HYBRIDE ORGANISATIES VAN NU

Informatiebeveiliging in de hybride werkomgeving

MAKE IT HERE SECURE TOGETHER

Canon

VOORWOORD

Tim Rawlins, Director en Senior Adviser, NCC Group

Hoewel het hoogtepunt van de pandemie inmiddels voorbij is, zal het effect ervan op onze manier van werken waarschijnlijk nog vele jaren zichtbaar zijn.

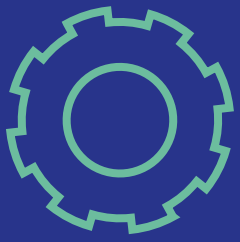
Om de crisis het hoofd te bieden, vonden de meeste organisaties al snel nieuwe manieren van werken, vele al tijdens de eerste dagen van de lockdown. Dit was voornamelijk te danken aan de IT-teams die, binnen een aantal dagen (of soms zelfs binnen een paar uur), erin wisten te slagen om voor iedereen werken op afstand mogelijk te maken. Dat is echt iets om trots op te zijn!

Maar in de haast om manieren te vinden om organisaties operationeel te houden, moesten er concessies worden gedaan, vooral met betrekking tot informatiebeveiliging. De normale beveiligingsprocedures werden niet altijd meer toegepast; men ging opeens een stuk minder voorzichtig te werk.

Nu hybride werken inmiddels voor velen normaal is geworden, **is het tijd dat we ook de beveiliging op orde krijgen.** We moeten dringend de schade herstellen die is veroorzaakt door de snelle oplossingen die op dat moment (uit noodzaak) door organisaties werden toegestaan; denk aan niet-beveiligde Wi-Fi-thuisnetwerken, zwakke wachtwoorden, onzorgvuldige compliancy-procedures of het niet-versleuteld delen van bestanden.

Er zijn ook grotere, meer fundamentele kwesties waar rekening mee moet worden gehouden. In een netwerk dat niet langer feilloos is afgeschermd in een eenvoudig te beheren kantooromgeving, is het lastiger geworden om criminele activiteit te detecteren. Door de voortdurende groei van hybride werken zijn de grenzen van netwerken niet langer duidelijk afgebakend, en is de beveiliging van elk afzonderlijk eindpunt – laptop, server of telefoon – van essentieel belang geworden.

Deze verandering in de werkpraktijk vraagt om nieuwe manieren van denken en werken, maar ook om nieuwe strikte maatregelen op het gebied van informatiebeveiliging.



NIEUWE TIJDEN...

Het is tijd om na te denken over praktijken zoals effectieve netwerksegmentatie – door het interne netwerk onder te verdelen in meerdere segmenten kunnen we een betere controle en bescherming voor belangrijke bedrijfsmiddelen bereiken. Met netwerksegmentatie kunnen medewerkers die geen toegang nodig hebben tot bepaalde informatie, niet meer vrij in het netwerk bewegen zoals ze dat nog konden in de tijd dat iedereen op kantoor werkte. Dat betekent echter dat kwaadwillende personen ook geen toegang hebben!

We moeten de bewaking van laptops en systemen verbeteren zodat we snel kunnen zien of ze worden gecompromitteerd en zo nodig effectief kunnen reageren. We moeten ook naar de volledige levenscyclus van onze technologieën kijken, en ervoor zorgen dat elk apparaat wordt voorzien van de nieuwste updates. Net zo belangrijk is dat goed wordt nagedacht over de beveiliging van apparaten die niet langer worden gebruikt, zelfs nadat het apparaat het gebouw verlaat. Gevoelige informatie kan namelijk nog steeds worden gehackt als deze niet is verwijderd.

We moeten meer controle krijgen over, en beter inzicht in wie precies welke informatie te zien krijgt. Er zijn oplossingen beschikbaar waarmee organisaties een geautomatiseerd beleid kunnen opstellen voor de toegang tot informatie en het bewerken en delen ervan. Zo kan een organisatie de controle houden over kritieke en gevoelige gegevens en wordt de kans op lekken, opzettelijk of per ongeluk, een stuk verkleind.

EEN NIEUWE MINDSET

We hebben natuurlijk ook te maken met de eigen medewerkers, en hun gedrag buiten de veilige omgeving van het kantoor. Tegenwoordig is het niet ongebruikelijk dat gevoelige zakelijke gesprekken plaatsvinden via mobiele telefoons. Microsoft Teams- en Zoom-vergaderingen worden tegenwoordig vaak bijgewoond vanuit koffiebars, de trein, of zelfs soms vanuit het café.

Met de groei van hybride werken, waarbij medewerkers veelal digitaal moeten communiceren, kunnen zij het doelwit worden van cybercriminelen op berichtenplatforms als WhatsApp of socialemediaplatforms als LinkedIn. Als een mobiele telefoon wordt gecompromitteerd omdat een medewerker op een phishing-link heeft geklikt of een wachtwoord of pincode met iemand heeft gedeeld, kan het hele netwerk in gevaar worden gebracht.

We moeten werken aan een cultuur waarin beveiliging centraal staat, waarin medewerkers wordt gewezen op al de mogelijke risico's en implicaties van hun handelen. Dat begint met het in gesprek gaan met medewerkers over beveiliging op een manier die ze aanspreekt en het effect dat het heeft op hun persoonlijke leven. Als we het bijvoorbeeld hebben over de voordelen die het gebruik van een wachtwoordmanager of meerstapsverificatie biedt voor aanmelding bij persoonlijke accounts, het gevaar van klikken op links in niet-verwachte e-mails en de mogelijke effecten van het doorgeven van informatie, hopen we dat dit goede gedrag zich ook laat vertalen naar hun werk.

Er is geen allesomvattende wondertechnologie die alle problemen met informatiebeveiliging in één keer oplost. Voor het verbeteren van de beveiliging in het hybride tijdperk moeten ook de medewerkers hun mindset veranderen en zich dringend nieuwe werkwijzen eigen maken. Echt succes op dit gebied komt voort uit de juiste combinatie van mensen, processen en technologie, die samen de organisatie het juiste niveau van cyberbeveiliging en veerkracht bieden. Doe dus de juiste dingen, en op de beste manier - veel succes.

Als wereldwijde experts op het gebied van cyberbeveiliging en risicobeheersing wordt NCC Group door meer dan 14.000 klanten wereldwijd vertrouwd voor het beschermen van hun meest kritieke bedrijfsmiddelen in een steeds veranderende dreigingsomgeving. Met de kennis, ervaring en wereldwijde aanwezigheid van de organisatie is het in de beste positie om organisaties te helpen bij het beoordelen, ontwikkelen en beheren van hun cyberveerkracht.

www.nccgroup.com

DE WERELD VERANDERT – EN STELT NIEUWE EISEN AAN INFORMATIEBEVEILIGING

Om succesvol hybride te kunnen werken, zijn samenwerkingstools nodig waarmee medewerkers kunnen communiceren en informatie kunnen delen via netwerken. Hoewel deze tools essentieel zijn voor het hybride bedrijfsproces, kunnen ze ook bijzonder kwetsbaar zijn. Cybercriminelen maken daar graag misbruik van.

We hebben dat ook al regelmatig zien gebeuren. Medewerkers op afstand vormden in het begin van de pandemie een gemakkelijk doelwit voor hackers, omdat ze relatief onbekende systemen moesten gebruiken en zichzelf onbewust kwetsbaar maakten voor cyberaanvallen. In dezelfde periode verlaagden veel organisaties hun beveiligingsuitgaven als onderdeel van algemene bedrijfsbesparingen, waardoor hun cyberbestendigheid nog verder afnam.[1] Dit alles tegen de achtergrond van een steeds sterkere focus op gegevensbescherming, een richting die al lang voordat Covid-19 opdook, werd ingezet.

De gewijzigde regelgeving voor gegevensbescherming betekent dat organisaties een grotere controle dienen te hebben over de manier waarop zij bedrijfs- en persoonlijke gegevens verzamelen, verwerken en opslaan. Dit omvat gegevens die zich op printers en multifunctionele apparaten in de organisatie bevinden. Organisaties die zich niet aan de voorschriften houden, kunnen boetes opgelegd krijgen tot 4% van hun jaarlijkse wereldwijde omzet of tot € 20 miljoen (afhankelijk van welk bedrag hoger is) volgens de AVG-regelgeving van de EU.[2] De Britse Data Protection Act van 2018 kent vergelijkbare, fiscale boetes.

Maar naast de financiële risico's die kwetsbaarheden in de cyberbeveiliging met zich meebrengen, bestaat de kans op aanzienlijke reputatieschade. Die kan net zo destructief - zo niet destructiever - zijn voor de organisatie. Een voorbeeld: het softwarebedrijf SolarWinds was begin 2020 het slachtoffer van een enorme cyberaanval die zich verspreidde naar de klanten van de organisatie.[3] Grote organisaties zoals Microsoft en belangrijke overheidsinstanties werden aangevallen, en gevoelige gegevens werden gecompromitteerd, wat leidde tot boetes van in totaal $ 3 miljoen en blijvende reputatieschade.[4]

Dat was toen, dit is nu.

De werkplek is sinds de eerste dagen van de pandemie inmiddels zo veranderd dat het nu nog moeilijker is om deze bedreigingen buiten de deur te houden. Bij de ontwikkeling van nieuwe plannen voor hybride werken, is het belangrijker dan ooit om prioriteit te geven aan een robuuste beveiliging.

[1] https://www.computerweekly.com/news/252484783/Coronavirus-Cyber-security-spend-to-slow-in-2020
[2] https://www.itgovernance.co.uk/dpa-and-gdpr-penalties
[3] https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?r=US&IR=T
[4] https://www.jdsupra.com/legalnews/the-solarwinds-cyber-attack-the-6179862/

Successen op het gebied van informatiebeveiliging komen zelden voorbij in het nieuws. Sommige organisaties hebben geluk, anderen zijn waakzaam. Maar er zijn een aantal typische gedragingen die deze organisaties gemeen hebben. In dit e-book wordt gekeken naar deze specifieke gedragingen en hoe u deze binnen uw organisatie kunt toepassen, te beginnen met **drie belangrijke aandachtsgebieden die elke leidinggevende en IT-besluitvormer prioriteit zou moeten geven.**

1 INFORMATIEBEVEILIGING BEGINT BIJ UW MEDEWERKERS

Hackers maakten in de begindagen van de pandemie vaak misbruik van de onbekendheid van medewerkers met nieuwe communicatieplatforms, zoals videovergaderingen, en de algemene onzekerheid die op dat moment heerste.[5]

In het Business Data Breach Investigations Report van Verizon uit 2020 wordt een aanzienlijke stijging van cyberdreigingen over de hele linie gezien, waarbij het bij meer dan 67% van de schendingen om diefstal van aanmeldgegevens en sociale aanvallen, zoals phishing en inbreuk op zakelijke e-mail bleek te gaan.[6] Volgens het rapport was 82% van alle inbreukincidenten (ten minste deels) te wijten aan menselijk handelen, inclusief sociale aanvallen, fouten en onjuist gebruik. Ook als uw personeel inmiddels meer ervaring heeft in het gebruik van tools voor werken op afstand en uw IT-team beter voorbereid is op incidenten, blijft de kans op cyberaanvallen en gegevensinbreuk nog steeds zeer groot.[7]

Bovendien gebruiken medewerkers mogelijk nog steeds niet de veiligste manier om informatie te delen. 'Schaduw-IT' is het gebruik van IT-systemen (software, apparaten zoals printers en scanners, apps en bestandsopslag) , die niet zijn geleverd of goedgekeurd door de werkgever, maar worden gebruikt door personeel omdat ze daar beter mee vertrouwd zijn of deze gebruiksvriendelijker vinden. Hoewel dit meestal wordt gedaan om redenen van gemak en efficiëntie in plaats van met kwaadwillende bedoelingen, kan dit tot ernstige problemen leiden.

Niet alleen zijn kant-en-klare systemen voor consumenten minder veilig dan systemen die zijn ontwikkeld voor zakelijk gebruik, maar als IT-teams ze niet hebben goedgekeurd, kunnen ze niet goed zicht op de beveiliging houden, wat de deur openzet voor potentiële aanvallers. Volgens Canon-onderzoek uit 2022 moet een op de vijf medewerkers nog steeds hun eigen apparatuur gebruiken. Eenzelfde deel van de medewerkers heeft moeite om IT-ondersteuning te krijgen op afstand.

Naast de behoefte aan IT-standaardisatie en -ondersteuning, is er ook een cruciaal gedragselement waarmee rekening moet worden gehouden: het kost tijd om nieuwe gewoonten en manieren van werken aan te leren. 77% van de IT-teams meldt dat medewerkers de beveiligingsprocedures niet langer volgen zodra ze op afstand werken.

En naarmate de grenzen tussen werk en privé vervagen, is de veiligheid van bedrijfskritische gegevens niet altijd meer gegarandeerd. Zelfs de experts kunnen laks worden. In een enquête onder medewerkers in de IT-beveiliging in Noord-Amerika en Europa gaf 20% toe dat personen in hun huishouden hun werkapparaten mochten gebruiken tijdens de lockdown.[8] Kinderen die schoolwerk doen of partners die YouTube-video's kijken – het lijkt wellicht onschuldig, maar een onervaren persoon hoeft maar één keer met de muis te klikken om een hacker toegang te geven tot het bedrijfssysteem.

77% VAN DE IT-TEAMS MELDT DAT MEDEWERKERS DE BEVEILIGINGSPROCEDURES NIET LANGER VOLGEN ZODRA ZE OP AFSTAND WERKEN.

Wanneer laptops, telefoons en gedeelde printers zonder toereikende beveiligingsvoorzieningen in het openbaar worden gebruikt, – in luchthavenlounges, bibliotheken en zelfs in professioneel beheerde samenwerkingsruimten –, bestaat er een extra risico dat onbekenden hun kans ruiken en tot gegevensdiefstal overgaan. **U weet nooit wie er over uw schouder meekijkt.**

Ook personen die onderweg werken, kunnen de gegevensbeveiliging in gevaar brengen, door een niet goed beveiligde laptop of telefoon aan te sluiten op een openbaar netwerk. Als een cyberaanvaller deze toegangspunten ontdekt, kan dit niet alleen de dagelijkse bedrijfsactiviteiten verstoren, maar ook ernstige gevolgen hebben voor de lange termijn.

Zelfs organisaties waarvan het volledige personeel nog op de bedrijfslocatie werkt, dienen zich er bewust van te zijn dat ze onderdeel uitmaken van een toeleveringsketen waarin andere organisaties mogelijk wel al op afstand werken of op hybride werkvormen zijn overgestapt. Bovendien kunnen door de overstap naar de cloud traditionele netwerkbeveiligingsstructuren ontoereikend zijn geworden. De beveiligingsindustrie ontwikkelt zich echter net zo snel als criminele activiteiten, met moderne services zoals Zero Trust die continue cyberveerkracht bieden.

Maar ook door middel van training kunnen risico's worden beperkt. Het is van essentieel belang dat werkgevers richtlijnen voor beveiliging en naleving opstellen en medewerkers worden getraind in het handhaven hiervan. Beveiliging moet een prioriteit zijn waarvoor continue investeringen zijn vereist, zodat organisaties met vertrouwen beslissingen kunnen nemen en vooruitgang kunnen boeken. Een ad-hocbenadering volstaat hier niet.

ZERO TRUST, EEN BEVEILIGINGSFRAMEWORK DAT VEREIST DAT ALLE GEBRUIKERS WORDEN GEVERIFIEERD, GEAUTORISEERD EN CONTINU WORDEN GEVALIDEERD, IS EEN CONCEPT DAT SPECIFIEK IS ONTWIKKELD VOOR DE HYBRIDE WERELD.[9] WAAR VOOR TRADITIONELE BEVEILIGINGSPROCEDURES DOORGAANS ALLEEN EEN GELDIGE AANMELDINGS-ID EN WACHTWOORD NODIG ZIJN OM TOEGANG TE KRIJGEN TOT EEN NETWERK, VOERT ZERO TRUST MEERDERE CONTROLES UIT VOORDAT EEN PERSOON (OF APPARAAT) TOEGANG WORDT VERLEEND.

[5] *https://www.theguardian.com/technology/2020/may/24/hacking-attacks-on-home-workers-see-huge-rise-during-lockdown*
[6] *https://www.verizon.com/business/resources/reports/dbir/*
[7] *https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-april-2022-14-3-million-records-breached*
[8] *https://www.securitymagazine.com/articles/94997-it-security-professionals-demonstrate-excessive-trust-despite-concerns-with-remote-work-security-programs*
[9] *https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/*

2 HET BELANG VAN INFORMATIEBEVEILIGING VOOR UW APPARATEN

Onbeveiligde printers, scanners en apparaten binnen het Internet of Things kunnen eenvoudig de deur openzetten voor hackers die weten hoe en waar ze moeten zoeken. Binnen een vertrouwd netwerk, zoals bij de meeste organisaties op kantoor, biedt de mogelijkheid om op afstand toegang te krijgen tot apparaten talloze voordelen. Maar soms, en vaak onbedoeld, kunnen apparaten zoals thuisprinters zonder wachtwoord of firewall worden aangesloten op niet-vertrouwde omgevingen, en zelfs rechtstreeks op internet.[10]

Moderne multifunctionele printers zijn **eindpuntapparaten** en zijn net zo krachtig als een pc. Hierdoor is het mogelijk dat de printerfirmware het doelwit wordt van hackers die toegang proberen te krijgen tot het netwerk en bedrijfsgegevens. Hackers kunnen wijzigingen aanbrengen in e-mailmappen, zodat een document kan worden verzonden naar een ontvanger buiten de organisatie. Of ze kunnen een verzonden document onderscheppen als het document en de bijbehorende gegevens niet zijn versleuteld.

WAT IS EEN EINDPUNT?

EEN EINDPUNT IS ELK APPARAAT DAT VERBINDING MAAKT MET HET BEDRIJFSNETWERK VANAF EEN LOCATIE BUITEN DE FIREWALL, ZOALS LAPTOPS, TABLETS, MOBIELE APPARATEN, POS-SYSTEMEN EN, NATUURLIJK, DIGITALE PRINTERS.

PRINTJACKING:
HET WATERGATE-SCHANDAAL VAN DE PRINTSECTOR

Eind 2021 publiceerde een team van Italiaanse onderzoekers een rapport waarin 50.000 printers in Europa aan het licht kwamen die kwetsbaar bleken te zijn voor virtuele aanvallen op afstand. Zij identificeerden hierbij drie soorten 'Printjack'-aanvallen.[11]

Bij het eerste soort aanval wordt misbruik gemaakt van een netwerklek om printers met kleine bugs te infecteren, waardoor ze continu een te zware werklast hebben en slechter gaan functioneren met de tijd. Het tweede soort is ernstiger van aard. Een 'papieren DoS-aanval' dwingt apparaten om herhaald dezelfde opdrachten te printen totdat het papier op is, waardoor het werk aanzienlijk wordt verstoord. Het derde en meest ingrijpende soort is een Man-in-the-Middle-aanval, waarbij hackers toegang hebben tot alle geprinte gegevens en toch onzichtbaar blijven.

Alle drie de soorten 'printjack'-aanvallen worden mogelijk gemaakt door beveiligingslekken in de netwerkverbindingen van de apparaten. Met strikte verificatieprotocollen en een solide beveiligingsframework kunnen deze aanvallen echter worden voorkomen.

Het onderzoek maakte duidelijk dat zowel de AVG- als ISO/IEC 27005:2018-richtlijnen op grote schaal niet werden nageleefd in Europa. Van de 50.000 printers die ze aan het licht brachten, bevond de meerderheid zich in Duitsland, Rusland, Frankrijk, Nederland en het Verenigd Koninkrijk.

Beveiligingsmaatregelen zijn niet alleen nodig voor de apparaten waar uw teams actief gebruik van maken. Hebt u ook nagedacht over die oude, stoffige laptops, harde schijven en printers die ergens in een opslagruimte liggen opgeborgen? Hoe zit het daarmee?

Gegevens die zijn opgeslagen op apparaten op de werkplek worden vaak over het hoofd gezien, maar de realiteit is dat ook als u een apparaat niet meer gebruikt en wegbergt, er nog steeds beveiligingsrisico's aan zijn verbonden. Ook hiervoor zijn richtlijnen nodig. Wanneer deze apparaten het einde van de levensduur bereiken en gegevens niet grondig en professioneel worden verwijderd, vormt dit een serieuze bedreiging.

Denk eens aan een oude printer die al jaren in die opslagruimte van het back-office staat, misschien zelfs al tientallen jaren. Ondanks het feit dat het apparaat nooit wordt gebruikt, werkt het nog steeds en kan het worden verbonden met internet. Vergeten achterdeuren zoals deze vormen voor slimme hackers een alternatieve route, vooral als medewerkers hier doorgaans alert op zijn.

Kortom, een sterke en robuuste beveiliging betekent dat u inzicht hebt in de volledige levenscyclus van de apparaten die in uw organisatie in gebruik zijn en deze beschermt gedurende de gehele levensduur, inclusief het moment dat ze niet langer worden gebruikt.

Hybride werken brengt eveneens nieuwe uitdagingen met zich mee doordat een deel van uw apparaten zich bij medewerkers thuis bevindt. Uit ons onderzoek blijkt dat 73% van de IT-besluitvormers niet in staat is om veilig gegevens te verwijderen van printers en scanners die zich buiten de bedrijfslocatie bevinden. Het is daarom van essentieel belang dat u goed zicht houdt op de volledige levenscyclus van uw apparaten.

Dit begint met ervoor te zorgen dat alles wat is aangesloten op het bedrijfsnetwerk actief wordt bewaakt en bijgewerkt met de meest recente beveiligingspatches. Volg bij het afvoeren van oude apparaten een vooraf gedefinieerde procedure. Denk hierbij aan het veilig wissen van alle gegevens en loskoppelen van apparaten, het op de juiste wijze vernietigen van harde schijven en het uitvoeren van een volledige controle of eventuele resterende fysieke informatie van apparaten, USB-sleuven, medialaden enz. is verwijderd.

U kunt nooit voorzichtig genoeg zijn. En al helemaal als het gaat om het verwijderen van gegevens, waarbij u hebt te voldoen aan regelgeving. Het is daarom net zo belangrijk dat u nauwkeurig een administratie bijhoudt van uw gegevensverwijderingsactiviteiten. voor het geval u door een officiële instantie wordt gevraagd uw compliancy aan te tonen.

[10] *Onderzoek van Canon, 2022*
[11] *https://arxiv.org/abs/2111.10645*

3 BEST PRACTICES COMBINEREN MET SLIM TECHNOLOGIEBELEID

Het komt vaak voor, en met name in het begin van de implementatie van hybride werkvormen, dat medewerkers eigen apparaten gebruiken, die niet door de organisatie zijn verstrekt of goedgekeurd. Het is voor IT-teams ook lastiger ervoor te zorgen dat deze apparaten correct zijn ingesteld, de vereiste updates krijgen, of dat gegevens op deze apparaten veilig worden beheerd.

Hoewel het belangrijk is om medewerkers te trainen en hen duidelijke richtlijnen te bieden, is dit waarschijnlijk niet afdoende om alle informatiebeveiligingsrisico's in te perken of te elimineren. Het selecteren van de juiste technologieprocessen en -protocollen kan ongewenste toegang tot informatie als gevolg van menselijke fouten helpen voorkomen.

WELKE FYSIEKE BEPERKINGEN VOOR INFORMATIETOEGANG KAN UW IT-TEAM GEBRUIKERS OPLEGGEN?

Er zijn functies op multifunctionele printers waarmee wordt voorkomen dat personen ongewenst toegang krijgen tot documenten, zoals pincodes, ID-kaarten en machtigingen op basis van rol, afdeling, anciënniteit en meer. Deze functies bieden de zekerheid dat informatie die op locatie wordt bewaard, niet in verkeerde handen valt.

Een andere mogelijkheid is software voor e-mailbewaking te gebruiken. Deze is bedoeld om menselijke nieuwsgierigheid in te dammen wat betreft het openen van e-mails van onbekende afzenders, en wel zonder inbreuk te maken op de privacyrechten van medewerkers – die horen immers onaangetast te blijven, zelfs in risicovolle tijden zoals deze.

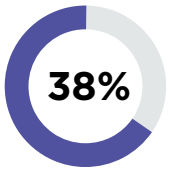
MAAR HOE ZIT HET MET GEGEVENS DIE HET KANTOOR VERLATEN?

Alle hybride organisaties zouden regels moeten afdwingen voor alle draagbare, informatiebevattende apparaten, waaronder laptops, werktelefoons en, het allerbelangrijkste, USB-stations. Bovendien wordt het ten zeerste aanbevolen om downloads en installaties op bedrijfshardware niet toe te staan zonder dat daar uitdrukkelijke toestemming voor is.

"MEER DAN EEN KWART (27%) VAN DE ORGANISATIES VERTELDE ONS IN 2020 TE MAKEN HEBBEN GEHAD MET BUDGETVERLAGINGEN, WAARDOOR ZE MINDER KONDEN INVESTEREN IN CYBERVEERKRACHT."[13]

[12]https://www.youtube.com/watch?v=ZpGZEoYv8Ts
[13]Insight Space-rapport van NCC Group, 'Paying off the cyber debt: How are decision makers approaching cyber resilience in 2021?'
[14]https://www.securitymagazine.com/articles/94997-it-security-professionals-demonstrate-excessive-trust-despite-concerns-with-remote-work-security-programs

In een enquête onder professionals in IT-beveiliging in Noord-Amerika en Europa, gaf 38% aan dat gegevensbeheer tijdens de pandemie een zeer lastige opgave was. Bijna 20% gaf aan dat hun werkapparaten ook door andere leden in het huishouden werden gebruikt.[14]



gaf aan dat gegevensbeheer tijdens de pandemie een zeer lastige opgave was

gaf aan dat hun werkapparaten door andere personen in het huishouden werden gebruikt

NCC GROUP WERD GETROFFEN DOOR EEN MAN-IN-THE-MIDDLE-INCIDENT, EEN BIJNA ONZICHTBARE AANVAL.[12]

AANVAL

Kwaadwillenden hadden de klantportal van NCC aangevallen. Door het verkeer van de portal door te sturen naar hun eigen systeem, konden ze toegang krijgen tot alle inkomende en uitgaande klantcommunicatie Dit waren ervaren hackers, zoals blijkt uit de naadloze integratie van hun infrastructuur met de aanmeldingspagina van de portal

RESPONS

Toen NCC Group besefte dat de bestanden waren gecompromitteerd, namen ze onmiddellijk contact op met de klanten die dit betrof. Vervolgens werden twee teams gevormd om de schade zoveel mogelijk te beperken: een technisch onderzoeksteam en een crisisteam dat het bestuur moest adviseren

LESSEN

Handel snel en zorg ervoor dat u bij uw beveiligingsmaatregelen rekening houdt met de beveiliging van elke externe organisatie waar u mee samenwerkt. Stel ook de juiste beveiligingsmaatregelen in op het gebied van preventie, detectie en respons.

"DOOR ZO SNEL TE REAGEREN KONDEN WE DE IMPACT ECHT BEPERKEN."
– NCC GROUP

NIEUWE WERKMODELLEN, NIEUWE BEVEILIGINGSUITDAGINGEN

Beveiliging en compliancy dienen centraal te staan bij de planning van elk toekomstig bedrijfsmodel. Of het nu gaat om softwareplatforms, hardware of data governance, uw organisatie moet haar beveiligingsstrategie voortdurend aanpassen aan de veranderende dreigingsomgeving die wordt gevormd door hybride werken.

Veel organisaties hebben al actie ondernomen. In een enquête onder Europese IT-besluitvormers geeft 48% aan van plan te zijn om bij technologie-investeringen op het gebied van hybride werken prioriteit te geven aan cybersecurity-infrastructuur, en 40% geeft aan van plan te zijn meer te investeren in IT-training voor hun personeel.[15] Als u ziet dat uw concurrenten in actie komen, wilt ook u niet achterblijven. Criminelen zullen actief op zoek gaan naar de meer kwetsbare organisaties.

De digitale transformatie - die voor veel organisaties als gevolg van de pandemie in een hogere versnelling is gekomen - zal voor veel beveiligings- en compliance-problemen een oplossing hebben geboden. Naleving van de AVG kan bijvoorbeeld worden geautomatiseerd en ingebouwd in processen.

Maar er zijn nog veel vragen die moeten worden gesteld...

- Waar bevinden zich precies de kwetsbaarheden in uw beveiliging?
- Beschikt u over de middelen om deze intern te detecteren en te dichten, of zou een externe specialist u gemoedsrust geven?
- Begrijpen alle medewerkers – van nieuwe medewerkers tot het hogere management – de risico's die inherent zijn aan hybride werken?
- Zou training u vertrouwen geven bij het nemen van belangrijke zakelijke beslissingen?
- En moet u nieuw beleid opstellen voor het gebruik van kantoorhardware om de risico's gekoppeld aan menselijk handelen te beperken?

PROBLEMEN, OPGELOST:
OPTIMALE BEVEILIGING IN DE NIEUWE WERKOMGEVING

Het bieden van richtlijnen voor menselijk gedrag is één ding. Door slimme implementatie van werkplektechnologieën zijn er echter verdere manieren om risico's op het laagst mogelijke niveau te houden.

Canon wordt door de IDC MarketScape erkend als wereldleider op het gebied van oplossingen en services voor beveiligd printen en documentbeheer. Canon's oplossingen en diensten helpen u alle documenten en gevoelige gegevens – op papier of digitaal – te beveiligen gedurende de hele levenscyclus van de documenten, zonder dat dit invloed heeft op de toegankelijkheid van de informatie die medewerkers nodig hebben om hun werk te doen. Dit betekent dat de oplossingen en services van Canon beveiligd zijn door het ontwerp, bescherming bieden conform de hoogste industrienormen en gericht zijn op alle aspecten van informatiebeveiliging.

Deze benadering van beveiliging stopt niet na de verkoop. Canon kan ondersteuning bieden bij de bescherming van print- en scanapparaten gedurende hun gehele levensduur, van het robuuster maken van apparaten tot het veilig afvoeren van apparaten wanneer ze niet langer worden gebruikt, om ervoor te zorgen dat gegevens te allen tijde beschermd blijven.

[15] *https://www.computerweekly.com/news/252500569/New-normal-of-remote-hybrid-working-sees-two-thirds-of-European-businesses-increase-IT-spend*

DE HOLISTISCHE AANPAK

Canon's holistische benadering van informatiebeveiliging maakt het beschermen van uw gegevens eenvoudig, waar de informatie ook wordt geopend, beheerd en verwerkt:

PRINTMANAGEMENT
Beveilig het proces van het verzenden van documenten naar de printer tot het vrijgeven van printopdrachten op het apparaat. Voorkom datalekken door printers te beschermen die op het netwerk zijn aangesloten en alle gebruikersactiviteiten met betrekking tot printen te beveiligen.

SCANMANAGEMENT
Beveilig de digitalisering van papieren documenten en de distributie naar de gewenste bestemming. Verbeter de documentbeveiliging door de toegang tot scanfuncties te beheren en gedigitaliseerde documenten te beschermen.

DOCUMENT- EN CONTENTMANAGEMENT
Beveilig de opslag en verwerking van documenten, of het nu gaat om toepassingen op locatie of in de cloud. Zorg voor naleving van de regelgeving voor gegevensbescherming en versterk de maatregelen voor document- en contentbeveiliging.

Waar u en uw medewerkers ook werken, Canon's aanpak zorgt voor optimale beveiliging – van uw cloud- of lokale oplossingen, tot en met uw apparaten.

In gesprekken met onze klanten in de EMEA-regio hebben we vier soorten werkplekken geïdentificeerd die organisaties vaak in combinatie gebruiken om tot een nieuwe hybride werkomgeving te komen.

We noemen ze de hybride hubs: de kantoor-hub (het traditionele centrale kantoor), de coworking-hub (samenwerkingsruimten en kleinere satellietkantoren), de thuiswerk-hub (thuiswerken) en de mobiele-hub (onderweg werken – in cafés, op stations, op luchthavens of onderweg).

Het is belangrijk om duidelijk te definiëren op welke verschillende locaties uw medewerkers werken en hoe deze met elkaar zijn verbonden, omdat elke hub zijn eigen unieke beveiligingsbehoeften heeft. Door deze werkplekspecifieke aanpak kunnen we u helpen ervoor te zorgen dat informatie wordt beschermd, van kantoor tot keukentafel.

Canon's focus op de veranderende werkplek zorgt ervoor dat alle aspecten van informatiebeveiliging als onderdeel van de levering van elke klantoplossing worden beschouwd. Uiteindelijk ondersteunt het digitaliseren van belangrijke bedrijfsprocessen via een reeks Canon-oplossingen niet alleen de productiviteit en samenwerking, maar geeft dit IT-teams en -afdelingen ook de transparantie en controle die ze nodig hebben om goede beveiligings- en nalevingspraktijken in hun teams te garanderen.

Informatiebeveiliging is van cruciaal belang en in een hybride werkomgeving meer dan ooit. Een goede beveiliging is echter eenvoudiger dan u denkt. Houd uw situatie zelf in de hand en onderneem actie voor een succesvolle toekomst.

Ga voor meer informatie naar:
www.canon.nl/business/solutions

Canon Inc.
Canon.com

Canon Europe
canon-europe.com
Dutch edition

Contact opnemen met Canon
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