

IT-SECURITY

Wie ist die aktuelle Cyber-Bedrohungslage und wie könnt ihr euch schützen?

In diesem E-Book erfahren IT-Service-Provider mehr darüber, welche Cyber-Bedrohungen aktuell lauern und wie sie die IT-Umgebungen ihrer Kunden bestmöglich vor Hackerangriffen und Datenklau schützen können.



SEID GEFASST AUF PERFIDE CYBER-ATTACKEN



Autor: Michael Dudli
CEO, Xelon AG

Ob Datenklau, DdoS-Attacken oder Ransomware: Cyber-Kriminelle werden immer raffinierter und kein Unternehmen ist sicher. Hier gibt es einen Überblick über die aktuellen Angriffsmethoden.

Das Thema Cyber-Security steht derzeit wohl bei allen IT-Service-Providern weit oben auf der Agenda. Seit Jahresbeginn sorgen wieder mehr Cyber-Attacken für Schlagzeilen und viele Schweizer Unternehmen fürchten um ihre Daten, die Verfügbarkeit ihrer Systeme oder die Erreichbarkeit ihrer Websites. So wurde beispielsweise das Internationale Komitee vom Roten Kreuz mit Sitz in Genf im Januar 2022 Opfer eines grossangelegten Hackerangriffs. Laut «Tages-Anzeiger» sind durch den Angriff personenbezogene Daten und vertrauliche Informationen über mehr als 515'000 besonders gefährdete und schutzbedürftige Menschen kompromittiert worden. Die Daten stammten von mindestens 60 nationalen Gesellschaften des Roten Kreuzes und des Roten Halbmonds in aller Welt. Auch Europas grösster Autohändler Emil Frey war 2022 im Visier von Cyber-Kriminellen: Noch unbekannte Internet-Kriminelle erpressten die Emil Frey Gruppe und drohten mit der Veröffentlichung von fast 300 Gigabyte an «vertraulichen Daten», die sie laut eigenen Angaben bei einem Hackerangriff im Januar erbeutet hatten. Die Hacker machten ihre Drohung Anfang Februar dieses Jahres teilweise wahr und teilten auf einer Filehosting-Plattform eine komprimierte Datei, die laut der News-Plattform «Watson» Kundendaten aus der Schweiz und aus Deutschland enthalten haben soll.

Bei kleineren Betrieben sorgen Cyber-Attacken und Datenlecks zwar nicht immer für Schlagzeilen, doch Security-Schwachstellen können für Unternehmen aller Grössen verheerende Folgen haben. Die Konsequenzen reichen von finanziellen Einbussen über Strafverfolgung bis hin zu langfristigen Reputationsverlusten. Wir von Xelon hören immer wieder, dass kleinere Unternehmen das Thema Cyber-Security nicht so ernst nehmen, wie sie es sollten. Wir sehen deshalb IT-Service-Provider in der Pflicht, ihre Kunden und Kundinnen zu sensibilisieren.

Welche Cyber-Bedrohungen lauern momentan?

Altbekannte Maschen wie Phishing, Ransomware, Trojaner und Botnets zählen nach wie vor zu den grössten Cyber-Bedrohungen. 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, laut Cyber-Security-Experten sind sie jedoch aktuell ein Aufwärtstrend.

Manchmal identifizieren Cyber-Kriminelle Sicherheitslücken nicht in Anwendungen, sondern im Prozessablauf. In den letzten Monaten und 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.

CHECKLISTE: SO KÖNNEN SICH EURE KUNDEN VOR CYBER-ATTACKEN SCHÜTZEN



Autor: Matias Meier
Head of Technology, Xelon AG

Hackerangriffe, Datenklau oder unbefugte Netzwerkzugriffe können Kosten in Millionenhöhe, Strafverfolgungen und irreparable Reputationsschäden verursachen. IT-Service-Provider müssen die IT-Umgebungen ihrer Kunden daher bestmöglich schützen. Hier gibt es eine Checkliste für eure Kunden.

Da Cyber-Kriminelle ihre Angriffsstrategien ständig weiterentwickeln, müssen IT-Dienstleister ihre Ansätze für Cybersicherheit und Datenschutz ebenfalls anpassen. Standardisierte Antivirus-Software reicht oftmals nicht mehr aus, um die Cyber-Bedrohungen von heute zu bekämpfen. Ihr müsst die Workloads, Daten und Anwendungen eurer Kunden über mehrere Ebenen hinweg schützen.

Wir haben hier eine Liste mit Security-Tipps zusammengestellt, die ihre euren Kunden zur Verfügung stellen könnt:

Security-Check für KMU

- ☐ Speichert keine Firmenkreditkartendaten auf euren Arbeitsgeräten.
- ☐ Sensible Daten dürfen nur auf passwortgeschützten Plattformen und Systemen hinterlegt werden.
- ☐ Erstellt komplexe Passwörter, die Klein- und Grossbuchstaben, mindestens ein Sonderzeichen und Zahlen beinhalten.
- ☐ Verwendet nicht für alle Systeme und Anwendungen das gleiche Passwort.
- ☐ Gebt keine Logindaten an externe Personen heraus. Falls ihr von einem Arbeitskollegen oder dem IT-Team um die Herausgabe eines Passwortes gebeten werdet, solltet ihr euch vergewissern, dass hinter der Anfrage tatsächlich diese Person steckt. Ruft kurz an, geht am Pult vorbei oder nehmt über einen anderen Kanal Kontakt auf. Es kann auch nicht schaden, wenn ihr nachfragt, wofür das Passwort genau verwendet wird.
- ☐ Öffnet keine Links von unbekannten Absendern.
- ☐ Macht einen Virenskan, bevor ihr Dateien von ausserhalb der Organisation herunterlädt.
- ☐ Schützt eure Arbeitsgeräte vor Fremdzugriffen zum einen mit starken Passwörtern und zum anderen vor einer physischen Entwendung.
- ☐ Bei Reisen gehören Arbeitsgeräte immer ins Handgepäck, wo ihr sie stets im Blick habt.
- ☐ Falls ihr unabsichtlich Daten löscht, solltet ihr euch so schnell wie möglich bei den IT-Verantwortlichen – ob intern oder ein externer IT-Dienstleister – melden.
- ☐ Führt regelmässig Backups durch, sodass sich der Datenverlust bei einem Serverausfall oder Hackerangriff in Grenzen hält. Euer IT-Service-Provider hilft gerne dabei.
- ☐ Bei Fragen, Verdachtsfällen oder Unsicherheiten: Wendet euch an euer internes IT-Team oder den IT-Dienstleister, mit dem euer Unternehmen zusammenarbeitet.



Bei Schweizer IaaS-Providern sind eure Daten deutlich sicherer als bei Hyperscalern

Der Unternehmensstandort spielt bei der Wahl des passenden IaaS-Providers eine wichtige Rolle. In Zeiten von Datenlecks und Hackerangriffen möchten wohl die meisten Unternehmen und deren Endkunden wissen, wo ihre Daten gespeichert werden. Die meisten Hyperscaler wie Amazon oder Microsoft haben ihren Hauptsitz in den USA, wo der Zugriff auf Unternehmensdaten mittels des Patriot Acts ohne richterliche Kontrolle praktiziert wird. In der Schweiz hingegen ist dies nicht erlaubt. Laut dem Schweizerischen Datenschutz- und Öffentlichkeitsbeauftragten soll der Datenschutz gewährleisten, dass in jedem Fall die Verhältnismässigkeit beachtet wird. Dies heisst, dass immer nur so viele persönliche Daten wie nötig und so wenig persönliche Daten wie möglich gesammelt und bearbeitet werden, und dass man als betroffene Person die Möglichkeit hat, die Bearbeitung der Daten über sich so weit wie möglich zu kontrollieren und notfalls zu verhindern.

Unternehmen müssen die Sicherheit aller gespeicherten personenbezogenen Daten garantieren. Sowohl Mitarbeiter- als auch Kundendaten gilt es bestmöglich zu schützen. Werden diese Daten versehentlich oder absichtlich kompromittiert und stellt sich nach dem Cyberangriff oder dem Datenleck heraus, dass das betroffene Unternehmen keine geeigneten Sicherheitsmassnahmen ergriffen hatte, drohen möglicherweise Bussen und Sanktionen. Das Schweizer Datenschutzgesetz (DSG) sieht Strafbestimmungen vor bei vorsätzlichen Verletzungen der Auskunft-, Melde und Mitwirkungspflichten sowie der beruflichen Schweigepflicht. Das DSG wird momentan überarbeitet. Mit der Revision sollen mehr Transparenz geschaffen und die Mitbestimmungsrechte von betroffenen Personen gestärkt werden. Der Entwurf zur Revision lehnt sich stark an die EU-Datenschutz-Grundverordnung (DSGVO) an. Unternehmen mit Kunden im EU-Raum unterstehen bereits heute der DSGVO, wobei für die effektive Durchsetzung des Datenschutzrechts seit 2018 weitaus höhere Bussgelder als zuvor möglich sind. Lokale Provider befolgen Schweizer Datenschutzgesetze und können dadurch höchste Datensicherheitsstandards garantieren.





WAF – EIN UNVERZICHTBARES TEIL IM SECURITY- PUZZLE



Autor: Michael Dudli
CEO, Xelon AG

Die meisten Security-Experten sind sich einig, dass eine Web Application Firewall (WAF) heutzutage zum Standardinventar jeder IT-Umgebung gehören sollte. Selbst eine Enterprise WAF kann innerhalb weniger Minuten konfiguriert und einsatzbereit sein. Wir zeigen euch hier, worauf ihr achten müsst.

Ob CRM, Projektverwaltung oder Buchhaltung: Der Trend zu Webapplikationen ist nichts Neues und hat sich bereits seit Jahren durchgesetzt. Wo früher lokale Applikationen zum Einsatz kamen, werden heute Programme als webbasierte Applikation betrieben und via Browser ausgeführt. Aufgrund der Anforderungen an Funktionalität und Benutzerfreundlichkeit sind diese Applikationen oft sehr komplex aufgebaut und beinhalten zahlreiche Interaktionsformen wie beispielsweise über Javascript, Formulare oder Datei-Uploads. Daher schrecken viele KMU davor zurück, selbst eine WAF zu verwenden und brauchen dafür die Unterstützung eines IT-Service-Providers.

Eine 100-prozentig sichere Applikation gibt es nicht. Wo Menschen arbeiten, schleichen sich Fehler ein. So finden auch immer wieder Bugs und Sicherheitslücken den Weg in den Code der von euch betreuten Unternehmen. Vielfach werden die Applikationen aufgrund der bedeutenden Vorteile in einem abgekürzten Prozess in Cloud-Umgebungen oder auf lokalen Webservern installiert und ausgerollt. Klassische Firewalls bieten hier wenig bis keinen Schutz. Zum Einsatz kommen speziell auf die Webapplikation abgestimmte Firewalls: WAF. Diese schützen eure Applikationen vor Missbrauch, unerlaubtem Zugriff und Datenverlust und sind somit nicht zuletzt auch im Hinblick auf die neue EU-Datenschutzverordnung (DSGVO) ein unverzichtbares Teil im Cyber-Security-Puzzle.



■ Eine WAF ist ein effektiver Schutzschild für wichtige Webapplikationen

Die WAF hat sich dem Schutz von Webapplikationen verschrieben. Der komplette Traffic zum Webserver passiert erst die WAF, dabei wird der Datenverkehr auf Muster geprüft. So kann die WAF Angriffe erkennen und blockieren. Darunter fallen sowohl allgemeine Muster wie beispielsweise Cross-Site Scripting (XSS) oder SQL Injections – aber auch applikationsspezifische Sicherheitslücken, sogenannte Zero-Day Vulnerabilities. Zero-Day-Lücken gehören mitunter zu den grössten Problemen von Webapplikationen. Im Normalfall vergehen zwischen der Bekanntgabe einer Sicherheitslücke und der Veröffentlichung eines Bugfixes mehrere Tage. Bis der Bugfix anschliessend vom Kunden getestet und eingespielt wird, vergehen erneut wichtige Stunden oder sogar Tage. In dieser Zeit ist die Applikation eures Kunden den Angriffen ausgeliefert. Eine WAF verschafft hier Abhilfe. Die Enterprise-WAF-Hersteller verpacken diese neu veröffentlichten Angriffsmuster in jeweilige Patterns, sodass sogar applikationsspezifische Angriffe in der Regel innerhalb weniger Stunden nach Bekanntgabe erkannt und automatisch blockiert werden. Sie überbrücken somit die Zeit, bis der Applikationshersteller einen Patch zur Verfügung stellt.

■ Worauf ihr bei der Wahl der passenden WAF achten müsst

WAF gibt es in verschiedensten Ausführungen und Preisklassen. Entsprechend gross sind auch die Unterschiede. Von kostenlosen Open-Source-Projekten bis hin zu Enterprise-Lösungen – alle versprechen den idealen Schutz eurer Webserver. Doch wie sieht es in der Praxis aus? Weit verbreitet sind Lösungen, die direkt auf dem Linux-Server in Apache integriert werden. Für kleinere Projekte kann dies Sinn machen, im Geschäftsumfeld empfehlen wir aber eine Lösung, die sich mehr auf Business-Applikationen konzentriert und somit auch Zero-Day Protection innert kürzester Zeit liefern kann. Im Grundsatz kann bei Business-WAF-Lösungen zwischen zwei Ansätzen unterschieden werden: In das Gateway (Next-Gen/UTM) integrierte WAF-Funktionalitäten wie etwa bei Sophos XG, oder als Standalone-Lösung, wie dies beispielsweise Barracuda anbietet. Implementationen in UTM- und Next-Gen-Lösungen sind meist sehr benutzerfreundlich, doch nicht immer umfangreich genug für grössere Projekte. So eignen sie sich gut für einen Standardschutz bei geläufigen Applikationen wie OWA oder Sharepoint.

Insbesondere bei Sophos XG lässt sich die WAF per einfachem Mausklick aktivieren und innert weniger Minuten konfigurieren. Dedizierte WAF-Lösungen wie beispielsweise von Barracuda empfehlen sich für komplexe Webshop-Konstrukte und individuelle Firmenportale mit sensiblen Kundendaten oder anderen schützenswerten Informationen. Oftmals sind die dedizierten Produkte so aufgebaut, dass sowohl einfache Konfigurationen als auch komplexe und tiefe Integrationen möglich sind. Falls ihr bereits eine UTM- oder Next-Gen-Firewall mit WAF-Funktionalität im Einsatz habt, könnt ihr diese in den meisten Fällen einfach per Mausklick aktivieren, vorausgesetzt die Funktion ist in der Lizenz enthalten. Oftmals bieten die Hersteller die Möglichkeit, solche Funktionen über eine Trial-Lizenz zu testen. Im [Xelon HQ](#) kann neben sämtlichen auf dem Markt erhältlichen Lösungen wie unter anderem Sophos XG und der Barracuda WAF auch die Xelon Managed WAF innerhalb von wenigen Minuten bereitgestellt werden.

DARUM SOLLTEN DIE DATEN Eurer KUNDEN IN DER SCHWEIZ BLEIBEN



Autor: Ueli Schwegler
BD Manager, Xelon AG

Viele Unternehmen brauchen Jahre, um sich von den Folgen von Hacks und Datendiebstählen zu erholen, da das Vertrauen der Kunden langfristig zerstört ist. Daher ist es zentral, dass ihr sensible Kundendaten bestmöglich vor unerlaubten Zugriffen durch Cyber-Kriminelle schützt. Dazu sollte unbedingt der Datenaufbewahrungsort berücksichtigt werden.

Daten werden mitunter als wichtigste Währung der digitalen Welt bezeichnet. Sie erlauben es Unternehmen, die Kundenbindung zu vertiefen und den Marktanteil zu erhöhen. Gleichzeitig sorgen Hackerangriffe und Datendiebstähle regelmässig für Schlagzeilen. Wieso sind Daten so wertvoll?

Daten sind allgegenwärtig, existieren in verschiedenen Formen, und kreieren kombiniert Muster. Werden diese Muster mit anderen Datenquellen vernetzt, bilden sich wiederum Cluster. Es wird davon ausgegangen, dass die Datenmenge künftig exponentiell zunehmen wird. Ohne passende Auswertungen und Analysen sind Daten nur wenig wert; sie müssen in einen Kontext gestellt werden, um für Unternehmen Wert zu stiften. Dabei werden grosse Datenmengen unabhängig von Quelle und Format verarbeitet. Die richtigen Daten und Muster helfen dabei, geschäftskritische Entscheidungen zu treffen. Datenwissenschaftler sind überzeugt, dass Unternehmen in allen Branchen von der zielgerichteten Datennutzung profitieren könnten.

Personalisierte Werbeanzeigen, die Differenzierung von Stammkunden und Erstbesuchern im Online-Shop oder Ausloten des Marktpotenzials für eine neue Idee: Kundendaten ermöglichen es Unternehmen, die Beziehung zu ihren Kunden laufend zu vertiefen und verbessern, das Angebot zu erweitern sowie den Marktanteil zu erhöhen. Hat ein Unternehmen Zugang zu einer repräsentativen Menge an Nutzerdaten, steigen die Chancen, sich erfolgreich auf dem Markt zu positionieren. Marktbeobachter gehen davon aus, dass Datenanalysen in Zukunft eine noch wichtigere Rolle bei der Weiterentwicklung der Geschäftsstrategie spielen wird.

| Datenlecks können für Unternehmen das Aus bedeuten

Eure Kunden müssen die Sicherheit aller gespeicherten personenbezogenen Daten garantieren. Sowohl Mitarbeiter- als auch Kundendaten gilt es bestmöglich zu schützen. Werden diese Daten versehentlich oder absichtlich kompromittiert und stellt sich nach dem Cyberangriff oder dem Datenleck heraus, dass das betroffene Unternehmen keine geeigneten Sicherheitsmassnahmen ergriffen hatte, drohen möglicherweise Bussen und Sanktionen.

Datenlecks und Cyber-Attacken können wie oben bereits erwähnt Kosten in Millionenhöhe, irreparable Reputationsschäden verursachen und Strafuntersuchungen verursachen. Viele Unternehmen brauchen Jahre, um sich von den Folgen von Datendiebstahl zu erholen und für nicht wenige Betriebe bedeuten Cyber-Attacken das Aus. «Die Informationstechnologie macht bekanntlich gewaltige Fortschritte, so dass es möglich ist, enorme Mengen von Personendaten zu erfassen und miteinander in Verbindung zu setzen. Leider hält das Sicherheitsbewusstsein der Datenbearbeiter oft nicht mit den technischen Neuerungen Schritt», schreibt der Schweizerische Datenschutz- und Öffentlichkeitsbeauftragte dazu.

| Bei einem Schweizer IaaS-Provider sind Kundendaten besser aufgehoben als bei einem Hyperscaler

In Zeiten von Datenlecks und immer perfideren Hackerangriffen möchten wohl die meisten Unternehmen und deren Endkunden wissen, wo ihre Daten gespeichert werden. Die meisten Hyperscaler wie Amazon oder Microsoft haben ihren Hauptsitz in den USA, wo der Zugriff auf Unternehmensdaten mittels des Patriot Acts ohne richterliche Kontrolle praktiziert wird. In der Schweiz hingegen ist dies nicht erlaubt.

Möchtet ihr die IT-Infrastrukturen eurer Kunden auf einer sicheren und stabilen Schweizer Cloud-Plattform betreiben und verwalten? [Kontaktiert uns jetzt für eine kostenlose Demo des Xelon HQ.](#)

Wisst ihr, wo sensible Daten gespeichert werden?

Cyber-Attacken können Kosten in Millionenhöhe, irreparable Reputationsschäden verursachen und Strafuntersuchungen verursachen. Viele Unternehmen brauchen Jahre, um sich von den Folgen von Hackerangriffen oder Datendiebstahl zu erholen und für nicht wenige Betriebe bedeuten Cyber-Attacken das Aus. «Die Informationstechnologie macht bekanntlich gewaltige Fortschritte, so dass es möglich ist, enorme Mengen von Personendaten zu erfassen und miteinander in Verbindung zu setzen. Leider hält das Sicherheitsbewusstsein der Datenbearbeiter oft nicht mit den technischen Neuerungen Schritt», schreibt der Schweizerische Datenschutz- und Öffentlichkeitsbeauftragte dazu. In Zeiten von Datenlecks und immer perfideren Hackerangriffen möchten wohl die meisten Unternehmen und deren Endkunden wissen, wo ihre Daten gespeichert werden. Die meisten Hyperscaler wie Amazon oder Microsoft haben ihren Hauptsitz in den USA, wo der Zugriff auf Unternehmensdaten mittels des Patriot Acts ohne richterliche Kontrolle praktiziert wird. In der Schweiz hingegen ist dies nicht erlaubt.

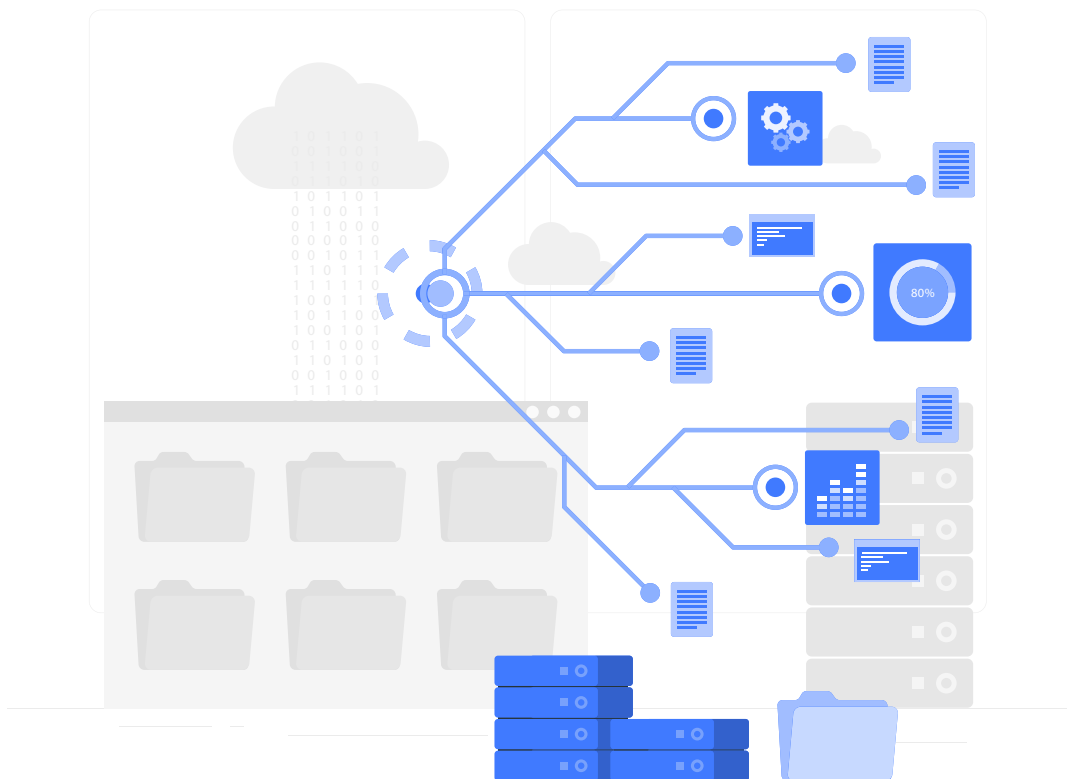
Xelons Cyber-Security- und Datenschutz-Experten raten Unternehmen aller Grössen dazu, ihr Datenschutz-Konzept regelmässig zu überprüfen. So können allfällige Schwachstellen entdeckt und behoben werden. Bei der Zusammenarbeit mit einem IaaS-Provider kümmert sich in der Regel der externe Partner um die Sicherheit der IT-Umgebung. Der Unternehmensstandort spielt eine wichtige Rolle bei der Wahl eines IT-Infrastruktur-Providers. Lokale Provider befolgen Schweizer Datenschutzgesetze und können dadurch höchste Datensicherheitsstandards garantieren. Unsere Infrastruktur befindet sich in Rechenzentren in den Kantonen Aargau und Zürich und sämtliche Kundendaten unterliegen dem Schweizer Datenschutzgesetz. Xelon erhielt im Juli 2020 die ISO-Zertifizierung 27001. Dabei handelt es sich um die international führende Norm für Informationssicherheits-Managementsysteme und um die wichtigste Cyber-Security-Zertifizierung.



Use Case: Patientendaten werden ausschliesslich in der Schweiz aufbewahrt

Ein interessantes Beispiel für eine komplett in der Schweiz gehostete Infrastruktur-Lösung ist die Zusammenarbeit von Xelon und dem IT-Dienstleister Teleinformatik für die Migration der IT-Infrastruktur von SOS AERZTE. Die Ärztevereinigung berät und versorgt pro Jahr rund 20'000 Patienten im Kanton Zürich. Angesichts dieser wichtigen Funktion in der Gesundheitsversorgung in zahlreichen Gemeinden dürfte es selbsterklärend sein, dass die IT-Umgebung inklusive telefonischem Notfalldienst von SOS AERZTE zu jeder Tag- und Nachtzeit verfügbar sein muss. Das Unternehmen möchte keine eigene Infrastruktur betreiben und lagerte die komplette IT- und Telefonie-Infrastruktur in ein externes Datacenter aus.

SOS AERZTE wandte sich für eine externe Stellvertretung und Unterstützung in IT-Fragen an das Schweizer IT-Traditionsunternehmen Teleinformatik Services AG. Ein wichtiger Punkt bei der Migration war, dass die IT-Systeme jederzeit von überall aus erreichbar sind, denn die meisten Benutzer arbeiten entweder im Homeoffice oder unterwegs. Teleinformatik migrierte die IT-Infrastruktur von SOS AERZTE und baute eine geo-redundante 3CX-Telefonanlage auf, was die Ausfallsicherheit der Notfallnummer erhöhte und den Mitarbeitenden von SOS AERZTE sowohl im Homeoffice als auch bei Ausseneinsätzen jederzeit Zugriff auf die IT-Umgebung garantiert. Xelon unterstützte die Migration.





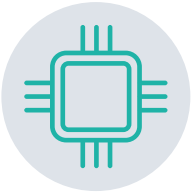
DISASTER RECOVERY – DAS GEHÖRT IN EINEN NOTFALLPLAN



Autor: Janic Voser
System Engineer, Xelon AG

Ob Hackerangriff, Feuer oder Überschwemmung: Hier erfahrt ihr, wie ihr die Dokumente, Anwendungen und Daten eurer Kunden vor Cyber-Attacken und Naturkatastrophen schützen könnt und was es beim Erstellen eines Disaster-Recovery-Plans zu beachten gilt.

Die von euch betreuten Unternehmen sind auf Dokumente, Anwendungen und Daten angewiesen, um Ziele zu erreichen, Gewinne zu erzielen und die Marktposition zu festigen. Kann nicht mehr auf wichtige Tools zugegriffen werden, führt dies zu Gewinneinbussen, Reputationsschäden und teilweise sogar rechtlichen Konsequenzen. Wie nicht zuletzt die vergangenen Jahre und Monate bewiesen haben, sind nach wie vor viele Ereignisse nicht 100-prozentig planbar – doch man kann sich immer auf allfällige Krisensituationen vorbereiten. Nachfolgend zeigen wir die häufigsten Notfallszenarien auf und erklären, wie ihr diesen begegnen könnt.



Ausfall von Hardware

Serverkomponenten sind dafür ausgelegt, rund um die Uhr betrieben zu werden. Wie ihr wisst, sind viele Bestandteile selbst bei sorgfältigster Behandlung anfällig und es geht nicht selten etwas kaputt. Die am häufigsten ausfallenden Komponenten sind HDD, SSD und Netzteile. Verhindern lassen sich diese Ausfälle nicht, man kann jedoch Komponenten redundant auslegen, damit kein Betriebsunterbruch entsteht.

Bei HDD/SSD wird dies üblicherweise mit einem RAID-Verbund gelöst. Bei der Stromzufuhr werden mehrere Netzteile verwendet, dabei gilt: minimum Anzahl Netzteile +1, um eine Redundanz zu gewährleisten. In virtualisierten Umgebungen empfiehlt es sich zudem, VMs auf einem redundanten Shared Storage zu betreiben. Die VMs können somit einfach auf einem anderen Server gestartet werden, falls mehr als eine Disk oder ein Netzteil nicht mehr funktioniert. VMs können auch auf einen weiteren redundanten Storage repliziert werden, zum Beispiel in ein zusätzliches Rechenzentrum. Hierbei wird zwischen asynchroner und synchroner Replizierung unterschieden. Bei der asynchronen Replizierung wird der aktuelle VM-Stand in einem selbst gewählten Intervall in den zweiten Standort repliziert. Bei einer synchronen Replizierung werden die Daten in Echtzeit an zwei Standorten geschrieben, sofern die entsprechende Bandbreite zwischen den beiden Standorten zur Verfügung steht.

Auch auf Applikationsebene können Replikate realisiert werden, dort wird dann umgangssprachlich von einem Cluster gesprochen. In jedem Fall empfiehlt es sich, zusätzlich eine Datensicherung zu verwenden.



Probleme mit dem OS

Probleme mit dem Betriebssystem gibt es häufig, nachdem man Updates installiert hat. Die schnellste und einfachste Methode ist der VM Snapshot. Vor der Installation grösserer Updates empfiehlt es sich, immer einen Snapshot der VM zu erstellen. Im Falle eines Problems kann innert Sekunden auf den alten Stand zurückgesprungen werden. Dies wäre auch möglich mit einem asynchronen VM Replikat, solange dies noch den alten Stand hat.



Datenverlust

Ob ein Benutzer eine Datei überschreibt oder löscht, jemand unbefugt auf das System zugreift oder Unternehmen Datenlecks übersehen: Datenverlust kann durch verschiedenste Möglichkeiten entstehen.

Als längerfristige Lösung verwendet man üblicherweise eine Datensicherung. Wichtig: Die Datensicherung muss durch den IT-Service-Provider überwacht und regelmässig getestet werden. Wir empfehlen zudem, dass vom gesicherten Server nicht direkt auf die Backups zugegriffen werden kann wie zum Beispiel mittels SMB. Ansonsten wäre es für einen Cyber-Angreifer leichtes Spiel, die Backups ebenfalls zu löschen. Für den Fall eines Brandes empfiehlt es sich, eine externe Sicherung zu haben – umso mehr, wenn keine Replikationen existieren. Um kurzfristig Daten zurückzuspielen, können mittels VSS auf dem Server mehrere Generationen eines Laufwerks erstellt werden. Der Vorteil dabei ist, dass die System-Performance nur sehr gering bis gar nicht beeinträchtigt wird. Zudem können die Daten sehr schnell und einfach auf dem Server direkt wiederhergestellt werden. Dieser Ansatz ersetzt jedoch kein Backup, da bei einem Hardware-Ausfall oder einer Naturkatastrophe die Daten trotzdem weg sind. Auch beim Zugriff durch unberechtigte Dritte können die VSS-Daten gelöscht werden, sollten die Hacker administrativen Zugriff auf das System erlangen.

Welche Software schützt wertvolle Daten bestmöglich?

Mit der richtigen Backup-Lösung können Datenverluste selbst bei Naturkatastrophen oder Hackerangriffen vermieden werden. Welche Software für das Sichern von Daten verwendet werden soll, hängt von 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.

Backups für On-Premise-Infrastrukturen und dedizierte Server werden vielfach mit der Software Acronis kreiert. Bei dieser Option erstellen wir einen Acronis-Account für unsere Kunden, die anschliessend den Backup Agent auf den gewünschten Systemen installieren und ihre Backup Jobs über Acronis verwalten. Die Daten werden in den ISO-zertifizierten Xelon Datacentern in der Schweiz gespeichert.

Für virtuelle Umgebungen und On-Premise virtualisierte Umgebungen eignet sich das Veeam Cloud Connect Backup. Dabei handelt es sich um eine leistungsstarke, einfach bereitzustellende Cloud-Technologie, die IT-Dienstleister und Systemintegratoren als Basis für Cloud-Backups verwenden können. Xelon ist zertifizierter Veeam-Partner.

A portrait of a man with short brown hair and light eyes, wearing a dark green and black plaid sweater. He is looking directly at the camera with a slight smile. The background is a solid dark blue.

MICHAEL DUDLI

Wir freuen uns, dass ihr das E-Book rund um das Thema Cyber-Security heruntergeladen habt und sind gespannt auf eure Feedbacks.

Welche Herausforderungen seht ihr in Bezug auf die Security bei der Betreuung der IT-Infrastrukturen eurer Kunden?

[Kontaktiert](#) uns für einen Austausch über die aktuelle Bedrohungslage und Gegenmassnahmen.