Canon

VODIČ ZA DIJAGNOSTICIRANJE SIGURNOSTI ISPISIVANJA I SKENIRANJA

Kako prepoznati i spriječiti povrede sigurnosti ispisivanja i skeniranja

UVOD

Bez obzira na to je li riječ o plaći glavnog izvršnog direktora, dokumentima o novom predstojećem spajanju ili samo o dogovoru s klijentima koji još nije javan – svaka organizacija ima dokumente koji moraju ostati privatni.

Ispisivanje i skeniranje često se previde kao potencijalni sigurnosni rizik ako se njima ne upravlja ispravno. Međutim, čin ispisivanja ili skeniranja dokumenta obično ukazuje na njegovu vrijednost; ti su dokumenti povezani s najznačajnijim ili potencijalno osjetljivim trenucima za vašu organizaciju.

Pisači i skeneri ključan su dio vaših poslovnih operacija i IT infrastrukture. To su sofisticirani uređaji povezani s mrežom koji vam pomažu u prijenosu informacija kroz organizaciju i istovremeno omogućuju moćne digitalne procese. No ako se previde u strategiji kibernetičke sigurnosti vaše organizacije, mogli bi pružiti zaobilazan pristup, širom otvoren napadačima.

U ovom vodiču opisuju se uobičajeni simptomi povrede sigurnosti i rješenja za dijagnosticiranje uzroka u ispisivanju i skeniranju. Isto tako, pruža se potpora u prepoznavanju povreda sigurnosti i sprječavanju istih u budućnosti.

SCENARIJ 1: OČITA POVREDA

Primijetili ste očitu povredu? Naknadni pregled pomoći će vam da utvrdite kako određene ranjivosti ispisivanja i skeniranja mogu biti uzrok.

STRANICA 3

SCENARIJ 2: NEŠTO SE ČINI DRUKČIJIM

Postoje sumnjivi simptomi povrede, ali nije jasno što se događa? Saznajte kako različite vrste povreda mogu biti povezane s napadom zaobilaznim pristupom putem pisača ili skenera.

STRANICA 8

SCENARIJ 3: MRAČNA PRIJETNJA – BEZ SIMPTOMA

Istražite „mračne prijetnje” – na koji način vaša organizacija kao i ispisivanje i skeniranje zaposlenika potajno ugrožavaju sigurnost.

STRANICA 10

SCENARIJ 1: OČITA POVREDA

Utvrdili ste da su osjetljive informacije procurile iz organizacije i uočene su na internetu.

MOGUĆI UZROK

VANJSKA POVREDA – HAKIRAN UREDSKI UREĐAJ:

Zlonamjeran akter ušao je u jedan od vaših uredskih višenamjenskih pisača i pristupio zapisniku ispisanih i skeniranih dokumenata.

RJEŠENJE 1

UPRAVLJANJE PERIMETROM

Stalno, automatsko skeniranje svih vaših mjesta za napad.

Zašto to pomaže

Kad pokušavate zaštititi teoretski sigurnosni perimetar organizacije, to je kao da stalno patrolirate zgradom sa 100 katova. Osim ako stalno ne nadzirete sva vrata, izlažete se vanjskim zlonamjernim akterima koji isprobavaju vrata i potencijalno ih mogu naći otključanima i bez zaštitara.

RJEŠENJE 2

VIŠESTRUKA PROVJERA AUTENTIČNOSTI I TELEMETRIJA

Spriječite pristup uređaju od strane neprovjerenih korisnika – sumnjiva aktivnost može se automatski prijaviti vašoj platformi za upravljanje sigurnošću i događajima (SIEM).

Zašto to pomaže

Uređaji tvrtke Canon svoje zapisnike aktivnosti šalju na vašu postojeću platformu za upravljanje sigurnošću i događajima, što vam omogućuje bržu reakciju kad otkrijete neovlaštenu upotrebu ili neovlašten pristup. Osim toga, dijeljenjem identiteta korisnika i uređaja s kojeg su uzeli ispis može pomoći vašoj organizaciji u prepoznavanju fizičke lokacije radnika i pružiti dodatne dokaze u slučaju problema.

SCENARIJ 1: OČITA POVREDA

MOGUĆI UZROK

INTERNA POVREDA – ISPISIVANJE ILI SKENIRANJE KOD KUĆE:

Zaposlenik je ispisao ili skenirao povjerljivi dokument na svom uređaju za kućni ured, koji nije zaštićen. To predstavlja rizik od neovlaštenog pristupa hakera zadacima ispisivanja i podacima, kao i potencijalnih napada zlonamjernog softvera.

RJEŠENJE

uniFLOW ONLINE

Odabrani uređaji tvrtke Canon mogu se upotrebljavati za rad na daljinu uz uniFLOW Online, tako da radnici mogu slijediti iste sigurne radne procese za dokumente, bez obzira na lokaciju.

Zašto to pomaže

uniFLOW Online replicira sigurna okruženja tvrtki za hibridni rad, što vašem IT timu omogućuje da postavi kućne uređaje s istim sigurnosnim profilima dokumenata kao u uredu, uz sveobuhvatno šifriranje podataka i dokumenata.

SCENARIJ 1: OČITA POVREDA

MOGUĆI UZROK

INTERNA POVREDA – NEOVLAŠTENA UPOTREBA UREĐAJA:

Korisnik je neovlašteno upotrijebio uređaj i njegovu konfiguraciju, mijenjajući postavke kako bi samom sebi dao pristup ispisanim ili skeniranim dokumentima.

RJEŠENJE

SIGURNO UPRAVLJANJE PROFILOM

Paket sigurnosnih značajki i usluga dizajniranih za zaštitu pisača i skenera tvrtke Canon i podataka koje obrađuju, na samom uređaju i u mreži. To uključuje prilagođene sigurnosne profile, proaktivno praćenje sigurnosti, prepoznavanje prijetnji i brz oporavak

Zašto to pomaže

Bez praćenja sigurnih profila na uređajima možda neće odmah biti očito da je netko neovlašteno upotrijebio uređaj osim ako IT timovi ne provjere, što osigurava trenutnu identifikaciju pokušaja neovlaštene upotrebe.

SCENARIJ 1: OČITA POVREDA

MOGUĆI UZROK

INTERNA POVREDA – FIZIČKA KRAĐA:

Netko je fizički ukrao dokumente s odlagača za ispis, a da ga nitko nije primijetio zato što ih je udaljeni korisnik slučajno poslao na ispisivanje ili ih je izvorni vlasnik zaboravio.

RJEŠENJE

uniFLOW ONLINE

uniFLOW Online pruža funkciju My Print Anywhere ako se zadaci ispisivanja mogu pokrenuti samo kada se predviđeni korisnik identificira na uređaju.

Zašto to pomaže

Sprječava korisnike da ispišu dokumente i ostave ih na izlaznom odlagaču kako nikad ne bi bili ostavljeni na uređaju bez nadzora.

SCENARIJ 1: OČITA POVREDA

MOGUĆI UZROK

INTERNA POVREDA – MEDIJ ZA POHRANU PODATAKA:

Netko je ukrao medij za pohranu podataka s aktivnog uređaja ili uređaja na kraju vijeka trajanja koji je zbrinut.

RJEŠENJE 1

OBAVEZNO ŠIFRIRANJE POHRANE

Uređaji tvrtke Canon isporučuju se s obaveznim šifriranjem pohrane koje osigurava da su podaci vaše organizacije uvijek sigurni.

Zašto to pomaže

Ako zlonamjeran akter pokuša ukrasti aktivni medij za pohranu s uređaja, ne može pristupiti informacijama.

RJEŠENJE 2

USLUGA UKLANJANJA PODATAKA

Naša usluga uklanjanja podataka trajno briše digitalne i fizičke podatke iz suvišnih uređaja.

Zašto to pomaže

Nije uvijek moguće jamčiti sigurno zbrinjavanje ili uništenje uređaja na kraju vijeka trajanja, pa automatsko šifriranje osigurava da ne morate brinuti o sigurnosti svojih podataka čak i kada napuste organizaciju.

SCENARIJ 2: KAD SE NEŠTO ČINI DRUKČIJIM

Ponekad je jasno da je došlo do povrede sigurnosti – primjerice kada osjetljive informacije završe na internetu – ali što kada se stvari čine „drukčijima”? U tim slučajevima možda neće odmah biti očito da je došlo do povrede ili koji je njezin izvor.

Napadač može iskoristiti pisač koji je loše konfiguriran i izložen internetu kao stepenicu u infrastrukturu vaše tvrtke. Ako uređaj pohranjuje osjetljive lozinke, napadač bi mogao iskoristiti pisač za ugrožavanje mreže.

Na sljedećoj stranici nalaze se neki primjeri simptoma povrede koji bi mogli voditi do pisača ili skenera koji se upotrebljavaju za zaobilazni pristup.

SCENARIJ 2: KAD SE NEŠTO ČINI DRUKČIJIM

Raspon simptoma koji ukazuju na sve ozbiljniju povredu

Simptom 1:

NEUOBIČAJENA AKTIVNOST E-POŠTE

Priljev sumnjivih ili lažiranih poruka e-pošte može ukazivati na to da je napadač pristupio popisima kontakata zaposlenika i da pokušava dobiti njihove lozinke.

Simptom 2:

NEOBIČNA AKTIVNOST RAČUNA

Neprepoznate prijave, promjene lozinke ili transakcije mogu ukazivati na preuzimanje računa, pri čemu napadač ima pristup određenom korisničkom imenu i lozinki.

Simptom 3:

PROMJENE DOPUŠTENJA ZA PRISTUP DATOTECI

Iznenadne promjene u pristupu dokumentima mogu pokazivati da je napadač osigurao poboljšana dopuštenja i da pristupa osjetljivim dokumentima ili da onemogućuje pristup drugima kako bi pripremio napad ucjenjivačkog softvera.

Simptom 4:

SKOK U MREŽNOM PROMETU

Do iznenadnog, neobjašnjenog povećanja mrežne aktivnosti, naročito tijekom sati izvan radnog vremena, može doći zbog toga što napadač u mreži izvlači osjetljive podatke.

MOGUĆI UZROK

NAPADAČ NA SLOBODI:

Ove znakove možda je uzrokovao napadač u vašim sustavima koji traži vrijedne informacije, bilo putem phishinga, izravne krađe ili pristupa dokumentima. Imajte na umu da uređaji za ispisivanje ili skeniranje s lošim upravljanjem mogu omogućiti zaobilazni pristup napadačima.

RJEŠENJE

JAČANJE SIGURNOSTI UREĐAJA

Naša usluga jačanja sigurnosti uređaja čini vašu mrežu sigurnom od samog početka dodavanjem uređaja koji su unaprijed konfigurirani s preporučenim sigurnosnim postavkama i funkcijama koje su u skladu s vašim okruženjem.

Zašto to pomaže

Jačanje sigurnosti uređaja obuhvaća naše stručno savjetovanje o najboljim sigurnosnim postavkama za vaš uređaj, osiguravanje ispravnog postavljanja pisača i skenera od početka i sprječavanje da pisač omogući zaobilazni pristup za iskorištavanje ranjivosti.

SCENARIJ 3: MRAČNA PRIJETNJA – BEZ SIMPTOMA

Što se događa kada nema simptoma koje bi vaša tvrtka mogla dijagnosticirati, ali i dalje postoji sigurnosna prijetnja?

ČESTA PRIJETNJA

Jedna od najznačajnijih prijetnji za vaše poslovanje je nedijagnosticirani IT iz sjene. Može imati mnoge oblike, uključujući:

Preuzimanje softvera zasnovanog na informatičkom oblaku za koji IT tim ne zna, a u koji se unose podaci tvrtke.

Slanje dokumenata ili podataka na kućne uređaje, čime im se omogućuje pristup i rad na njima od kuće.

Povezivanje neovlaštenih uređaja (kao što su kućni uređaji) na radnu mrežu i preuzimanje dokumenata.

IT iz sjene frustrira IT timove, ali je u konačnici simptom neostvarene potrebe zaposlenika. Organizacija nema tehnologiju koja bi podržala taj zahtjev ili se ono što trenutačno postoji pokazuje kao nedostatno za svoj zadatak. Zaposlenici obično zaobilaze tehnologiju koju osigurava tvrtka ako je naporna ili oduzima mnogo vremena u usporedbi sa široko dostupnim alternativama.

SCENARIJ 3: MRAČNA PRIJETNJA – BEZ SIMPTOMA

Mnoge pojave IT-a iz sjene nastavljaju se neprimjetno jer nisu dovele do povezane povrede. Međutim, IT iz sjene je kao medicinska ranjivost bez simptoma koja može napredovati ako se ne prepozna i proaktivno ne riješi.

RJEŠENJE 1

PROVJERA STANJA UREDSKOG OKRUŽENJA

Tvrtka Canon klijentima može pružiti podršku kroz jačanje vidljivosti njihove IT strukture putem usluge provjere stanja uredskog okruženja.

Zašto to pomaže

Organizacije se ne mogu boriti protiv onoga čega nisu svjesne. Ovom sveobuhvatnom revizijom utvrđuju se potencijalne slabe točke perimetra i savjetuje se kako možete učvrstiti obranu i prepoznati potencijalne prijetnje prije nego što se realiziraju.

RJEŠENJE 2

SIGURNOSNE USLUGE NA PRETPLATU

Pruža sveobuhvatne pakete kojima se lako može upravljati, a koji nude jednostavna rješenja za upravljanje sigurnošću skupine uređaja. Usluge su dostupne u dvije razine, „Poboljšana sigurnost” i proširena „Premium sigurnost”, i pružaju poboljšanu zaštitu uređaja i sveobuhvatnu zaštitu koja se može prilagoditi specifičnim potrebama poslovanja.

Zašto to pomaže

Osigurava neprekidan pristup organizacije uslugama zaštite i mogućnostima za sigurnost uređaja, na primjer, sigurnosnim kopijama podataka i najnovijim ažuriranjima programskih datoteka.

ZAŠTO CANON

Informacije su žila kucavica suvremenih organizacija. Zato morate biti sigurni da su vaši podaci zaštićeni – stoga je presudno odabrati tehnologiju kojoj možete vjerovati.

Morate zaštititi krajnje uređaje kako biste spriječili neovlašteni pristup podacima. Za poboljšanje sigurnosti i sukladnosti kontroliranjem pristupa vašim sustavima. I za neprekidnu zaštitu osjetljivih digitalnih dokumenata, sadržaja i podataka.

U tvrtki Canon svaki proizvod, rješenje i usluga koje isporučujemo dizajnirani su za sigurnost. Naši pisači i skeneri imaju napredne sigurnosne značajke koje onemogućuju da pogrešne osobe vide vaše dokumente, a naša pametna softverska rješenja smanjuju mogućnost ljudske pogreške kako bi se pojednostavila sukladnost. Osim toga, naše mogućnosti možete iskoristiti na način koji odgovara vašem poslovanju uz opsežni i prilagodljivi paket sigurnosnih usluga.

Svojim klijentima pružamo pristup istoj stručnosti u području sigurnosti koju upotrebljavamo kako bismo zaštitili svoju organizaciju. Naš tim za rješavanje sigurnosnih incidenata povezanih s proizvodima radi na prvoj liniji, reagira na nove kibernetičke prijetnje kako se pojavljuju i to znanje upotrebljava za unapređenje naših tehnologija. To znači da ćete kao naš partner uvijek imati koristi od najnovijih poboljšanja u kibernetičkoj sigurnosti.

Rezultate tog rada možete vidjeti u pohvalama koje dobivamo od analitičara u industriji kao što su IDC i Quocirca, koji hvale naš holistički pristup i navode da se izdvajamo zbog usmjerenosti na tijek rada i optimizaciju procesa.

Kad je sigurnost podataka stalni izazov, povjerenje je od presudne važnosti, a ono dolazi od partnera koji vas štiti svake sekunde svakoga dana.

ZAŠTO CANON

DIZAJNIRAN ZA SIGURNOST

Uz Canon, sigurnost informacija ne dolazi tek na kraju. Povezuje sve što radimo, od dizajna hardvera do kraja vijeka trajanja. Strogo testirana rješenja, stalne sigurnosne zakrpe uz prepoznavanje prijetnji s pomoću umjetne inteligencije, opsežan paket usluga za zahtjeve sigurnosnog okruženja... pokrivamo sve dijelove životnog ciklusa dokumenata i održavamo sigurnost tijekom cijelog vijeka trajanja naših proizvoda. To je sveobuhvatna zaštita, bez prekida.

PAMETNA I SIGURNA RJEŠENJA

Protok informacija unutar tvrtke pomaže zaposlenicima surađivati, održavati produktivnost i pristupati vrijednim uvidima. No također vas izlaže riziku. Naša softverska rješenja za tvrtke pružaju potpunu vidljivost i kontrolu vaših informacijskih sustava. Izbjegnite ljudske pogreške sigurnim i automatiziranim procesima koje pruža Therefore Online. Pristupajte centraliziranom sigurnom upravljanju ispisivanjem uz uniFLOW Online. Dokumente držite podalje od pogrešnih ruku uz sigurno slanje zadataka ispisivanja.

uniFLOW online

Therefore™
PEOPLE PROCESS INFORMATION

ZAŠTO CANON

PODRŠKA INDUSTRIJE

Mi smo predvodnici u zaštiti informacija za poslovanje. Ali nemojte samo nama vjerovati na riječ. Analitičari iz industrije kao što su IDC i Quocirca smatraju da naša rješenja i usluge za tehnologiju radnog prostora snažno jačaju sigurnost informacija kroz zaštitu uređaja, dokumenata i podataka u cijeloj infrastrukturi organizacije za ispisivanje. Riječima potpredsjednika istraživanja tvrtke IDC, Roberta Palmera, „holistički pristup upravljanju informacijama tvrtke Canon, u kombinaciji sa strateškim fokusom na područja kao što su tijek rada, optimizacija procesa i sigurnost, izdvajaju je među konkurentima".

QUOCIRCA

IDC

HARDVER S NAPREDNOM ZAŠTITOM KAO STANDARD

Vaši pisači i skeneri ključni su za vaše poslovne operacije. Međutim, ako se ne uključe u strategiju kibernetičke sigurnosti, mogu postati ulazne točke za napadače.

U svoj hardver ugrađujemo napredne sigurnosne značajke kako bismo to spriječili i upravljali pristupom dokumentima, uključujući višestruku provjeru autentičnosti, prepoznavanje prijetnji u stvarnom vremenu i sveobuhvatno šifriranje podataka. Možete čak i pratiti aktivnosti uređaja i primati sigurnosna upozorenja za neobične radnje kao što su višestruki pokušaji prijave ili određene ključne riječi koje se ispisuju, skeniraju, kopiraju ili dijele.

ZAŠTO CANON

UZ PODRŠKU ELITNOG TIMA ZA KIBERNETIČKU SIGURNOST

Kao jedinstven primjer u industriji ispisivanja, prelazimo s riječi na djela: kupci tvrtke Canon dobivaju podršku našeg tima za rješavanje sigurnosnih incidenata povezanih s proizvodima, istih stručnjaka za sigurnost koji implementiraju našu vrhunsku zaštitu proizvoda. Oslanjajući se na najnovija istraživanja i primjenjujući najbolje prakse u industriji u cilju očuvanja sigurnosti vaših uređaja i aktivnosti ispisivanja te zaštite dokumenata i podataka od neovlaštenog pristupa, naš tim neprestano radi kako bi identificirao i neutralizirao nove kibernetičke prijetnje prije nego što počnu utjecati na vaše poslovanje.

USLUGE KOJE POBOLJŠAVAJU SIGURNOST

Naš paket sigurnosnih usluga obuhvaća svaku fazu životnog ciklusa uređaja. Možda želite na siguran način uvesti nove uređaje u mrežu. Za to vam nudimo uslugu jačanja sigurnosti uređaja koji su unaprijed konfigurirani s preporučenim sigurnosnim postavkama i funkcijama. Možda trebate održavati sigurnost na kraju radnog vijeka uređaja. Naša usluga uklanjanja podataka trajno briše digitalne i fizičke podatke iz suvišnih uređaja. Sigurnosno kopiranje podataka pomaže u zaštiti kritičnih informacija na uređajima u slučaju neočekivanih događaja. Naše sigurnosne usluge na pretplatu pružaju kontinuiranu zaštitu od prijetnji, prilagođenu vašim potrebama. Ako se suočavate sa sigurnosnim izazovom u ispisivanju, imamo uslugu zaštite sigurnosti koja će vam pomoći da ga savladate.

Canon d.o.o.
Kovinska 4a
10090 Zagreb
Hrvatska
Tel: + 385 1 5579 843
Fax: + 385 1 5579 856
canon.hr

Canon Inc.
Canon.com

Canon Europe
canon-europe.com

Croatian edition