Bild: GettyImages

Auch KMU sind Zielscheibe von Hackern.

Incident Response als Antwort auf Cyber-angriffe

Ob ein Unternehmen zur Zielscheibe für Hacker wird, hängt nicht von dessen Grösse ab, sondern auch von den Sicherheitsmassnahmen. Sind diese schwach, haben die Angreifer leichtes Spiel. Dieser Tatsache sind sich viele kleine und mittelständische Unternehmen jedoch nicht bewusst. Als fester Bestandteil einer umfassenden Security-Strategie hätten sie mit Incident Response ein Werkzeug für den Ernstfall an der Hand.

Dass Hackerangriffe nur global agierende Unternehmen treffen und KMU verschont bleiben, ist ein Irrglaube – auch in der Schweiz. Diese Fehleinschätzung führt dazu, dass Cybersicherheit vielerorts keine grosse Bedeutung beigemessen wird und macht sie so zu einem leichten Angriffsziel für Hackergruppen. Via Ransomware verschaffen sie sich Zugriff auf hochsensible Unternehmensdaten. Ahnungslose Mitarbeitende öffnen eine Phishing-Mail mit Link zu einer nachgebauten Anmeldeseite oder einem Office-Dokument – und schon ist die Umgebung infiltriert. Am meisten gefährdet sind öffentliche Server, da diese direkt angreifbar sind und es keine dritte Instanz braucht, die den Weg ebnet. Mit den erbeuteten Daten lassen sich oft beachtliche Mengen an Lösegeld erpressen.

Hundertprozentiger Schutz ist zwar nicht möglich, dennoch lassen sich die Auswirkungen eines Hackerangriffs minimieren – und zwar mithilfe eines Incident-Response-Plans. Ein solcher Plan bereitet Unternehmen auf den Ernstfall vor und wird im Idealfall nicht erst in Betracht gezogen, wenn es bereits zu spät ist. Doch selbst wenn Hacker bereits eingedrungen sind, verschafft Incident Response dem Unternehmen einen Vorteil: Meistens halten sich die Angreifer nämlich über Monate als stille Beobachter auf dem Server auf. Auf diese Weise kann man sie über regelmässige Analysen als Teil des Incident-Response-Plans ausfindig machen, bevor sie die Chance zum Angriff nutzen. Hier liegt der Fokus also auf Schadensminimierung.

Incident Response ist ein Fünf-Phasen-Modell

Diese Schadensminimierung erfolgt in der Praxis zwar auf Basis individueller Faktoren wie etwa der Betriebsgrösse, dennoch gibt es auch hier ein Mastermodell, welches aus fünf aufeinander aufbauenden Stadien besteht. An erster Stelle steht immer die Einsicht: Cyber-Security darf nicht vernachlässigt werden, denn sie ist ein wichtiger Wettbewerbsfaktor.

Bevor ein Angriff überhaupt stattgefunden hat, können Unternehmen bereits einen externen Dienstleister hinzuziehen. In diesem Szenario hat dieser genug Zeit, die Umgebung präventiv umfassend zu analysieren. Über realitätsnahe Simulationen sind Managed Service Provider (MSP) in der Lage, Schwachstellen ausfindig zu machen und das Unternehmen bezüglich Nachbesserungen zu beraten. Ist der Ernstfall bereits eingetreten, kann er noch eine Kurzanalyse durchführen. Am ehesten geben Log-Daten Auskunft darüber, wo und wie ein Hacker in die Umgebung eingedrungen ist. Anhand dieser Daten lassen sich Sicherheitslücken demnach am besten herausfiltern. Da sich die Grundstrukturen eines Hackerangriffs häufig ähneln, ist es für die Experten nach abgeschlossener Analyse sinnvoll, einen Datenabgleich mit öffentlich bekannten Informationen durchzuführen. Auch die umgesetzten Änderungen überprüfen die Spezialisten anschliessend auf ihre Wirksamkeit im Rahmen der Incident-Response-Strategie.

Ist die Analyse abgeschlossen, folgt Phase zwei: die Eindäm-

mung. Damit die Hacker ihren Angriff nicht weiter fortsetzen können, trennen die Experten Server und infizierte Geräte vom Hauptnetzwerk. Hierzu nutzt er ein zusätzliches Netzwerk als eine Art Quarantänesegment. Die dorthin verschobenen Entitäten können den Hauptserver nicht mehr kontaktieren. Ein weiterer Scan folgt, um die Reinheit des Main-Servers sicherzustellen.

Ist dies sichergestellt, werden die Hacker selbst ausgebremst: Entweder werden hierfür die von den Angreifern verwendeten IP-Adressen des Command-and-Control-Servers blockiert oder deren Malware unter Quarantäne gestellt.

Drei Fehler bei der Datenwiederherstellung

Das Finale einer Incident-Response-Strategie ist die Datenwiederherstellung. Allerdings lassen sich an dieser Stelle drei häufige Fehler feststellen. Oft haben kleine und mittlere Unternehmen ihre Daten nämlich nicht als Backup abgesichert. Dies resultiert aus dem Glauben heraus, dass sie aufgrund ihrer Firmengrösse schlicht nicht für Hacker interessant sind. Und gibt es doch ein Backup besteht dies aus diesem Grund häufig nur aus einzelnen, bestimmten Datensätzen, aber selten aus dem Gesamtpaket. An umfänglichen Backups sollte jedoch nicht gespart werden, denn genau diese Einstellung weckt das Interesse von Cyberkriminellen.

Der zweite verbreitete Fehler ist, Daten nicht getrennt von der Firmenumgebung abzulegen. Auf diese Weise können Hacker auch das Backup infizieren. Um dies zu vermeiden, sollten Backup-Daten über vom Hauptnetzwerk abgekoppelte Archive sicher verwahrt werden.

Oft funktioniert die Datenwiederherstellung trotzdem nicht. Denn der dritte Fehler, den Unternehmen meist begehen, ist ihre Backups nicht zu prüfen. Selbst wenn das Backup also getrennt vom Hauptnetzwerk verwahrt wurde, heisst das nicht, dass der Datenwiederherstellungsprozess auch funktioniert. Unternehmen sollten ihre Backups regelmässig prüfen, um Fehler nicht erst aufzudecken, wenn ein Angriff bereits stattgefunden hat. Wer sich unsicher ist, kann sich von einem externen Security-Dienstleister beraten lassen oder den Aufgabenbereich gänzlich auslagern.

Lesson Learned

Neben den genannten Aspekten einer Incident-Respond-Strategie – nämlich Hackerangriffe zu entlarven und Schadensminimierung zu betreiben – ist auch die Auswertung im Nachhinein essenziell. Gewonnene Erkenntnisse darüber, welche Massnahmen funktionieren und an welchen Ecken Nachholbedarf besteht, ermöglichen es den Experten, eine auf das Unternehmen zugeschnittene Cybersecurity auszuarbeiten. Denn Schwachstellen in der digitalen Infrastruktur gibt es zuhauf in der Software, in Programmen sowie der Systemkonfiguration. Diese müssen kontinuierlich überprüft werden, wenn man gegen Hackerangriffe gewappnet sein will. Anhand der Anzahl an Sicherheitslücken lässt sich auch eine Wahrscheinlichkeit an möglichen Hackerangriffen ausmachen.

Was nach einem Angriff zudem wichtig ist: alle Systeme neu konfigurieren. Wird dieser Schritt ausgelassen, ist es für erfahrene Hacker ein Leichtes, über denselben Weg erneut ins Unternehmensnetzwerk zu gelangen. Erst wenn der Weg versperrt wird, verlieren Angreifer das Interesse. Daher wird Unternehmen dringend geraten, in eine Incident-Response-Strategie zu investieren. Denn die Spezialisten, die den Plan ausführen, können sich in die Denkweise von Hackern hineinversetzen. Diese spezielle Fähigkeit verschafft ihnen das Wissen darüber, wie bei einem Angriff vorgegangen wird und auf welche Anzeichen bei der Analyse zu achten ist. Sie beraten, welche Sicherheitsmassnahmen für welche Unternehmen notwendig sind. Eine schwache Cybersecurity macht Unternehmen zur Zielscheibe für Hackerangriffe. Mit einer gut durchgeplanten Incident-Response-Strategie und dem richtigen Partner verblasst diese merklich.

INFOS | KONTAKT

SEC Consult (Schweiz) AG
Freilagerstrasse 28
CH-8047 Zürich

T +41 (0)44 271 77 70
www.sec-consult.com
office-switzerland@)sec-consult.com