Fallstudie

Penetrationstestning visar att dataintrånget hos Torvik Industries orsakat av "The Wolf" kunde ha stoppats av HP-skrivare

Officiell sammanfattningsrapport över dataintrånget

Bransch
Transport

Målsättning
Analysera och åtgärda sårbara platser i nätverket.

Metod
Penetrationstestning för att hitta sårbarheterna som ledde till attacken.

Fynd och rekommendationer:
- Lär användarna att de måste vara försiktiga med att öppna misstänkta e-postmeddelanden och bilagor.
- Driftsätt HP-skrivare med hotupptäckt.
- Konfigurera alla enheter för säkerhet, inklusive enheter som flyttas och infrastruktur på tillfälliga platser.

Verksamhetsfrågor
Tillämpa starkare säkerhetsåtgärder för att undvika driftstopp samt förbättra varumärkets förtroende. Implementera policyer för att övervaka nätverkets enheter på tillfälliga platser.

Översikt

Torvik Industries* fraktar 8 miljoner containrar varje år. För 22 000 tillverkare och grossister är Torvik en viktig länk mellan produkterna och människor världen över. Företaget äger bland annat lastanläggningar, fartyg, lagerlokaler och all teknik som stödjer Torviks breda nätverk.

I och med att företaget har vuxit har de kämpat med att anpassa sin tekniska infrastruktur. IT-säkerhetspersonalen har konfigurerat företagets servrar, men en del skrivare på satellitkontor eller tillfälliga platser har inte någon managerad säkerhet.

Den 23 april 2018 använde cyberterroristen känd som "The Wolf" en osäkrad skrivare för att sabotera Torvik Industries verksamhet, från datorer till kranar och containerskepp. Företagets säkerhetsrådgivare använde sedan penetrationstestning för att analysera händelsen och ge rekommendationer om att öka säkerheten och utbilda personalen.

Vad hände?

Torvik Industries ledning var vana vid att ha en position av kontroll i stora affärer – och det var en chock för företaget att hackare kunde infiltrera deras nätverk så djupt att de kunde stänga av företagets lastkranar och omdirigera skepp ute till havs.

Allt The Wolf behövde göra var att ta sig in i en storformatskrivare på en byggplats. Sedan kunde cyberterroristen röra sig genom företagets nätverk till stora måltavlor inom deras verksamhet. På bara några ögonblick drabbades det ledande fraktbolaget av massiva driftstörningar, med internationell granskning och tusentals upprörda kunder som följd.

Hur gick det till?

Företagets IT-säkerhetspersonal trodde att de var skyddade. Deras teknik- och logistikteam övervakade hela tiden den globala verksamheten och var uppmärksamma på potentiella säkerhetsproblem. De hade till och med säkerhetsrutiner på plats för slutpunkter som skrivare. Men de hade förbisett en sak: säkerhetskonfigurationen på en storformatsskrivare som tillfälligt placerats i en manskapsvagn.

Hackaren behövde inte ens komma åt skrivaren själv, utan skickade bara ett e-postmeddelande med en PDF-bilaga till medarbetaren hos Torvik som ansvarade för att skriva ut storformatsdokument. I PDF-filen fanns en dold skadlig Postscript-fil, som kunde öppna och köra sig själv när PDF-filen skickats till skrivaren. När medarbetare skickat utskriften spred sig malware i skrivaren, och sedan ut i nätverket. Genom att bädda in malware i en till synes ofarlig e-postbilaga kunde hackaren ta sig förbi anti-malware-programvaran på företagets datorer.

Intrånget var möjligt eftersom storformatskrivaren inte hade starka inbyggda säkerhetsfunktioner, som hotupptäckt. Företaget hade inte heller övervakat konfigurationen på varenda skrivare i skrivarparken – till exempel inte skrivare på tillfälliga platser och i satellitkontor.

Reparera skadan

Torvik Industries anlitande en ledande firma för att utföra penetrationstester och noggranna analyser av företagets cybersäkerhet.

Testteamet rekommenderade installering av HP-skrivare med inbyggda säkerhetsfunktioner, bland annat HP DesignJet-serien med Säker start och vitlistning av inbyggd programvara. Med de funktionerna kan skrivare upptäcka skadlig kod och stänga av sig, och sedan larma IT-personalen om behovet av att installera legitim inbyggd HP-programvara.

De rekommenderade också användning av den snabbstartande säkerhetsfunktionen hos HP JetAdvantage Security Manager, som är ett säkerhetshanteringsprogram för hela skrivarparken. På så sätt kan säkerhetspolicyer automatiskt tillämpas så fort som enheter läggs till i nätverket. HP Security Manager kan även skapa efterlevnadsrapporter som visar alla HP-skrivare, även på avlägsna eller tillfälliga platser. Rapporterna bidrar till att visa att parkens säkerhetskonfigurationer bibehålls.

Säkerhetsrådgivarna föreslog också ett utbildningsprogram för att lära medarbetarna känna igen misstänkta e-postmeddelanden och undvika att skriva ut okända bilagor.

Sammanfattning

Torvik Industries lider fortfarande av följderna från störningen i sin verksamhet samt från publiciteten med anledning av VD:ns okonventionella åsikter och illegala handlingar. Företaget försöker utveckla en ny riktning för sin ledning, och riktningen för deras cybersäkerhet är klar: de vänder sig till HPs skrivare och lösningar för att hindra nästa varg som angriper.

** Torvik Industries är ett fiktivt företag som utsätts för en stor cyberattack i HP Studios film "THE WOLF: TRUE ALPHA".*

Mer information om HPs lösningar finns på:
HP DesignJet: hp.com/go/designjetsecurity
Skrivarsäkerhet: hp.com/go/reinventsecurity

Du kan se filmerna om "The Wolf" genom att besöka: hp.com/thewolf

Registrera dig för att få uppdateringar
hp.com/go/getupdated

Dela med kollegor

4AA7-3562SVE, augusti 2018