Cyberangriffe – Wie sie ablaufen und wie Unternehmen sich schützen

«Es ist nicht die Frage ob, sondern wann es passiert» – Eine Aussage, die im Zusammenhang mit Cyberangriffen immer wieder fällt. Bettina Zimmermann, Expertin für Krisenmanagement und Sicherheit sowie Gastrednerin bei Rochester-Bern Executive Programs erklärt, was ein Angriff bedeutet und wie Unternehmen richtig reagieren.

Cyberangriffe haben zugenommen. Gründe hierfür sind unter anderem die Corona-Pandemie und der Ukraine-Krieg. «Während der Corona-Pandemie haben viele Unternehmen Homeoffice eingeführt, bevor die ganzen Sicherheitsmassnahmen bereit waren», sagt Zimmermann. Dadurch gab es Sicherheitslücken, die jetzt von Hackern ausgenutzt werden. Seit dem Beginn des Ukraine-Kriegs geht in europäischen Ländern zudem die Angst vor Cyberangriffen aus Russland um. «Cyberangriffe in diesem Zusammenhang können eine Form der hybriden Kriegsführung sein», so Zimmermann.

Der Ablauf eines Angriffs

Die Hacker wählen in der Regel nicht gezielt ein Unternehmen aus, sondern suchen nach Sicherheitslücken. Wenn sie Lücken gefunden haben, starten sie Angriffe. Bei einem erfolgreichen Angriff verteilt sich die Ransomware – das Schadprogramm – anschliessend im IT-System des Unternehmens, und zwar ohne, dass es das Opfer bemerkt. Bei den heutigen sog. Double Extorsion Angriffen werden zuerst Unternehmensdaten abgezogen und dann verschlüsselt. Die Opfer stellen mit der Zeit oftmals fest, dass sie sich z. B. nicht mehr in gewisse Programms einloggen können. Was folgt, ist der Schrecken jeder Unternehmensführung, die Daten werden verschlüsselt und ein Erpresserschreiben wird auf dem Server gefunden oder als Pop-up angezeigt.

Sollte das angegriffene Unternehmen ein Backup haben, welches erfolgreich zurückgespielt werden kann und aus diesem Grund nicht auf die Lösegeldforderung der Erpresser eingeht, gehen die Hacker in die zweite Runde und drohen, die abgezogenen Daten zu veröffentlichen. «Dies kann einerseits ein Datenschutzproblem werden und andererseits zu einem grossen Reputationsschaden führen», so Zimmermann. Mittlerweile gibt es auch den Tripple Extorsion Angriff: Dabei werden die Daten abgesaugt, verschlüsselt und anschliessend werden zusätzlich noch mit DDoS-Angriffen weitere Systeme lahmgelegt.

Gut vorbereiten und richtig reagieren

«Cyberangriffe müssen im Risikomanagement aufgenommen und beurteilt werden. Die Verantwortung über das Riskmanagement obliegt dem Verwaltungsrat», sagt Zimmermann. Um die IT auf einem aktuellen Stand zu halten, ist eine regelmässige Sicherheitsprüfung nötig: Sind die Mitarbeitenden bezüglich Sicherheitsrisiken geschult? Werden Updates zeitnah durchgeführt? Hat das Unternehmen ein effizientes Passwortmanagement? Werden Back-Ups regelmässig zur Überprüfung zurückgespielt? Vorteilhaft ist auch, wenn bereits vor dem Ernstfall der Krisenstab definiert wurde. «Ich empfehle einen so kleinen wie möglich, aber so gross wie nötigen Krisenstab. Massvoll aufgebaut auf die Unternehmensstruktur. Wichtig ist, dass Entscheidungsträger Einsitz haben, die die verschiedenen unternehmensspezifischen Fachbereiche abdecken», so Zimmermann.

Der Verwaltungsrat nimmt in Bezug auf den Krisenstab meist die Rolle der Rückfallebene ein. «Krisenmanagement ist grundsätzlich ein operatives Thema. Der Verwaltungsrat soll aber regelmässig informiert werden, damit er über den Fortgang der Krisenbewältigung im Bilde ist und sich einbringen kann, sollte es nötig sein, bspw. wenn es strategische Themen tangiert.», sagt Zimmermann.

Ist der Ernstfall eingetroffen, geht es erstmals darum, die IT vom Netz zu nehmen, damit die Ransomware sich nicht weiter ausbreitet. Der Krisenstab sollte umgehend einberufen werden, da die Fragen, die sich bei einem Cyberangriff im Unternehmen stellen mitunter zu den komplexesten gehören. Bezüglich Kommunikation rät Zimmermann Zurückhaltung. «Stakeholder werden in der Regel nur informiert, wenn sie persönlich betroffen sind und eine Information nach aussen an die Medien/Öffentlichkeit soll gut geprüft und abgewogen werden. Auch mit dem Wording würde ich aufpassen: Müssen wir von einem Cyberangriff sprechen? Oder können wir es auch IT-Vorfall nennen?», so Zimmermann. Nach dem Angriff sollten die Schwachstellen behoben und grundsätzliche Lehren aus dem Vorfall gezogen werden, damit die IT-Sicherheit verbessert werden kann.

Weitere Gefahren nicht vergessen

«Über Cyberangriffe wird aktuell viel gesprochen und die Bedrohung ist real. Es gibt aber auch weitere Gefahren, die in das Risikomanagement einfliessen sollten. Ich denke hier insbesondere an Lieferkettenschwierigkeiten, künstliche Intelligenz oder zukünftige Quantencomputer», sagt Zimmermann. Alle diese Themen bieten neue Chancen und auch Sicherheitsrisiken. Führungskräften und Verwaltungsrät/-innen wird daher empfohlen, sich über diese Themen zu informieren. Ein guter Weg, um in Bezug auf Cybersicherheit und grundsätzlich zu Management-Themen auf dem Laufenden zu bleiben, sind Weiterbildungen, wie jene von Rochester-Bern Executive Programs.