BECHTLE direct

1/2020 SECURITY

Your strong IT partner.
Today and tomorrow.

BECHTLE

Beste lezer,

Het zijn vreemde tijden voor iedereen, zowel privé als zakelijk. Ook bij Bechtle gaat het er anders aan toe dan normaal. Gelukkig konden we, als grote internationale IT-organisatie, snel en eenvoudig schakelen en met elkaar connecten. Onze werkplekken thuis werden goed uitgerust en snel in gebruik genomen. Ook in tijden van thuiswerken spreken we elkaar dagelijks: een appje, via de mail, videobellen of zelfs op afstand borrelen tijdens de digitale vrijmibo. Zo blijven we met elkaar verbonden.

Verbondenheid is één van onze kernwaarden, en belangrijker dan ooit in deze tijd. Ons hoofddoel voor deze periode is dan ook om er met onze expertise voor te zorgen dat jouw business zo goed mogelijk (digitaal) blijft doorlopen. Zodat ook jouw medewerkers verbonden blijven met elkaar én met klanten. En zou het ook niet mooi zijn dat we er met zijn allen na deze periode digitaal op vooruit gaan? Het nieuwe werken wint nog sneller aan terrein.

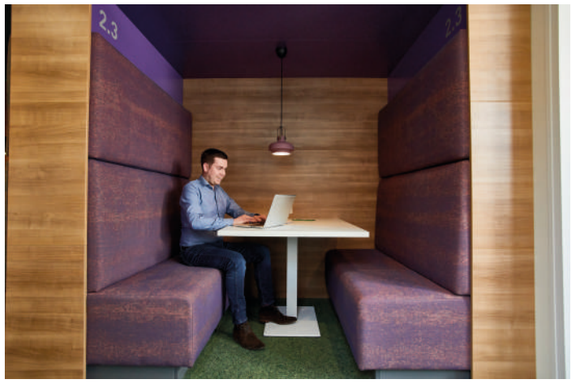
Dit magazine heeft als hoofdthema security. Juist nu is een goed ingerichte IT-infrastructuur en sterke security van groot belang. Er duiken steeds meer ‘corona-oplichters’ op die onder andere via mail of appjes organisaties binnen proberen te dringen. Het beschermen van gevoelige data, nu iedereen massaal thuiswerkt, is belangrijker dan ooit. Wij denken graag met je mee over welke security oplossing jouw organisatie **#toekomststerk** maakt.

Samen komen we hier sterker uit!

Vriendelijke groet,

Jean-Paul Bierens
Algemeen Directeur

Your trusted IT partner in a hybrid world.



Bechtle direct B.V.
Meerenakkerplein 27
5652 BJ Eindhoven
Telefoon 040 250 9000
bechtle.nl
sales.direct-nl@bechtle.com

Wij leveren uitsluitend aan bedrijven en instellingen. Druk- en zetfouten voorbehouden.

Bechtle's lees-, kijk- en luistertips

Podcast: Darknet Diaries

True stories from the dark side of the Internet. In verschillende afleveringen gaat het over hackers, breaches, ATPs, hackactivisme en alle andere dingen die bij de verborgen kant van het internet horen. De New York Times geeft, net als andere toonaangevende mediabedrijven, een goede beoordeling: "De hypnotiserende vertelling en diepgaande expertise zorgt voor resultaten die nooit minder dan aangrijpend zijn."

Nieuwsgierig geworden? De podcast is onder andere te beluisteren via Spotify en Apple Podcasts. **www.darknetdiaries.com**

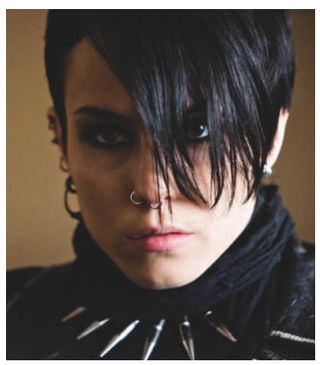
Blog: The New Frontier

Op de blogsite van ESET **(www.thenewfrontier.nl)** kun je heel wat interessante blogposts vinden over diverse security issues. Je leest er bijvoorbeeld over hoe je in deze tijden een cyberveilig thuiskantoor inricht, hoe je waakzaam kunt blijven voor online 'corona-oplichters' of hoe je kunt voorkomen dat je WhatsApp-account gekaapt wordt.

Films over hacking

Nu we wat meer thuis zitten dan anders heb je waarschijnlijk meer tijd voor goede films. F-Secure maakte een leuke lijst met films over internetbeveiliging: de ultieme lijst met hacker movies. Veel kijkplezier.

Bekijk de lijst via: **blog.f-secure.com/nl/de-ultieme-lijst-met-hacker-movies/**



Boek: Millennium reeks

Vind je hacken interessant? De Millennium reeks is zeker een aanrader om in je vrije tijd te lezen. De Millennium-triologie werd geschreven door de Zweedse Stieg Larsson, die helaas overleed in 2004. De rest van de reeks is afgemaakt door David Lagercrantz. Met de zes boeken ben je wel even zoet. Lisbeth Salander, een van de hoofdpersonages, staat officieel te boek als psychotisch en uiterst introvert, maar ze is in de praktijk erg scherpzinnig. Ze is een fenomeen in de internationale wereld van computerhackers.

De Millennium reeks is online via diverse webshops te koop in de vorm van een paperback of luisterboek.

Bechtle's nieuws

Let op voor corona phishing

In deze crisistijd moet je extra goed opletten voor phishing i.v.m. het coronavirus. De afgelopen tijd duiken er veel domeinnamen op die sterk afgeleid zijn van instanties zoals het RIVM, de WHO, de GGD of afgeleiden daarvan. Hierdoor kan het zijn dat je e-mails ontvangt die legitiem lijken, maar je via een link of bijlage doorsturen naar malware. Wees daarom extra alert wanneer je berichten ontvangt over het coronavirus en klik niet zonder te verifiëren op een bijlage of link. Ook op je (zakelijke) smartphone!

Hack Microsoft Exchange servers

Meerdere hackgroepen maken misbruik van een recent gepatcht beveiligingslek in e-mailservers van Microsoft Exchange. De uitbuitingspogingen werden voor het eerst opgemerkt door het Britse cybersecurity bedrijf Volexity. De hackgroepen maken misbruik van een kwetsbaarheid in Microsoft Exchange e-mailservers die Microsoft in februari 2020 heeft gepacht. Het beveiligingslek wordt bijgehouden onder het ID van CVE-2020-0688. Heb jij de patch nog niet uitgevoerd? Doe dit dan zeker. In theorie kan jouw organisatie niet worden aangevallen als de patch is uitgevoerd.

Bron: www.zdnet.com

Fysieke security bij de KVK

Ook 'fysieke' security is belangrijk! Bij de Kamer van Koophandel (KVK) leverden wij zo fysieke beveiligingsbeugels die we rondom de thinclients plaatsten. De KVK klopte bij ons aan nadat ze bezoek hadden gehad van een mystery guest. Die legde de pijnpunten in de fysieke toegangsbeveiliging in de kantoren van de KVK bloot. De mystery guest merkte op dat in de openbare ruimtes, zoals ruimtes waar klanten komen om zich in te schrijven, zich security issues voordeden. Zo was het mogelijk dat vreemden makkelijk USB-sticks konden inpluggen in de pc's zonder dat het medewerkers opviel. De fysieke beveiligingsbeugels maken dit nu onmogelijk.

Heb je vragen rondom deze nieuwsberichten of een algemene security vraag? Neem contact op met Joris Rooijackers, solution advisor security bij Bechtle.

Joris Rooijackers
Solution advisor security
T +31 40 760 2813
joris.rooijackers@bechtle.com

Interview: Rob Stoop over de positionering van Bechtle

Sinds enkele maanden heeft Bechtle direct een propositiemanager: Rob Stoop. Zijn taak? Bechtle's transitie van reseller naar solution seller verder ontwikkelen. Met het uitrollen van enkele proposities laten we aan de markt zien waarom wij 'your trusted IT partner in a hybrid world' zijn.

Toen Rob enkele maanden geleden tekende voor de functie als propositiemanager lag er een grote uitdaging op zijn bureau: alle losse oplossingen die nu worden verkocht vertalen naar sterke Bechtle proposities. "Ik merkte dat we voor onze klanten winst kunnen behalen, door de kennis over onze IT-oplossingen beter op elkaar af te stemmen. Het is mijn rol om te structureren wat we doen. Dat we één sterk Bechtle verhaal vertellen aan onze klanten."

Het vertrekpunt was het 6-vlakkenmodel van Bechtle. Dit model gebruiken we om de IT-infrastructuur inzichtelijk te maken, een goed overzicht te creëren van ons aanbod naar de vendoren, collega's en partners en bij trainingen. Rob vertelt: "We hebben gekozen om een eerste propositie te maken rondom datacenters. Er ontstaat steeds meer connectie tussen alle componenten in het model. Als een accountmanager een laptop verkoopt, draait daar een applicatie op. Die app genereert data. Waar ga je die data neerzetten? In een datacenter bij jou of in de cloud? Hoe zit dit met beveiliging? GDPR en AVG dwingen je om steeds zorgvuldiger met je data om te gaan. Zo zie je dat veel workspace vraagstukken die wij behandelen automatisch een link hebben met bijvoorbeeld datacenter en security."

Rob Stoop, propositiemanager

Datacenter propositie

"Datacenter is razend interessant. Vroeger konden we op een computer van 100.000 kilo 5MB aan data kwijt, of één PowerPoint presentatie. Inmiddels kunnen we natuurlijk veel meer. Steeds meer mensen en werkplekken maakt dat we steeds meer data opslaan, data groeit exponentieel. Dit jaar verwachten we dat er 44ZB opslag in gebruik zal zijn in de hele wereld. Dat is gigantisch. De grootste uitdaging die hierbij komt kijken kun je vergelijken met een grote zolder. Hoe meer ruimte je hebt, hoe meer rommel je bewaart, ook al heb je het niet nodig en bewaar je het in principe voor altijd. Wanneer je naar een klein appartement verhuist moet je veel weggooien."

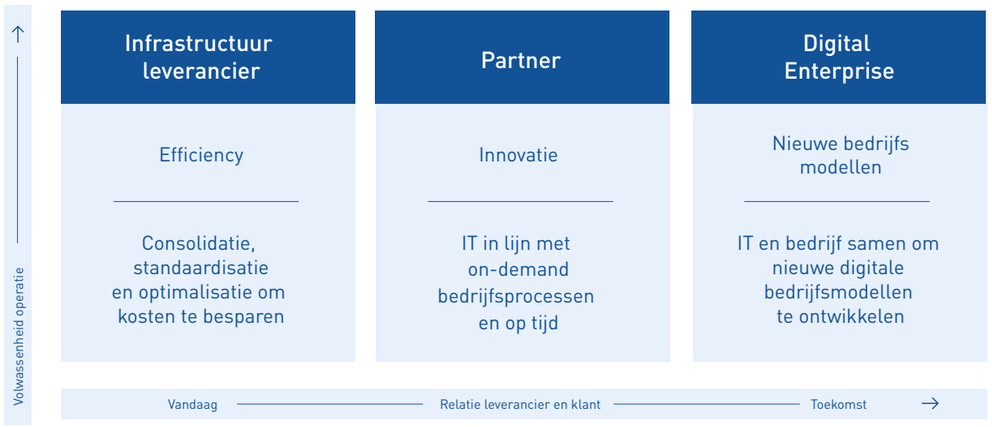
Het gaat dan over het gebruik van clouddiensten en de mogelijkheden die zij aanbieden. Je kunt 'zolderruimte' blijven kopen. "De belangrijkste vraag die we hieruit trekken: kies je er als organisatie voor om bedrijfkritische data en applicaties zelf te houden of breng je dit juist naar de cloud, uitgaande van de klanteisen rondom beveiliging, flexibiliteit en beheersbaarheid? Veel klanten hebben nog een eigen datacenter, maar lopen tegen het probleem aan dat hun systeembeheerder bijvoorbeeld met pensioen gaat en dat het steeds lastiger wordt om aan technisch personeel te komen." Ook de complexiteit van het managen van een datacenteromgeving en het steeds vaker 24/7 beschikbaar stellen van data vraagt om een grote inspanning en beschikbare technische kennis.

Daar biedt de Future Ready Datacenter Propositie van Bechtle hulp. "We willen met klanten het gesprek aangaan. Wanneer een klant nu 1000 tablets bestelt, leveren wij deze netjes af. We moeten meer naar het grotere geheel kijken en vragen: voor welke werkzaamheden wil je de tablets inzetten? Werken jouw medewerkers buiten de deur of op kantoor? Wil je de tablets laten werken met een simkaart of via wifi? Hoe veilig is het dataverkeer dat via de tablets wordt uitgewisseld? Door op deze manier met klanten het gesprek aan te gaan zijn we klaar voor de veranderende vraag van de markt. We doen een healthcheck aan de hand van assessments. Samen met de klant stellen we een roadmap op die de weg naar verandering het beste ondersteunt. Na de verkoop van de propositie begint het namelijk pas. We zorgen voor een soepele uitrol en stellen een projectplan op. Dit kunnen we bij Bechtle met één groot team doen, dat is onze kracht. Het is een teamproject."

Van leverancier naar IT partner

“Door meer met uitgewerkte Bechtle proposities te werken schuiven we op in de keten van IT leverancier naar IT partner. Daar zijn we al een tijd mee bezig, maar de proposities moeten dit finetunen. In die rol horen we thuis en willen we ook blijven. We hebben geen ambitie om een bedrijf zoals Amazon te worden dat volledig digitaal gestuurd is.”

Rob is de afgelopen tijd bezig geweest met het inventariseren en structureren van alle oplossingen die we in huis hebben, zowel in Nederland als bij Bechtle AG. Hij keek naar welke verbeterd kunnen worden of juist mogen worden geschrapt, omdat ze erg lijken op een andere oplossing in het portfolio. “Zo zetten we de stip op de horizon bij onze klanten: wij zijn dé IT partner waar ze terecht kunnen voor alle IT-vraagstukken.”



Toekomststerk

‘Your trusted IT partner in a hybrid world’: dit is de value statement die we hanteren bij het ontwikkelen van onze proposities en in de relatie met onze klanten. Hoe nu verder? “De manier waarop we de eerste propositie verder ontwikkelen vormt de basis van waaruit we de andere proposities gaan uitrollen. Ook zullen er sterke interacties tussen de verschillende proposities ontstaan en stimuleren we hergebruik van componenten en diensten zo veel mogelijk. We hebben nu een sterke basis en een conceptueel model. Verder zetten we een technology board op die als gatekeeper voor alle nieuwe proposities dient.”

2020 staat dus in het teken van meerdere proposities. “De Future Ready Datacenter Propositie zal rond de zomer beschikbaar zijn. Het is de bedoeling om een aantal proposities per jaar te lanceren. Tijdens het proces komen we vast nog uitdagingen tegen en constateren we wat we missen als groep. Zo willen we onszelf versterken en blijven verbeteren.”

“Zo zetten we de stip op de horizon bij onze klanten: wij zijn dé IT partner waar ze terecht kunnen voor alle IT-vraagstukken.”

Rob Stoop
Propositiemanager
T +31 62 186 9435
rob.stoop@bechtle.com

Overheidsinstanties kiezen voor andere manieren van verzenden

Kees Janssen, teamleider Government

Bij Bechtle merken we dat overheidsklanten kiezen voor andere manieren van verzenden om gevoelige informatie uit te wisselen, zoals met encrypted USB-sticks. Dit heeft onder andere te maken met de strengere privacywetgeving (AVG/GDPR) en het steeds groter wordende gevaar voor hacking.

Kees Janssen is teamleider Government bij Bechtle. Hij merkt dat overheidsklanten steeds vaker kiezen voor andere vormen van verzenden wanneer het gaat om gevoelige data. “Overheden stappen over naar meer fysiekere vormen van informatie uitwisselen. Bijvoorbeeld door gebruik te maken van USB-sticks met een hardware- of softwarematige encryptie. In sommige gevallen worden er ook speciale netwerken opgezet om gevoelige informatie tussen verschillende overheden of instanties te versturen. Als je dat doet zorg je ervoor dat er een los kanaal staat voor gevoelige informatie. Ze versturen zo niet via het netwerk. Onze klanten worden zich steeds meer bewust van het feit dat je niet alles klakkeloos via mail kunt doorsturen.”

Nieuwe vormen van hacken

Gevoelige informatie kan onderschept en misbruikt worden. Mailaccounts worden steeds vaker gehackt. Aanvallers doen zich bijvoorbeeld voor als de CEO. “Denk maar aan de case waarbij Pathé 19 miljoen euro verloor vanwege CEO-fraude.” Er duiken ook steeds vaker aanvallen met een politiek doel op. Het bekendste voorbeeld is misschien wel de discussie rond het hacken van de Russische Inlichtingendienst van de Amerikaanse Democratische Partij in 2016. Kees: “Het gaat niet meer alleen om het beveiligen van data of dat klanten rekening houden met hackers met commerciële doelen. Hacken krijgt ook vaker een politiek karakter. Daar houden onze overheidsklanten rekening mee.”

Bechtle levert bijvoorbeeld encrypted USB-sticks aan grote overheidsinstanties, waar strikt confidentiële informatie op gezet wordt. Lees meer over encrypted USB’s op pagina 27. “Naast dit soort hardware oplossingen zijn er ook op het gebied van software genoeg mogelijkheden. Bijvoorbeeld Software Defined Networking (SDN), waar een gecentraliseerd controller-systeem het netwerk bestuurt. SDN maakt geautomatiseerde provisioning binnen virtuele netwerken mogelijk. Op een slimme maar eenvoudige manier kun je zo zien wat er zich afspeelt in het netwerk. Daarop kun je acteren en zaken in quarantaine plaatsen, net zoals dat gaat met mensen bij echte virussen.”

Inburgeren

De digitale beveiliging van je organisatie is net zo sterk als de zwakste schakel in de keten. “Wanneer je medewerkers geneigd zijn om snel op een link of afbeelding te klikken, zul je hier ook aandacht aan moeten besteden. Hardware en software- oplossingen zijn maar een gedeeltelijke oplossing. Dat proberen we klanten ook altijd mee te geven. Het begint bij het goed opleiden en bijscholen van jouw personeel.” Inburgering in de maatschappij is noodzakelijk, maar dit kost tijd.

Bechtle werkt samen met tal van security fabrikanten die goede oplossingen aanbieden, zoals je kunt lezen in dit magazine.

Benieuwd hoe Bechtle het verschil maakt voor publieke organisaties? Neem contact met ons op.

Joris Rooijackers
Solution advisor security
T +31 40 760 2813
joris.rooijackers@bechtle.com

Kees Janssen
Teamleider Government
T +31 40 250 9095
kees.janssen@bechtle.com

Hoge IT-kasteelmuren vangen veel wind

Blijk dat IT-security budgetten verkeerd besteed worden

Joris Rooijackers is solution advisor security bij Bechtle. In dit stuk schrijft hij over waarom de toename van nieuwsberichten over ransomware en exploits positief nieuws is.

Het bewustzijn over ransomware en exploits begint te groeien, zowel bij de media als bij het grote publiek. Het gebeurde al vaker, maar haalde nooit zo uitgebreid het nieuws. Hierdoor worden de tactieken van aanvallers steeds beter zichtbaar en kunnen we gerichte investeringen doen om deze nare activiteiten onmogelijk te maken.

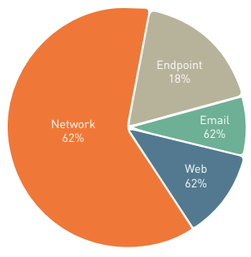
Waar we traditioneel gezien een mooie muur om onze bedrijfsdata hebben gebouwd en alles netjes voorzien van MFA, blijkt dit allang niet meer afdoende te zijn. Aanvallers richten zich enkel en alleen op de medewerkers. Deze zijn 'gewoon' bereikbaar, per mail, per webbrowser, per SaaS applicatie, per mobieltje... Om het nog makkelijker te maken plaatst iedereen z'n specifieke IT-skills online. De verkenningsfase van een aanvaller is nog nooit zo eenvoudig geweest als vandaag de dag. Domeinen die niet geauthentificeerd worden via DMARC kunnen handig worden ingezet om de medewerker te benaderen per mail via een gespooft adres.

We verschuilen ons achter een gedegen back-up, maar wat als de back-up oplossing bestanden opslaat die al besmet zijn? Zodra de retentie voorbij is, zijn alle back-ups waardeloos geworden. Los van kosten van het terugzetten van een offline back-up, zorgt het niet voor de oplossing tegen ransomware.

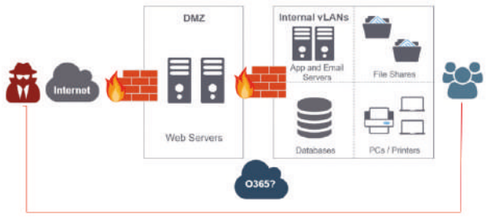
Nee, het antwoord ligt niet 1, 2, 3 voor de hand. Maar één ding is zeker: er moet op basis van een goede inventarisatie van de risico's investeringen worden gedaan in kennis, tooling en beleid. Dit doe je door te starten met een inventarisatie van alle software en hardware binnen de organisatie, met daarbij een kwetsbaarheidsscan om de grootste problematiek te spotten. Vervolgens classificeer je welke bedrijfsdata en persoonsgegevens kritisch zijn voor de bedrijfsvoering.

Elke organisatie is daardoor anders en elk security plan zal hierop aangepast moeten worden. Wij helpen als Bechtle graag bij het opstellen van zo'n plan. Er is een conceptversie beschikbaar die we op aanvraag met je delen. Bij Bechtle geloven we dat we door kennis te delen en transparantie dit soort aanvallers buiten de deur kunnen houden. Hiervoor moeten we echter wel gericht blijven investeren in de juiste technieken.

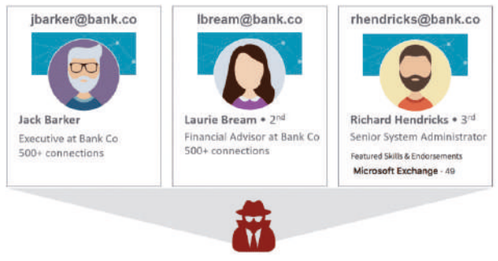
IT security uitgaven



Standpunt verdediger



Standpunt aanvaller



Joris komt graag een keer koffie drinken om jouw security plannen voor 2020 te bespreken. Je kunt Joris bereiken via onderstaande contactgegevens!

Joris Rooijackers
Solution advisor security
T +31 40 760 2813
joris.rooijackers@bechtle.com

Interview: Olaf de Ruiter van Dell over dataprotectie

Olaf de Ruiter is Senior Systems Engineer Data Protection Solutions bij Dell Technologies. Zijn specialisme: dataprotectie: “Onze Cyber Recovery oplossing helpt klanten te herstellen van een cyberaanval.” Olaf’s carrière stond altijd al in het teken van dataprotectie. Hij vertelt over de aanpak van Dell Technologies op het gebied van Cyber Recovery.

Organisaties maken al jarenlang back-ups van hun belangrijkste data om beschermd te zijn tegen dataverlies. Helaas halen cyberaanvallen de laatste jaren steeds vaker het nieuws. Bedrijven komen erachter dat hun back-up-oplossing niet voldoende is om van een aanval te kunnen herstellen. Tijdens een cyberaanval wordt door cybercriminelen veelal gebruik gemaakt van malware en ransomware. Malware is kwaadaardige of schadelijke software die als doel heeft data te vernietigen zodat bedrijven ten gronde worden gebracht. Ransomware betekent letterlijk ‘gijzelsoftware’. Dit is software waarmee criminelen computers of bestanden versleutelen met het doel om losgeld te vragen in ruil voor het weer beschikbaar maken van de data.

Helaas is het betalen van losgeld niet altijd een garantie voor het daadwerkelijk terugkrijgen van je data. De meeste organisaties denken dat ze door het maken van back-ups kunnen herstellen van een cyberaanval, maar aanvallers nemen ruim de tijd tussen inbraak en het uitvoeren van de cyberaanval. Ze gebruiken deze tijd om inzichtelijk te krijgen waar de kritische productie- en back-up-data staat, zodat ze primaire data als back-ups tijdens de aanval kunnen vernietigen of versleutelen. Onlangs is bij een universiteit in Nederland een paar ton losgeld betaald aan hackers. De back-ups die nodig waren voor het herstel waren versleuteld. Om de schade te beperken en snel data te herstellen, besloot de universiteit het losgeld te betalen. De totale geleden schade is een veelvoud van het betaalde losgeld.

Strategie

Uit onderzoek uitgevoerd door SecureWorks is gebleken dat 59% van de IT-beheerders nog steeds denkt dat ze kunnen herstellen van een cyberaanval met het terugzetten van een back-up. Er zijn in een half jaar tijd al 95% nieuwe vormen van ransomware opgedoken welke lastig te detecteren zijn. Organisaties moeten zich realiseren dat deze nieuwe manier van aanvallen vraagt om nieuwe maatregelen. Maar hoe kunnen organisaties zichzelf dan beschermen? Zij moeten voor zichzelf een security-strategie bepalen die gebaseerd is op preventie en de juiste tools bevat voor wanneer het dan tóch misgaat.

Olaf de Ruiter, Senior Systems Engineer Data Protection Solutions bij Dell Technologies

Cyber Recovery Solution

Dell Technologies heeft met de Cyber Recovery Solution een sterke beveiligingsoplossing in zijn portfolio. In deze oplossing wordt een veilig, op disk gebaseerd kopie van de back-up data en back-up catalog geplaatst in een afgeschermde omgeving. Dit wordt ook wel de ‘vault’ of kluis genoemd. De Cyber Recovery vault is afgeschermd van het productie netwerk en internet. Tijdelijk wordt er een verbinding geactiveerd tussen productie en vault voor het opslaan van een back-up-kopie van bedrijfskritische data in de vault. Deze methode wordt ook wel Air Gap (offline) genoemd. De back-up data wordt vervolgens automatisch op bestaande malware en verdachte activiteiten, die kunnen duiden op een cyberaanval, gecontroleerd met behulp van artificial intelligence en machine learning.
De resultaten worden gerapporteerd zodat de organisatie snel en adequaat kan reageren en geen slachtoffer wordt van de cyberaanval. Sommige organisaties menen dat een traditionele tape back-up - waarbij de tapes gewoonlijk offline worden opgeslagen een optie is. Met de huidige hoeveelheid data die in omloop is binnen een organisatie en tijd die nodig is om de schone data te vinden is dit meestal geen geschikte oplossing. Het herstellen van dataverlies na een cyberaanval met behulp van tape kan weken tot maanden in beslag nemen.

Wil je met ons in gesprek over hoe je jouw organisatie kunt beschermen? Wil je voorbereid zijn op ransomware aanvallen? Neem contact op met onze security specialist.

Joris Rooijackers
Solution advisor security
T +31 40 760 2813
joris.rooijackers@bechtle.com

DELL Technologies TITANIUM PARTNER

Bron: SecureWorks 2017 Ransomware Defense Survey

Gastlessen mediawijsheid bij Playing for Success Eindhoven

Interview: Gijs van der Putten

Gijs van der Putten van Bechtle geeft sinds dit schooljaar gastlessen mediawijsheid bij Playing for Success Eindhoven. Hij wil ervoor zorgen dat kinderen zich meer bewust worden van de gevaren van social media en online sterker in hun schoenen staan.

Over Playing for Success Eindhoven

Playing for Success is ontstaan in Engeland. Daar zijn alle clubs in de Premier League verplicht om iets terug te doen voor de maatschappij. Ze kwamen zo op het idee om kinderen naar de voetbalclub te halen en daar spelenderwijs te focussen op leerproblemen. In Nederland richt Playing for Success Eindhoven (PFS) zich op kinderen die een steuntje in de rug kunnen gebruiken. Denk aan kinderen die onzeker zijn of worden gepest op school.

Playing for Success Eindhoven is een uniek concept gevestigd in het Philips Stadion, en sinds kort ook in het Parktheater. Ontwikkelingskansen van kinderen en jongeren worden er vergroot. Samen met de kinderen werkt PFS aan doelen zoals positiever over jezelf zijn en samenwerken met andere kinderen om zo het optimale rendement op school te halen en te zorgen dat ze lekkerder in hun vel zitten.

www.playingforsuccesseindhoven.nl

In 2019 klopte Playing for Success Eindhoven bij Bechtle aan voor een sponsoring. Al snel merkte het management bij Bechtle dat ze eigenlijk méér met dit mooie initiatief wilde doen dan alleen geld overmaken. PFS sluit namelijk goed aan bij Bechtle: onze kernwaarden zijn **verbonden**, **ondernemend** en **ervaren**. Dat maakt ons **toekomststerk**. We steunen lokale goede doelen omdat we verbondenheid met de samenleving belangrijk vinden. Met onze jarenlange ervaring willen we de kinderen die naar PFS komen toekomststerk maken. Niet alleen op het gebied van IT-kennis, maar ook door zichzelf zekerder te voelen.

De vraag restte: wat konden wij aanbieden naast een sponsoring? Het antwoord op die vraag was Gijs van der Putten. Gijs is manager IT-Solutions bij Bechtle. IT-Solutions is het kennisteam van consultants en advisors met elk hun eigen specialiteit. Gijs vertelt: "Naast de sponsoring hebben we enkele eenvoudige IT-vraagstukken van PFS opgepakt. We hebben hardware geleverd, zodat de begeleiders en kinderen met goede spullen aan de slag konden." Maar daar stopte het niet. "We wilden graag inhoudelijk iets toevoegen en de kinderen iets bijbrengen op het gebied van IT. IT is de toekomst."

Mediawijsheid door Bechtle

Gijs ging met PFS het gesprek aan. Hij vertelt: "Elke partner van PFS heeft zijn eigen kracht en levert naast een financiële bijdrage ook een aandeel binnen het eigen specialisme waar dat kan. Onze kracht zit onder andere in kennis van IT en zo kwamen we dan ook op het idee om met de eerste gastlessen binnen het programma te beginnen." De kinderen worden door school aangemeld voor een traject bij PFS. Ze doorlopen dan een cyclus van gemiddeld twaalf namiddagen per schooljaar. Gijs geeft nu in elke cyclus één gastles.

"De bedoeling van alle lessen van PFS is dat de kids op een actieve manier een steuntje in de rug krijgen, bijvoorbeeld om zelfverzekerder te worden. Denk dus niet aan een klassieke manier van lesgeven waar kinderen braaf op hun stoeltje moeten zitten of luisteren. De 'lessen' zijn in een eigen gave PFS leercentrum in het Philips Stadion, met een echte tribune! Tijdens iedere bijeenkomst gaat de groep ook het stadion in om activiteiten te doen. We blijven niet de hele middag in het leercentrum."

De lessen die verzorgd worden door Bechtle gaan over mediawijsheid. "Het is belangrijk dat kinderen zich bewust zijn van de risico's van social media", onderstreept Gijs. "Er zijn nog geen 'gedragsregels', het is allemaal nog zo nieuw. Wat doe je als je een appje krijgt waar je van schrikt? Geef je iemand zomaar jouw wachtwoord van Instagram?" Gijs en de begeleiders van PFS gingen aan de slag en stelden een programma samen.

Gijs van der Putten
Manager IT-solutions
T +31 40 250 9000
gijs.vanderputten@bechtle.com

Awareness

De gastles bevat een beetje theorie, maar het is geen les waar kinderen drie uur droge materie voorgeschoteld krijgen. “We bereiden enkele casussen voor, gebaseerd op situaties waar kinderen op social media mee in aanraking komen. De kinderen werken in groepjes en we leggen de situaties door het hele lokaal verspreid. Die lossen ze samen op: wat doe je in zo’n situatie, wat kan er misgaan?” Tijdens deze opdracht blijven de kinderen in beweging. Na de theorie gaat de hele groep naar buiten. Daar doen ze een spel over beïnvloeding (het Hustle-spel), want beïnvloeden gaat een stuk makkelijker via social media dan in het echte leven.

Gijs: “Tijdens het spel moeten de kinderen proberen een begeleider zo ver te krijgen om een schoen uit te trekken. Dat lukt zonder probleem! Maar daarna komen er opdrachten zoals: probeer het wachtwoord van Instagram van jouw begeleider te ontfutselen. Dat lukt de kids dan niet, we spreken van tevoren af dat de begeleiders dit niet geven hoe hard die kinderen ook hun best doen. Na het spel bespreken we klassikaal waarom ze denken dat begeleiders dit niet doen. Je ziet dat de kinderen aan het denken gezet worden, en zo leren ze dat het niet normaal is als iemand ze bijvoorbeeld onder druk zet in een WhatsApp groep om een wachtwoord te geven of om iets door te sturen.”

Volgens Gijs weten de kinderen wel abstract over de gevaren van social media, maar moet er toch nog meer awareness gecreëerd worden. “Dat begint al bij volwassenen. Veel volwassenen gaan zelf niet goed om met social media en reageren bijvoorbeeld heel anders dan dat ze face-to-face zouden doen. Dat is een risico als je jezelf achter een schermpje verstopt, en dat probeer ik mee te geven aan de kinderen. Met een quiz breng ik ze nog graag wat dingen bij en behandel ik vragen zoals: wat is de naam van een bekend computervirus? Of: welke naam in het rijtje is van een IT-security merk? Kinderen kunnen vaak tien kledingmerken opnoemen, maar geen één IT-security merk.”

Toekomststerk

Als afsluiter geeft Gijs een goodiebag mee, waar onder andere een licentie Safe Kids van Kaspersky in zit. “De reacties hierop zijn erg positief. Met Safe Kids kunnen ouders regels instellen voor apparaat- en appgebruik, ongewenste content blokkeren en overzichten ontvangen over wat je kinderen googelen. Soms kennen ouders zo’n licentie wel, en willen ze het een keer aanschaffen, maar komt het er nooit van. Ik ben blij dat we ze er zo kennis mee kunnen laten maken.”

En de toekomstplannen? Gijs is in ieder geval nog niet klaar met het geven van gastlessen: “Dankzij het succes van de samenwerking met PFS ben ik ook benaderd om namens Bechtle een gastles te geven aan de Fontys Hogeschool. Ik vind het mooi dat we als organisatie ook op deze manier het verschil kunnen maken, naast een gewone sponsoring. Ik heb vanuit mijn omgeving dan ook veel enthousiaste reacties ontvangen. Laten we samen de jongere generatie toekomststerk maken!”

Gijs van der Putten
Manager IT-solutions
T +31 40 250 9000
gijs.vanderputten@bechtle.com

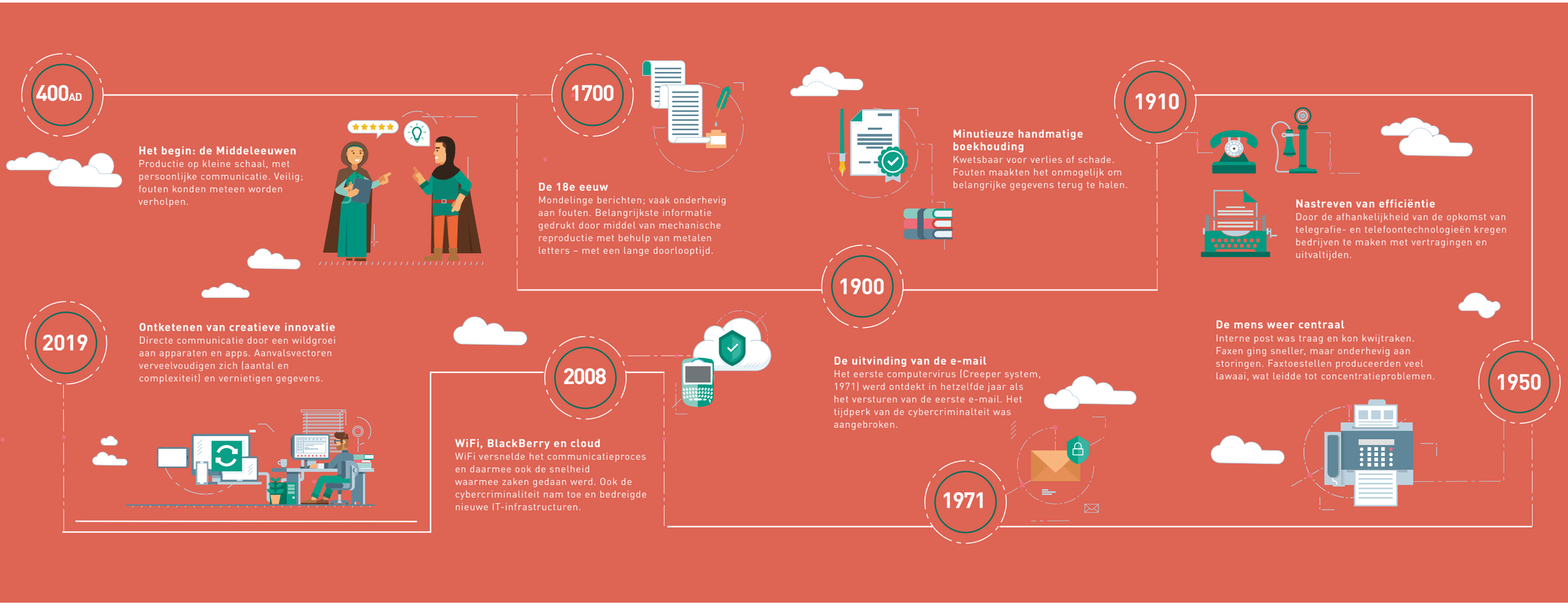
De revolutie van samenwerken

Een korte geschiedenis van de technologie die werken op afstand mogelijk maakt.

Met welke security gevaren komt jouw organisatie in aanraking?

De digitale nomaden van de toekomst bereiken meer – in minder tijd – dan de kantoormedewerkers van voor de cloud. Alles is met elkaar verbonden en direct binnen handbereik dankzij de cloud. Maar één gaatje in je cyber-pantser en cybercriminelen vallen je bedrijf aan en laten een spoor van vernietiging achter... Ben je je bewust van de gevaren voor jouw organisatie? Heb je hier hulp bij nodig?

Kaspersky Endpoint Security is bekroond en biedt directe bescherming voor endpoints en mobiele apparaten op maat, met verschillende opties voor jouw IT-team, budget en eisen. Als jouw medewerkers veilig zijn verbonden, zit er geen 'afstand' in werken op afstand. Kaspersky maakt veilig werken op ieder apparaat mogelijk. Neem contact op met onze security specialist voor meer informatie.



kaspersky

Joris Rooijackers
Solution advisor security
T +31 40 760 2813
joris.rooijackers@bechtle.com

Zorginstelling op zoek naar nieuwe security software

Zorgklanten van Bechtle komen geregeld met security vraagstukken naar ons toe. In dit artikel nemen we een voorbeeldcase door samen met Joris Rooijackers, solution advisor security bij Bechtle. Leer meer over hoe Bechtle jouw organisatie kan helpen om de juiste keuzes te maken.

De zorginstelling, die we niet bij naam noemen, klopt bij ons aan omdat hij ontevreden is over zijn huidige antivirus oplossing, die werd aangeboden door een andere reseller. De klant werkt met een oplossing die niet voldoende voorziet in bescherming tegen ransomware en biedt hem geen inzicht in wat er op zijn endpoints gebeurt. Het kostte hem veel mankracht én tijd om enkele geïsoleerde ransomware aanvallen op te lossen en hij is bang dat het gebrek aan inzicht grotere problemen zullen veroorzaken. Het management wil duidelijkheid vanuit het IT-beheerteam om herhaling te voorkomen.

Security advies op maat

Na in contact te zijn gekomen met zijn vaste accountmanager, wordt er een gesprek ingepland met Joris. Tijdens het gesprek bespreken ze de huidige problemen en na even sparren komt een oplossing naar boven die niet alleen zijn problemen tackelt, maar hem ook ontzorgt bij de migratie en het correct configureren. Er wordt direct een proof of concept ingepland

> **"De aanschaf van nieuwe security software is niet goedkoop. Daarom geven we de klant eerst de ruimte en tijd om het nieuw voorgestelde product te testen in een testomgeving."**

voor het merk. Na het eerste kennismakingsgesprek vinden er een aantal workshops plaats waarbij we achterhalen welk(e) security product(en) het meest geschikt zijn. Vanuit Bechtle komt er advies op maat waarin we onderbouwen waarom dit product beter werkt voor de zorginstelling én waarom het beheer veel eenvoudiger is.

Demo

De aanschaf van nieuwe security software is niet goedkoop. Daarom geven we de klant eerst de ruimte en tijd om het nieuw voorgestelde product te testen in een testomgeving. Samen met de fabrikant zetten we een demo op. De zorginstelling heeft enkele weken om te testen of het nieuwe systeem hem bevalt en past bij zijn organisatie. Tijdens deze periode houden we nauw contact: Joris of de accountmanager bellen elke week even om te zien hoe het gaat. Het is voor ons belangrijk om te weten waar de klant tegenaan loopt, wat hij goed of niet goed vindt, zodat we kunnen bijsturen indien nodig.

Happy customer

De nieuwe beveiligingssoftware bevalt goed, dus wordt het ook op een aantal productielaptops geïnstalleerd. De klant is vol lof. Het beheer is makkelijker geworden, bovendien krijgt hij meer inzicht in alle threats die er via een laptop van zijn medewerkers binnenkomen. Met de nieuwe software kan de klant betere rapportages maken. Deze toont hij aan het management, waardoor zij sneller overtuigd zijn van het nieuwe product. Na een zorgvuldige evaluatie wordt de handtekening dan ook snel gezet. Na een korte migratieperiode van twee à drie dagen zijn alle endpoints omgezet. Het contract met deze klant loopt drie jaar. Na de implementatie houden Joris en de klant contact. We vinden het belangrijk dat het product naar behoefte blijft functioneren en sturen graag bij wanneer dit niet zo is.

Worstel je ook met een security vraagstuk?
Neem contact op met Joris voor advies op maat.

Joris Rooijackers
Solution advisor security
T +31 40 760 2813
joris.rooijackers@bechtle.com

De security uitdagingen waar je waarschijnlijk mee worstelt

Lenovo heeft onderzoek gedaan naar de security uitdagingen waar organisaties vandaag de dag tegenaan lopen. Uit het onderzoek kwam naar voren dat organisaties zich oprecht zorgen maken over de constante evolutie van de beveiligingsrisico's en steeds slimmere cybercriminelen.

Maar wat houdt hen tegen om betere oplossingen te implementeren? Dit zijn de grootste uitdagingen:

Beperkte kennis van eindgebruikers

De kenniskloof tussen de weerstand van eindgebruikers tegen nieuwe pc-beveiliging en de beperkte kennis toont aan dat security niet in handen zou moeten zijn van de eindgebruikers. Toch staan ze in de frontlinie en zijn ze kwetsbaar voor bedreigen zoals phishing en ransomware.

De kosten van security oplossingen

Het implementeren en beheren van security oplossingen draagt bij aan hoge kosten en complexiteit en kunnen gevaarlijke hiaten in de veiligheidsdekking achterlaten.

Het up-to-date blijven op het gebied van security

Vaak kampen organisaties met onvoldoende IT-budgetten. Dit kan leiden tot gevaarlijke hiaten, wanneer IT-professionals geen resources hebben om up-to-date te blijven en hun kennis bij te spijkeren.

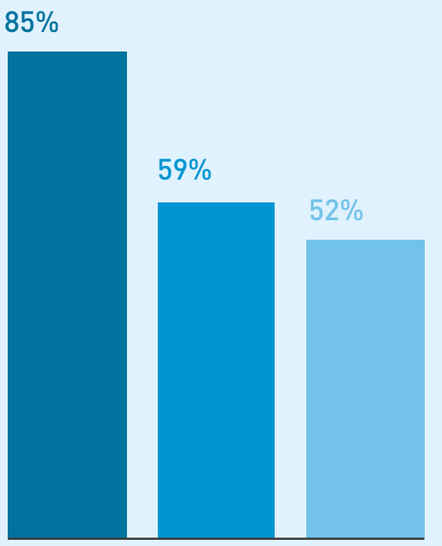
Tijd en middelen nodig voor het beheer

Het dagelijks beheer van een groeiend aantal devices is tijdrovend en neemt tijd en middelen weg van andere kritieke IT-taken.

Weerstand van eindgebruikers

Eindgebruikers verzetten zich tegen nieuwe beveiligingsmaatregelen die extra effort van hun kant vraagt.

Hoe organisaties deze uitdagingen aanpakken:



Lenovo

Customize jouw security dekking met ThinkShield

Bedreigingen zijn overal. Dit is geen tijd om een compromis te sluiten.

Jouw organisatie heeft geen tijd voor inbreuken op security. Daarom creëerden wij ThinkShield, een aanpasbaar beveiligingsplatform. Ons innovatieve portfolio beschermt je tegen de gesofisticeerde cybercriminelen van vandaag de dag en zorgt ervoor dat je ze een stap voor bent.

Cybersecurity begint voordat je de doos opent!

Bij Lenovo begint de beveiliging met het ontwerp en gaat verder via de supply chain, de levering en de volledige levenscyclus van je devices. Het beschermen van jouw organisatie is onze prioriteit: van de ontwikkeling tot het uitpakken.

- Ontwikkeling
- Veilige verpakking
- Vertrouwde leverancier
- Programma beveiligde verwijdering

Customize jouw security dekking

Device security
- Intel Boot Guard
- Absoluut
- Slimme USB-bescherming
- Transparante supply chain
- Intel Hardware Shield
- Windows Defender System Guard

Identiteit security
- Intel Authenticate Multifactor
- FIDO
- Match op chip vingerafdruklezer
- Windows Hallo

Online security
- MobileIron Unified Endpoint Management
- Intel Software Guard Uitbreidingen
- Lenovo Wifi-beveiliging
- Lenovo Security console

Data security
- Absolute endpoint zichtbaarheid en controle
- Intel Remote Wipe
- ThinkPad® Privacy Guard
- BitLocker
- Windows Information Protection

Vind de juiste oplossing voor jouw organisatie

Lenovo ThinkShield is een uitgebreide, end-to-end security oplossing waarop je kunt vertrouwen. Wil je meer informatie? Neem contact op met onze expert. Samen kijken we welke beveiligingsoplossing het beste bij jouw organisatie past.

ThinkShield

Bron: Lenovo ThinkShield_Security Trends Research Ebook

Joris Rooijackers
Solution advisor security
T +31 40 760 2813
joris.rooijackers@bechtle.com

Bescherm je mobiele devices met Lookout

Waarom Lookout

Vaak staan organisaties niet genoeg stil bij de dreigingen die via mobiele devices binnenkomen. Lookout biedt extra bescherming voor mobiel, door een krachtige verdedigingslinie toe te voegen tegen phishing aanvallen via persoonlijke mail, teksten, berichtenplatforms en apps. Versnel de digitale transformatie van je organisatie en omarm met vol vertrouwen het gebruik van mobiele devices. Met Lookout beschik je over uitgebreide bescherming, ongeacht of de werknemer zich in het beveiligde bedrijfsnetwerk bevindt of niet. Zo ben je beschermd over het hele spectrum van mobiel risico.

Lookout maakt het verschil

- We hebben een van 's werelds grootste mobiele beveiligingsdatasets verzameld op meer dan 180 miljoen apparaten, 80 miljoen apps en voegen hier dagelijks 90.000 nieuwe apps aan toe.
- Dankzij dit wereldwijde sensornetwerk werkt ons platform voorspellend en kunnen we aan de hand van machine-intelligentie complexe patronen identificeren die op risico wijzen die menselijke analisten mogelijk over het hoofd kunnen zien.
- Mobiel is het nieuwe tijdperk van computergebruik en vraagt een nieuwe beveiligingsoplossing, exclusief voor mobiele devices. Lookout is sinds 2007 expert op dit gebied.

Mobile Phishing Killchain

1. Attacker sends a message Aimed at social engineering victim
2. Attacker successfully tricks victim into clicking a phishing link

   Without Lookout
   Malicious link can lead to A or B

3A. Upon clicking the link, victim is brought to a phishing site meant to look legitimate

3B. Link silently downloads surveillanceware to the device

4A. Attacker gains access to everything on the device

4B. Surveillanceware monitors and harvests all activity on device

5. Attacker impersonates, tracks, or spies on the victim, leading to sensitive corporate data leakage

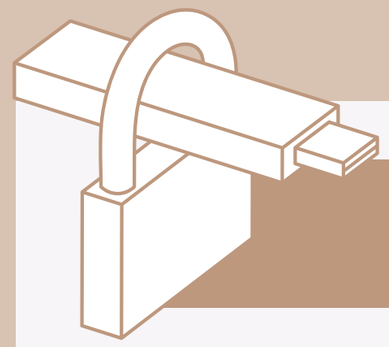
Lookout helpt jouw organisatie op weg naar veilig mobiel gebruik zonder de productiviteit in gevaar te brengen. Neem contact op met Bechtle voor meer informatie!

Joris Rooijackers
Solution advisor security
T +31 40 760 2813
joris.rooijackers@bechtle.com

Lookout

Ontdek de encrypted USB's van Kingston

Sinds de invoering van de nieuwe AVG-privacywetgeving zijn de regels een stuk strenger geworden, en staat Security vaak hoger op de agenda in organisaties. De hoogste kosten ontstaan in de **gezondheids**-, **onderwijs**- en **financiële** sector.



Benieuwd naar hoe je het gebruik van beveiligde USB's kunt implementeren binnen jouw organisatie? Neem contact op met onze Security expert of ga naar: www.bechtle.com/nl/actie/kingston

5 Stappen naar AVG-naleving

1. **Bewustzijn:** Inzicht in de nieuwe verordening en begrijpen wat deze inhoudt
2. **Evaluatie:** Begrijpen wie welke gegevens gebruikt en wie hiertoe toegang heeft
3. **Beleid:** Het vaststellen van een strategie voor gebruik van gegevens onderweg
4. **Technologie:** Nadenken over hardwareversleuteling en mogelijkheden voor endpointbeheer
5. **Onderwijs:** Uw personeel op de hoogte brengen van de AVG en best practices op het gebied van beleid voor gegevensbescherming

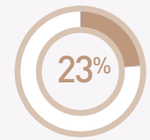
Een kleine USB-stick kan zorgen voor veel narigheid

Als medewerkers gegevens meenemen buiten het kantoor, neemt het risico toe dat de gegevens **gecompromitteerd raken.**

Bedrijven riskeren hierdoor **zware boetes**, herstelkosten en een mogelijke PR-ramp.

Vergeet niet dat dit niet alleen geldt voor gegevens die u **moet** beschermen, maar ook gegevens die u **wilt** beschermen.

De gemiddelde kosten van een gegevensinbreuk zijn sinds 2013 met 23% gestegen



Kingston TECHNOLOGY

Houd mobiel werken veilig en beheersbaar met Samsung Knox

Bechtle is de beste start voor organisaties die mobiel werken ondersteunen én hun mobiele devices veilig en beheersbaar willen houden.

De moderne medewerker wil zorgeloos kunnen werken. Veiligheid moet standaard geborgd zijn, zowel voor medewerkers als voor jouw IT-afdeling. Niemand wil zich zorgen maken over de veiligheid van data, applicaties en privacy. Het uitrollen en inregelen van toestellen is echter een karwei dat om heel wat handelingen vraagt en niet zo eenvoudig is.

Samsung maakt de invulling makkelijk én het beheer overzichtelijk met het Samsung Knox platform voor Unified Endpoint Management. Dit vormt samen met Bechtle's Device as a Service (DaaS) concept, een ijzersterke, kostenefficiënte combinatie.

Maak kennis met Samsung Knox

Hoe passen de verschillende onderdelen van Samsung Knox binnen de DaaS lifecycle?

- **Knox Enrollment (uitrol van de Mobile Device Management cliëntprofielen naar devices)**
  Zodra de gebruiker verbinding maakt met internet, wordt het IMEI-nummer van de smartphone automatisch verbonden aan het ingerichte profiel. Handmatig, repeterend werk behoort tot het verleden.

- **Knox Configure (toestelconfiguratie)**
  Organisaties zetten met Configure zelf toestel knoppen aan en uit. Er zijn diverse configuraties mogelijk, van eenvoudig tot complex. Personalisatie met een welkomsttekst of bedrijfslogo op het startscherm is een van de opties.

- **Knox Manage (beheer en monitoring)**
  Dit is de Mobile Device Management oplossing van Samsung. Na de uitrol kunnen kun je als beheerder instellingen van devices op afstand eenvoudig aanpassen, op een manier die aansluit bij het beleid binnen jouw organisatie.

- **E-FOTA (updaten van de firmware)**
  Met Enterprise Firmware Over The Air kun je updates forceren zodat iedere smartphone optimaal is beveiligd. Ook updates vooraf testen is nu mogelijk, evenals inplannen op een moment dat de impact op de productiviteit gering is.

- **Knox Platform for Enterprise (toestelbeveiliging)**
  Deze toepassing maakt mobiel werken met Samsung devices nóg veiliger. Het voegt een extra beveiligingslaag toe die een strikte scheiding aanbrengt tussen zakelijke- en privédata door containering. Data wordt extra beveiligd opgeslagen op een veilige, afgeschermde plek (container) op de telefoon.

Samsung Knox via Bechtle

Wij ontzorgen je compleet. Tegen een vast maandbedrag regelen we alles rondom jouw zakelijke smartphones en tablets. Naast devices en accessoires verhogen we de tevredenheid van jouw eindgebruikers en bieden we gerichte handvatten om de IT-desk in jouw organisatie te ontzorgen. De combinatie van hardware, services, diensten en Samsung Knox leidt tot optimalisatie van alle processen rondom mobility, met Device as a Service.

Wil je meer weten over hoe Bechtle jou helpt om alles uit je zakelijke telefonie te halen, neem dan vrijblijvend contact met ons op.

Koen Buis
Workspace consultant
T +31 40 760 2873
koen.buis@bechtle.com

SAMSUNG

Hoeveel tijd moet je eigenlijk besteden aan cybersecurity?

En hoeveel tijd heb je er daadwerkelijk voor?

Beveiligingsrisico's worden geavanceerder, en device- en databeveiliging wordt een steeds grotere uitdaging. We zijn constant op zoek naar oplossingen om onze assets beter te beveiligen. Tijd is echter wat ontbreekt: De gemiddelde IT-afdeling is overbelast en onderbezet terwijl de hoeveelheid aan taken alleen maar groeit. Hoeveel tijd heb jij nog over om te besteden aan cybersecurity?

Jouw rol als IT-manager

Mede door de digitalisatie is de rol van IT-managers de afgelopen tijd sterk veranderd. Er wordt steeds meer van je verwacht. Hierdoor is jouw werk een stuk interessanter, maar ook complexer geworden. Naast het onderhouden van de IT, blijft er echter te weinig tijd over voor andere belangrijke zaken.

Tijd vrijmaken voor wat écht belangrijk is, hoe doe je dat?

Hoe zorg je er voor dat je voldoende tijd hebt voor belangrijke zaken, zoals IT security? Makkelijk: Zorg ervoor dat je je minder hoeft bezig te houden met low value, high effort taken. Bijvoorbeeld met Device as a Service van Bechtle. Met Device as a Service ontzorgen we jouw IT-afdeling op het gebied van apparaatbeheer. Voor een vast maandelijks bedrag heb je beschikking over de nieuwste, altijd werkende apparatuur.

We nemen het gehele lifecycle management van je over. Zo heb jij meer tijd om je te focussen op wat echt belangrijk is, zoals cybersecurity.

Apparaten worden gebruiksklaar en op maat geconfigureerd geleverd, en eventuele incidenten worden voor je opgelost. Oude apparaten worden veilig en GDPR-proof afgevoerd. Data wordt systematisch verwijderd en je ontvangt een wiping-certificaat. Daarnaast bieden wij ook ondersteuning voor de eindgebruiker. Zeg maar vaarwel tegen alle support tickets!

Doordat we een gestandaardiseerd pakket leveren, is er tevens minder complexiteit binnen de devices. Hierdoor ondersteunen we in een veiligere IT-omgeving en beter te managen databeveiliging.

Van de IT-managers vindt....

Werkdruk
51% de werkdruk te hoog.

Apparaatbeheer
meer dan 60% dat ze te veel bezig zijn met apparaatbeheer.

Reparatie
meer dan 50% dat ze erg veel tijd spenderen aan het repareren van apparaten die nog onder garantie zijn.

Nieuwsgierig naar wat Device as a Service nog meer te bieden heeft? Ga naar bechtle.com/nl/daas of neem direct contact op met onze specialist.

Er wordt veel gevraagd van IT-managers binnen een snel groeiend bedrijf.

Laptops repareren hoort daar niet bij

Device as a Service van Bechtle is onderdeel van onze Just Press Play solutions: praktische oplossingen die je direct kunt inzetten in de dagelijkse praktijk. Zo ondersteunen wij je en heb jij weer tijd om te doen waar je goed in bent. Wij ontzorgen en helpen jouw organisatie bij het maken van IT-keuzes zodat jij je kunt richten op de zaken die écht belangrijk zijn.

Just press play

Hernieuwde focus met DaaS

De grootste uitdagingen van jou als IT-manager zijn tijdgebrek en werkdruk. De IT-sector kampt al jaren met een groot personeelstekort en IT-managers zijn te veel tijd kwijt met low value, high effort taken. Met Device as a Service verlichten we je werkdruk door het gehele device lifecycle management over te nemen.

Voor een vast bedrag per maand ben jij gegarandeerd van de nieuwste én altijd werkende devices. Tevens geniet je andere voordelen, zoals proactieve monitoring, on-site support en een schaalbaar contract. Hierdoor heb jij meer tijd voor wat écht belangrijk is: innovatie en transformatie.

Just press play

Daniel Maelissa
Workspace consultant
T +31 40 250 9011
daniel.maelissa@bechtle.com

Event: Bechtle NEXT

Today and beyond. Wat kan Bechtle voor jou betekenen?

Inspirerende sprekers, lekker eten én kennismaken met de nieuwste producten

Dit jaar staat de volgende editie van Bechtle NEXT op de planning. Wij zoeken nog naar een gepaste datum vanwege de huidige coronacrisis. Tijdens dit event zullen er verschillende interessante sprekers langskomen, die aansluiten op het thema **today and beyond**.

Vanuit Bechtle organiseren we bijvoorbeeld een sessie over hoe Bechtle je op de korte termijn, in de nabije toekomst en daarna kan helpen. Bas Verkaik, oprichter van SPIKE Technologies, zal ons vertellen hoe de toekomstige werknemer en werkgever eruit zullen zien. Daarnaast zal Joost de Kluijver, directeur en oprichter van Closing the Loop, vertellen over hoe zijn organisatie omgaat met e-waste.

Tijdens de sessies zorgen we voor een lekkere lunch en drankje op het (hopelijk) zonnige dakterras. Tussen de sessies door kun je langsgaan bij de fabrikantenmarkt. Maak er kennis met verschillende fabrikanten en bewonder en test de nieuwste producten.

Na afloop van het programma voorzien we een gezellige afsluitende borrel en genieten we samen na van de dag.

Blijf op de hoogte

Vanwege COVID-19 is de datum van Bechtle NEXT 2020 nog niet bekend. Wil je daarom graag op de hoogte blijven van alle ontwikkelingen? Meld je aan via de website om geen enkele update te missen.

bechtle.com/nl/over-bechtle/events/bechtle-next