Strategien für die Krise

Know-how Naturkatastrophen, technische Störungen und vor allem Cyberangriffe: Unternehmen müssen sich intensiv vorbereiten, um IT und Prozesse für einen Krisenfall zu rüsten. Ein komplexes, aber immer drängenderes Vorhaben.

Von Stefan Adelmann

INHALT

Strategien für die Krise	28
Disaster-Recovery-Plan: Vorbereiten auf den Ernstfall	32
Interview: «Jeder Fall ist einzigartig»	35
Mit Cyber-Resilienz gegen Hackerangriffe	37
Interview: «Nur wenn man darüber redet, können andere davon lernen»	39
Disaster-Recovery-Plan testen, Cyber-Resilienz aufbauen	42

Mittlerweile kann es jeden treffen!», warnt Sebastian Schäffer, Business Consultant beim Schweizer IT-Dienstleister UMB. Für Unternehmen aller Branchen, Grössen und jedes Standortes gilt: «Der Ansatz ‹Ach, wir sind viel zu uninteressant für Hacker› ist schlicht falsch.» Wie Statistiken zeigen würden, seien Unternehmen in den USA, im mittleren Osten oder in Deutschland zwar weit häufiger Ziel von Cyberattacken als Firmen in der Schweiz. Zudem unterscheiden sich die Zahlen auch nach Branchen. Besonders betroffen sind demnach das Gesundheitswesen, der Finanzbereich sowie Unternehmen aus Energie, Pharma und Industrie. Aber die Dunkelziffer sei trotz Meldepflicht gross, mahnt Schäffer. Die vergangenen Jahre haben ohne Frage verdeutlicht, dass es letztlich jedes Unternehmen treffen kann und dass profitorientierte Cyberkriminelle kaum mehr unterscheiden. Auch Marco Eggerling, Global CISO des IT-Security-Anbieters Check Point, warnt vor diesem Hintergrund: «Kleine Betriebe sind zumeist eher betroffen, weil das Budget für Cybersicherheit geringer ist als in Grosskonzernen. Dafür ist dort die Risikofläche wiederum dramatisch grösser.» Eggerlings ernüchterndes Fazit: «Es gibt leider keine Industrie, die sich aktuell ausruhen kann oder sich ausgenommen fühlen sollte.»

Grundsätzlich müssen sich daher alle Unternehmen auf einen möglichen Ernst-

Sebastian Schäffer, Business Consultant, UMB: «Viele Unternehmen wiegen sich in falscher Sicherheit und vertrauen auf ungeprüfte Backups und Disaster-Recovery-Lösungen. Das kann in einer Katastrophe enden. Nur ein umfassendes, geprüftes und durchexerziertes Disaster-Recovery-Konzept kombiniert mit präventiven Cybersecurity-Schutzmassnahmen bietet heute noch den notwendigen Schutz.»

Thorsten Henning, Director Systems Engineering DACH, Fortinet: «Selbst wenn ein Angriff scheinbar beendet ist, ist es sehr wahrscheinlich, dass die Cyberkriminellen noch immer im Unternehmensnetzwerk präsent sind. Daher sollten aktive Malware oder hartnäckige Überreste identifiziert und beseitigt werden. Wichtig dabei ist, den Status quo und alle Erkenntnisse über den Angriff zuerst sorgfältig zu dokumentieren.»

fall intensiv vorbereiten. Dieser kann jedoch vielfältige Ursachen haben, längst nicht nur Cyberangriffe. Auch Stromausfälle, Naturkatastrophen oder gar militärische beziehungsweise terroristische Angriffe können Betriebsausfälle bedingen. Aufgrund der zunehmenden Frequenz und immer perfideren Methoden gehören die Cyberbedrohungen aber sicherlich zu den drängendsten Risiken, für die Unternehmen einen Notfallplan in petto haben sollten. So beobachtet das Cyber Defence Center von UMB aktuell vor allem Identitätsklau und Ransomware als besonders häufig genutzte Angriffsvektoren. Zudem hat sich auch das anschliessende Vorgehen der Akteure geändert, nachdem der Zugriff auf die Systeme gelungen ist. «Kriminelle nisten sich oft über eine längere Zeit in der Infrastruktur von Unternehmen ein, bevor sie zuschlagen», berichtet Schäffer. Cybersecurity-Spezialist Thorsten Henning, Director Systems Engineering DACH bei Fortinet, warnt zudem vor häufigen Angriffen auf die Betriebstechnologie, also die OT. «Ein solcher Angriff geht meist mit der Verschlüsselung wichtiger Unternehmensdaten einher, was für die betroffenen Unternehmen grosse Auswirkungen auf ihren Geschäftsbetrieb haben kann.»

Ausfall ganzer Systeme und Prozesse

Im Worst Case werden bei einem erfolgreichen Cyberangriff ganze Systeme und Prozesse lahmgelegt, berichtet Henning. Dies führe in den meisten Fällen wiederum zu einer Unterbrechung des Geschäftsbetriebs, was für kritische Infrastrukturen wie die Stromversorgung erhebliche Auswirkungen hat. «Aber auch für kleinere Unternehmen kann ein erfolgreicher Angriff schnell zu einer existenziellen Bedrohung werden. Neben den unmittelbaren Folgen besteht ausserdem gerade auch bei einem Ransomware-Angriff das Risiko, dass gestohlene und meist sensible Daten veröffentlicht oder im Darknet verkauft werden.»

Ein Szenario, das vor rund einem Jahr der Münsingener Cloud-Dienstleister Unico am eigenen Leib erfahren musste. Die kriminelle Gruppe Play hatte über Pfingsten Zugriff auf die Infrastruktur des Providers erlangt und konnte zahlreiche Kundendaten erbeuten. Lediglich das schnelle Handeln und die umfassenden, eingeübten Vorkehrungen verhinderten, dass die Daten zugleich auch gelöscht beziehungsweise verschlüsselt wurden (mehr lesen Sie ab Seite 39). Vor dem Hintergrund vergleichbarer Fälle appelliert Fortinet-Manager Thorsten Henning: «Unternehmen müssen sich dieser Gefahren bewusst werden und taktisch genauso effizient sein wie ihre Gegner.» Denn diese müssen heute wiederum keine Cyberexperten mehr sein, um Erfolg zu haben. Via Cybercrime-as-a-Service könne sich laut Henning grundsätzlich jeder entsprechende Dienstleistungen im Darknet kaufen und somit Cyberattacken durchführen. «Unternehmen sollten daher ihre Systeme, Tools und Technologien immer auf dem neusten Stand halten und an die neusten Taktiken und Angreifer anpassen.»

Drohende Insolvenz

Doch nicht nur der Case Unico zeigt: Selbst das Know-how sowie die IT-Security-Vorkehrungen eines erfahrenen IT-Dienstleisters können bei einem gezielten Angriff oftmals nicht vor Schäden bewahren. Der Ausfall ganzer Systeme droht und damit gegebenenfalls ein langwieriger Prozess, den Betrieb wieder zum Laufen zu bekommen. «Nach heutigem Stand dauert die Neubeschaffung von Hardware Tage oder sogar Wochen», erklärt Schäffer von UMB. «Ohne wasserdichtes Backup-Konzept, welches auch Konfigurationen von Infrastrukturen, Servern und Applikationen beinhaltet, kann der Neustart der eigenen Geschäftstätigkeit so lange dauern, dass es für viele Firmen lebensbedrohlich wird.» Längst kein Ausnahmeszenario. Nach einem Ransomware-Angriff rutschte 2019 beispielsweise der Fensterhersteller Swisswindows in die Pleite, Ende 2022 traf es den E-Bike-Hersteller Prophete, 2023 den Textilkonzern Erfo: die Liste ist mittlerweile lang.

Die richtigen, detaillierten und regelmässig durchgeprobten Massnahmen können also zum Überlebenskriterium werden. Denn ein erfolgreicher Cyberangriff reicht oft aus, «um den Betrieb eines Unternehmens vollständig lahmzulegen», warnt auch Henning. Deshalb ist es wichtig, sich vorzubereiten – ein Disaster-Recovery-Plan sollte dabei ein wichtiges Element dieser Vorbereitung sein.» Aber auch hier gilt es zu differenzieren, wie Schäffer von UMB unterstreicht. Punktuelle Investitionen reichen heutzutage nicht mehr aus oder haben gar einen gegenteiligen Effekt. «Viele Unternehmen wiegen sich in falscher Sicherheit und vertrauen auf ungeprüfte Backups und Disaster-Recovery-Lösungen. Das kann in einer Katastrophe enden.» Nur ein umfassendes, geprüftes und durchexerziertes Disaster-Recovery-Konzept kombiniert mit präventiven Cybersecurity-Schutzmassnahmen biete heute noch den notwendigen Schutz.

Grundsätzlich sollte sich laut dem UMB-Experten jedes Unternehmen Gedanken zur eigenen Verletzlichkeit machen und mit einer Analyse der Risiken (Business-Impact-Analyse) bezüglich seiner Geschäftstätigkeit starten. «Daraus

abgeleitet wird in der Regel eine Business-Continuity-Strategie mit konkreten Krisen- und Notfall-Management-Plänen entsprechend der zu erreichenden Resilienz und der erforderlichen Wiederherstellungszeit der Geschäftsprozesse.»

Proaktive und reaktive Mechanismen

Schäffer ist sich sicher, dass ein gut erarbeiteter und erprobter Disaster-Recovery-Plan die schlimmsten Folgen eines erfolgreichen Cyberangriffs abfedern kann. Unter der Voraussetzung, dass dieser Plan aktuell ist und laufend an Veränderungen angepasst wird, helfe er, Ausfallzeiten zu minimieren und die Wiederherstellung der normalen Geschäftstätigkeit so schnell wie möglich wieder zu erreichen. Ideal sei es zudem, die Notfallpläne mit proaktiven Schutzmechanismen zu ergänzen.

Marco Eggerling weist ebenfalls darauf hin, dass das Business-Continuity-Management reaktiver Natur ist und Schäden eines Angriffs daher zwar nicht abwendet, dafür aber dabei hilft, schnell wieder auf die Beine zu kommen beziehungsweise den Betrieb überhaupt wieder aufzunehmen. «Ein ordentliches Krisenmanagement beginnt damit, Backups zu machen und diese periodisch zu testen, ergo zurückzuspielen», erklärt der Check Point-CISO. «Wenn alles gut ist, ist man schon mal einen Schritt weiter. Dann muss entschieden werden, ob die Backups verschlüsselt werden sollen. Das ist eine Weggabelung.» Denn im Krisenfall gehe es heiss her. Ein zuvor definiertes und etabliertes Krisen-Management-Team kann die betroffenen Mitarbeiter in dieser anspruchsvollen Situation psychologisch stark entlasten. Auch die regelmässige Erprobung von Krisenszenarien, ein sogenanntes Table-Top-Exercise, trägt dazu bei. «Dafür können auch gerne ein paar Franken für externe Dienstleister investiert werden, weil diese geübt sind in der Durchführung solcher Übungen», rät Eggerling.

Nur ein Feld brennt

Aus der jahrelangen Praxiserfahrung gibt der CISO zudem eine Handlungsempfehlungen für den Ernstfall: «Als ich noch im Consulting gearbeitet haben, habe ich bei Krisensimulationen immer darauf gedrungen, die wichtigsten Telefonnummern ausgedruckt im Portemonnaie zu haben. Auf die digitale Kommunikationsinfrastruktur à la MS Teams oder Whatsapp ist allenfalls dann kein Verlass mehr und auch das Active Directory ist allenfalls down.» Zudem legt der IT-Security-Experte betroffenen Unternehmen eine sehr engmaschige Segmentierung des Netzwerks ans Herz. Das sei zwar nicht einfach umzusetzen, helfe aber im Krisenfall. «Stellen Sie sich ein Schachbrett vor: Wenn es brennt, dann nur in einem Feld. Die Felder rundherum sind nicht betroffen.»

Zudem nennt der CISO einen zusätzlichen wichtigen Punkt einer detaillierten Vorbereitung, der heutzutage weit über reine Cyberrisiken hinausreicht: Was, wenn die Cloud nicht mehr erreichbar ist? In Zeiten von Azure, AWS und Google Cloud können von einer entsprechenden Unterbrechung immerhin Datenzugriff, Tools oder ganze Systembereiche betroffen sein. «Wenn hier Störungen vorliegen und SaaS die einzige Möglichkeit war, dann muss bereits heute an einem Plan B gearbeitet werden – und wenn dieser noch so unwahrscheinlich ist», untermauert Eggerling. «Der Tag kommt, an dem er benötigt wird und dann ist man froh, wenn es man etwas in der Hinterhand hat, auch wenn es nicht komfortabel oder innovativ anmutet.»

«Besonnen und überlegt agieren»

Das Wichtigste bleibt laut den Experten aber auch im Krisenfall: Ruhe bewahren. «Wer sich gut vorbereitet, kann sich auf seine Massnahmen verlassen», sagt Schäffer. Er empfehle, auch bei einem Vorfall jederzeit strategisch zu handeln. «In kritischen Momenten ist es essenziell, besonnen und überlegt zu agieren. Entwickeln Sie eine durchdachte Strategie unter Einsatz aller verfügbaren Ressourcen, um effektiv auf die Situation reagieren zu können. Notfallpläne sind dafür die Basis.» Ein zentraler Bestandteil dieser Pläne muss zudem eine zielgerichtete Kommunikation sein. In Richtung betroffener Kunden, aber auch in Richtung der eigenen Belegschaft, der Behörden und letztlich der Öffentlichkeit – selbst wenn das im ersten Moment wie ein Reputationsschaden wirken mag.

Wie der Fall Unico (ab Seite 40) zeigt, bringt eine an den richtigen Stellen transparente, proaktive Kommunikation aber nicht nur Vorteile für das betroffene Unternehmen, sondern den gesamten Markt mit sich. Andere Betriebe werden gewarnt, können gegebenenfalls aus dem individuellen Vorgehen lernen. «Die Bedeutung einer klaren und zielgerichteten Kommunikation sollte nicht unterschätzt werden», sagt auch Schäffer. «Ein umfassender Kommunikationsplan, der alle relevanten Stakeholder berücksichtigt, ist entscheidend für den Erfolg und die Bewältigung der Krise. Stellen Sie also sicher, dass alle Stakeholder erreicht werden und transparent, klar und regelmässig Informationen weitergegeben werden.» Nur so könne das Vertrauen aufrechterhalten und eine effiziente Bewältigung der Krise gewährleistet werden. ■

Marco Eggerling, Global CISO, Check Point: «Als ich noch im Consulting gearbeitet haben, habe ich bei Krisensimulationen immer darauf gedrungen, die wichtigsten Telefonnummern ausgedruckt im Portemonnaie zu haben. Auf die digitale Kommunikationsinfrastruktur à la MS Teams oder Whatsapp ist allenfalls dann kein Verlass mehr und auch das Active Directory ist allenfalls down.»