Případová studie

Testování průniku prokázalo, že narušení kybernetického zabezpečení organizace Torvik Industries útočníkem známým jako „The Wolf“ bylo možné předejít použitím tiskáren HP

Oficiální závěr k neoprávněnému přístupu k datům

Odvětví
Přeprava

Cíl
Analýza a odstraňování slabých míst v zabezpečení sítě

Přístup
Testování průniku s cílem vyhledat slabá místa v zabezpečení sítě, která umožnila provedení útoku

Zjištění a doporučení
- Uživatele je třeba upozornit na nutnost zvýšené opatrnosti při otvírání podezřelých e-mailů a tisku příloh
- Nasazení tiskáren HP podporujících detekci hrozeb
- Zavedení zabezpečení pro všechny koncové body a infrastrukturu, která je v pohybu nebo v dočasném umístění

Obchodní záležitosti
Zajištění důslednějšího zabezpečení, které zabrání vzniku provozních prostojů a zvýší důvěru v danou značku. Zdokonalení zásad sledování koncových bodů v síti, které se nachází v dočasném umístění.

Přehled

Společnost Torvik Industries* každoročně přepraví 8 milionů kontejnerů. Pro více než 22 000 výrobců a velkoprodejců se jedná o zásadní spojení mezi produkty a lidmi z celého světa. Rozsáhlá síť společnosti Torvik závisí na celé řadě přístavů, lodí a skladů, stejně jako na souvisejících technologiích.

Tato technologická infrastruktura se nicméně nestihla dostatečně přizpůsobit rozrůstání firmy. Zaměstnanci IT sice zajistili potřebnou konfiguraci podnikových serverů, ale u několika tiskáren na předsunutých či dočasných pracovištích nebylo zajištěno vhodné zabezpečení.

Toho využil 23. dubna 2018 kybernetický útočník známý pouze pod přezdívkou „The Wolf“ (Vlk) a prostřednictvím nezabezpečené tiskárny sabotoval veškerý provoz společnosti Torvik Industries od počítačů přes jeřáby až po kontejnerové lodě. Poradce pro zabezpečení firmy provedl testování průniku, při kterém analyzoval celou událost a poskytl potřebná doporučení vedoucí ke zvýšení zabezpečení a lepšímu školení zaměstnanců.

Co se stalo

Vedení společnosti Torvik Industries bylo zvyklé na rozhodování na nejvyšší úrovni. Byli proto zcela zaskočeni, když se hackerovi podařilo proniknout do sítě natolik hluboko, že mohl postupně vypínat jejich portálové jeřáby nebo navádět lodě na širý oceán.

Jediné, co Vlk musel udělat, bylo proniknout jednou velkoformátovou tiskárnou na staveništi. To mu umožnilo pohybovat se volně podnikovou sítí až ke konfiguraci provozu ve společnosti. V jednom krátkém okamžiku se jedna z největších přepravních společností musela potýkat s rozsáhlým narušením provozu, čelit intenzivní mezinárodní kontrole a utišit tisíce rozhořčených zákazníků.

Jak se to stalo?

Firemní oddělení IT mající na starost zabezpečení bylo přesvědčeno o úplnosti zabezpečení. Technologické a logistické týmy neustále monitorovaly celosvětové operace a hledaly jakýkoli potenciální problém se zabezpečením. Společnost dokonce používala bezpečností procesy pro koncové body, jako jsou tiskárny. Něco ale přece přehlédli: zabezpečení velkoformátové tiskárny v maringotce na staveništi.

Hacker dokonce ani nepotřeboval přímý přístup k tiskárně. Stačilo mu sestavit e-mail s přiloženým souborem PDF a odeslat jej zaměstnanci společnosti Torvik odpovědnému za tisk velkoformátových dokumentů. Součástí tohoto souboru PDF byl skrytý škodlivý PostScriptový kód, který se po odeslání souboru PDF do tiskárny automaticky spustil. Jakmile zaměstnanec odeslal tiskovou úlohu, malware se uložil v tiskárně a začal se šířit celou sítí. Navázáním škodlivého kódu na nevinně vypadající přílohu e-mailu se hackerovi podařilo zcela obejít program chránící před malwarem nainstalovaný na podnikových počítačích.

Útok byl možný z důvodu, že velkoformátová tiskárna nenabízela spolehlivé integrované zabezpečení, jako je např. detekce hrozby. Společnost navíc nemonitorovala a nespravovala konfigurace ve všech podnikových tiskárnách, jako např. na dočasném pracovišti.

Odstranění následku útoku

Společnost Torvik Industries oslovila špičkovou firmu pro testování průniku, která provedla komplexní analýzu kybernetického zabezpečení.

Tým pověřený testováním průniku doporučil instalaci tiskáren HP s integrovanými bezpečnostními funkcemi, jako jsou tiskárny řady HP DesignJet s funkcí Secure Boot a vkládáním firmwaru do seznamu povolených položek. Tyto funkce v případě odhalení škodlivého kódu tiskárnu vypnou a upozorní oddělení IT na nutnost přeinstalování správného firmwaru HP.

Tým dále doporučil používání bezpečnostní funkce Instant-On softwaru HP JetAdvantage Security Manager pro správu všech podnikových tiskáren, která dokáže použít bezpečnostní zásady okamžitě po přidání zařízení do sítě. Nástroj HP Security Manager dokáže navíc vytvářet hlášení o souladu všech tiskáren HP včetně těch, které se nachází na dočasném pracovišti. Hlášení je zárukou dodržování konfigurací zabezpečení.

Poradce v oblasti zabezpečení současně doporučil zahájit vzdělávací program, který zaměstnance naučí lépe rozeznávat podezřelé e-maily a vyhýbat se tisku neznámých příloh.

Závěr

Společnost Torvik Industries se stále ještě vzpamatovává z následků kybernetického útoku na provoz firmy a zájmu veřejnosti o nekonvenční názory a trestné činy jejího prezidenta. I když další postup a směr ve vedení společnosti je zatím nejasný, potřebné zákroky v ochraně před kybernetickými útoky jsou dané: používání tiskáren a řešení HP je zbraní, která dokáže útok dalšího Vlka odvrátit.

**Torvik Industries je fiktivní společností, která se stala cílem rozsáhlého kybernetického útoku v krátkém filmu společnosti HP Studio: „THE WOLF: TRUE ALPHA“.*

Další informace o řešení HP:
HP DesignJet: hp.com/go/designjetsecurity
Zabezpečení tisku: hp.com/go/reinventsecurity

Film „The Wolf“ můžete vidět zde:
hp.com/thewolf

Přihlásit se k odběru novinek
hp.com/go/getupdated

Sdílet dokument s kolegy

4AA7-3562CSE, srpen 2018