Abwehr von „Ransomware-Angriffen“ bedingt etabliertes Krisenmanagement

Dr. Christoph U. Eichel,
CEO,
Result Group GmbH

Sebastian Reis,
Senior Consultant,
Result Group GmbH

Die Münchener Wohnungsgesellschaft GWG und die Funke-Medien Gruppe sind die jüngsten Opfer verheerender Ransomware-Angriffe, denen in den Medien große Aufmerksamkeit zu Teil wurde. Sie sind jedoch nur prominente Beispiele, denn wie so oft, stellen sie nur die Spitze des Eisberges dar. Viele Unternehmer und Firmen sehen die Gefahr krimineller Angriffe auf ihre IT-Systeme als reines Problem ihrer IT-Abteilung und unterschätzen zudem die Eintrittswahrscheinlichkeit eines solchen Angriffes. Das liegt zum einen an der genannten selektiven Berichtserstattung, die ausschließlich die bekannt gewordenen Fälle thematisiert, die entsprechend Aufsehen erregen. Zum anderen liegt es aber auch an der Komplexität der Problematik, die es schwer macht, die Angriffsmöglichkeiten und deren Auswirkungen zu erfassen.

Ransomware ist nicht nur Ransomware

Einem Angriff auf die IT kann aus verschiedenen Motivationen erfolgen, aber auch unterschiedliche Schäden hervorrufen. Neben der Erpressung von Lösegeld könnten auch politische Forderungen („Hacktivism“), oder die Behinderung von Geschäften durch ein Konkurrenzunternehmen oder einen Staat die Motivation für einen Angriff sein.

Ransomware-Angriffe sind für Hacker sehr lukrativ und besonders effizient. Möglichst alle Daten werden dabei mit sehr komplexen Algorithmen verschlüsselt und sind somit kurzfristig nicht mehr verfügbar. Da ein Unternehmen vom ersten Moment an stark eingeschränkt wird und somit Geld verliert, ist eine Lösegeldzahlung folglich naheliegend. Doch Vorsicht:

- Lösegeldzahlungen können durch staatliche Autoritäten sanktioniert sein, besonders in den USA. Im Oktober 2020 erst veröffentlichte das US Department of Treasury Office of Foreign Assets Control (OFAC) ein „Advisory“. Fokus ist die Sanktionsmöglichkeit für Zahlung an Täter, die mit der Zahlung Schaden an US-Interessen herbeiführen (können). Viele Hackergruppen sind weltweit aktiv und werden dementsprechend auch verfolgt. Sie mit Lösegeld zu „unterstützen“ könnte auch für den Zahlenden rechtliche und wirtschaftliche Konsequenzen haben.

- Lösegelder sind oft verhandelbar, Sicherheiten sollten eingefordert werden. Professionelle Verhandlungsführer können hierbei Risiken senken und Kosten reduzieren. Grundsätzlich gilt: Lösegeldzahlungen geben keinerlei Garantie dafür, dass die Systeme auch tatsächlich wieder entschlüsselt werden. Die Angreifer sind durch ihre Anonymität im Vorteil, sie ausfindig zu machen ist fast unmöglich. Auch hier können im Rahmen der Lösegeldverhandlungen durch Experten wertvolle Informationen zur späteren Strafverfolgung der Täter gewonnen werden.

- Mit einer Lösegeldzahlung vergrößert sich das Problem für den Betroffenen und andere: Sie „subventionieren“ die „Ransomware-Industrie“ und fördern somit eine Weiterentwicklung der Angriffsmethoden. Zudem macht sich das angegriffene Unternehmen weiter verwundbar: wer einmal zahlt, zahlt auch wieder. Und, die Einfallstore für den „Gegner“ sind im schlimmsten Fall nach Entschlüsselung der Systeme weiterhin offen.

Auch die Angreifer entwickeln sich weiter: Da viele Unternehmen die Angreifbarkeit durch Ransomware in den vergangenen Jahren durch die Schaffung von physisch getrennten Backups verringert haben, mussten die Angreifer ihre Methoden anpassen. Die neuesten Angriffe beschränken sich nicht nur auf die Verschlüsselung ihrer Unternehmens-IT. Häufig werden mittlerweile vor der Verschlüsselung unternehmenskritische Daten aus dem Netzwerk gezogen und mit deren Veröffentlichung, Vernichtung oder Missbrauch gedroht, falls kein Lösegeld gezahlt wird. In einem aktuellen prominenten Fall wurde die argentinische Visa-Behörde erpresst und nach Scheitern der Erpressung die gesamten Pass-Daten hunderttausender Reisender im Internet veröffentlicht.

Weiterhin greifen die Hacker nicht mehr nur Unternehmensnetzwerke an, sondern entwickeln hochkomplexe Schadsoftware, die in Regelungstechnik eindringt und diese verschlüsselt. Die zentrale IT bleibt davon unbetroffen, jedoch können

beispielsweise ausgelagerte Anlagen wie Pumpen, Sensoren und Stellwerke betroffen sein, die in Folge komplett ausfallen. Jedes System müsste in diesem Fall vor Ort durch geschultes Personal mit neuer Software versehen, neu angelernt und wieder an das zentrale Netz angebunden werden. Die Ausfallzeiten und -Kosten können hier besonders bei international agierenden Großkonzernen beträchtlich sein.

Keine Investition in Sicherheit? So werden Cyber-Attacken schnell existenzbedrohend

Krisenmanagement- und Sicherheitsberatungsunternehmen befassen sich regelmäßig mit der Koordination der Abwehr entsprechender Angriffe und helfen Unternehmen wie auch Privatkunden in Notlagen. Die Erfahrung zeigt, dass der Großteil deutscher Unternehmen schon unvorbereitet in eine Attacke hineingerät und dadurch das Schadensausmaß oftmals größer ist, als es sein müsste. Doch woran liegt das? Welche präventiven Maßnahmen außer der Optimierung der IT können das Schadensausmaß verringern?

1. Angriffe auf die IT sind immer ein massives Problem des Business Continuity Managements

Ein großangelegter Angriff auf die IT eines Unternehmens kann sehr lange Zeit unentdeckt bleiben; das Ausmaß ist entsprechend fatal. Sich auf die Daten-Backups zu verlassen, ist für Unternehmen nicht ausreichend. Im Falle einer Verschlüsselung durch Ransomware müssen alle Systeme physisch vom Internet getrennt und in einer sicheren Umgebung einzeln und sehr zeitaufwendig auf Schadsoftware untersucht werden. Das gilt auch für die Backups, die im Falle eines langwierigen Angriffs schon längst mit Schadsoftware verseucht sein können.

Durch die Verflechtung der IT in alle Unternehmensbereiche bedeutet das, dass jeder Bereich im Rahmen des Business Continuity Managements in der Lage sein sollte, mehrere Wochen bis Monate die Grundfunktionen aufrecht erhalten zu können – und das ohne Zugriff auf Daten und IT-Systeme. Das erfordert eine umfassende Risikoanalyse des gesamten Unternehmens, die Identifikation aller unternehmenskritischen Prozesse und Assets, Entwicklung von Maßnahmenkatalogen zur Absicherung selbiger, sowie Vorbereitung von Ausweichoptionen im Falle von temporären oder dauerhaften Verlust kritischer Elemente. Dies sollte natürlich vor dem Eintritt eines Angriffs geschehen und regelmäßig überprüft und angepasst werden.

2. Angriff existenzbedrohend? Das löst nur ein Krisenstab

Ja, einen Krisenstab kann man bilden, wenn er nötig wird. Dann ist er aber womöglich nicht effektiv genug. Krisenstäbe müssen gut vorbereitet sein, das Personal mit Bedacht ausgewählt und geschult sein, die Alarmierungswege müssen funktional sein, das Equipment muss bereitstehen und der Handlungsspielraum sollte umfassend sein, denn bei der Rettung der Existenz darf es keine Grenzen geben. Krisenstäbe arbeiten per Definition außerhalb der Linienorganisation des Unternehmens; agil und kreativ.

Ein Krisenstab sollte zudem speziell auf die konkreten Fragestellungen für ein solches Szenario geschult werden. Beispielsweise die Einhaltung gesetzlich vorgegebener Meldefristen gegenüber Datenschutzinstitutionen, Notwendigkeit der Einbeziehung von Behörden, Fähigkeiten und Kosten von IT-Forensikern, Dauer und Umfang des Ausfalls von IT-Anlagen etc.

3. Wahrscheinlich lässt einer Ihrer Mitarbeiter die Kriminellen rein

IT-Angreifer finden in den meisten Fällen durch Menschen ihren Weg in das Netzwerk. In 70 bis 80 % der Ransomware-Angriffe ist das Eindringen in die IT-Infrastruktur auf Fehlverhalten eines Mitarbeiters oder einer Mitarbeiterin zurückzuführen. Und das liegt nicht an böser Absicht oder fahrlässigem Verhalten, sondern meist an fehlendem Bewusstsein oder ganz menschlichen Schwächen. Angreifer nutzen immer mehr Methoden des „Social Engineering“: sie ermitteln mögliche Zielpersonen in Ihrem Unternehmen, informieren sich über diese und sprechen diese gezielt in Telefonaten oder Emails, oftmals sogar im privaten Bereich, an, um deren Vertrauen zu gewinnen. In den allermeisten Fällen platzieren die Angreifer so ihre Schadsoftware, ohne dass den „Türöffnern“ überhaupt bewusst ist, dass sie etwas falsch gemacht haben.

Schulungen, Seminare und regelmäßige Awareness-Trainings im Einklang mit Ihrer Unternehmenskultur können hier die Wahrscheinlichkeit eines Einbruchs in Ihre IT minimieren und sogar zu einer Erkennung möglicher Angriffsversuche beitragen.

Fazit

Die Vorbereitung auf einen Schadensfall durch Ransomware ist essentiell für eine effektives Krisenmanagement und die Aufrechterhaltung der Unternehmensprozesse. Mit einem ganzheitlichen Ansatz, der sich nicht nur auf die IT-Sicherheit und die Arbeit Ihrer IT-Abteilung stützt, können Eintrittswahrscheinlichkeit und Schadensausmaß deutlich reduziert werden. ■