Fallstudie

Pentest deckt auf, dass Cyberangriff auf Torvik Industries durch „The Wolf“ mit HP Druckern hätte verhindert werden können

Offizieller Abschlussbericht über das Datenleck

Branche
Logistik

Ziel
Analyse und Behebung von Schwachstellen im Netzwerk

Vorgehensweise
Penetrationstest zur Ermittlung von Schwachstellen, die zum Angriff führten

Ergebnisse und Empfehlungen
- Schulung von Nutzern, verdächtige E-Mails und Druckanhänge nicht unbedarft zu öffnen
- Einsatz von HP Druckern mit Bedrohungserkennung
- Konfiguration aller Endpunkte auf Sicherheitsaspekte, einschließlich Infrastruktur, deren Standort sich verändert hat oder die sich an einem temporären Standort befindet.

Geschäftliche Aspekte
Anwendung besserer Sicherheitsmaßnahmen, um Ausfallzeiten zu vermeiden und das Vertrauen in die Marke zu optimieren. Optimierung von Richtlinien zur Überwachung von Netzwerk-Endpunkten an temporären Aufstellorten.

Überblick

Torvik Industries* verschifft jedes Jahr 8 Millionen Container. Torvik ist für 22.000 Hersteller und Händler der Dreh- und Angelpunkt zwischen Produkten und Menschen auf der ganzen Welt. Das Unternehmen betreibt Hafenanlagen, Schiffe, Lagerhäuser und die gesamte Technologie, die das weit verzweigte Netzwerk von Torvik am Laufen hält.

Während das Unternehmen weiter wuchs, verlor die Technologie-Infrastruktur nach und nach den Anschluss. Obwohl das IT-Sicherheitsteam die Unternehmensserver konfiguriert hat, werden einige Drucker an Außenstellen oder temporären Standorten nicht unter Sicherheitsaspekten verwaltet.

Am 23. April 2018 nutzte ein als „The Wolf“ bekannter Cyberterrorist einen ungesicherten Drucker, um den Betrieb von Torvik Industries lahmzulegen, von den PCs bis hin zu Kränen und Containerschiffen. Der Sicherheitsberater nutzte einen Penetrationstest, um das Ereignis zu analysieren und gab Empfehlungen für eine optimierte Sicherheit und Mitarbeiterschulungen aus.

Was ist passiert?

Die Unternehmensleitung von Torvik Industries war es gewohnt, in der 1. Liga mitzuspielen und den Ton anzugeben. Sie rechnete nicht damit, dass Hacker ihr Netzwerk so tief infiltrieren könnten, dass Containerbrücken lahmgelegt und Schiffe auf offenem Meer umgeleitet werden.

The Wolf musste lediglich einen gezielten Angriff auf einen Großformatdrucker an einer Baustelle durchführen. Von dort aus bewegte er sich seitwärts durch das Unternehmensnetzwerk zu den eigentlichen Zielen in der Betriebsstruktur. Im Handumdrehen stand dieser Global Player für Frachtlogistik vor massiven Betriebsstörungen und befand sich im Fokus der internationalen Aufmerksamkeit und tausender wütender Kunden.

Wie konnte es passieren?

Die IT-Sicherheitsmitarbeiter des Unternehmens dachten, das Unternehmen sei geschützt. Ihre Technik- und Logistikteams überwachten ununterbrochen die weltweiten Betriebsabläufe auf potenzielle Sicherheitsprobleme. Es gab sogar Sicherheitsverfahren für Endpunkte, z. B. für Drucker. Aber sie hatten etwas übersehen: die Sicherheitskonfiguration eines Großformatdruckers, der vorübergehend in einem Baustellencontainer aufgestellt war.

Der Hacker musste nicht einmal direkt auf den Drucker zugreifen, es genügte, eine E-Mail mit PDF-Anhang an einen Torvik Mitarbeiter zu schicken, der für den Druck großformatiger Dokumente zuständig ist. Die PDF enthielt eine versteckte, als eine Art Waffe ausgerüstete PostScript-Datei, die sich eigenständig öffnen und ausführen konnte, sobald die PDF an den Drucker gesendet war. Nachdem der Mitarbeiter den Druckauftrag erteilt hatte, setzte sich die Malware in den Drucker und verbreitete sich von dort im gesamten Netzwerk. Dadurch dass die Malware huckepack mit einem harmlos erscheinenden Mail-Anhang verschickt wurde, umging der Hacker die Anti-Malware-Software auf den Unternehmens-PCs.

Das Leck konnte entstehen, weil der Großformatdrucker nicht über solide integrierte Sicherheitsfunktionen verfügte, z. B. einer Bedrohungserkennung. Das Unternehmen hatte es außerdem versäumt, die Konfiguration jedes einzelnen Druckers im Bestand zu überwachen und zu verwalten, die vorübergehend auch an Außenstellen aufgestellt werden können.

Reparatur des Lecks

Torvik Industries konnte ein Top-Unternehmen in Sachen Penetrationstest gewinnen, eine gründliche Analyse der Cybersicherheit im Unternehmen durchzuführen.

Das Pentest-Team empfahl die Installation von HP Druckern mit eingebetteten Sicherheitsfunktionen, u. a. der HP DesignJet Serie mit Secure Boot und Whitelisting von Firmware. Diese Funktionen helfen dem Drucker dabei, bösartigen Code zu erkennen, herunterzufahren und die IT zu alarmieren und zur Neuinstallation einer richtigen HP Firmware aufzufordern.

Sie empfahlen außerdem die Sicherheitsfunktion Instant-On im HP JetAdvantage Security Manager: Die Software zum Sicherheitsmanagement sorgt dafür, dass Sicherheitsrichtlinien automatisch auf Geräte angewandt werden, die neu in das Unternehmensnetzwerk integriert werden. HP Security Manager erstellt außerdem Compliance-Berichte, die jeden HP Drucker anzeigen – auch an entfernten oder vorübergehenden Standorten. Dadurch kann geprüft werden, ob die Sicherheitsfunktionen in sämtlichen Geräten beibehalten wurden.

Zusätzlich schlug der Sicherheitsberater vor, ein Schulungsprogramm für Mitarbeiter aufzulegen, damit verdächtige E-Mails ausgemacht und unbekannte Anhänge gar nicht erst gedruckt werden.

Zusammenfassung

Torvik Industries hat sich nach wie vor nicht vollständig von dem Cyberangriff auf seine Betriebsabläufe sowie von den Folgen der erhöhten öffentlichen Aufmerksamkeit und den unkonventionellen Ansichten und kriminellen Handlungen seiner Führungsspitze erholt. Während das Unternehmen auf der Führungsebene nach neuen Wegen sucht, ist die Marschrichtung in Sachen Cybersicherheit klar: Ein Umstieg auf Drucker und Lösungen von HP wird The Wolf auf seiner Jagd das Handwerk legen.

**Torvik Industries ist ein fiktives Unternehmen, das im Film „THE WOLF:TRUE ALPHA" von HP Studio Ziel eines großangelegten Cyberangriffs wird. TRUE ALPHA."*

Weitere Informationen zu den Lösungen von HP siehe
HP DesignJet hp.com/go/designjetsecurity
Druckersicherheit. hp.com/go/reinventsecurity
Hier können Sie die Filme der Serie „The Wolf" sehen: hp.com/thewolf

Melden Sie sich noch heute an.
hp.com/go/getupdated

An Kollegen weiterleiten

4AA7-3562DEE, August 2018