77500

ISSN 1866-2420

SECURITY INSIGHT

FACHZEITSCHRIFT FÜR UNTERNEHMENSSICHERHEIT UND WIRTSCHAFTSSCHUTZ

IM FOKUS

115 Jahre Haft für REvil-Gangster?

Weltweite Polizeiaktionen gegen Ransomware-Erpresser

November/Dezember
06/2021
EPr. 15,– €

www.prosecurity.de

Hilfe, Hackerangriff!

Was Unternehmen im Ernstfall tun sollten

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 möglichst keine Beweise zu vernichten. Dann kann ein Incident-Response-Team an die Arbeit gehen und die Integrität der Systeme wiederherstellen.

Wenn Unternehmen einen Angriff bemerken, breitet sich schnell Panik aus: Mitarbeiter werden nach Hause geschickt und man versucht, den Schaden zu begrenzen. Es gilt aber: Ruhe bewahren und schnellstmöglich einen Experten einschalten.

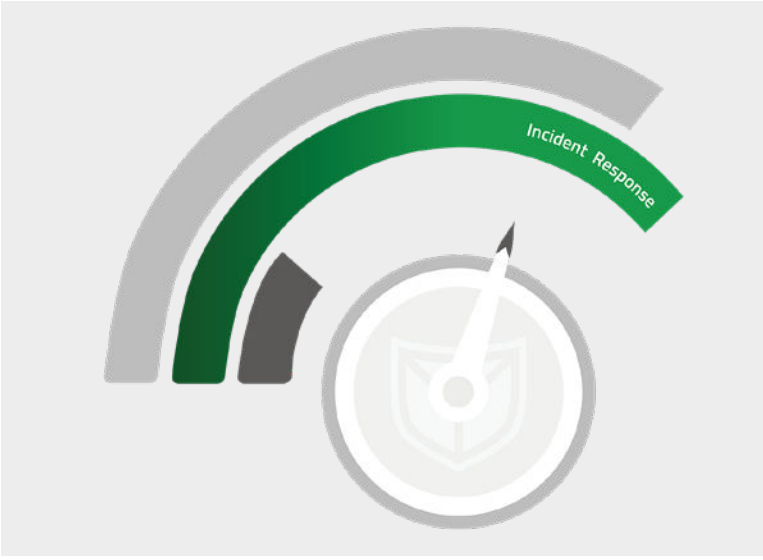
Malware darf, wenn sie identifiziert wurde, nicht gelöscht werden. Das erschwert dem Incident-Response-Team die Arbeit, da auf diese Weise Spuren vernichtet oder manipuliert werden können. Auch eine Weiternutzung des Systems sollte unterbleiben. Es ist ebenfalls nicht ratsam, Backups selbst einzuspielen, da auch diese infiziert sein können. Sinnvoll kann es dagegen sein, die infizierten Systeme zu isolieren. Zwar weiß der Angreifer dann, dass er entdeckt wurde. Eine frühe Isolation kann ihn aber daran hintern, sich im Netzwerk weiter fortzubewegen.

Systemverhalten zentral überwachen

IT-Verantwortliche haben die Möglichkeit, das Verhalten der Systeme und Prozesse zu überwachen und Daten aller Geräte im Netzwerk zu sammeln.

Das erlaubt im Angriffsfall schnelle Rückschlüsse. Mit einer solchen zentralen Lösung können durch die Auswertung Angriffsmuster bestenfalls sofort entdeckt werden – etwa, wenn sich auf einem Gerät hunderte Login-Versuche in wenigen Minuten häufen.

Bild: SECUINFRA



Alle Beobachtungen und ergriffenen Maßnahmen sollten für das Einsatz-Team schriftlich dokumentiert werden. Dazu gehören alle Änderungen, die am System vorgenommen wurden, aber auch das Verhalten des Systems oder Hinweise von Mitarbeitern. 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?

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 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.

Cyber-Detektive mit Informationen versorgen

Die Cyber-Detectives nutzen 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 und muss wissen, ob Mitarbeiter mit eigenen Geräten arbeiten dürfen – was nicht ein zusätzliches Risiko für Angriffe darstellt. 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 längerer Zeit nicht mehr gepatcht, können sie ein wahrscheinliches Einfallstor für Hacker sein.

Fazit

Ein Hackerangriff trifft viele Unternehmen als Schock. Das Wichtigste: Ruhe bewahren und Experten hinzuziehen. Je weniger an den Systemen gemacht wird, umso besser – so 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