brother
at your side

Accurate printbeveiliging

Onderdeel van de
‘Digitale transformatie’
serie van Brother

Serie rapporten op basis van
onderzoek in diverse branches

www.brother.nl

Barrières voor investering in printbeveiliging

Door de toename van cyberaanvallen en datalekken, zijn de meeste kleine en middelgrote bedrijven, zich inmiddels wel bewust van de noodzaak om hun IT-systemen goed te beveiligen.

Het beveiligen van de IT-structuur is een uitdaging die op grote schaal moet worden aangepakt. Printers, scanners en kopieerapparaten moeten net zo veilig zijn als andere apparatuur. Als deze apparaten over het hoofd worden gezien, is dit een achterdeur waarmee cybercriminelen en hackers gemakkelijk binnen kunnen komen. Het MKB wordt zich steeds meer bewust van het belang van dit probleem, waarbij 72% van de bedrijven aangeeft dat het voor hen van cruciaal belang is dat hun printapparatuur goed beveiligd is. Dit speelt nog meer bij organisaties die werken met privacygevoelige gegevens in zoals bedrijven in de professionele dienstensector (82%) en de gezondheidszorg (81%).

Dit betekent echter dat bijna een derde van ondervraagde bedrijven het belang van de beveiliging van randapparatuur nog niet onderkent. Tevens geeft bijna de helft aan dat hun organisatie niet voldoende heeft geïnvesteerd in de beveiliging van de printers.

Als bedrijven de noodzaak inzien om in te investeren in printbeveiliging, waarom doen ze dat dan niet?

Uit ons onderzoek komen twee duidelijke redenen naar voren:

- Onvoldoende verantwoordelijkheid voor het beveiligen van de printers
- Gebrek aan kennis en begrip over mogelijke bedreigingen en geldende normen

Dit rapport is bedoeld om besluitvormers binnen het MKB duidelijk te maken hoe belangrijk printbeveiliging is en hoe ze veilige printoplossingen kunnen implementeren. Het rapport maakt deel uit van een bredere serie rapporten die tot doel heeft beslissers te informeren over hoe ze digitale technologieën het beste kunnen gebruiken binnen kleine en middelgrote organisaties. De rapporten zijn gebaseerd op een uitgebreid onderzoek sat werd uitgevoerd onder besluitvormers binnen bedrijven in de EMEA-regio (Europa, Midden-Oosten en Afrika). De serie is opgedeeld in vier rapporten, die elk één van de volgende thema's behandelen:

- Digitale werkprocessen
- Implementatie
- Beveiliging
- Duurzaamheid

Wie is er verantwoordelijk voor de printbeveiliging?

Er is vaak een gebrek aan duidelijkheid over wie de verantwoordelijkheid draagt voor de beveiliging van printapparatuur. Bijna de helft van het MKB in West-Europa (44%) geeft aan dat het onduidelijk is wie precies verantwoordelijk is voor printerbeveiliging binnen de organisatie. Dit heeft tot gevolg dat de beveiliging vaak onvoldoende is, waardoor bedrijven kwetsbaar zijn.

Het is aannemelijk dat de verantwoordelijkheid voor de printerbeveiliging niet wordt opgepakt, omdat printapparatuur traditioneel niet wordt gezien als een ‘zwak punt’ binnen de IT-structuur. Hoewel ons onderzoek aantoont dat beslissers binnen grote organisaties zich wel beginnen te realiseren dat printbeveiliging van cruciaal belang is, lijkt dit in het MKB nog niet te gebeuren.

Het MKB is bijzonder kwetsbaar omdat er vaak een klein aantal werknemers verantwoordelijk zijn voor de hardware en software. Als IT-professionals zich niet voldoende bewust zijn van de risico’s, kan printbeveiliging gemakkelijk over het hoofd worden gezien.

Dit neemt niet weg dat alle werknemers binnen een organisatie een bepaalde mate van verantwoordelijkheid dragen, voor het veilig bewaren van gevoelige informatie.

De IT-specialisten zijn verantwoordelijk voor de beveiliging van apparaten binnen de organisatie. Toch hebben werknemers zelf ook een verantwoordelijkheid om ervoor te zorgen dat gegevens veilig worden bewaard. Dataverlies is een van de grootste risico’s voor commerciële bedrijven.

Bij het beveiligen van gegevens die worden geprint, zijn er een aantal potentiële gevaren:

- onbevoegde hebben toegang tot gemaakte afdrukken
- gebruikers vergeten uit te loggen na het afdrukken van vertrouwelijke documenten
- gebrek aan traceerbaarheid van de gebruikers die toegang hebben gehad tot documenten

Bijna 9 op de 10 bedrijven hebben te maken gehad met printergerelateerde beveiligingsincidenten

De meerderheid van het MKB geeft aan dat de veiligheid van gegevens voor hen een topprioriteit is. Databeveiliging wordt gezien als een belangrijke uitdaging en kan de productiviteit en efficientie ernstig belemmeren. Zeven op de tien ondervraagde bedrijven (72%) geven aan dat databeveiliging een hogere prioriteit heeft dan apparaatbeveiliging. Slechts een op de drie bedrijven heeft er vertrouwen in dat hun printinfrastructuur voldoende is beveiligd.

Bijna de helft van de MKB-bedrijven heeft weinig of geen overzicht wie binnen de organisatie printopdrachten afdrukt of verzamelt. Het is daarom niet verassend dat 86% aangeeft weleens te maken hebben gehad met een printgerelateerd beveiligingsincident. Deze incidenten houden meestal verband met vertrouwelijke documenten die onbeheerd op de printer worden achtergelaten, niet worden opgehaald of worden meegenomen door collega's waarvoor de documenten niet bedoeld zijn.

Als gevolg hiervan heeft de meerderheid van de bedrijven binnen het MKB (64%) al maatregelen genomen om printgerelateerde beveiligingsproblemen aan te pakken. Ze doen dit door de toegang tot bepaalde printers te beperken of door ID-kaarten of pincodes in te voeren, zodat printtaken alleen door de juiste gebruikers vrijgegeven kunnen worden.

Dit is een stap in de goede richting. In de komende jaren zal het voor alle bedrijven belangrijk worden om veilige protocollen in te voeren. Degenen die hiermee al begonnen zijn zullen hun processen moeten blijven controleren, om zodoende een optimale beveiliging te garanderen en te verbeteren.

Er zijn drie hoofddoelstellingen voor de beveiliging van gegevens, die samengevat kunnen worden in de afkorting CIA.

Deze hebben betrekking op zowel apparaat- als databeveiliging:

Confidential

Beschermen van vertrouwelijke bedrijfsgegevens zodat deze alleen worden gedeeld met de beoogde ontvanger. De sleutel hiervoor zijn authenticatie- en autorisatiemaatregelen, die vereisen dat gebruikers hun identiteit verifiëren, voordat documenten op de printer worden vrijgegeven.

Integrity

Zekerheid dat de juiste firmware geïnstalleerd is, zodat apparaten veilig en beschermd zijn tegen cybercriminaliteit en andere externe bedreigingen.

Availability

Zorgen dat het apparaat actief en toegankelijk is voor geautoriseerde gebruikers om cruciale werkzaamheden uit te voeren.

Gebrek aan kennis oorzaak van slechte printbeveiliging

Minder dan een derde (32%) van de belangrijkste IT-besluitvormers die binnen het MKB werken, zegt geavanceerde kennis te hebben van cybersecurity en mogelijke bedreigingen. Als IT-managers en medewerkers niet over voldoende kennis van bedreigingen beschikken, zullen bedrijven blijven worstelen om de juiste beschermende maatregelen te nemen. In het MKB heeft de IT-beslisser doorgaans een rol die veel verschillende disciplines en technologieën omvat. Het is begrijpelijk dat ze geen experts zijn in een specifiek gebied als printbeveiliging.

Vaak is jargon de boosdoener. Meer dan de helft (51%) van het MKB zegt dat er te veel vaktermen worden gebruikt rond printerbeveiliging.

Hieruit kunnen we afleiden dat het onwaarschijnlijk is dat IT-teams en besluitvormers voldoende kennis hebben van merk specifieke printtechnologieën, die relevant zijn voor hun eigen beveiligingsbehoeften. Als gevolg hiervan is het niet verwonderlijk dat bedrijven kiezen voor merken die ze al ‘kennen’, zodat de beveiliging van de printers eenvoudig opgezet kan worden. Er wordt dan echter niet gekeken welke beveiligingsmaatregelen er werkelijk nodig zijn binnen de organisatie en of deze wel of niet worden afgedekt door de gekozen oplossing.

Het is belangrijk dat printerleveranciers bedrijven duidelijk informeren en meer inzicht geven in de relevante beveiligingsnormen, zodat er voor de juiste oplossing wordt gekozen.

Het inzicht van Brother

Brother heeft zeven cruciale aanbevelingen opgesteld, waarmee MKB'ers zich kunnen beschermen tegen het gevaar van dataverlies, die ingrijpende financiële, juridisch en reputatieschade tot gevolg kan hebben.

Betrokkenheid van de directie

De omvang van de schade die veroorzaakt kan worden door cyberaanvallen en datalekken, in combinatie met de vereisten van de Algemene Verordening Gegevensbescherming (AVG), betekent dat printbeveiliging verder moet reiken dan de IT-afdeling. Er is een strategische aanpak nodig op directieniveau, in samenspraak met de Chief Information Officer (CIO) en de Chief Information Security Officer (CISO).

Terugkerende controles en monitoring

Het is voor bedrijven van cruciaal belang om mogelijke kwetsbaarheden in de printbeveiliging aan het licht te brengen. Dit kan door de printerinfrastructuur mee te nemen in terugkerende beveiligingscontoles en audits. Dit is vooral belangrijk als een bedrijf een combinatie van nieuwe en oude apparaten in gebruik heeft. De aanbieders van Managed Print Service (MPS) bieden naast een uitvoerige assessment, na implementatie ook een voortdurende monitoring van het printerpark.

Wijzig vooringestelde wachtwoorden

Standaard of vooraf ingestelde beheerderswachtwoorden vormen een zwakke schakel in de beveiliging van printapparatuur. Gelukkig is dit snel op te lossen, door na installatie de wachtwoorden direct te wijzigen en te kiezen voor veilige en sterke beheerderswachtwoorden.

Update regelmatig de firmware

Potentiële beveiligingsproblemen voor printapparatuur kunnen aanzienlijk worden verminderd door de firmware regelmatig bij te werken en het apparaat in te stellen voor het automatisch uitvoeren van updates. Mocht u hierover vragen hebben, neem dan contact op met uw fabrikant.

Printopdrachten beveiligen

Het zijn niet alleen de printers die beschermd moeten worden, maar ook de documenten die worden verzonden. End-to-end encryptie van het netwerkverkeer zorgt voor een veilige overdracht van printopdrachten naar de printers. Aangezien de meeste printers opdrachten tijdelijk opslaan, is het raadzaam dat de printgegevens versleuteld zijn.

Apparaten monitoren

Bedrijven kunnen diverse software applicaties gebruiken om apparaten te monitoren en ervoor te zorgen dat problemen worden opgelost zodra deze zich voordoen. Apparaten genereren een schat aan gegevens en deze kunnen gebruikt worden om potentiële beveiligingsproblemen te identificeren en snelle reacties op cyberaanvallen mogelijk te maken. MPS-gebruikers kunnen diverse rapportages instellen voor het monitoren van mogelijke datalekken.

Medewerkers trainen

Aangezien veel gegevensverlies incidenten per ongeluk worden veroorzaakt, is het van vitaal belang dat bedrijven medewerkers voorlichten over het belang van het beschermen van gevoelige informatie en het vergroten van het bewustzijn over kwaadaardige cyberdreigingen. MPS-aanbieders bieden vaak hulp bij interne training van medewerkers.

Eindconclusie

Printers werden in het verleden vaak over het hoofd gezien binnen de beveiliging van organisatie. Inmiddels wordt het belang van het beschermen van bedrijfsgevoelige informatie binnen het MKB steeds meer onderkend. Daaruit voort vloeit het besef dat het ook belangrijk is om de printapparatuur goed te beschermen tegen cyberdreigingen en andere vormen van informatie verlies. Toch zijn er nog grote uitdagingen en obstakels te nemen, als het gaat om het implementeren van een accurate printbeveiliging binnen bedrijven.

Bedrijven zullen de verantwoordelijkheid rond printbeveiliging moeten toewijzen aan specifieke teams of personen. Alleen dan is het mogelijk om apparaten goed te beschermen en kunnen toekomstige bedreigingen het hoofd worden geboden. Binnen apparaatbeveiliging speelt databeveiliging een essentiële rol. Daarnaast is medewerking nodig van alle interne medewerkers binnen de organisatie, om de risico's zoveel mogelijk te minimaliseren.

Zelfs als er duidelijkheid is over de verantwoordelijkheden, is voldoende kennis om printbeveiliging effectief te beheren nog steeds een grote uitdaging. Printtechnologie wordt steeds complexer en de printwereld staat bol van vakjargon. Bedrijven moeten erop kunnen vertrouwen dat hun leveranciers goede adviezen geven, zodat de juiste beslissingen genomen kunnen worden.

Een effectief printsysteem moet echter niet alleen de veiligheid waarborgen. De andere rapporten in onze 'Digitale transformatie' serie bevatten meer informatie over het opzetten van digitale werkprocessen, het maximaliseren van de productiviteit en het implementeren van een duurzame oplossing.

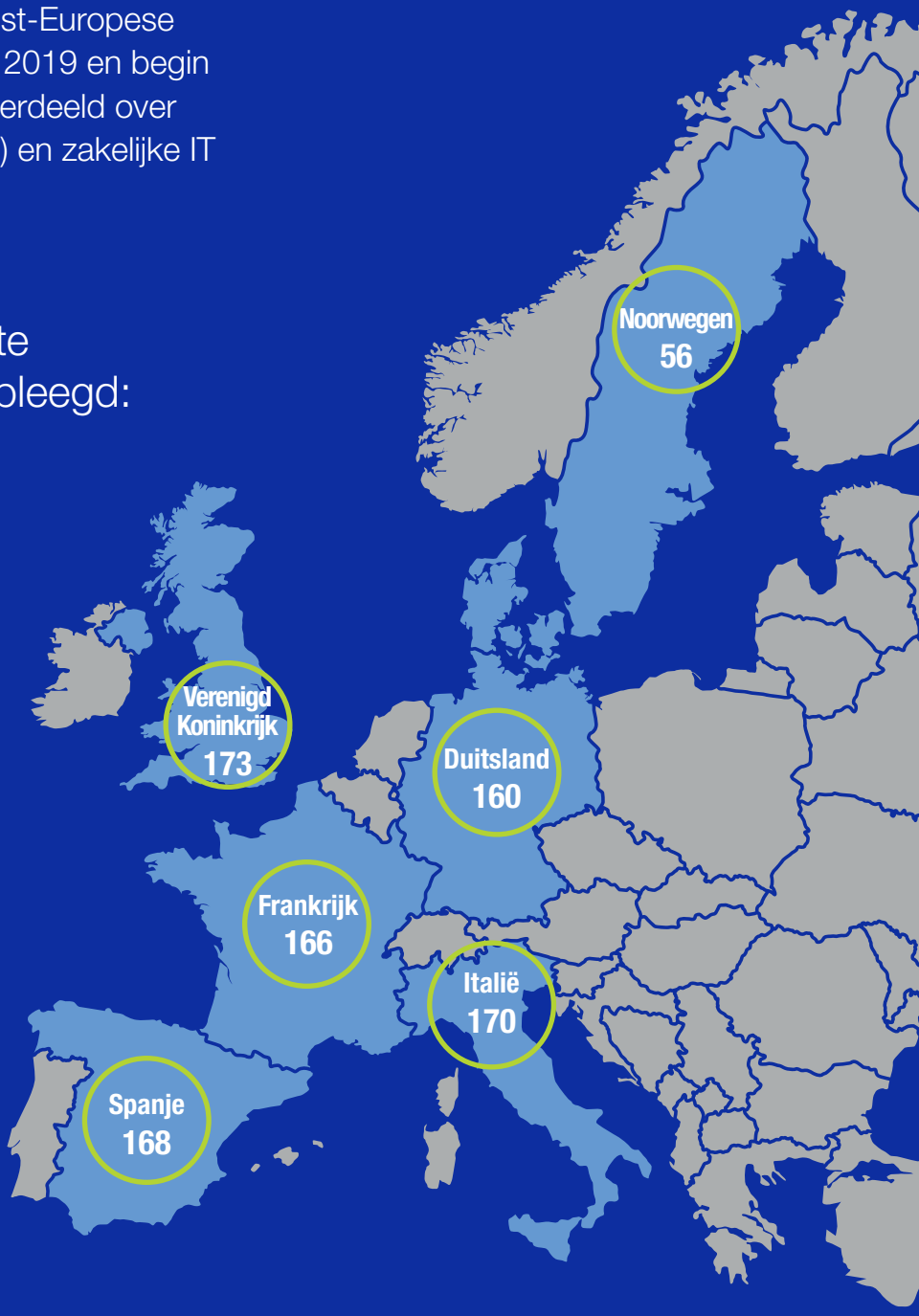
Onderzoeksmethode

Dit rapport is gebaseerd op 893 online enquêtes onder zakelijke beslissers.

De ondervraagden werken in bedrijven met 10 tot 499 werknemers in verschillende West-Europese landen. Veldwerk werd uitgevoerd in 2019 en begin 2020. De interviews zijn gelijkmatig verdeeld over strategische zakelijke beslissers (448) en zakelijke IT verantwoordelijke (445).

Overzicht van de belangrijkste sectoren die werden geraadpleegd:

- Gezondheidszorg - 152
- Retail - 117
- Logistiek - 113
- Horeca en hospitality - 81
- Transport en magazijn - 62
- Professionele diensten - 65
- Productie - 54
- Financiële diensten - 53
- Onderwijs - 51
- Bouw en infrastructuur - 39



Aanvullende interviews waren afkomstig uit andere sectoren, waaronder energie, farmaceutica, landbouw, defensie, onroerend goed, sport en entertainment.

Het onderzoek is uitgevoerd door marktonderzoeksbureau Savanta.

De nieuwste inzichten

Ontvang automatisch alle rapporten uit de ‘Digitale transformatie’ serie:

brother.nl/digitale-transformatie

www.brother.nl

Brother International (Nederland) B.V.
Postbus 600, 1180 AP Amstelveen
Zanderij 25, 1185 ZM Amstelveen
Tel: 020 – 545 12 51
e-mail: info@brother.nl

Zet- en drukfouten voorbehouden. Specificaties kunnen zonder tegenbericht worden gewijzigd. Brother is een geregistreerd handelsmerk van Brother Industries Ltd. Merk- en productnamen zijn geregistreerde handelsmerken of handelsmerken van de betrokken bedrijven.