Schnell und angemessen auf Angriffe reagieren

Notfallverfahren richtig planen

Sicherheitsvorfälle sind in der heutigen Zeit allgegenwärtig, aus diesem Grund sollte sich jedes Unternehmen auf einen möglichen IT-Sicherheitsvorfall vorbereiten und eine Incident-Response-Strategie implementieren, um Datendiebstahl zu verhindern. Das Kernstück einer solchen Strategie bildet ein definiertes Notfallverfahren.

→ **VON SINA HERBERT**

DIE AUTORIN

Sina Herbert
ist Senior Cyber Security Expert bei NTT Security Switzerland.
→ **www.nttsecurity.com**

Die Einstellung der Unternehmen gegenüber IT-Security hat sich in den vergangenen Jahren stark verändert. Vielen Unternehmen sind die Auswirkungen eines erfolgreichen Cyberangriffs weitgehend bewusst. Eine gute Cyber-Security-Strategie, die Methoden und Prozesse zur Identifizierung Business-kritischer Daten beinhaltet und Techniken zum Schutz dieser Daten vorsieht, ist darum nach wie vor auch die wichtigste Verteidigung, reicht aber längst nicht mehr aus, um dem Bedrohungspotenzial der Gegenwart angemessen entgegenzutreten. Der Trend weist eindeutig in Richtung Threat Detection, einer Echtzeitüberwachung des Datenverkehrs unter Einsatz modernster Technologien wie künstliche Intelligenz und Threat Intelligence. Darauf aufbauend, geht es heute um Cyber-Resilienz, also darum, eine Stärkung der Widerstandskraft gegen Angriffe zu erreichen.

SICHERHEITSVORFÄLLE UND RISIKEN EINSCHÄTZEN

Wenn Sicherheitsvorfälle häufiger werden, stellen sich neben der Frage nach der angemessenen Reaktion vor allem die, ob und wie schnell ein Vorfall überhaupt festgestellt werden kann. Antworten liefert eine umfassende Echtzeitsicht des Netzwerkverkehrs und ausgereifte Logiken für eine erfolgreiche Analyse. Kommt es zu einem Ereignis, müssen die Verantwortlichen einen Sicherheitsvorfall zuerst qualifizieren, bewerten und klassifizieren. Entscheidend dafür sind der Kontext und die damit verbundenen Risiken, denn nicht alle Störungen sind Security Incidents und haben dieselben Auswirkungen. Die Schwere des Ereignisses ergibt sich aus der Business-Kritikalität der Systeme sowie den Logfiles, angereichert mit Informationen über Bedrohungen, sogenannten Indicators of Compromise (IoC), die es unter Verwendung einer automatisierten Analyse ermöglichen, Bedrohungen in der Infrastruktur aufzudecken. Bei der Anzahl von Störungen und Fehlern, die in einem Unternehmen auftreten können, besteht die Gefahr, dass Sicherheitsvorfälle nicht als solche identifiziert werden und ein Angriff oder der Versuch unerkannt bleibt. So kann es passieren, dass ein Bitcoin Miner grosse Performance-Probleme verursacht, jedoch erst bei genauem Hinsehen anhand der Monitoring-Auslastung der Maschine festgestellt wird. Fehler bei der Behandlung und Bewertung von Sicherheitsvorfällen können gravierende Folgen haben, insbesondere dann, wenn für die Aufklärung oder spätere juristische Verfolgung Beweisspuren zerstört werden. Eine mangelnde Fehlerkultur verhindert also eine gewissenhafte Analyse des Problems. Ein typisches Beispiel aus der Praxis ist, wenn Systeme kein zentrales Logging haben und bei einem Incident einfach runtergefahren werden, ohne Log-Daten zu sammeln, ein Disk Image zu erstellen oder einen Memory Dump vorzunehmen.

Für die richtige Behandlung von Sicherheitsvorfällen ist es also unumgänglich, dass in einem Anwenderunternehmen eine klare Vorstellung herrscht, was überhaupt ein Sicherheitsvorfall ist. Die besten Erkennungstechnologien nützen nichts, wenn das IT-Personal die Hinweise nicht richtig zu interpretieren versteht und schwere Sicherheitsvorfälle mit normalen Störungen im Tagesbetrieb verwechselt oder gar nicht erkennt.

Vier Schritte für mehr Sicherheit

Eine frühzeitige Planung hilft, auf Security-Vorfälle besser vorbereitet zu sein und zu reagieren. Hierzu gehören:

- Erstellung von Guidelines/Standardabläufen
- Erstellung von Security Playbooks
- Einbindung der Rechtsabteilung, Kommunikationsabteilung und HR
- Durchspielen von Security-Vorfällen, Zusammenspiel der unterschiedlichen Abteilungen, Reviews und Lessons Learned

Bild: Fotolia

Eine gute Vorbereitung hilft Unternehmen, im Notfall richtig zu reagieren

ANGRIFFE STOPPEN UND SCHÄDEN EINDÄMMEN

Zuerst müssen das Ausmass und die betroffenen Systeme eines Sicherheitsvorfalls ermittelt werden. Nur so können Unternehmen in Abstimmung auf die eigenen Geschäftsziele und Compliance-Anforderungen angemessen darauf reagieren und die vorhandenen Ressourcen effizient zur Minimierung des Schadens und der Betriebsunterbrechung einsetzen. Nach der Identifizierung des Problems besteht die nächste Aufgabe darin, die Cyberattacke zu stoppen und den Schaden zu begrenzen. Je nach Art, Umfang und Auswirkungen eines Angriffs müssen Unternehmen unterschiedliche Massnahmen ergreifen; das ist auch abhängig davon, ob sie intern über die erforderlichen technischen und personellen Ressourcen verfügen. Viele mittelständische Unternehmen, aber auch einige grosse Firmen und Organisationen, sind auf solche Situationen nicht vorbereitet und vertrauen der Expertise eines Sicherheitsspezialisten. Das Spektrum der angemessenen Abwehrmassnahmen reicht vom kontrollierten Abschalten einzelner Systeme über die Isolierung eines oder mehrerer Netzwerksegmente bis hin zur Trennung aller Internetverbindungen.

Bei schwerwiegenden Sicherheitsvorfällen erstellen Experten Disk Images und Memory Dumps der betroffenen Systeme und benötigen Log-Daten der Umsysteme, um diese im Nachgang forensisch zu analysieren. Eine solche forensische Analyse liefert Antworten auf Fragen wie: Was ist geschehen? Welche Art von Sicherheitsvorfall liegt vor? Wie sind der oder die Täter vorgegangen? Wurden Daten entwendet? Wenn ja, welche? Über welchen Weg haben die Angreifer das Unternehmen verlassen? Wie lässt sich eine Wiederholung vermeiden?

SCHÄDEN BEHEBEN, SYSTEME WIEDERHERSTELLEN

Parallel dazu steht im Rahmen eines Incident-Response-Plans die Beseitigung aller Schäden an. Dazu müssen die IT-Mitarbeiter anhand eines Security Playbooks, das die Vorgehensweise genau beschreibt, alle potenziell betroffenen Komponenten wie Betriebssysteme, Konfigurationsdateien, Applikationen und Daten detailliert untersuchen und im Bedarfsfall auch die erforderlichen Data-Recovery-Massnahmen einleiten. Im Idealfall existiert ein Disaster-Recovery-Plan (DRP). Dieser beschreibt genau, wie das geschädigte Unternehmen mit einem Sicherheitsvorfall umzugehen hat, welche Massnahmen einzuleiten sind und wer verantwortlich ist. Ein DRP kann von einem Unternehmen unterstützt durch Incident-Response-Experten entwickelt oder als Software sowie als Service erworben werden. Viele Anwenderunternehmen berücksichtigen in ihren Budgets zwar bereits ein Disaster-Recovery-Szenario, sind aber aufgrund fehlender Tests und Übungen trotzdem nicht ausreichend gut vorbereitet.

Im Verlauf der Wiederaufnahme des gewohnten IT-Betriebs müssen alle zwischenzeitlich deaktivierten Systeme umfassende Anwendungsfunktionstests durchlaufen. Unternehmen, die über eine Incident-Response-Strategie verfügen, können Cyberangriffe im Rahmen der vorgesehenen Prozesse behandeln und abwehren. Sicherheitsvorfälle lassen sich mit definierten und wiederholbaren Verfahren bewältigen. Ein ausgereifter Ansatz minimiert die Auswirkungen eines Sicherheitsvorfalls und schützt unternehmenskritische Daten. Die dabei erzielten Lerneffekte sollten Unternehmen zur weiteren Optimierung eines durchgängigen Cyber-Security-Lifecycle-Konzepts nutzen. ←

«Wenn es zu einem Vorfall kommt, müssen die Verantwortlichen einen Sicherheitsvorfall qualifizieren, bewerten und klassifizieren»

Sina Herbert