Casestudie

Penetrationstestning viste, at HP's printere kunne have forhindret cybersikkerhedsbruddet af "The Wolf" mod Torvik Industries

Officiel sammendragsrapport om databruddet

Industri
Shipping

Mål
Analyse og løsning af problemer relateret til netværkssårbarhed

Fremgangsmåde
Penetrationstestning til identifikation af sårbarhederne, der førte til angrebet

Resultater og anbefalinger
- Uddannelse af brugere til at være påpasselige i forhold til at åbne mistænkelige e-mails og udskrive vedhæftede filer
- Implementering af HP-printere med trusselsregistrering
- Konfigurering af alle slutpunkter for øget sikkerhed, inklusive infrastruktur, der er flyttet eller på midlertidige lokaliteter

Virksomhedsanliggender
Indførelse af stærkere sikkerhedstiltag for at undgå driftsnedetid og styrke brandtillid. Forbedring af politikker for overvågning af netværksslutpunkter på midlertidige lokaliteter.

Oversigt

Torvik Industries* fragter otte millioner containere årligt. For 22.000 producenter og grossister fungerer Torvik som den vitale forbindelse mellem produkter og mennesker over hele verden. Virksomhedens aktiver inkluderer skibsværfter, fartøjer, varelagre og al den teknologi, der understøtter Torviks vidtstrakte netværk.

Efterhånden som virksomheden er vokset, er tilpasningen af teknologiinfrastrukturen ikke fulgt med. Selvom it-sikkerhedspersonalet har konfigureret virksomhedens servere, er nogle printere på satellitkontorer eller midlertidige lokaliteter ikke sikkerhedsstyret.

D. 23. april 2018 brugte cyberterroristen "The Wolf" en usikker printer til at sabotere Torvik Industries' drift – fra pc'er til kraner og containerskibe. Deres sikkerhedsrådgiver brugte penetrationstestning til at analysere hændelsen og gav efterfølgende anbefalinger om øget sikkerheds- og personaleuddannelse.

Hvad skete der?

Torvik Industries' ledelse var vant til at bestemme og operere med stor risici – så de forventede ikke, at hackere infiltrerede deres netværk så dybt, at de var i stand til at sætte virksomhedens kranbaner ud af drift og omdirigere skibe langt ude på havet.

Alt, hvad The Wolf skulle gøre, var at kompromittere en storformatprinter på en byggeplads. Derefter kunne han bevæge sig gennem virksomhedens netværk og nå frem til de store mål i virksomhedens drift. På kort tid stod denne store shippingvirksomhed over for massive driftsafbrydelser, internationale undersøgelser og tusinder af rasende kunder.

Hvordan skete det?

Virksomhedens it-sikkerhedspersonale troede, at de var beskyttet. Deres tekniske og logistiske teams overvågede konstant den globale drift mod potentielle sikkerhedsproblemer. De havde endda sikkerhedsprocedurer for slutpunkter, som printere. Men de havde overset noget: sikkerhedskonfigurationen af en storformatprinter, der var midlertidigt placeret i en skurvogn.

Hackeren behøvede endda ikke at få direkte adgang til printeren – han sendte blot en e-mail med en vedhæftet pdf-fil til en medarbejder i Torvik, der var ansvarlig for udskrivning af storformatdokumenter. Denne pdf-fil indeholdt en hemmelig PostScript-fil, der blev brugt som våben, da den kunne åbnes og køres, når pdf-filen blev sendt til printeren. Da medarbejderen sendte udskriftsopgaven, blev malwaren aktiveret i printeren og derefter videresendt i hele netværket. Ved at sende malware, der var skjult i en uskyldigt udseende fil vedhæftet en e-mail, undgik hackeren antimalwaresoftwaren på virksomhedens pc'er.

Bruddet kunne ske, da storformatprinteren ikke havde nogen stærk, indbygget sikkerhed, såsom trusselsregistrering. Det lykkedes heller ikke for virksomheden at overvåge og administrere hver enkelt printer i deres flåde – som dem, der var placeret midlertidigt i satellitkontorer.

Udbedring af bruddet

Torvik Industries hyrede et penetrationstestningsfirma til at gennemføre en omfattende analyse af organisationens cybersikkerhed.

Penetrationstestningsteamet anbefalede at installere HP-printere med indbyggede sikkerhedsfunktioner, inklusive HP DesignJet-serien med Secure Boot og firmwarehvidlistefunktion. Disse funktioner hjælper printeren med at registrere skadelig kode og lukke ned. Herefter underrettes it-afdelingen om behovet for at geninstallere legitim HP-firmware.

De anbefalede også brug af Instant-On-sikkerhedsfunktionen HP JetAdvantage Security Manager – et softwareprogram til sikkerhedsstyring af hele flåden, der automatisk anvender sikkerhedspolitikker, så snart enheder tilføjes til netværket. HP Security Manager kan også lave overholdelsesrapporter, der viser hver eneste HP-printer, selv på fjernlokaliteter eller midlertidige lokaliteter. Det hjælper med at vise, at flådesikkerhedskonfigurationer er vedligeholdt.

Derudover foreslog sikkerhedsrådgiveren et uddannelsesprogram, der skal hjælpe ansatte med at genkende mistænkelige e-mails og undgå at udskrive ukendte vedhæftede filer.

Konklusion

Torvik Industries kæmper stadig med cybersikkerhedsbruddets effekt på driften samt den øgede omtale af deres direktørs utraditionelle holdninger og kriminelle handlinger. Mens organisationen søger en ny retning for dens ledelse, er retningen for cybersikkerhed klar: Med HP's printere og løsninger kan den næste "The Wolf" forhindres i at udrette skade.

** Torvik Industries er en fiktiv virksomhed, der blev målrettet i et stort cyberangreb i HP Studios film, "THE WOLF: TRUE ALPHA".*

Få flere oplysninger om HP's løsninger:
HP DesignJet: hp.com/go/designjetsecurity
Printersikkerhed: hp.com/go/reinventsecurity
Se "The Wolf"-filmene på:
hp.com/thewolf

Tilmeld dig for at få opdateringer
hp.com/go/getupdated

Del med kolleger

4AA7-356DAE, august 2018