Casestudy

Penetratietesten tonen aan dat de cyberbeveiligingsinbreuk op Torvik Industries door "The Wolf" door HP printers had kunnen worden gestopt

Officieel afsluitend rapport van de data-inbreuk

Industrie
Goederenvervoer

Doelstelling
Gebieden waar het netwerk kwetsbaar is analyseren en verhelpen

Aanpak
Penetratietesten om de kwetsbaarheden te vinden die tot de aanval hebben geleid

Bevindingen en aanbevelingen
- Gebruikers informeren om beducht te zijn op het openen van verdachte e-mails en het printen van bijlagen
- HP printers met detectie van bedreigingen implementeren
- Configureren van alle eindpunten voor beveiliging, inclusief infrastructuur die verplaatst is of zich op tijdelijke locaties bevindt

Bedrijfsmatige aspecten
Sterkere beveiligingsmaatregelen toepassen om operationele downtime te voorkomen en vertrouwen in het merk te vergroten. Verbeteren van het beleid om netwerk-eindpunten op tijdelijke locaties te bewaken.

Overzicht

Torvik Industries* verscheept elk jaar 8 miljoen containers. Voor 22.000 fabrikanten en groothandelaren is Torvik de vitale verbinding tussen producten en mensen over de hele wereld. Het bedrijf bezit onder meer scheepswerven, schepen, magazijnen en alle technologie die het uitgebreide netwerk van Torvik ondersteunt.

Terwijl het bedrijf is gegroeid, kon de technologische infrastructuur zich moeilijk aanpassen. Hoewel IT-beveiligingsmedewerkers de servers van het bedrijf hebben geconfigureerd, worden sommige printers op satellietkantoren of tijdelijke locaties niet voor beveiliging beheerd.

Op 23 april 2018 heeft de cyberterrorist die alleen bekend staat als "The Wolf" een onbeveiligde printer gebruikt om de activiteiten van Torvik Industries te saboteren, van pc's tot kranen en containerschepen. Hun beveiligingsadviseur heeft penetratietests gebruikt om de gebeurtenis te analyseren en heeft aanbevelingen gegeven voor het verhogen van de beveiliging en training van het personeel.

Wat er gebeurde

De leiding van Torvik Industries was het gewend om het voor het zeggen te hebben als er grote belangen op het spel stonden. Ze verwachtten dus niet dat hackers zo diep in hun netwerk zouden infiltreren dat ze de portaalkranen van het bedrijf zouden kunnen sluiten en schepen naar de open oceaan zouden kunnen leiden.

Het enige wat The Wolf hoefde te doen, was een grootformaatprinter op een bouwplaats compromitteren. Vervolgens kon hij zich lateraal door het netwerk van het bedrijf verplaatsen naar e grote doelen in de bedrijfsoperaties. In een oogwenk kreeg dit topvervoersbedrijfte maken met enorme operationele storingen, een zwaar internationaal onderzoek en duizenden woedende klanten.

Hoe het gebeurde

Het IT-beveiligingspersoneel van het bedrijf dacht dat ze beveiligd waren. Hun technische en logistieke teams hielden de wereldwijde operaties constant in de gaten voor mogelijke beveiligingsproblemen. Ze hadden zelfs beveiligingsprocedures ingesteld voor eindpunten zoals printers. Maar ze hadden iets over het hoofd gezien: de beveiligingsconfiguratie van een grootformaatprinter die tijdelijk in een bouwtrailer was gestationeerd.

De hacker hoefde niet eens rechtstreeks toegang tot de printer te hebben – hij stuurde gewoon een e-mail met een pdf-bijlage naar de medewerker van Torvik die verantwoordelijk was voor het printen van documenten in grootformaat. Die pdf had een verborgen gewapend PostScript-bestand bij zich dat zichzelf kon openen en uitvoeren wanneer de pdf naar de printer werd gestuurd. Nadat de medewerker de printtaak had verzonden, plaatste de malware zichzelf in de printer en verspreidde zich vervolgens over het netwerk. Door malware op een onschuldig ogende e-mailbijlage te laten meeliften, heeft de hacker de anti-malwaresoftware op de pc's van het bedrijf omzeild.

De inbreuk was mogelijk omdat de grootformaatprinter geen sterke ingebouwde beveiliging had, zoals dreigingsdetectie. Ook kon het bedrijf de configuratie van elke afzonderlijke printer in de hele vloot niet volgen en beheren, zoals de printers die tijdelijk in satellietkantoren zijn geplaatst.

De breuk herstellen

Torvik Industries heeft een topfirma voor het testen van penetraties gebruikt voor het uitvoeren van een grondige analyse van de cyberbeveiliging van de organisatie.

Het penetratietestteam heeft aanbevolen om HP printers met ingebouwde beveiligingsfuncties te installeren, waaronder de HP DesignJet-serie met Secure Boot en firmware-whitelisting. Met deze functies kan de printer ook schadelijke code detecteren en uitschakelen, en vervolgens IT aarschuwen voor de noodzaak om legitieme HP firmware opnieuw te installeren.

Zij hebben ook aanbevolen om de Instant-On-beveiligingsfunctie van HP JetAdvantage Security Manager te gebruiken, een softwareprogramma voor beveiligingsbeheer in de vloot, om beveiligingsbeleid automatisch toe te passen zodra er apparaten aan het netwerk worden toegevoegd. HP Security Manager kan ook nalevingsrapporten maken die elke HP printer laten zien, zelfs op externe of tijdelijke locaties. Zo kan worden aangetoond dat configuraties voor beveiliging van de vloot onderhouden zijn.

Daarnaast heeft de beveiligingsadviseur een onderwijsprogramma voorgesteld om werknemers te helpen verdachte e-mails te herkennen en te voorkomen dat onbekende bijlagen worden geprint.

Conclusie

Torvik Industries is nog steeds aan het bijkomen van de gevolgen van de cyberbeveiligingsinbreuk op de activiteiten, evenals de verhoogde publiciteit van de onconventionele opvattingen en criminele handelingen van hun president. Terwijl de organisatie een nieuwe richting in leiderschap probeert te ontwikkelen, is de richting voor cyberbeveiliging duidelijk: overschakelen op HP printers en oplossingen zal de jacht van de volgende Wolf verijdelen.

**Torvik Industries is een fictief bedrijf dat het doel is van een grote cyberaanval in de film van HP Studio, "THE WOLF: TRUE ALPHA."*

Kijk voor meer informatie over HP oplossingen op:
HP DesignJet: hp.com/go/designjetsecurity
Printerbeveiliging: hp.com/go/reinventsecurity

Als u films van "The Wolf" wilt zien, gaat u naar:
hp.com/thewolf

Meld u aan voor updates op
hp.com/go/getupdated

4AA7-3562NLE, augustus 2018