Canon

DIAGNOSEGIDS VOOR DE BEVEILIGING VAN PRINTEN EN SCANNEN

Hoe u schendingen van uw print- en scanbeveiliging kunt identificeren en voorkomen

INLEIDING

Of het nu gaat om het salaris van uw CEO, documenten over een nieuwe aanstaande fusie of alleen een deal met een klant die nog niet openbaar is - elke organisatie heeft documenten die zeer vertrouwelijk zijn.

Van printen en scannen wordt vaak vergeten dat ze een potentieel beveiligingsrisico kunnen vormen wanneer deze niet goed worden beheerd. Toch hebben prints en scans van documenten vaak betrekking op de belangrijkste en mogelijk gevoeligste momenten in uw organisatie.

Uw printers en scanners vormen een essentieel onderdeel van uw bedrijfsactiviteiten en IT-infrastructuur. Deze geavanceerde, op het netwerk aangesloten machines verplaatsen informatie door uw organisatie en maken tegelijkertijd krachtige digitale processen mogelijk. Maar als u ze in de cyberbeveiligingsstrategie van uw organisatie over het hoofd ziet, kunnen ze mogelijk ook een achterdeur worden die helemaal openstaat voor aanvallers.

In deze gids bekijken we veelvoorkomende symptomen van beveiligingsschendingen en helpen we u te bepalen hoe printen en scannen schendingen kunnen veroorzaken. Zo kunt u deze niet alleen nu identificeren, maar ze ook in de toekomst voorkomen.

SCENARIO 1: EEN DUIDELIJKE SCHENDING

Hebt u een duidelijke schending ontdekt? Deze post mortem helpt u te identificeren hoe specifieke beveiligingsproblemen rond printen en scannen de boosdoener kunnen zijn.

PAGINA 03

SCENARIO 2: WANNEER IETS 'NIET GOED VOELT'

Verdachte symptomen van een schending, maar niet duidelijk wat er aan de hand is? Ontdek hoe verschillende soorten schendingen een aanval via de achterdeur van uw printer of scanner kunnen zijn.

PAGINA 08

SCENARIO 3: ONBEKENDE DREIGING - GEEN SYMPTOMEN

Ontdek 'onbekende dreigingen' - hoe het print- en scangedrag van uw organisatie en medewerkers uw beveiliging mogelijk ongemerkt in gevaar brengt.

PAGINA 10

SCENARIO 1: EEN DUIDELIJKE SCHENDING

U hebt vastgesteld dat er gevoelige informatie uit de organisatie lijkt te zijn gelekt en dat deze online is ontdekt.

MOGELIJKE OORZAAK

SCHENDING VAN BUITENAF - GEHACKT APPARAAT OP KANTOOR:

Een crimineel is een van uw multifunctionele printers op kantoor binnengedrongen en heeft het logboek met afgedrukte en gescande documenten geopend.

OPLOSSING 1

PERIMETER BEHEREN

Constant, automatisch scannen van al uw aanvalsoppervlakken.

Waarom het helpt

Proberen de theoretische beveiligingsperimeter van uw organisatie te beschermen, is te vergelijken met voortdurend patrouilleren in een gebouw met 100 verdiepingen. Tenzij u elke deur voortdurend in de gaten houdt, stelt u zichzelf bloot aan externe probleemveroorzakers die steeds aan de deuren rammelen om te kijken of ze niet op slot en onbemand zijn.

OPLOSSING 2

MULTI-FACTOR VERIFICATIE EN TELEMETRIE

Voorkom toegang tot het apparaat door niet-geverifieerde gebruikers. Verdachte activiteiten kunnen automatisch worden gemarkeerd op uw SIEM (Security and Event Management Platform).

Waarom het helpt

De apparaten van Canon verzenden hun activiteitenlogboeken naar uw bestaande beveiligings- en eventmanagementplatform, zodat u sneller kunt optreden wanneer u ongeautoriseerd gebruik of onbevoegde toegang detecteert. Bovendien kan het delen van de identiteit van de gebruiker en het apparaat waarmee is geprint, uw organisatie helpen om de fysieke locatie van werknemers te identificeren, wat extra bewijs levert in geval van een probleem.

SCENARIO 1: EEN DUIDELIJKE SCHENDING

MOGELIJKE OORZAAK

SCHENDING VAN BINNENUIT - THUIS PRINTEN OF SCANNEN:

Een medewerker heeft op een apparaat in zijn of haar kantoor aan huis een vertrouwelijk document geprint of gescand, wat niet veilig is. Het risico bestaat dat onbevoegden zoals hackers toegang krijgen tot printopdrachten en gegevens, en dan is er nog het risico van mogelijke malwareaanvallen.

OPLOSSING

uniFLOW ONLINE

Met geselecteerde Canon-apparaten met uniFLOW Online kan op afstand worden gewerkt, zodat werknemers dezelfde beveiligde documentworkflows kunnen volgen, ongeacht hun locatie.

Waarom het helpt

uniFLOW Online repliceert beveiligde bedrijfsomgevingen om hybride te kunnen werken, waardoor uw IT-team thuisapparaten met dezelfde documentbeveiligingsprofielen als op kantoor kan instellen, met end-to-end gegevens- en documentcodering.

SCENARIO 1: EEN DUIDELIJKE SCHENDING

MOGELIJKE OORZAAK

SCHENDING VAN BINNENUIT - APPARATEN MANIPULEREN:

Een gebruiker heeft het apparaat en de configuratie gemanipuleerd, waardoor de instellingen zijn gewijzigd. Hij of zij heeft hierdoor toegang tot geprinte of gescande documenten.

OPLOSSING

SECURE PROFILE MANAGEMENT

Een reeks beveiligingsfuncties en -services die is ontworpen om Canon-printers en -scanners en de gegevens die ze verwerken te beschermen, op het apparaat zelf en in het netwerk. Hiertoe behoren beveiligingsprofielen op maat, proactieve monitoring, bedreigingsdetectie en snel herstel

Waarom het helpt

Zonder de beveiligingsprofielen op apparaten te monitoren, is het misschien niet meteen duidelijk dat iemand een machine heeft gemanipuleerd, tenzij IT-teams dit controleren. Zo kunnen pogingen tot manipulatie direct worden geïdentificeerd.

SCENARIO 1: EEN DUIDELIJKE SCHENDING

MOGELIJKE OORZAAK

SCHENDING VAN BINNENUIT - FYSIEKE DIEFSTAL:

Iemand heeft documenten gestolen uit de printlade zonder dat dit is opgemerkt, omdat een externe gebruiker ze per ongeluk naar de printer heeft verzonden of omdat de oorspronkelijke eigenaar de documenten is vergeten.

OPLOSSING

uniFLOW ONLINE

uniFLOW Online biedt de functie My Print Anywhere, waarbij printopdrachten alleen kunnen worden vrijgegeven wanneer de beoogde gebruiker zichzelf op het apparaat identificeert.

Waarom het helpt

Voorkomt dat gebruikers documenten printen en in de uitvoerlade laten liggen, zodat deze documenten nooit onbeheerd achterblijven op het apparaat.

SCENARIO 1: EEN DUIDELIJKE SCHENDING

MOGELIJKE OORZAAK

SCHENDING VAN BINNENUIT - GEGEVENSOPSLAGMEDIA:

Iemand heeft de gegevensopslagmedia van een actief apparaat of van een afgevoerd apparaat aan het einde van zijn levensduur gestolen.

OPLOSSING 1

VERPLICHTE OPSLAGCODERING

Canon-apparaten worden geleverd met verplichte opslagcodering, zodat de gegevens van uw organisatie altijd veilig zijn.

Waarom het helpt

Als een crimineel de actieve opslagmedia van een apparaat probeert te stelen, is het niet mogelijk om toegang tot de informatie te krijgen.

OPLOSSING 2

DATA REMOVAL SERVICE

Onze Data Removal Service verwijdert digitale en fysieke gegevens definitief van overtollige apparaten.

Waarom het helpt

Het is niet altijd mogelijk om te garanderen dat apparaten aan het einde van hun levensduur veilig worden verwijderd of vernietigd. Automatische codering zorgt ervoor dat u zich geen zorgen hoeft te maken over de veiligheid van uw gegevens, zelfs niet als deze gegevens uw organisatie hebben verlaten.

SCENARIO 2: WANNEER IETS 'NIET GOED VOELT'

Soms is het duidelijk wanneer er een schending van de beveiliging is opgetreden, bijvoorbeeld wanneer gevoelige informatie online is komen te staan, maar hoe zit het met als er iets niet goed voelt? In dergelijke gevallen is het niet direct duidelijk dat er sprake is of is geweest van een schending, of wat de bron ervan is.

Een printer die niet goed is geconfigureerd en op internet is aangesloten, kan door een aanvaller als koevoet worden gebruikt om in de infrastructuur van uw organisatie te komen. Als op het apparaat gevoelige wachtwoorden zijn opgeslagen, kan een aanvaller de printer gebruiken om uw netwerk in gevaar te brengen.

Op de volgende pagina vindt u enkele voorbeelden van schendingen waarbij er een achterdeur in uw printer of scanner wordt gebruikt.

SCENARIO 2: WANNEER IETS 'NIET GOED VOELT'

Een schaal met symptomen die op een steeds ernstigere schending wijzen

Symptoom 1:

ONGEBRUIKELIJKE E-MAILACTIVITEIT

Een toestroom van verdachte e-mails of vervalste e-mails kan erop wijzen dat een aanvaller toegang heeft tot de lijsten met contactpersonen van medewerkers en probeert hun wachtwoorden te achterhalen.

Symptoom 2:

ONGEBRUIKELIJKE ACCOUNTACTIVITEIT

Niet-herkende aanmeldingen, wachtwoordwijzigingen of transacties kunnen duiden op een overname van een account, waarbij een aanvaller toegang tot de gebruikersnaam en het wachtwoord van een specifieke gebruiker heeft.

Symptoom 3:

WIJZIGING VAN TOEGANGSRECHTEN VOOR BESTANDEN

Plotselinge wijzigingen in de toegang tot documenten kunnen erop wijzen dat een aanvaller verhoogde machtigingen heeft weten te krijgen en toegang tot gevoelige documenten heeft gekregen, of dat hij of zij anderen blokkeert ter voorbereiding op een ransomware-aanval.

Symptoom 4:

EEN PIEK IN HET NETWERKVERKEER

Een plotselinge, onverklaarbare toename van de netwerkactiviteit, met name tijdens daluren, kan het gevolg zijn van een aanvaller in het netwerk die gevoelige gegevens steelt.

MOGELIJKE OORZAAK

EEN AANVALLER DIE VAN ALLES PROBEERT:

Deze signalen kunnen erop wijzen dat een aanvaller in uw systemen op zoek is naar waardevolle informatie, of dit nu via phishing, directe diefstal of toegang tot documenten is. Vergeet niet dat slecht beheerde print- of scanapparaten achterdeuren voor aanvallers kunnen worden.

OPLOSSING

APPARATEN BETER BEVEILIGEN

Onze Device Hardening Service houdt uw netwerk direct veilig door apparaten vooraf te configureren met aanbevolen beveiligingsinstellingen en -functies afgestemd op uw omgeving.

Waarom het helpt

Device Hardening bestaat uit een deskundige consultancysessie van Canon over de beste beveiligingsinstellingen voor uw apparaat, zodat uw printers en scanners vanaf het begin correct zijn ingesteld en uw printer geen achterdeur wordt via welke misbruik van uw apparaat wordt gemaakt.

SCENARIO 3: ONBEKENDE DREIGING - GEEN SYMPTOMEN

Wat gebeurt er als er geen symptomen zijn maar er toch sprake is van een bedreiging van de veiligheid?

VEELVOORKOMENDE BEDREIGING

Een van de belangrijkste bedreigingen voor uw organisatie is ongediagnosticeerde schaduw-IT. Een dergelijke bedreiging kan vele vormen hebben, waaronder:

Op de cloud gebaseerde software downloaden waarvan het IT-team zich niet bewust is, waarin gegevens van de organisatie worden ingevoerd.

Documenten of gegevens naar thuisapparaten verzenden, zodat ze deze thuis kunnen openen en eraan kunnen werken.

Niet-geautoriseerde apparaten (zoals thuisapparaten) verbinden met het bedrijfsnetwerk en documenten downloaden.

Schaduw-IT is frustrerend voor IT-teams, maar uiteindelijk een symptoom van een niet-gerealiseerde wens of behoefte van medewerkers. Ofwel de organisatie beschikt niet over de technologie om die vereiste te ondersteunen, ofwel wat er momenteel is geïmplementeerd, blijkt niet tegen de taak opgewassen. Medewerkers hebben de neiging om door de organisatie geleverde technologie te omzeilen wanneer deze lastig of tijdrovend is in vergelijking tot beschikbare alternatieven.

SCENARIO 3: ONBEKENDE DREIGING - GEEN SYMPTOMEN

Veel schaduw-IT-methoden blijven bestaan zonder dat ze worden opgemerkt en dit komt doordat ze niet hebben geleid tot een bijbehorende schending. Schaduw-IT is echter als een symptoomloos medisch probleem dat groter kan worden als dit niet wordt geïdentificeerd en proactief wordt opgelost.

OPLOSSING 1

OFFICE HEALTH CHECK

Canon kan klanten ondersteunen door ze via een Office Health Check meer inzicht te geven in hun eigen IT-omgeving.

Waarom het helpt

Organisaties kunnen niet vechten tegen iets waarvan ze zich niet bewust zijn. Deze uitgebreide audit identificeert potentiële zwakke plekken in het netwerk en geeft advies over hoe u uw verdediging kunt versterken en potentiële bedreigingen kunt identificeren voordat deze zich manifesteren.

OPLOSSING 2

SUBSCRIPTION SECURITY SERVICES

Bestaan uit uitgebreide, eenvoudig te beheren pakketten met vereenvoudigde oplossingen om de beveiliging van uw assets te beheren. De services zijn beschikbaar in twee vormen, 'Enhanced Security' en de uitgebreidere 'Premium Security'. Ze bieden verbeterde apparaatbeveiliging en end-to-end beveiliging die flexibel in de specifieke behoeften van een bedrijf voorziet.

Waarom het helpt

Zorgt ervoor dat uw organisatie continu toegang heeft tot beveiligingsservices en mogelijkheden om uw apparaat te beveiligen, bijvoorbeeld door back-ups van gegevens te maken en de nieuwste firmware-updates beschikbaar te stellen.

WAAROM CANON

Informatie is de essentie van moderne organisaties. Daarom moet u weten dat uw informatie veilig is en waarom het cruciaal is dat u technologie kiest die uw informatie gegarandeerd kan verdedigen.

U moet endpoint-apparatuur beschermen om datalekken te voorkomen. Om de beveiliging en compliance te verbeteren door de toegang tot uw systemen te beheren. En om gevoelige digitale documenten, content en gegevens 24/7 te beschermen.

Bij Canon is elk product, elke oplossing en elke service die we leveren, ontworpen om veilig te zijn. Dat noemen we Secure by Design. Onze printers en scanners beschikken over geavanceerde beveiligingsfuncties die ervoor zorgen dat de verkeerde mensen uw documenten niet kunnen zien. Onze slimme softwareoplossingen verminderen de kans op menselijke fouten, zodat compliance eenvoudiger is. Bovendien kunt u dankzij onze uitgebreide en flexibele suite met beveiligingsservices gebruikmaken van onze mogelijkheden op een manier die bij uw bedrijf past.

We geven onze klanten toegang tot dezelfde beveiligingsexpertise die wijzelf gebruiken om onze eigen organisatie te beschermen. Ons Product Security Incident Response Team werkt aan de frontlinie en reageert op nieuwe cyberdreigingen zodra deze zich aandienen. Het team past die kennis vervolgens rechtstreeks in onze technologieën toe. Dit betekent dat u altijd profiteert van de nieuwste ontwikkelingen op het gebied van cyberbeveiliging wanneer u met ons samenwerkt.

Dit blijkt onder andere uit de erkenning die we ontvangen van sectoranalisten zoals IDC en Quocirca, die onze holistische aanpak prijzen en melden dat onze focus op workflow- en procesoptimalisatie ons onderscheidt van de rest.

Wanneer informatiebeveiliging een voortdurende uitdaging is, is vertrouwen onmisbaar - en vertrouwen komt voort uit het hebben van een partner die u elke dag en elke seconde steunt.

WAAROM CANON

SECURE BY DESIGN

Voor Canon is informatiebeveiliging niet iets waar we pas achteraf over nadenken. Het verbindt alles wat Canon doet, van hardwareontwerp tot het einde van de levensduur van apparaten. Grondig geteste oplossingen, continue beveiligingspatches met AI-gestuurde detectie van bedreigingen en een uitgebreide reeks services die voldoen aan alle vereisten van het beveiligingslandschap: wij bieden oplossingen voor alle onderdelen van de levenscyclus van documenten, en zorgen bovendien voor de beveiliging gedurende de levensduur van onze producten. Zo bent u 24/7 verzekerd van 360°-bescherming.

SLIMME EN VEILIGE OPLOSSINGEN

Informatie die door uw organisatie stroomt, helpt medewerkers om samen te werken, productief te blijven en toegang te krijgen tot waardevolle inzichten. Maar het stelt u ook bloot aan risico's. Canon's softwareoplossingen voor organisaties bieden een volledig inzicht in en complete controle over uw informatieomgeving. Voorkom menselijke fouten met veilige, geautomatiseerde processen op basis van Therefore Online. Krijg toegang tot veilig gecentraliseerd printbeheer met uniFLOW Online. Voorkom dat documenten in verkeerde handen vallen met beveiligde vrijgave van printopdrachten.

uniFLOW online

Therefore™ PEOPLE PROCESS INFORMATION

WAAROM CANON

GEROEMD DOOR DE BRANCHE

Wij zijn toonaangevend op het gebied van informatiebeveiliging voor organisaties. Maar geloof ons niet op ons woord. Brancheanalisten zoals IDC en Quocirca geven aan dat onze oplossingen en diensten voor werkplektechnologie de informatiebeveiliging sterk verbeteren door apparaten, documenten en gegevens in de printinfrastructuur van organisaties te beveiligen. Robert Palmer, Research Vice President van IDC, verwoordt het als volgt: "Canon onderscheidt zich van concurrenten door haar holistische benadering van informatiebeheer, gecombineerd met een strategische focus op gebieden als workflow, procesoptimalisatie en beveiliging."

QUOCIRCA

IDC

HARDWARE MET STANDAARD GEAVANCEERDE BEVEILIGING

Uw printers en scanners zijn cruciaal voor de activiteiten van uw organisatie. Als deze apparaten echter niet in uw cyberbeveiligingsstrategie zijn opgenomen, kunnen ze toegangspunten worden voor aanvallers.

Canon neemt geavanceerde beveiligingsfuncties op in haar hardware om dit te voorkomen en de toegang tot uw documenten te beheren, bijvoorbeeld met multi-factor verificatie, realtime detectie van bedreigingen en end-to-end gegevenscodering. U kunt zelfs de activiteit van het apparaat controleren en beveiligingswaarschuwingen ontvangen voor ongebruikelijke acties, zoals meerdere aanmeldingspogingen of specifieke trefwoorden die worden geprint, gescand, gekopieerd of gedeeld.

WAAROM CANON

ONDERSTEUND DOOR EEN ELITE CYBERBEVEILIGINGSTEAM

Uniek voor de printsector is dat wij doen wat we beloven: klanten van Canon krijgen ondersteuning van ons Product Security Incident Response Team - dezelfde beveiligingsexperts die onze toonaangevende productbeveiliging implementeren. Met behulp van up-to-the-minute research en best practices uit de sector om uw apparaten, printactiviteiten, documenten en gegevens te beschermen tegen onbevoegde toegang, werkt ons team 24 uur per dag aan het identificeren en neutraliseren van opkomende cyberdreigingen voordat ze uw organisatie treffen.

SERVICES DIE DE BEVEILIGING VERBETEREN

Ons pakket aan beveiligingsservices is geschikt voor elke fase van de levenscyclus van apparaten. Misschien wilt u hulp bij het veilig toevoegen van nieuwe apparaten aan uw netwerk. Onze Device Hardening Service komt daarbij van pas, omdat u hiermee apparaten toevoegt die vooraf zijn geconfigureerd met aanbevolen beveiligingsinstellingen en -functies. Misschien wilt u zorgen voor beveiliging aan het einde van de levensduur van apparaten. Onze Data Removal Service verwijdert digitale en fysieke gegevens definitief van overtollige apparaten. Met Data Backup kunt u kritieke apparaatgegevens beschermen bij onverwachte gebeurtenissen. En onze Subscription Security Services bieden doorlopende bescherming tegen bedreigingen, afgestemd op uw specifieke behoeften. Voor welke uitdaging op het gebied van printbeveiliging u ook staat, wij vinden de perfecte beveiligingsservice voor u.

Canon Nederland N.V.
Brabantlaan 2
5216 TV ‘s-Hertogenbosch
Telefoon: (073) 6 815 815
canon.nl
b2b@canon.nl

Canon Belgium NV
Berkenlaan 3
1831 Diegem
Telefoon: 02 722 04 11
canon.be
contact@canon.be

Canon Inc.
Canon.com

Canon België / Canon Nederland N.V.
nl.canon.be / canon.nl