI) und das Internet der Dinge (IoT) eröffnen neue Angriffsflächen, da immer mehr Geräte miteinander vernetzt sind und potenziell für Angreifer zugänglich werden.

In diesem Whitepaper findet ihr nicht nur eine Übersicht, welche Cyber-Gefahren aktuell lauern, sondern vor allem konkrete Tipps, wie ihr eure Daten und Systeme vor IT-Ausfällen und Cyber-Kriminellen schützen könnt.

Wird die (Cyber-)Welt immer gefährlicher?

Unsere Welt scheint zunehmend unsicherer zu sein. Jeden Tag werden wir mit einer Flut von Negativereignissen konfrontiert, sei es durch Zeitungsartikel, Nachrichten oder Social Media. Wie sieht es bei der Cyber-Security aus?

Abertausende Medienberichte über Kriege, Kriminalität in der Offline- und Online-Welt, Naturkatastrophen, Versorgungsengpässe oder Ressourcenknappheit verstärken oft das Gefühl, dass die Welt Jahr für Jahr unsicherer wird, auch wenn die objektive Wahrscheinlichkeit für persönliche Gefährdungen in vielen Fällen nicht steigt. So ist und bleibt das Leben in der Schweiz im globalen Vergleich äusserst sicher.

Mit der zunehmenden Digitalisierung und Vernetzung entstehen allerdings neue Risiken, etwa Cyberangriffe auf kritische Infrastrukturen oder der Diebstahl persönlicher Daten.

Unten findet ihr drei zentrale Risiken:

Gesundheitswesen

Spitäler und medizinische Systeme werden weltweit zunehmend Opfer von Cyberkriminellen, die Patientendaten verschlüsseln oder geschäftskritische Systeme stören. Dies kann die Leben zahlreicher Patientinnen und Patienten bedrohen.

Transportwesen

Hacker könnten Systeme in der Luftfahrt, bei Bahnnetzen oder auch im Strassenverkehr sabotieren, was zu grossen Störungen und potenziellen Katastrophen führen könnte.

Energieversorgung

Cyberangriffe auf Stromnetze, Wasseraufbereitungsanlagen oder Öl- und Gaspipelines können weitreichende Folgen für die Versorgungssicherheit einer Region haben.

Wir stehen also vor neuen und komplexen Herausforderungen, die Unsicherheit verstärken können. Angriffe auf kritische Infrastrukturen könnten weite Teile eines Landes oder sogar einer Region lahmlegen. Gleichzeitig hat die Menschheit aber auch mehr Werkzeuge und Wissen als je zuvor, um Herausforderungen zu begegnen.

Mit diesem Whitepaper erhält ihr eine Möglichkeit, eure Kenntnisse im Bereich Cyber-Security zu vertiefen und ergänzen.

Diese Cyber-Bedrohungen lauern 2025

Hackerangriffe, Datenklau oder unbefugte Netzwerkzugriffe können Kosten in Millionenhöhe, Strafverfolgungen und irreparable Reputationsschäden verursachen. Hier findet ihr einen Überblick, wie die aktuelle Cyber-Bedrohungslage aussieht.

Altbekannte Maschen wie **Phishing, Ransomware, Trojaner und Botnets** zählen weltweit nach wie vor zu den grössten Cyber-Bedrohungen. In der Schweiz noch eher neu sind hingegen **dateilose Angriffe**. Diese sind eine Untergruppe der sogenannten Living-off-the-Land»Angriffe (LotL) und nutzen Tools und Funktionen, die bereits in der Umgebung des Opfers vorhanden sind. Dateilose Angriffe verlassen sich nicht auf dateibasierte Nutzungsdaten und generieren in den meisten Fällen auch keine neuen Dateien. Daher haben sie das Potenzial, unter dem Radar vieler Präventions- und Erkennungslösungen zu fliegen. Üblicherweise beginnt ein dateiloser Angriff mit einem per E-Mail versandten Link zu einer unsicheren Website. Social-Engineering-Tricks auf dieser Website können Systemtools starten, die zusätzliche Nutzungsdaten direkt im Systemspeicher abrufen und ausführen. Die Unterscheidung zwischen der böswilligen Verwendung integrierter System-Tools im Gegensatz zu ihren vielen legitimen Automatisierungs- und Skriptverwendungen ist oftmals eine grosse Herausforderung für herkömmliche Security-Massnahmen. Die Verwendung von System-Tools als Hintertüren gibt es schon seit Jahrzehnten, aktuell sind sie jedoch ein Aufwärtstrend.

Ein bedeutender Trend ist die zunehmende Nutzung von Künstlicher Intelligenz (KI) bei Cyber-Attacken. **KI-gestützte Angriffe** werden immer ausgefeilter und stellen erhebliche Her-

ausforderungen für traditionelle Sicherheitsmassnahmen von Schweizer Unternehmen dar. Diese Cyber-Angriffe nutzen Machine Learning, um sich anzupassen, zu automatisieren und Verteidigungen zu überholen, was sie schwer zu erkennen und entschärfen macht. Beispiele hierfür sind KI-generierte Phishing-E-Mails und adaptive Malware, die Standard-Schutzmassnahmen umgehen kann.

Manchmal identifizieren Cyber-Kriminelle Sicherheitslücken nicht in Anwendungen, sondern im Prozessablauf. In den letzten Jahren konnte eine Zunahme von **Kompromittierungen von Geschäftsprozessen** beobachtet werden. Dabei nutzen die Angreifer systemische Schwachstellen zu ihrem finanziellen Vorteil aus. Angriffe auf Geschäftsprozesse erfordern erhebliche Kenntnisse über die Systeme und Abläufe der Opfer. Sie beginnt oft mit einem kompromittierten System im Zielnetzwerk, über das die Cyberkriminellen die Prozesse des Unternehmens beobachten und nach und nach Security-Lücken identifizieren können. Diese Angriffe auf Prozessabläufe sind meistens diskret und die betroffenen Organisationen erkennen sie möglicherweise nicht rechtzeitig. Dies kann vor allem dann der Fall sein, wenn der betroffene Prozess auf den ersten Blick weiterhin wie erwartet funktioniert.

Unternehmen scheuen manchmal Updates, weil diese vorübergehenden Unterbrechungen im Betrieb verursachen könnten. Dies kann verheerende Folgen haben: **Veraltete Software und mangelnde Updates gehören zu den häufigsten Ursachen für Sicherheitslücken in digitalen Systemen.** Dies liegt daran, dass ältere Softwareversionen oft bekannte Schwachstellen aufweisen, die von Cyberkriminellen ausgenutzt werden können. So scannen Hacker häufig Netzwerke nach Geräten oder Systemen nach Schwachstellen und nutzen diese gnadenlos aus.

Da Cyber-Kriminelle ihre Angriffsstrategien ständig weiterentwickeln, müssen IT-Teams ihre Ansätze für Cybersicherheit und Datenschutz ebenfalls anpassen. Standardisierte Antivirus-Software reicht oftmals nicht mehr aus, um die Cyber-Bedrohungen von heute zu bekämpfen. Es gilt, die Workloads, Daten und Anwendungen über mehrere Ebenen hinweg zu schützen. Wie dies in der Praxis aussehen kann, zeigen euch Xelons Security- und Infrastruktur-Experten gerne in einem kostenlosen Beratungsgespräch.

Warum Disaster Recovery 2025 unerlässlich ist

Wie können sich Unternehmen vor IT-Katastrophen schützen? Wann ist der richtige Zeitpunkt, die IT-Notfallplanung in Angriff zu nehmen? Und was beinhaltet eine gute Disaster-Recovery-Strategie?

Dieser Artikel von Ueli Schwegler, Director der Cloud Infrastructure Unit bei Xelon, erschien erstmals im August 2024 im ICT-Branchenmagazin «Netzwoche».

IT-Ausfälle, die unter anderem durch Cyberangriffe oder Naturereignisse wie Überschwemmungen und Stürme verursacht werden können, generieren weltweit jedes Jahr Kosten in Milliardenhöhe und sorgen für kaum bezifferbare finanzielle Einbussen. Zahlreiche Firmen erholen sich nie mehr ganz von den Folgen einer IT-Katastrophe und gerade IT-Unternehmen haben oft Schwierigkeiten, ihren ehemals guten Ruf nach einem Totalausfall und dem Verlust von Kundendaten wiederherzustellen. Dennoch haben nicht wenige IT-Unternehmen in der Schweiz keinen kompletten oder aktuellen IT-Notfallplan und würden nach einem IT-Ausfall wertvolle Daten, Zeit und Arbeitsfortschritte verlieren. Mit einem durchdachten Disaster-Recovery-Plan könnten diese Verluste minimiert werden, weswegen jedes IT-Unternehmen eine solide IT-Notfallstrategie braucht und dies nicht länger aufschieben sollte.

Was zur IT-Notfallplanung gehört

Eine Disaster-Recovery-Strategie zielt darauf ab, schnellstmöglich und effektiv auf IT-Katastrophen reagieren zu können. Ein wichtiger Bestandteil der IT-Notfallplanung ist die Risikobewertung, wobei die potenziellen Security-Risiken und Cyber-Bedrohungen für das IT-Unternehmen analysiert werden. Wo sind mögliche Schwachstellen und wie riskant sind diese im Ernstfall? In einem nächsten Schritt geht es darum, die zu sichernden Daten und Systeme zu priorisieren. Was sind die Recovery Time Objectives (RTO), also in welchem Zeitraum müssen Systeme wiederhergestellt werden können? Und wie sieht es aus mit den Recovery Point Objectives (RPO), was ist der maximal zulässige Datenverlust? Basierend auf der Risikobewertung und der Priorisierung der Daten und Systeme lässt sich ein Backup-Verfahren ableiten. Wie oft und wann soll was mit welcher Backup-Lösung automatisch gesichert werden? Auch ein Kommunikationsplan für den Ernstfall darf nicht fehlen. Darin sollte festgehalten sein, welche Stakeholder nach einem IT-Ausfall zu informieren sind und wie kommuni-

ziert wird. IT-Notfallpläne müssen regelmässig getestet und aktualisiert werden.

Wie eine Cloud-Infrastruktur Disaster Recovery vereinfacht

Die Zusammenarbeit mit einem Cloud-Infrastruktur-Provider, der die Bedürfnisse und Herausforderungen von lokalen IT-Unternehmen versteht, kann das Planen und Umsetzen einer Disaster-Recovery-Strategie signifikant vereinfachen. So sind beispielsweise wichtige Daten extern – und im Idealfall in ISO-zertifizierten Rechenzentren – gespeichert, wodurch bei Bränden, Überschwemmungen und Sturmschäden keine Datenverluste entstehen. Eine redundante Netzwerkarchitektur stellt sicher, dass es im Falle eines Netzwerkausfalls alternative Verbindungen gibt, was Ausfallzeiten minimiert. In die Cloud-Infrastruktur integrierte Cloud-Backups sind anpassbar, sodass Daten in selbstgewählten Intervallen automatisch gesichert und extern aufbewahrt werden. Gute Cloud-Infrastruktur-Provider kennen zudem die aktuelle Cyber-Bedrohungslage und bieten oftmals Unterstützung bei der Risikobewertung und Definition der RTO und RPO, damit IT-Unternehmen eine passende Disaster-Recovery-Strategie entwerfen und im Notfall effizient Schadensbegrenzung betreiben können.

Möchtet ihr eure Disaster-Recovery-Strategie von Security- oder IT-Infrastruktur-Experten überprüfen lassen?
Bucht **hier** ein kostenloses Beratungsgespräch.

Wann der richtige Zeitpunkt für IT-Notfallplanung ist

Die passende IT-Notfallplanung minimiert die Risiken, die mit IT-Katastrophen wie Naturereignissen, Cyberangriffen und Hardwareausfällen verbunden sind, und bietet ein Sicherheitsnetz für unvorhergesehene Umstände. Wann ist der oft hohe finanzielle und zeitliche Aufwand für die IT-Notfallplanung gerechtfertigt?

Die Investitionen in Prävention und Notfallplanung mögen auf den ersten Blick hoch scheinen. Sie lohnen sich im Ernstfall jedoch für Unternehmen jeder Grösse. Das Uptime Institute schätzt nämlich, dass zwei Drittel aller IT-Ausfälle Kosten von mehr als 100'000 US-Dollar verursachen.

IT-Teams sollten mit der Notfallplanung so früh wie möglich beginnen, idealerweise bereits in der Planungsphase für neue IT-Infrastrukturen, Systeme, Services oder Funktionen. Ein proaktiver Ansatz ermöglicht es, Risiken frühzeitig zu identifizieren und geeignete Security-Massnahmen zu entwickeln, bevor ein Vorfall eintritt. Fragt euch dabei, was eure Daten und Systeme heute oder morgen bedrohen könnte.

Besonders wichtig ist die Notfallplanung bei der Ergänzung der bestehenden IT-Infrastruktur um neue Systeme, da diese oft unbekannte Schwachstellen mit sich bringen. In solchen Fällen sollte die Notfallplanung direkt in den Entwicklungs- oder Implementierungsprozess integriert werden, um potenzielle Risiken zu adressieren.

Erstellt eine ausführliche **Dokumentation eures IT-Notfallplans** einschliesslich Kontaktdaten, Rollen und Verantwortlichkeiten. Spezifiziert detaillierte Verfahren für die Datenwiederherstellung, Systemwiederherstellung und andere wichtige Prozesse. Definiert die Recovery Time Objectives (RTO), also in welchem Zeitraum Systeme wiederhergestellt werden müssen, und mit

den Recovery Point Objectives (RPO) den maximal zulässigen Datenverlust. Legt zudem fest, welche Mitarbeitende, Kundinnen und Kunden sowie andere relevanten Stakeholder während einer Katastrophe zu informieren sind und wie ihr kommunizieren möchtet.

Nach Security-Tests, Beinahe-Zwischenfällen oder Cyber-Angriffen auf andere Marktteilnehmende ist es ein Muss, den bestehenden IT-Notfallplan zu evaluieren. Nutzt den Warnschuss, um Schwachstellen zu identifizieren und die Prozesse auf Basis der gewonnenen Erkenntnisse zu verbessern. Auch bei Änderungen der Geschäftsstrategie oder neuen Compliance-Anforderungen sollten IT-Teams die Notfallplanung anpassen, um den neuen Gegebenheiten gerecht zu werden.

Achtung:

Die Notfallplanung sollte kein einmaliges Projekt, sondern ein kontinuierlicher Prozess sein. Je früher IT-Teams damit beginnen und je regelmässiger sie den IT-Notfallplan testen sowie allenfalls aktualisieren, desto besser sind sie auf unerwartete Ereignisse vorbereitet.

Worauf IT-Teams bei Backups achten müssen

Mit einer geeigneten Backup-Lösung können Datenverluste auch bei Naturkatastrophen wie Überschwemmungen oder Sturmschäden sowie bei Hackerangriffen vermieden werden. Doch welche Software schützt wertvolle Daten bestmöglich? Hier findet ihr eine Entscheidungshilfe für die Wahl eurer Backup-Lösung.

Eine geeignete Backup-Lösung bietet Unternehmen nicht nur Schutz vor Datenverlusten durch unvorhersehbare Ereignisse wie Naturkatastrophen, sondern auch vor digitalen Bedrohungen wie Ransomware-Angriffen, Datenkorruption oder versehentlichem Löschen von Arbeitsfortschritten.

Welche Backup-Lösung zu eurem Unternehmen passt, hängt vor allem von diesen drei Faktoren ab:

Aufbewahrungszeit: Wie lange sollen die Backups abrufbar und die verlorenen Daten wieder herstellbar sein?

Verwaltung: Ist technisches Know-how vorhanden? Wie viel Zeit kann für Backups aufgewendet werden? Wurden allfällige Lizenzkosten budgetiert?

Geräte: Je nachdem, ob es sich um physische Server, virtuelle Maschinen oder eine Cloud- Infrastruktur handelt, bieten sich andere Backup-Lösungen an.

Unsere Security- und Infrastruktur-Experten analysieren gerne gemeinsam mit euch, welches Backup am besten zu eurem Unternehmen passt.

Extratipp:

Regelmässige Tests der Backup- und Wiederherstellungsprozesse gewährleisten, dass Daten und Systeme im Ernstfall schnell und effektiv zurückgespielt werden können.

Vielen Dank!

Als Director der Cloud Infrastructure Unit von Xelon kenne und verstehe ich die Security-Herausforderungen, die Schweizer IT-Teams 2025 bewältigen müssen.

Ich hoffe, wir konnten euch mit diesem Whitepaper einige Bedenken nehmen. Gerne zeige ich in einem unverbindlichen Beratungsgespräch auf, wie ihr Cyber-Gefahren entschärfen und passgenaue Security-Massnahmen implementieren könnt.

Ueli Schwegler
Director Cloud-Infrastruktur bei Xelon