Kasusstudie

Pen-test viser at Torvik Industries' cybersikkerhetsbrudd av «The Wolf» kunne vært stoppet av HP-skrivere

Offisiell avslutningsrapport for databruddet

Bransje
Shipping

Mål
Analysere og reparere områder med nettverkssårbarhet

Tilnærming
Penetrasjonstesting for å finne sårbarhetene som førte til angrepet

Funn og anbefalinger
- Utdanne brukere til å være forsiktige med å åpne mistenkelige e-poster og skrive ut vedlegg
- Distribuere HP-skrivere som registrerer trusler
- Konfigurere alle sluttpunkter for sikkerhet, inkludert infrastruktur som flyttes eller er midlertidig plassert

Forretningsforhold
Iverksette strengere sikkerhetstiltak for å unngå driftsmessig nedetid og øke tilliten til merkevaren. Forbedre retningslinjer for å overvåke nettverkets sluttpunkter på midlertidige steder.

Oversikt

Torvik Industries* sender årlig 8 millioner containere. For 22 000 produsenter og forhandlere er Torvik den viktige forbindelsen mellom produktene og folk verden rundt. Konsernet eier blant annet verft, båter, varehus og all teknologien som støtter Torviks utbredte nettverk.

Etter hvert som konsernet har vokst, har teknologiinfrastrukturen deres hatt problemer med å tilpasse seg. Selv om de IT-sikkerhetsansatte har konfigurert konsernets servere, er noen skrivere ved satellittkontorer eller på midlertidige steder ikke administrert for sikkerhet.

23. april 2018 brukte cyberterroristen kun kjent som «The Wolf» en usikret skriver for å sabotere Torvik Industries' drift – fra PC-er til kraner og containerskip. Sikkerhetsrådgiveren brukte penetrasjonstesting for å analysere hendelsen, og ga anbefalinger for å bedre sikkerheten og de ansattes opplæring

Hva skjedde

Ledelsen ved Torvik Industries var vant til å ta beslutningene der mye sto på spill, så de forventet ikke at hackere skulle infiltrere nettverket deres så dypt at de kunne slå av brokranene deres og omdirigere skipene deres ute på det åpne havet.

Alt The Wolf måtte gjøre var å kompromittere en storformatskriver på en byggeplass. Så kunne han bevege seg lateralt gjennom bedriftens nettverk til hovedmålene i den sentrale driften. Plutselig hadde dette ledende shippingkonsernet enorme driftsavbrudd, intens internasjonal granskning og tusenvis av sinte kunder.

Slik skjedde det

Konsernets IT-sikkerhetsansatte trodde de var beskyttet. De tekniske og logistiske teamene overvåket kontinuerlig den globale driften for potensielle sikkerhetsproblemer. De hadde til og med etablert sikkerhetsprosedyrer for sluttpunkter som skrivere. Men de hadde oversett noe: sikkerhetskonfigurasjonen til en storformatskriver midlertidig plassert i en brakke på en byggeplass.

Hackeren trengte ikke engang direkte tilgang til skriveren – han bare sendte en e-post med et PDF-vedlegg til den Torvik-ansatte som hadde ansvaret for å skrive ut storformatdokumenter. Denne PDF-en inneholdt en skjult skadelig Postscript-fil, som kunne åpne og kjøre seg selv da PDF-en ble sendt til skriveren. Med en gang den ansatte sendte utskriftsjobben, la den skadelige programvaren seg inn på skriveren og spredte seg gjennom nettverket. Ved å knytte skadelig programvare til et e-postvedlegg som ser harmløst ut, hadde hackeren gått rundt beskyttelsen mot skadelig programvare på konsernets PC-er.

Dette kunne skje fordi storformatskriveren ikke hadde sterk innebygd sikkerhet, som for eksempel trusselregistrering. Videre hadde ikke konsernet overvåket og administrert konfigurasjonen for hver eneste skriver i flåten, som de som er midlertidig plassert på satellittkontorer.

Reparere bruddet

Torvik Industries ansatte et av de beste selskapene innen penetrasjonstesting for å utføre en grundig analyse av organisasjonens cybersikkerhet.

Pen-testing-teamet anbefalte å installere HP-skrivere med innebygde sikkerhetsfunksjoner, inkludert HP DesignJet-serien med Secure Boot og hvitelisting av fastvare. Disse funksjonene hjelper skriveren registrere skadelig kode og slå seg selv av samt varsle IT om at de må reinstallere legitim HP-fastvare.

De anbefalte også å bruke sikkerhetsfunksjonen Instant-On i HP JetAdvantage Security Manager, en flåteomfattende programvare for sikkerhetsadministrasjon, for automatisk å benytte retningslinjer for sikkerhet så snart enheter legges til nettverket. HP Security Manager kan også opprette samsvarsrapporter som viser alle HP-skrivere, selv på eksterne eller midlertidige steder. Dette er med på å vise at konfigurasjoner for flåtesikkerhet har blitt vedlikeholdt.

I tillegg anbefalte sikkerhetsrådgiveren et opplæringsprogram, for å hjelpe ansatte med å gjenkjenne mistenkelige e-poster og unngå å skrive ut ukjente vedlegg.

Konklusjon

Torvik Industries sliter fremdeles med ettervirkningene cybersikkerhetsbruddet hadde på driften, i tillegg til den omfattende publisiteten om presidentens ukonvensjonelle meninger og kriminelle handlinger. Selv om organisasjonen ønsker å finne en ny retning innenfor ledelsen, er retningen for cybersikkerhet tydelig: skrivere og løsninger fra HP hjelper dem med å spolere angrepet neste gang The Wolf går på jakt.

**Torvik Industries er et fiktivt konsern som var målet i et omfattende cyberangrep i HP Studios-filmen, «THE WOLF: ALFAULVEN».*

For mer informasjon om HP-løsninger:
HP DesignJet: hp.com/go/designjetsecurity
Utskriftssikkerhet: hp.com/go/reinventsecurity

Hvis du ønsker å se «The Wolf»-filmer, kan du gå til: hp.com/thewolf

Registrer deg for oppdateringer
hp.com/go/getupdated

Del med kolleger

4AA7-3562NOE, august 2018