Was Unternehmen im Ernstfall tun sollten

Hilfe, Hackerangriff! Wie das Incident-Response-Team vorgeht

09. November 2021

Vielleicht wurde eine kompromittierte Mail geöffnet oder Angreifer nutzten in der Breite eine Sicherheitslücke wie beim Microsoft Exchange Server im Frühjahr 2021: Hackerangriffe sind eine reale Bedrohung für Unternehmen und können schnell teuer werden.

Wenn der Worst Case eintritt, gilt es Ruhe zu bewahren und möglichst keine Beweise, das heißt, Angriffsspuren zu vernichten. Dann kann ein Incident-Response-Team an die Arbeit gehen, das Einfallstor und den Angriff nachvollziehen und die Integrität der Systeme wiederherstellen.

Ein Unternehmen ist ins Visier von Hackern geraten, Fehlermeldungen tauchen auf, vielleicht wurden erste Systemteile bereits gesperrt und Erpressungsbotschaften übermittelt. Der Angreifer wird versuchen, zu Accounts mit mehr Rechten vorzustoßen, um Daten zu stehlen oder mit einem Trojaner Systeme zu verschlüsseln. Erreicht er die Domain-Controller-Privilegien, ist das der Worst Case für Unternehmen, da dem Angreifer damit im wahrsten Sinne des Wortes alle Türen offenstehen.

Wenn Unternehmen einen Angriff bemerken, breitet sich schnell Panik aus, Mitarbeiter werden nach Hause geschickt und man versucht, den Schaden zu begrenzen. Hier gilt: Ruhe bewahren und so schnell es geht einen Experten einschalten, der mit einem Incident-Response-Team den Angriffsverlauf nachvollziehen und Empfehlungen geben kann, welche Systeme mit welchem Backup wiederhergestellt werden können. Um den Cyber-Detektiven die Arbeit zu erleichtern, sollten Unternehmen einiges beachten. Optimal ist es, wenn ein IT-Experte bereits den Umfang des Schadens abschätzen kann.

Malware nicht löschen, Systeme wenn möglich isolieren

Malware darf, wenn sie identifiziert wurde, nicht gelöscht werden. Das erschwert dem Response-Team die Arbeit, da auf diese Weise Spuren vernichtet oder manipuliert werden können. Zudem kommt der Löschvorgang meistens zu spät und die Wahrscheinlichkeit, alle betroffenen Systeme zu identifizieren, ist gering. Besser ist es, das System im Ist-Zustand zu belassen, so dass die Experten Beweise wiederfinden und analysieren können und Rückschlüsse auf die Vorgehensweise des Angreifers und seine Tools möglich werden. Auch eine Weiternutzung des Systems sollte wenn möglich unterbleiben. Es ist ebenfalls nicht ratsam, Backups selbst einzuspielen, da auch diese infiziert sein können.

Sinnvoll kann es dagegen sein, die infizierten Systeme wenn möglich zu isolieren. Zwar weiß der Angreifer dann, dass er entdeckt wurde, eine frühe Isolation kann ihn aber daran hintern, sich im Netzwerk weiter fortzubewegen. Man läuft allerdings Gefahr, dass die Isolation nicht vollständig ist, wenn man den Angriffsumfang noch nicht kennt. Es ist deswegen wichtig eine valide Einschätzung geben zu können, wie weit der Hacker vorgedrungen ist. Für die meisten Systemadministratoren keine einfache Aufgabe.

Es ist zudem sinnvoll, das Netzwerk zu trennen, bei einem Laptop das WLAN auszuschalten und an den Strom anzuschließen. Das Vorgehen bei Servern hängt von ihrer Funktionsweise und Verwendung ab: Ist er geschäftskritisch, weil er zum Beispiel den Online-Shop bereitstellt, wäre es ratsam, das Gerät zu isolieren, da ein Angreifer sich sonst im Netzwerk ausbreiten kann. Der Kunde muss die Entscheidung fällen, es ist meist aber empfehlenswert, mehr statt weniger zu isolieren.

Im Falle von Ransomware-Attacken sind Backups der einzige Weg, die Systeme wiederherzustellen.

Deswegen müssen sie gesondert außerhalb des Netzwerks gesichert werden und offline verfügbar sein. Nur so laufen Unternehmen nicht Gefahr, dass ihre Backups bei einem Angriff mitverschlüsselt und damit wertlos werden.

Systemverhalten überwachen und Auffälligkeiten schnell erkennen

IT-Verantwortliche haben die Möglichkeit, das Verhalten der Systeme und Prozesse zu überwachen, Daten aller Geräte im Netzwerk zu sammeln und zu visualisieren, was im Angriffsfall schnelle Rückschlüsse erlaubt und eine solide Entscheidungsbasis darstellt. So können zum Beispiel Meldungen von Antiviren-Scanner an den Admin kommuniziert werden, über die sonst nur der User im Bilde ist. Mit einer solchen zentralen Lösung können durch die Auswertung bestenfalls Angriffsmuster sofort entdeckt werden, etwa, wenn sich auf einem Gerät hunderte Login-Versuche in wenigen Minuten häufen.

Alle Beobachtungen und ergriffenen Maßnahmen sollten für das Einsatz-Team schriftlich und formlos dokumentiert werden. Sie sollten möglichst genau und dürfen gern ausführlich sein. Dazu gehören alle Änderungen, die am System vorgenommen wurden, wie ein Neustart, aber auch das Verhalten des Systems oder Hinweise von Mitarbeitern, etwa, wenn Phishing-Mails eingegangen sind, die nach wie vor das zentrale Einfallstor für Hackerangriffe sind. Diese Verdachtsmomente sind relevant, ebenso Antworten auf die Fragen: Wer hat das System als Letzter benutzt und was wurde im System gemacht, nachdem der Angriff bemerkt wurde? Zentral ist hier die Frage, was wann passiert ist. Denn herrscht Klarheit über den Beginn des Angriffs, kann zum Beispiel die Sicherheit von Backups eingeschätzt werden, wenn sie vor dem Angriff erfolgt sind.

Die Cyber-Detektive vollumfänglich mit Informationen versorgen

Ist das Einsatz-Team im Bilde, werden im nächsten Schritt der Scope und der Auftrag, das Einsatzziel, festgelegt: Welche Unterstützung benötigt das Unternehmen - wurden Daten entwendet, soll der Angriffsverlauf festgestellt werden, welche Systeme sind sauber, muss eine Wiederherstellung bzw. ein Wiederaufbau erfolgen? Von diesen Antworten hängen die Werkzeuge ab, die das Einsatz-Team mitbringt. Meist geht es darum, den Patient Zero in einer Root Cause Analyse zu finden und festzustellen, welche Systemteile infiziert sind.

Die Cyber-Detectives nutzen dann die zur Verfügung stehende Information und verschiedene Datenquellen, um dem Angreifer auf die Spur zu kommen: Das Team benötigt optimalerweise eine Übersicht der IT-Systeme mit Servern und Clients, der Art der Systeme - Linux- bzw. Mac - und muss wissen, ob Mitarbeiter mit eigenen Geräten arbeiten dürfen, was nicht nur ein zusätzliches Risiko für Angriffe darstellt, sondern auch den Datenschutz erschwert. Aus der Logging Policy gehen Prozesse und Verhalten von Sicherheitssystemen hervor, etwa, welche Quellen angebunden sind und in welchen Zyklen geloggt wird. Auch Sicherheitstools verfügen meist über eine Aufzeichnungsfunktion und liefern weitere Informationen.

Im besten Fall sind die Netzwerke segmentiert und die User mit Rollen und Zugriffsrechten ausgestattet, was einen Angriff erschwert. Wichtig für das Einsatzteam ist darüber hinaus die Kenntnis des Patch-Standes der Systeme wie Webserver, die von außen erreichbar sind. Wurden diese seit einer längeren Zeit nicht mehr gepatcht, können sie ein wahrscheinliches Einfallstor für Hacker sein. Threat Intelligence in Form von technischer Beschreibung von Spuren vergangener Angriffe lassen potenziell Rückschlüsse auf den aktuellen Fall zu: Im Frühjahr 2021 sorgte zum Beispiel eine Sicherheitslücke im Microsoft Exchange Server für eine Welle erfolgreicher Angriffe.

Im Austausch bleiben und aus Fehlern lernen

IT-Verantwortliche und Response-Experten stehen während des Einsatzes im engen Austausch. So wird

zum einen sichergestellt, dass das Response-Team alle notwendigen Informationen erhält und andererseits die IT-Verantwortlichen auf dem aktuellen Stand bleiben. In mehreren formlosen Telefonaten tauscht man sich täglich aus. Hilfreich für das Einsatz-Team ist dabei die Teilnahme eines IT-Spezialisten, der Fragen zu Systemen beantworten kann, so dass das Team diese nicht mit einer aufwändigen Analyse erschließen muss. Der zeitliche Umfang, bis ein Angriff abgewehrt werden kann, hängt von diversen Faktoren ab.

Ein Incident ist immer ein Schock und meist teuer - er kostet Zeit, Geld, Ressourcen und negative PR. Deswegen ist es umso wichtiger, daraus zu lernen und Handlungsempfehlungen mitzunehmen, wie man Angriffen künftig vorbeugen und seine Systeme sichern kann. Die Bedeutung von Cyber Security wird Unternehmen meist erst dann klar, wenn ein Angriff erfolgt ist. Auch hier kann das Response Team eine erste Empfehlung geben, welche Tools notwendig sind, um das Sicherheitsniveau zu erhöhen.

Unternehmen sollten außerdem die Kommunikation mit Behörden und ihre Meldepflichten berücksichtigen. Abhängig vom Schaden wie etwa Datenabfluss müssen verschiedene Stellen benachrichtigt werden, bei Unternehmen mit KRITIS zum Beispiel das BSI.

Ob ein Krisenmanager eingesetzt wird, entscheidet das Unternehmen. In manchen Fällen ist diese Rolle auch durch externe Dienstleister besetzt. Seine Funktion besteht darin, die Organisation zu leisten und interdisziplinär zu arbeiten. Denn von einem Angriff ist die Rechtsabteilung eines Unternehmens meist ebenso betroffen wie die Kommunikation.

Fazit

Ein Hackerangriff trifft viele Unternehmen als Schock. Das Wichtigste: Ruhe bewahren und Experten hinzuziehen. Je weniger an den Systemen gemacht wird, umso besser - auf diese Weise werden keine Spuren verwischt und das Incident-Response-Team kann den Angriffsverlauf leichter nachvollziehen, die Systeme bereinigen und wiederherstellen.

Evgen Blohm, Cyber Defense Consultant, SECUINFRA Falcon Team

www.secuinfra.com/de/services/incident-response