IDC MARKTSPOTLIGHT

GDPR – een blinde vlek: waarom printers vaak niet aan de regelgeving voldoen

Juli 2017

Door Duncan Brown

Gesponsord door HP

In deze IDC marktspotlight wordt aandacht besteed aan het kwetsbare karakter van printers in het enterprisenetwerk en aan de gevolgen van deze kwetsbaarheid voor een nalevingsprogramma dat gericht is op de gegevensbeschermingswet van de EU (de GDPR) en andere aangekondigde wetgeving. Er worden ook maatregelen beschreven om het risico van niet-beveiligde printers voor het bedrijf te reduceren.

Inleiding

De aandacht voor de beveiliging van het Internet of Things (IoT) is sterk toegenomen na een reeks opvallende Distributed Denial-of-Service-aanvallen (DDoS) waarbij met behulp van een gigantische hoeveelheid kwaadaardig verkeer van duizenden gehackte bewakingscamera's, digitale videorecorders en andere verbonden apparaten populaire websites werden platgelegd. Welk apparaat is het volgende doelwit?

Als we kijken welke andere IoT-apparaten een aantal kenmerken delen met de apparaten die bij deze aanvallen werden gebruikt, komen we uit bij consumenten-, MKB- en enterpriseprinters. Software-updates en toegangscontrole, die op traditionele IT-producten een hoge prioriteit hebben, worden bij printers vaak over het hoofd gezien. Printers kunnen het volgende instrument worden voor een grootscheepse IoT-aanval, maar ze creëren ook nieuwe gevaren voor de bedrijfsprocessen, omdat ze zich binnen het bedrijfsnetwerk bevinden en daar mogelijkheden bieden voor datadiefstal en DDoS in het interne gedeelte van het netwerk. Nu de GDPR en andere toekomstige regelgeving veel strengere straffen gaan opleggen voor inbreuken op persoonsgegevens, vragen printers als vergeten endpoint dringend om aandacht.

Uw printer Is een endpoint

Stelt u zich het volgende scenario voor: een onbekend apparaat wordt in een enterprisenetwerk geplaatst, achter de bescherming aan de rand zoals firewalls, inbraakpreventiesystemen en andere IT-infrastructuur, zodat het apparaat onbeperkt toegang heeft tot alle netwerkresources. In het apparaat is een webserver ingebouwd om te zorgen voor optimale functionaliteit. Alle poorten zijn standaard 'open' en bieden gigabit-ethernetconnectiviteit om het apparaat toegankelijk te maken. Het apparaat heeft een volwaardig besturingssysteem zoals Linux, voor maximale functionaliteit. Het wordt niet regelmatig gecontroleerd met de kwetsbaarhedenscanner, omdat de ingebouwde webserver de Security Information en Event Management (SIEM) tools van het bedrijf mogelijk valse meldingen verstrekt. De kwetsbaarhedenscanner is geconfigureerd om het apparaat te negeren. Dat heeft, afhankelijk van het merk, tot gevolg dat het apparaat tijdens zijn 5- tot 10-jarige levensduur niet wordt onderhouden en dat geen updates en patches worden geïnstalleerd. Apparaatbescherming bestaat uit een standaard wachtwoord en het apparaat wordt onderhouden door onvoldoende doorgelichte derde partijen. Het apparaat is essentieel voor de bedrijfsproductiviteit, dus voor elke 10 werknemers is er één aanwezig. Werknemers gebruiken het apparaat niet alleen, maar sturen er ook

gevoelige persoonsgegevens heen die erin worden opgeslagen. Erger nog, die gegevens kunnen zonder authenticatie of toegangscontrole door elke willekeurige omstander worden uitgevoerd.

Sommige mensen noemen dit een nachtmerrie; anderen noemen het een printer.

Hier moet een belangrijk punt worden opgehelderd. ‘Printbeveiliging' is een volwassen beveiligingsdiscipline, die voortkomt uit de noodzaak om gegevens te beveiligen. Zoals te begrijpen is, spelen nalevingsstandaarden een belangrijke rol in printbeveiliging. In EMEA betekent dit de GDPR, maar het strekt zich uit tot de Richtlijn voor beveiliging van netwerk- en informatiesystemen (NIS), de nieuwe e-Privacy richtlijn en de herziene Richtlijn betaaldiensten (PSD2). Deze standaarden vormen de basis voor beveiligingsresultaten, zonder dat ze specifieke technische details voor naleving voorschrijven.

De voornaamste kenmerken van de GDPR

De GDPR is een welkome herziening van de Europese wetgeving voor gegevensbescherming, die er al lang had moeten zijn. Hij vervangt de huidige wetgeving die dateert uit 1995, ruim vóór de hoge vlucht van dot-com en komst van Twitter, Facebook en de cloud. De GDPR vult de wetgeving aan om te voorzien in deze en toekomstige ontwikkelingen, waarbij persoonsgegevens worden gemaakt en gebruikt. Een extra voordeel van de GDPR is dat deze geldt voor alle lidstaten van de Europese Unie (EU).

De GDPR is ondertekend in april 2016 en treedt in werking op 25 mei 2018. Dit betekent dat ondernemingen nog minder dan een jaar hebben om naleving te waarborgen. De boetes voor het niet naleven van de verordening kunnen oplopen tot 4% van de wereldwijde jaaromzet van een bedrijf of € 20 miljoen (welk van beide hoger is). De GDPR introduceert ook het verplicht melden van inbreuken en dat heeft gevolgen voor directies die zich zorgen maken over reputatieschade.

De voorgenomen uittreding van het Verenigd Koninkrijk uit de EU (Brexit) heeft geen gevolgen voor de GDPR als geheel.

- Bedrijven in het Verenigd Koninkrijk die persoonsgegevens verwerken van EU-burgers moeten aan de GDPR voldoen, omdat de GDPR ook buiten de EU geldt voor persoonsgegevens van EU-burgers.
- Het Verenigd Koninkrijk zal waarschijnlijk lokale wetgeving implementeren die vergelijkbaar is met de GDPR om gegevensoverdracht vanuit de EU mogelijk te maken, conform 'adequaatheidsregels’.

De GDPR draait om méér dan alleen beveiliging. De verordening bevat een reeks nieuwe maatregelen, zoals uitwisselbaarheid van gegevens, toestemming en herroeping, leeftijdscontrole en het recht om vergeten te worden. De belangrijkste factor in de naleving is echter een goede beveiliging. Wat zegt de GDPR daar precies over?

De GDPR is opmerkelijk vaag in het definiëren van specifieke beveiligingsmaatregelen. Van de 99 artikelen gaat alleen Artikel 32 specifiek over beveiliging. De eis is dat ondernemingen 'passende technische en organisatorische maatregelen treffen om een op het risico afgestemd beveiligingsniveau te waarborgen'. Met andere woorden: elk bedrijf moet zelf het risico bepalen dat geassocieerd is met zijn persoonsgegevens en de beveiligingsmaatregelen implementeren die het nodig acht.

Eén aspect hierbij is de vraag wat de GDPR verstaat onder 'stand van de techniek'. Bedrijven zijn niet verplicht om de allernieuwste technologie te implementeren volgens de stand van de techniek. Ze moeten echter weten wat dit betekent om hun handelswijze te kunnen verdedigen. Bedrijven moeten voorkomen dat ze in een situatie belanden waarin ze moeten rechtvaardigen waarom ze een

bepaalde veiligheidsmaatregel of techniek niet hebben toegepast, als die nalatigheid rechtstreeks tot een gegevensinbreuk heeft geleid.

Een van de voornaamste criteria die de GDPR-toezichthouders waarschijnlijk zullen hanteren is wat IDC de 'How hard did you try'-test noemt. Niet op de hoogte zijn van een kwetsbaarheid is een kwalijke zaak. Wel op de hoogte zijn en niets doen is nog veel erger. Het negeren van een beveiligingsprobleem op een printerpark kan leiden tot een inbreuk op persoonlijke gegevens die, indien ernstig genoeg, een toezichthouder zou kunnen doen twijfelen of adequate organisatorische en technische maatregelen zijn geïmplementeerd om de gegevens te beschermen.

Het materiële toepassingsgebied van de GDPR is belangrijk: de verordening is van toepassing op de 'geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de niet-automatische verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen'. Met andere woorden: gegevens hoeven geen elektronisch formaat te hebben om binnen het toepassingsgebied te vallen. De verordening geldt ook voor gedrukte exemplaren van gegevens.

Richtlijn voor beveiliging van netwerk- en informatiesystemen

De EU begrijpt dat in een tijdperk waarin steeds meer cyberaanvallen plaatsvinden, belangrijke diensten moeten worden beschermd, met name diensten die onmisbaar worden geacht voor het economisch of sociaal verkeer. Om in alle lidstaten een consistente bescherming tegen cyberaanvallen te creëren, heeft de EU de NIS-richtlijn aangenomen.

De NIS bevat verrassend weinig details over de beveiligingsvereisten. Er is een brede focus op de bescherming van infrastructuur, inclusief fysieke apparatuur, en de nadruk ligt vooral op robuustheid (incidentenbeheer, bedrijfscontinuïteit enz.). De richtlijn bevat een verplichting tot het melden van inbreuken (zie Artikel 16), maar er zijn geen boetes vastgesteld voor het niet naleven van deze bepaling.

Omdat de NIS een richtlijn is, moet deze door elke lidstaat worden omgezet in wetgeving die door de wetgevende macht wordt bekrachtigd. NIS is in werking getreden in augustus 2016. Lidstaten hebben tot 10 mei 2018 de tijd om de richtlijn om te zetten in nationale wetgeving en daarna nog zes maanden om leveranciers van essentiële diensten te identificeren.

De voordelen van printerbeveiliging

Printerbeveiliging richt zich, in tegenstelling tot printbeveiliging, uitsluitend op de fysieke apparaten die worden gebruikt om te printen; het is dan ook een onderdeel van netwerkbeveiliging. Bij printerbeveiliging wordt de printer als endpoint beschouwd en met dezelfde zorg behandeld als andere endpoints zoals notebooks, servers en mobiele apparaten. Hoewel ze een gezamenlijke taal gebruiken en gedeeltelijk dezelfde problematiek kennen, zijn printbeveiliging en printerbeveiliging afzonderlijke disciplines.

Hoe kwetsbaar zijn netwerkprinters nu werkelijk?

Printers ontvangen een aanzienlijke hoeveelheid data, waartoe ook persoonsgegevens behoren. Weinig gebruikers, nalevingsdeskundigen of IT-beheerders denken na over de veiligheid van dergelijke data wanneer ze via het netwerk naar de printer worden gezonden of in de printer zijn opgeslagen. Artikel 5.f van de GDPR verplicht gebruikers tot "het nemen van passende technische of organisatorische maatregelen die op een dusdanige manier worden verwerkt dat een passende beveiliging van gegevens gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies,

vernietiging of beschadiging". Weinig ondernemingen denken daarbij aan de veiligheid van data op een printer.

Het gebeurt zelfs regelmatig dat afgedrukte documenten in de uitvoerlade van een printer blijven liggen. In het licht van de GDPR kunnen pull-printingoplossingen, waarbij gebruikers zichzelf bij de printer moeten authenticeren om het document op te halen, een vereiste worden voor ondernemingen die het printen van persoonsgegevens toestaan.

Printers zijn een gewild doelwit voor cybercriminelen, onder meer omdat ze niet als onderdeel van IT worden beschouwd en dus weinig aandacht krijgen van het beveiligingsteam. Printerbeheer wordt vaak als onderdeel van faciliteitenbeheer beschouwd. Toen printers netwerkapparaten werden, beschouwde men ze meestal als lage risicofactor, zolang ze zich achter de bedrijfsfirewall bevonden. De kwetsbaarheid van printerendpoints bleef onderbelicht.

Gecombineerde printer/scanner/faxmachines worden steeds geavanceerder en bevatten algemene computers om alle activiteiten te besturen. In veel moderne printers zijn al Windows- en Linux-systemen ingebouwd. Omdat deze besturingssystemen niet goed beveiligd worden en er geen patches op worden geïnstalleerd, zijn ze dikwijls kwetsbaar. Omdat ze bovendien voor sommige functies verbonden moeten zijn, worden veel printers omwille van het gebruiksgemak geleverd met een aantal open poorten.

Door de combinatie van onvoldoende aandacht, krachtige computerfunctionaliteit en een groot aantal verbindingsopties kunnen aanvallers zich op verschillende manieren toegang verschaffen tot printers, bijvoorbeeld via een modem, een wireless access point of via met spyware geïnfecteerde desktop-pc's. Wanneer ze eenmaal binnen zijn, kunnen aanvallers de computerkracht gebruiken om andere machines in het interne netwerk te hacken of ze deel te laten uitmaken van een Distributed Denial-of-Service-aanval. De meeste printers hebben onbeperkte toegang tot het interne bedrijfsnetwerk. Een aanvaller die de beveiliging van een printer schendt, kan het hele netwerk doorzoeken op systemen waarvan hij misbruik kan maken.

Net zoals andere endpointapparaten die moeten worden beschermd, zijn printers niet alleen een 'toegangspoort', maar ook een doelwit voor cybercriminelen. In de printspool zijn vaak vertrouwelijke documenten opgeslagen. Printers zijn ook vaak gecombineerd met een documentscanner en documenten worden veel langer in het scanarchief opgeslagen dan gebruikers verwachten.

Overwegingen

Als uw bedrijf zich nog niet intensief bezighoudt met printerbeveiliging, heeft IDC een aantal aanbevelingen om daarmee een begin te maken.

Het begint allemaal met zichtbaarheid

Net zoals bij ieder endpoint dat moet worden beveiligd, begint u bij de basis: zichtbaarheid is altijd de eerste stap. Maak een volledige inventaris van alle printers, met merk, model, functionaliteit en configuratie. Het opstellen van een dergelijke lijst is niet altijd eenvoudig, omdat individuele gebruikers vaak printers op onbekende plaatsen neerzetten (schaduw-IT). In laboratoria, directiekantoren of kantoorvestigingen worden printers soms voor het gemak op het netwerk of rechtstreeks op een pc aangesloten, zonder rekening te houden met de beveiliging.

Een endpointinventaris die ook printers bevat kan in het ideale geval worden afgeleid uit een netwerktoegangscontroller (NAC) of assetbeheertool die apparaatdetectie als standaardfunctie heeft. Het is bijzonder moeilijk om zonder een NAC een volledig overzicht te krijgen van alle printers. Bepaalde printermodellen bieden automatische detectie wanneer ze op het netwerk worden

aangesloten. Als uw netwerkomgeving niet over een homogeen apparatuurpark van dergelijke printers beschikt, is een NAC noodzakelijk.

Printerendpoints versterken

Printers in de onderneming moeten net zo worden beheerd als ieder ander aangesloten endpoint. Schakel overbodige services op de printer, zoals FTP, uit. De meeste ondernemingen hebben geen FTP-toegang tot hun printers nodig en het doet vaak meer kwaad dan goed. Op sommige printers kunnen aanvallers bijvoorbeeld FTP-verzoeken uitvoeren en printtaken anoniem uit een printspool halen. Ook zijn veel FTP-services op moderne printers gevoelig voor FTP-bounce-aanvallen. Met een tool als Nmap (Network Mapper) kan een aanvaller de bron van een poortscan verbergen en zo een compliant FTP-server overtuigen om proxy-FTP-verbindingen toe te laten. Weliswaar zijn dergelijke FTP-bouncescans al lang bestaande technieken, maar een opmerkelijk aantal gloednieuwe printservers is er nog gevoelig voor.

De allerbelangrijkste maatregel voor het versterken van printerendpoints is wachtwoordbeheer. De grootste fout die ondernemingen maken is het niet veranderen van standaard wachtwoorden. Volgens het *Data Breach Investigations Report* van Verizon uit 2016 werd bij 63% van de ontdekte gegevensinbreuken gebruikgemaakt van zwakke, standaard of gestolen wachtwoorden. Als printers worden beheerd door de faciliteitenafdeling of door derde partijen draait (voor deze beheerders) alles om gemak. Wanneer een apparaat onderhoud nodig heeft, is het soms een heel gedoe om het wachtwoord te achterhalen. Als er op elke 10 medewerkers één printer is, moet een onderneming met 10.000 personeelsleden dus 1000 wachtwoorden onderhouden. In dergelijke gevallen moet de veiligheid meestal wijken voor het gebruiksgemak. Wachtwoordbeheer is niet alleen een tekortkoming van niet-technisch personeel. De tweede grote fout die bedrijven maken is het vrij toegankelijk bewaren van gebruikersnamen en wachtwoorden in een niet-versleuteld tekstformaat die iedereen met een http://-verbinding kan vinden.

Onderhoud uitvoeren en patches installeren

De meeste inbreuken vinden plaats door een gebrek aan onderhoud. Volgens het *Data Breach Investigations Report* van Verizon uit 2016 was de top 10 van misbruikte kwetsbaarheden in 2015 goed voor 85% van het geslaagde misbruikverkeer. De kwetsbaarheden waarvan het meest gebruik wordt gemaakt zijn bekend en gepubliceerd. Cybercriminelen gebruiken wat werkt en willen hun investering in malware optimaal benutten.

Als u uw printerendpoints onderhoudt en patches installeert, bent u een minder gemakkelijk doelwit en zullen cybercriminelen geneigd zijn hun tools te gebruiken bij bedrijven die hun systemen minder goed onderhouden.

Als het gaat om patches, verschillen printers onderling sterk. Sommige fabrikanten bieden beheertools waarmee u bepaalde merken en printermodellen kunt bewaken, beheren en updaten. Dergelijke tools zijn uiterst waardevol, omdat de kwetsbaarhedenscanners van een bedrijf mogelijk problemen zullen hebben met printers, vanwege de ingebouwde webserver. Als u zulke printers met robuuste beheertools bezit, boft u. Als dat niet het geval is, moet u mogelijk op elke printer afzonderlijk patches installeren, omdat het creëren van een geautomatiseerde oplossing ingewikkeld is.

Om te voorkomen dat 'ruis' wordt geïmporteerd in de SIEM-tools, configureren bedrijven hun kwetsbaarhedenscanners vaak zo, dat ze printers negeren. Dat is net zozeer een probleem met SIEM en beheertools voor kwetsbaarhedenscanners als met printers. Het kan ingewikkeld zijn om dergelijke tools zo te configureren dat ze alleen bepaalde berichten van printers accepteren, maar op korte termijn helpt dat wel om het netwerk te beschermen tegen infecties die binnenkomen via printers.

De verbinding beveiligen

Ondersteun de beheerprotocollen die worden gebruikt voor de printer. De meeste moderne printers ondersteunen een vorm van beheer via HTTP en/of HTTPS en enkele ondersteunen zelfs Telnet of Secure Shell (SSH). Kies met zorg een beheerprotocol dat encryptie mogelijk maakt, zoals HTTPS of SSH, en schakel zwakke of gekraakte encryptiecodes zoals SSLv3 uit.

Zorg er tenslotte voor dat uw printers geen vrije toegang hebben tot de rest van uw interne netwerk. Het segmenteren van enterprisenetwerken is een best practice voor netwerkbeveiliging en dat moet zich uitstrekken tot printers. U kunt certificaten gebruiken om de toegang tot netwerkresources logisch te segmenteren en om verkeer te versleutelen. Houd er wel rekening mee dat deze extra beveiligingsmaatregelen de printerfunctionaliteit nadelig kunnen beïnvloeden, doordat ze bijvoorbeeld de toegang tot adresboekservices (zoals Active Directory) beperken en cloud-gebaseerd beheer en bewaking onmogelijk maken. Een juiste afweging tussen krachtige beveiliging van printers en het behoud van functionaliteit is altijd een kwestie van inschatting van het bedrijfsrisico.

Conclusie

Printers krijgen niet de aandacht die andere instrumenten van cybercriminaliteit ontvangen. De kwetsbaarheid en de daaruit voortvloeiende gevaren zijn reëel. Grote en kleine ondernemingen moeten snel maatregelen nemen om dit probleem aan te pakken. Cybercriminelen zijn allesverslindende imitators. Wanneer een aanvalsmethode eenmaal door één kwaadwillige voor eigen gewin is gebruikt, zullen anderen snel volgen.

Met de komst van de GDPR zullen de financiële en reputatieschade door het negeren van printerbeveiliging escaleren tot op directieniveau. Het zou zeer te betreuren zijn als een bedrijf dat op alle andere fronten de regels naleeft en dat hard gewerkt heeft aan zijn informatiebeveiligingsprocessen en -technologieën in de problemen kwam door een blinde vlek op het gebied van printers.

OVER DEZE PUBLICATIE

Deze publicatie is geproduceerd door IDC Custom Solutions. De hierin gepresenteerde mening, analyse en onderzoeksresultaten zijn gedestilleerd uit meer gedetailleerd onderzoek en analyses die onafhankelijk door IDC zijn uitgevoerd en gepubliceerd, tenzij de naam van een specifieke sponsor wordt vermeld. IDC Custom Solutions maakt informatie van IDC beschikbaar in diverse formaten, voor distributie door verschillende bedrijven. Een licentie voor het distribueren van IDC-content houdt geen aanbeveling van, of mening over, de licentiehouder in.

Wereldwijd hoofdkantoor: 5 Speen Street Framingham, MA 01701 VS T.+1 508.872.8200 F.508.935.4015 www.idc.com

4AA7-1155NLE