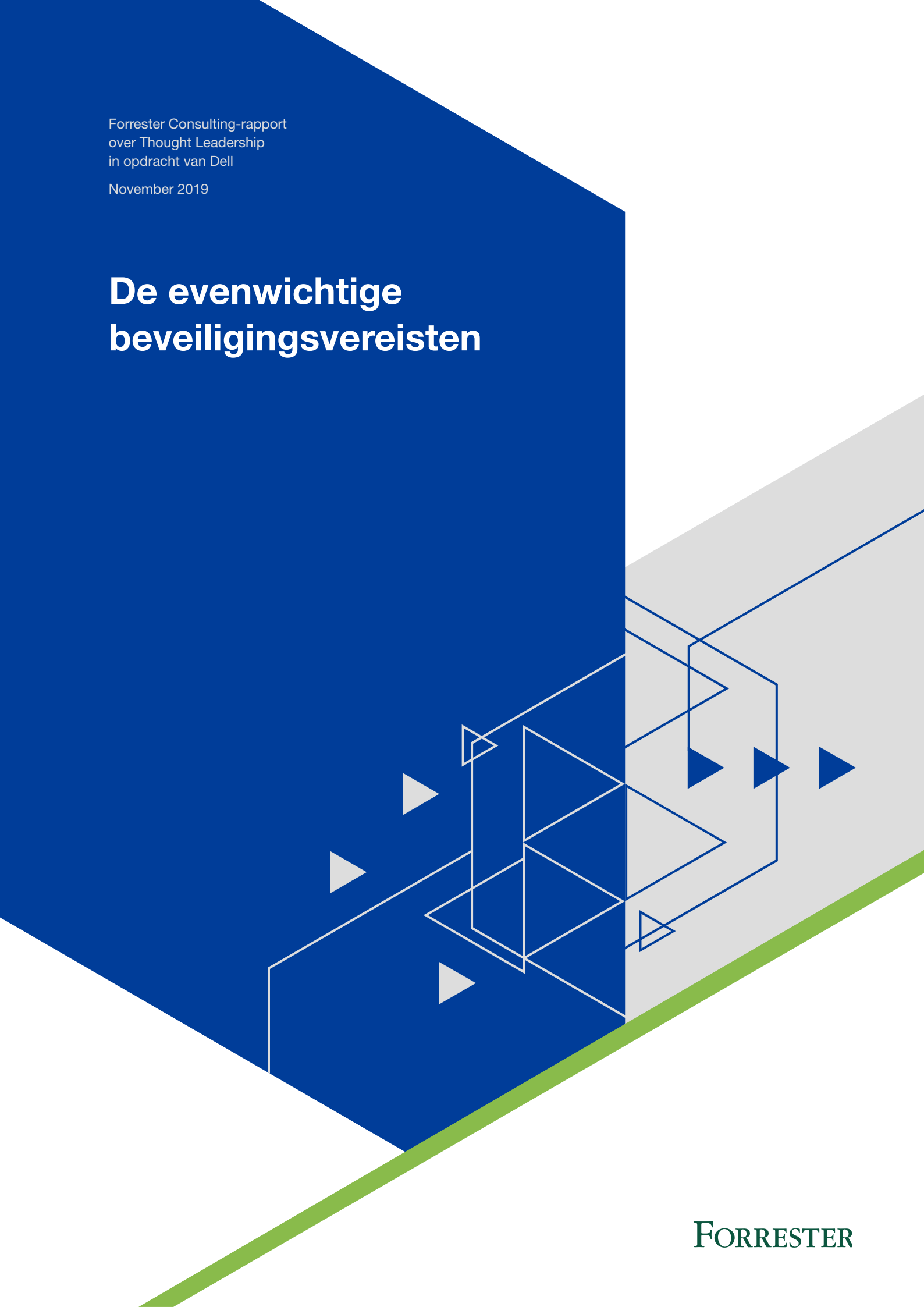
Forrester Consulting-rapport
over Thought Leadership
in opdracht van Dell

November 2019

De evenwichtige beveiligingsvereisten



FORRESTER

Inhoudsopgave

Projectleider:
Tarun Avasthy,
Market Impact Consultant

Contributing Research:
Onderzoeksgroep Infrastructure & Operations van Forrester

INFO OVER FORRESTER CONSULTING

Forrester Consulting biedt onafhankelijk en objectief advies op basis van onderzoek om leidinggevenden te helpen succesvol te zijn in hun organisatie. De Consulting Services van Forrester lopen van een korte strategie tot aangepaste projecten en brengen u direct in contact met onderzoeksanalisten die met deskundig inzicht uw specifieke zakelijke uitdagingen analyseren. Ga voor meer informatie naar forrester.com/consulting.

© 2019 Forrester Research, Inc. Alle rechten voorbehouden. Het zonder toestemming reproduceren is ten strengste verboden. De informatie is gebaseerd op de beste beschikbare bronnen. Meningen weerspiegelen beoordelingen van het moment en zijn onderhevig aan verandering. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar en Total Economic Impact zijn handelsmerken van Forrester Research, Inc. Alle andere handelsmerken zijn eigendom van hun respectieve eigenaren. Ga voor meer informatie naar forrester.com. [E-42637]

FORRESTER®

Beknopte samenvatting

Voor een evenwichtige beveiliging moeten bedrijven overstappen van het behandelen van privacy en databeveiliging als nalevingsvereisten op een beveiligingsstrategie waarbij de privacy hoog in het vaandel staat en de technologie wordt gebruikt om het merk onderscheidend te maken. Door elke misstap met of veranderingen in de IT-infrastructuur kan en zal de beveiligingsstrategie nog complexer worden. Daarom is een evenwichtige beveiligingsstrategie zo belangrijk. Bij een evenwichtige beveiligingsstrategie speelt complexiteit geen rol omdat er gelijke tred wordt gehouden met technologische veranderingen alsmede met de verstoring van de markt en de nalevering van een veranderende regelgeving.

In maart 2019 heeft Dell aan Forrester Consulting de opdracht gegeven om de veranderende beveiligingstrends en -technologie te evalueren die nodig zijn om werknemers te beschermen en om hen veilig hun werk te laten doen. Uit ons onderzoek is gebleken dat de productiviteit van werknemers wordt verbeterd als werknemers over alle noodzakelijke mogelijkheden beschikken en er wordt voldaan aan de beveiligingsprotocollen. Forrester heeft een online enquête onder 887 leidinggevenden van bedrijven en IT-beleidsmakers gehouden om dit onderwerp te onderzoeken.

BELANGRIJKSTE RESULTATEN

- **Door steeds geavanceerdere dreigingen worden bedrijven uit het middensegment gedwongen meer proactief dan reactief te zijn.** Nu er regelmatig in het nieuws melding wordt gemaakt van veel opvallende beveiligingslekken en/of cyberaanvallen, moeten bedrijven uit het middensegment vooruitstrevender worden in hun beveiligingsaanpak.
- **Uitgaven voor beveiliging alleen zijn niet de juiste oplossing.** Bedrijven uit het middensegment moeten een cultuur van enablement, voortdurende ontwikkeling van vaardigheden voor werknemers en, misschien wel het meest kritische, een solide en robuuste beveiligingsinfrastructuur in het middensegment van de markt aangeven.
- **Een restrictief IT-beleid zorgt dat werknemers de best practices voor IT-beveiliging ontwijken om hun werk te kunnen doen.** Creatief omgaan met de regels komt vaker voor op de werkplek, maar het volledig negeren van IT-beleid om werk te doen is riskant.

FORRESTER®

Organisaties hebben een evenwichtige beveiliging nodig om de EX en operationele efficiëntie te verbeteren

Een divers technologisch landschap en andere manieren van werken door werknemers hebben de deuren geopend voor tal van risico's die een bedreiging vormen voor de algehele beveiligingsmentaliteit en de reputatie van de organisatie. Een robuuste, evenwichtige beveiligingsinfrastructuur zorgt ervoor dat de bedrijfsprestaties gemaximaliseerd en beschermd zijn. Ondertussen neemt de ervaring van werknemers (EX) als bedrijfsinitiatief toe naarmate meer bedrijven geïnteresseerd zijn in de ontwikkeling van een strategie voor een personeelservaring met minder obstakels en die werknemers in staat stelt hun belangrijkste werkzaamheden op een efficiënte manier uit te voeren.

Een budget voor technologie alleen is geen garantie dat de ervaring van de werknemers verbetert. Organisaties, en dan met name bedrijven uit het middensegment, moeten ook investeren in meer faciliteiten voor werknemers, continue ontwikkeling van vaardigheden en een solide beveiliging om de risico's te beheren en tegelijkertijd de bedrijfsprestaties te ondersteunen. Voor een goede EX hebben bedrijven een evenwichtige aanpak van beveiliging op drie belangrijke gebieden nodig (zie afbeelding 1):

- **De productiviteit van de werknemers verbeteren.** De huidige drukke werkplek zorgt voor intense cognitieve eisen aan werknemers en daarom is ondersteuning van hun werkzaamheden een inherente dimensie van een hoge EX. Veel beveiligingsmaatregelen doen echter het tegenovergestelde en hinderen hun productiviteitsniveaus. Met dit in het achterhoofd willen bedrijven uit het middensegment de productiviteit van de werknemers in de komende 12 maanden (88%) verbeteren. Aangezien technologie steeds verder wordt ontwikkeld, zeiden respondenten ook dat zij meer aandacht zouden gaan besteden aan het trainen en behouden van werknemers (79%), zodat de kloof tussen talenten niet groter wordt.
- **Betere informatiebeveiliging.** Om werknemers optimaal te kunnen laten werken, hebben zij ook onbeperkte toegang nodig tot data die nodig zijn om hun werk te kunnen doen, ongeacht waar ze werken en de apparaten die ze daarvoor gebruiken. Bedrijven bevinden zich echter onder een spervuur van verschillende soorten cyberattacks en gebeurtenissen die een gevaar zijn voor de bedrijfsactiviteiten en vertrouwelijke data, of het nu gaat om de persoonlijke data van klanten/werknemers of om gevoelige bedrijfsinformatie. Bovendien zorgen problemen, zoals risico's van derden en de beveiliging van de leveringsketen, ervoor dat organisaties wat de risico's betreft, verder moeten kijken dan alleen hun eigen omgeving. Het is geen verrassing dat 86% van de bedrijven zei dat informatiebeveiliging voor hen prioriteit heeft.
- **Operationele efficiëntie verbeteren.** Beveiligingsteams die bedrijfsactiviteiten ondersteunen, moeten een veel consistenter proces opzetten voor de manier waarop ze werken, en ernaar streven om proactief te zijn in plaats van reactief bij hun aanpak van beveiliging. Bedrijven uit het middensegment moeten voor de beveiliging meer doen dan alleen het aanklikken van selectievakjes. De beveiliging moet zijn gebaseerd op nalevingsvereisten en moet vanuit een meer strategische en op risico's gebaseerde benadering worden aangepakt. Hiervoor zijn nodig processen ter ondersteuning van risico-intelligentie, onderkennen van en reageren op dreigingen, beoordelen van risico's en een flexibiliteit om de belofte van het uitvoeren en leveren van projecten gestand te kunnen doen (83%).

Middelgrote ondernemingen moeten investeren in het opbouwen van een cultuur van het faciliteren van werknemers, het voortdurend ontwikkelen van vaardigheden en het streven naar een solide beveiligingsinfrastructuur.

FORRESTER®

Afbeelding 1

"Welke van de volgende technologie-gerelateerde initiatieven heeft de komende 12 maanden prioriteit op uw afdeling of bij uw divisie?"

Basis: 887 zakelijke en IT-beleidsmakers die betrokken zijn bij de besluitvorming voor de aanschaf van laptops, computers en andere apparaten
Bron: een onderzoek uitgevoerd door Forrester Consulting namens Dell, september 2019

Steeds geavanceerdere dreigingen en de complexiteit van de IT stellen de IT voor alsmaar grotere problemen

Beveiligingsmanagers krijgen te maken met concurrerende prioriteiten, opkomende technologieën en nieuwe wettelijke vereisten, en moeten ervoor zorgen dat aanvallers voortdurend worden bestreden zodat zij niet slagen in hun opzet. Toen we de respondenten van de enquête echter vroegen wat de belangrijkste beveiligingsuitdagingen zijn, zagen we het volgende (zie afbeelding 2):

› **De veranderende aard van de bedreigingen zorgt ervoor dat de aandacht van bedrijven uit het middensegment nooit mag verslappen en dat zij altijd alert moeten zijn.** De IT moet vanuit een solide, aanpasbare strategie werken om het aanvallers lastig te maken. 65% van de organisaties wordt geconfronteerd met de steeds veranderende aard van beveiligingsaanvallen. Als leidinggevenden binnen de organisatie het laatste nieuws over cyberattacks en gebeurtenissen vernemen en zij zich vervolgens afvragen of dat bij hen ook kan gebeuren, is het zinvol om het waarom en hoe (of waarom niet, op basis van uw omgeving en controles) te evalueren en te communiceren. Laat deze reactieve benadering echter uw algehele beveiligingsstrategie niet in de weg staan.

FORRESTER®

› **Een complex IT-beheer is kwetsbaarder voor risico's en loopt meer gevaar.** Door elke misstap met of veranderingen in de IT-infrastructuur kan en zal een beveiligingsstrategie nog complexer worden. Daarom is een evenwichtige beveiligingsstrategie zo belangrijk. Een beveiligingsstrategie die gelijke tred kan houden met technologische veranderingen, verstoring van de markt en veranderende regelgeving en naleving zullen een katalysator zijn voor positieve veranderingen. Een strategie waarmee u vanaf het begin beveiliging kunt implementeren, verdient de voorkeur boven een strategie die u achteraf kunt uitbreiden, net als een strategie die het aantal beveiligingsproducten in uw omgeving consolideert om het IT-beheer te vereenvoudigen. 60% van de respondenten in de enquête bekijkt momenteel de complexiteit van hun IT-omgeving als een bedreiging voor hun organisatie.

Afbeelding 2

"Welke van de volgende uitdagingen zijn de IT-beveiligingsuitdagingen voor uw organisatie?"

Basis: 887 zakelijke en IT-beleidsmakers die betrokken zijn bij de besluitvorming voor de aanschaf van laptops, computers en andere apparaten
Bron: een onderzoek uitgevoerd door Forrester Consulting namens Dell, september 2019

WERKNEMERS MOETEN HET GEVOEL HEBBEN DAT ZIJ ERBIJ WORDEN BETROKKEN, OMDAT ZIJ ANDERS EEN LOOPJE ZULLEN NEMEN MET HET IT-BELEID

Werknemers zullen het pad van de minste weerstand kiezen om hun werk te kunnen doen. Als werknemers hun eigen software/applicaties willen installeren om hun werk te kunnen doen, zegt 54% van de respondenten van bedrijven uit het middensegment dat zij hun werknemers dat zullen afraden, hen zullen ontmoedigen en het zullen verbieden, maar ze beseffen ook dat ze dat niet volledig kunnen uitbannen. Werknemers moeten het gevoel hebben dat ze door het bedrijf serieus worden genomen (zie afbeelding 3).

Werknemers moeten ongestoord hun werk kunnen doen om productief te zijn en het beveiligingspersoneel moet ervoor zorgen dat het bedrijf beschermd wordt. 58% van de respondenten gaf aan dat werknemers tijdens hun werk soms het IT-beleid omzeilen waardoor het bedrijf kwetsbaar wordt. Daarom is het belangrijk om een goede balans te vinden tussen de EX en bruikbaarheid enerzijds en de beveiligingscontroles anderzijds, maar 57% zei dat dit een uitdaging blijft. Als organisaties de effectiviteit van hun beveiligingsprogramma (52%) echter niet kunnen meten, zullen zij achter de feiten aan blijven lopen en nooit tot een evenwichtige beveiligingsstrategie komen.

Afbeelding 3

"Wat is voor uw informatiewerkers het beleid van uw IT-organisatie voor het gebruiken/installeren van hun eigen software?"

Basis: 887 zakelijke en IT-beleidsmakers die betrokken zijn bij de besluitvorming voor de aanschaf van laptops, computers en andere apparaten
Bron: een onderzoek uitgevoerd door Forrester Consulting namens Dell, september 2019

Uw beveiligingsinfrastructuur moet meegaan met de tijd

Het idee van een bedrijfsperimeter is vandaag de dag achterhaald en verouderd. Werknemers werken op verschillende locaties en hebben overal toegang tot informatie nodig. De consumentenmarkt beïnvloedt de manier waarop werknemers werken in een bedrijfsomgeving en met welke apparaten. Een digitale onderneming heeft geen grenzen. Uw organisatie kan nu gebruikmaken van de cloud, mobiele werknemers ondersteunen en fysieke omgevingen met connectiviteit via sensoren en andere op internet aangesloten apparaten digitaliseren. Er zijn steeds meer mogelijkheden om gevoelige data bloot te leggen en aanvallers kunnen uw omgeving en data in gevaar brengen. In de huidige werk- en bedreigingsomgeving moeten de beveiligingsstrategie en -architectuur zich ontwikkelen tot een datacentrische en een Zero Trust-aanpak van de beveiliging.

Zero Trust is een conceptueel en architectonisch model voor de manier waarop beveiligingsteams netwerken opnieuw moeten ontwerpen tot veilige micro-perimeters, gebruik moeten maken van versluiering om de databeveiliging te verbeteren, de risico's die gepaard gaan met overmatige gebruikersrechten, moeten beperken en gebruik moeten maken van analyse en automatisering om de detectie van en respons op beveiliging drastisch te verbeteren. Deze aanpak verbetert de beveiliging van data aanzienlijk. Veel organisaties werken vandaag de dag al vanuit een Zero Trust-aanpak. De respondenten in de enquête gaven de volgende prioriteiten voor de infrastructuur aan die wijzen op een bereidheid voor Zero Trust (zie afbeelding 4):

- **Training van eindgebruikers ter verbetering van de veilige procedures voor het omgaan met data.** Om toegang te krijgen tot intellectueel eigendom zullen aanvallers zich richten op werknemers en aannemers. Op het werk maken werknemers gebruik van verbonden apparaten die communiceren met cloudservices via de systemen/netwerken van het bedrijf, maar vandaag de dag werken werknemers ook buiten het bedrijf, zoals onderweg, thuis, in openbare ruimten zoals luchthavens en cafés, en ook daar hebben zij toegang tot gevoelige informatie en data nodig vanaf persoonlijke apparaten die niet zo goed beveiligd zijn als de systemen/netwerken van het bedrijf. De noodzaak van werknemers om bijvoorbeeld data op een verantwoorde en veilige manier te verwerken, is niet bij iedereen gemeengoed.
- **Training van IT-medewerkers in het beperken van de risico's.** De continue ontwikkeling van de vaardigheden van IT-personeel is belangrijk om ervoor te zorgen dat de personen die verantwoordelijk zijn voor de technologie en de beveiliging, op de hoogte zijn van de huidige, aanbevolen procedures. Inzicht in veranderende technologieopties en in de steeds groter wordende risico's en bedreigingen is nodig om het IT-team uit te rusten met de noodzakelijke middelen. Daarom zei 79% van de respondenten dat ze IT-personeel beter zullen opleiden. Dit is goed nieuws op twee fronten: 1) Ervoor zorgen dat IT-medewerkers hun vaardigheden kennen en weten hoe zij moeten handelen, en 2) om werknemers binnen het bedrijf te houden in tijden wanneer er door andere bedrijven aan hen wordt getrokken.

› **De beveiligingsstrategie opnieuw bekijken.** Organisaties beseffen steeds meer dat voldoen aan de nalevingsvereisten niet gelijk staat aan het implementeren van een krachtige beveiliging. Externe zakelijke partners vragen om een gedegen beveiligings- en risicobeheer als voorwaarde om samen te werken. Een toekomstgerichte strategie ondersteunt de inspanningen van een organisatie om een robuust beveiligingsprogramma op te bouwen en om te anticiperen op gebieden waar ze op basis van zakelijke prioriteiten nieuwe vaardigheden moeten verbeteren of inbrengen om problemen aan te pakken. 80% van de respondenten gaf aan dat ze prioriteit gaven aan het ontwikkelen en uitvoeren van een beveiligingsstrategie voor de IT, apparaten en data.

Afbeelding 4

"Welke van de volgende initiatieven zijn in de komende 12 maanden waarschijnlijk de belangrijkste prioriteiten van de IT-infrastructuur van uw bedrijf?"

Basis: 887 zakelijke en IT-beleidsmakers die betrokken zijn bij de besluitvorming voor de aanschaf van laptops, computers en andere apparaten
Bron: een onderzoek uitgevoerd door Forrester Consulting namens Dell, september 2019

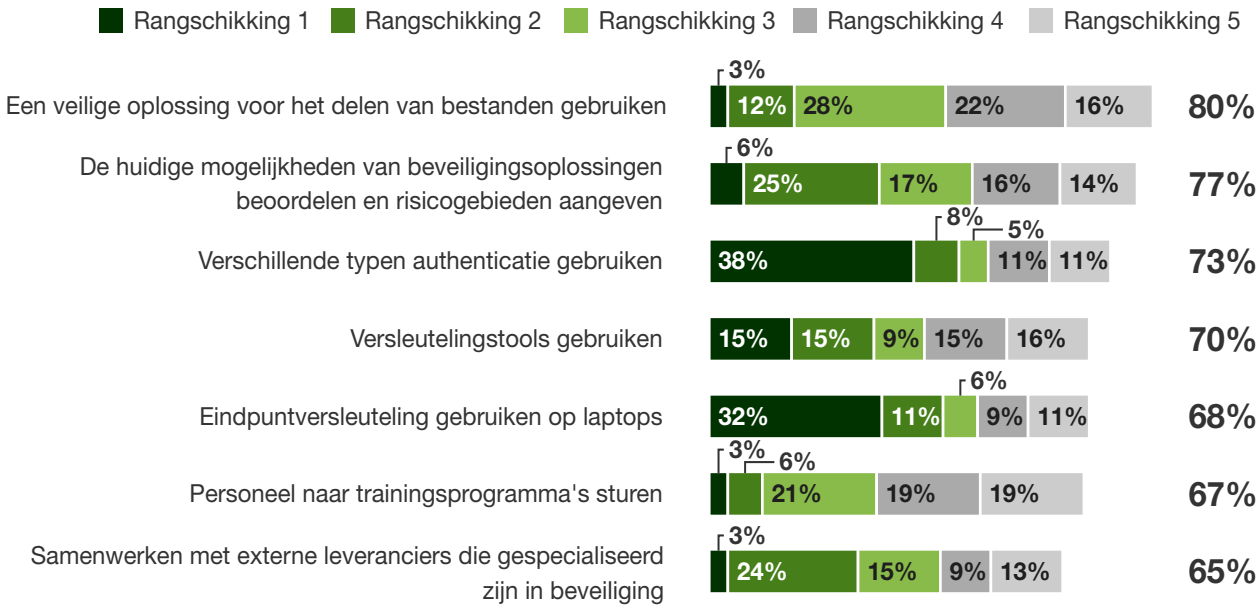
TACTIEK OM DE BEVEILIGING TE VERBETEREN

In het digitale tijdperk zijn cyberbedreigingen overal aanwezig, en inbreuken halen vrijwel dagelijks de voorpagina's van de kranten, wat bedrijven hun reputatie, kapitaal en de toekomstige groei en uitbreiding van de onderneming kost. Met andere woorden, de veiligheid van het bedrijfsresultaat is afhankelijk van de technologieën die de data beveiligen, d.w.z. de fundamentele valuta van digitaal zakendoen. Datalekken maken helaas deel uit van het leven. 50% van de wereldwijde beleidsmakers op het gebied van netwerkbeveiliging zei dat hun bedrijf in het afgelopen jaar ten minste één keer een aanval te verduren heeft gekregen, en dat aantal is nu 55% van de zakelijke respondenten. Met dit in gedachten gaven organisaties aan op welk gebied zij de beveiliging willen verbeteren (zie afbeelding 5):

- **Veilig bestanden delen om samenwerking met medewerkers te ondersteunen.** Technologie en werknemers spelen een cruciale rol in het laten samenwerken van organisaties om zo een blijvende economische waarde te creëren. 80% van de respondenten zei dat ze een veilige oplossing voor het delen van bestanden zullen gebruiken om hun beveiligingsmogelijkheden te helpen verbeteren. Dit moet echter niet alleen binnen de muren van het bedrijf worden gedaan, aangezien remote workers en degenen die voor hun werk onderweg zijn, ook toegang moeten kunnen krijgen tot de bestanden en deze moeten kunnen delen wanneer dat nodig is.
- **Authenticatie ter ondersteuning van veilige toegang van werknemers tot data.** In zijn eenvoudigste vorm houden authenticatieoplossingen de slechteriken buiten de deur en de goeden binnen. Met zo veel datalekken over de hele wereld staat het belang van het afdwingen van controle hoog op de agenda. 73% van de respondenten gaf aan dat ze verschillende vormen van authenticatie zullen gebruiken en voor 38% van de respondenten was authenticatie de belangrijkste strategische inspanning die ze zouden doen om de beveiliging te verbeteren. Deze processen mogen echter de productiviteit en het werk van de werknemers dat zij moeten doen, niet in de weg staan; een vlotte authenticatie van gebruikers maakt een groot verschil.
- **Versleuteling om data te beheren en aan de nalevingsvereisten te voldoen.** 73% van de respondenten gaf aan dat ze versleutelingstools zouden gebruiken, terwijl 68% specifiek wees op eindpuntversleuteling voor werknemers (Full-Disk Encryption) als wat zij belangrijk vonden voor het verbeteren van de beveiliging. Dit is een verstandige keuze, aangezien werknemers heel gemakkelijk een apparaat kunnen kwijtraken of slachtoffer kunnen worden van diefstal van een apparaat. Versleuteling van data at rest is er in vele vormen, en organisaties kunnen dienovereenkomstig kiezen op basis van hun behoeften, d.w.z. versleuteling van volledige schijf, op bestandsniveau, media, e-mail, app-/veldniveau, transparant of database.
- **Beveiligingsbeoordeling om de huidige ontwikkeling van beveiliging te begrijpen.** Hoewel de meeste beveiligingsteams een breed scala aan controles en standaarden hebben geïmplementeerd om hun bedrijf veilig te houden, zijn veel teams niet in staat om objectief vast te stellen waar er gaten in de beveiliging zitten. Anderzijds hebben ze moeite om vast te stellen of ze alle belangrijke kwesties hebben aangepakt of dat een bepaald aspect van de aanbevolen procedures niet aan de orde is gekomen. 77% van de respondenten is zich hiervan bewust en wil de beveiliging verbeteren door nauwkeurige saneringsplannen te ontwikkelen om ervoor te zorgen dat alle componenten voldoen aan de gewenste functionaliteit.

Afbeelding 5

"Wat zou u willen doen om de beveiliging te helpen verbeteren?"



Basis: 887 zakelijke en IT-beleidsmakers die betrokken zijn bij de besluitvorming voor de aanschaf van laptops, computers en andere apparaten
Bron: een onderzoek uitgevoerd door Forrester Consulting namens Dell, september 2019

Evenwichtige beveiligingsvoordelen voor werknemers en het bedrijf

Door gronding werk te maken van de beveiliging zal een bedrijf veiliger worden in plaats van zich te richten op het genereren van meer inkomsten en de beveiliging daardoor verwaarlozen. Om het bedrijf te bevrijden van belemmeringen, moeten beleidsmakers een menselijke en op risico's gebaseerde aanpak nastreven om de beveiligingservaring vorm te geven. Als u een geweldige ervaring van uw werknemers en een solide beveiliging met elkaar in evenwicht brengt, kunt u het volgende doen (zie afbeelding 6):

- **Extern werk mogelijk maken om de productiviteit te verhogen en concurrerender te kunnen zijn.** Of werknemers nu een betere support eisen voor een betere balans tussen werk en privéleven, of uw organisatie de beste persoon in dienst neemt ongeacht de afstand en duur van het woon-werkverkeer, ondersteuning voor werk op afstand is een concurrentievoordeel bij het aannemen en behouden van talent. Technologie is de sleutel tot werken op afstand en beveiliging is een belangrijke basis voor hoe uw bedrijf veilig werken op afstand mogelijk maakt. 69% van de respondenten gaf aan dat ze toegang tot bedrijfsdata op apparaten mogelijk maken wanneer werknemers buiten het bedrijf werken.
- **Bevorderen van samenwerking om innovatie te stimuleren.** Werknemers willen ervaringen delen en uiteindelijk willen ze bestanden en ideeën kunnen delen met collega's. Zowel de menselijke verbinding als de tools om deze verbinding mogelijk te maken, zijn voorwaarden voor het beheren van een omgeving, of cultuur, van innovatie, met name bij een gedistribueerd personeelsbestand, dat wil zeggen werknemers die niet altijd voor hun werk in het bedrijf aanwezig zijn. 49% van de respondenten zegt dat ze moeite hebben om hun werknemers de mogelijkheid te bieden om eenvoudig en veilig gegevens te kunnen delen. Er is ruimte voor verbetering ten einde voordelen te behalen.

FORRESTER®

› **De klantervaring verbeteren en de omzet van werknemers verlagen.** Het verbeteren van het goede gevoel van werknemers door een betere EX vertaalt zich in tevreden klanten die betere support van uw werknemers ontvangen en een beter contact met uw werknemers zullen hebben. Tevreden werknemers hebben meer kans om de juiste keuzes te maken, keuzes die juist zijn voor uw klanten. [1] Uit een onderzoek bleek dat organisaties met tevreden werknemers een 81% hogere klanttevredenheid zagen en de helft van de omzet van de werknemers. [2]

Afbeelding 6

"Welke maatregelen heeft uw bedrijf genomen om extern of flexibel werk mogelijk te maken?"

Basis: 887 zakelijke en IT-beleidsmakers die betrokken zijn bij de besluitvorming voor de aanschaf van laptops, computers en andere apparaten
Bron: een onderzoek uitgevoerd door Forrester Consulting namens Dell, september 2019

Belangrijkste aanbevelingen

Investeren in uw beveiligingsinfrastructuur en in controles zijn een essentieel onderdeel van uw beveiligingsprogramma. Investeringen in technologie alleen zijn echter onvoldoende. Bepaal het juiste niveau van een uitgebalanceerde beveiliging voor uw organisatie, op basis van uw specifieke behoeften en risicotolerantie.

Neem vandaag vier stappen om uw organisatie te positioneren voor succes bij het bereiken van de juiste balans tussen beveiliging en de ervaring van de werknemers:

Beoordeel uw huidige status van de ontwikkeling van de beveiliging. Het proces van het doorlopen van de beoordeling zelf kan ook zicht bieden op procedures of processen die institutionele kennis zijn. Aangezien sommige van deze procedures/processen niet zijn gedocumenteerd, zal het belangrijk zijn om de details naar boven te halen voor het geval dat belangrijke teamleden met pensioen gaan of de organisatie verlaten. Een beoordeling geeft een overzicht van de bestaande beveiligingscontroles, processen en het toezicht van uw organisatie om te helpen bij het bepalen van gebieden met mogelijke lacunes en het aanpakken van de behoeften. Deze beoordeling zal een belangrijke rol spelen bij het bieden van een leidraad voor wat er voor u nog in het verschiet ligt waar u uw aandacht op moet richten en waarom.

Geef aan wat gevoelige data zijn, waarom die gevoelig zijn en waar deze zich bevinden. Dit houdt onder meer in dat u begrijpt welke data worden gereguleerd door nalevingsvereisten en de waarde van data voor uw organisatie als geheel. Met de beveiligingscontroles en de juiste overwegingen voor het omgaan met data zorgt inzicht in uw data ervoor dat die ook een basis vormen ter ondersteuning van de privacy en het ethisch gebruik van persoonsgegevens. Door een gedegen overzicht en begrip van uw data bent u beter in staat om te bepalen wat er nodig is om die te beschermen en op de juiste manier te gebruiken.

Inzicht in het niveau van risicotolerantie binnen uw organisatie. Hoewel door de regelgeving bepaalde handelingen en activiteiten kunnen worden voorgeschreven, zijn de soorten controles en het controleniveau dat uw organisatie wil implementeren, afhankelijk van uw mate van risicotolerantie. Begrijp de risico's voor uw data en organisatie en neem op risico gebaseerde beslissingen voor beveiligingscontroles om de noodzaak daarvan en de productiviteit van uw werknemers met elkaar in evenwicht te brengen.

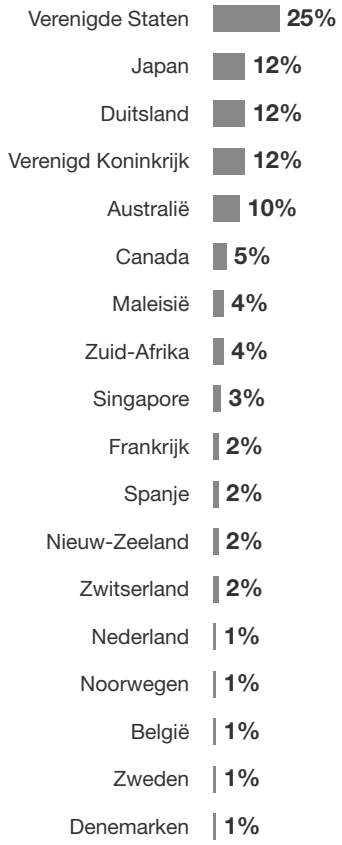
Evalueer hoe werknemers werken en hun werk doen. Breng in kaart waar de beveiligingscontroles invloed hebben op de werkervaring van werknemers en de impact die dit heeft op hun werkdag en productiviteit. Verschillende profielen van werknemers - van de functies die zij bekleden, tot de data waartoe zij toegang hebben om hun werk te kunnen doen - zullen ook van invloed zijn op hun technologische behoeften, de risico's waarmee zij waarschijnlijk te maken zullen krijgen, en de soorten beveiligingscontroles die u moet implementeren om deze risico's te beperken. Voer de nodige veiligheidscontroles uit in plaats van zaken die het werk verstoren.

Bijlage A: Methodologie

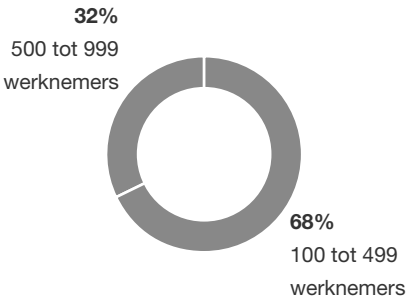
In dit onderzoek heeft Forrester een online enquête gehouden onder 887 leidinggevenden van bedrijven en IT-managers uit verschillende sectoren in de markt. Aan de deelnemers werden vragen voorgelegd over hoe hun uitgaven voor beveiliging zijn veranderd, over datgene wat invloed heeft op hun beveiligingsstrategie, naleving en wettelijke uitdagingen, en over hoe de toekomst van beveiliging eruitziet voor hun organisatie. Het onderzoek is gestart in maart 2019 en het Thought Leadership Paper is afgerond in augustus 2019.

Bijlage B: Demografie

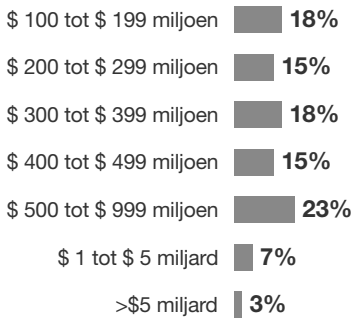
"In welk land bent u gevestigd?"



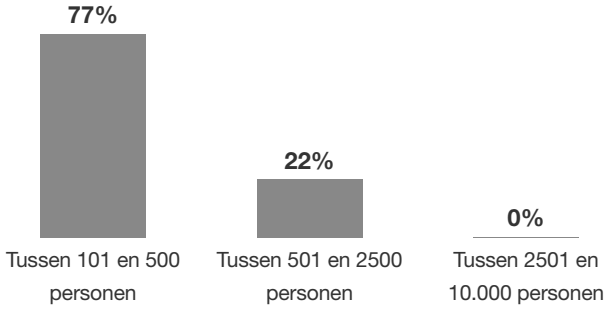
"Hoeveel mensen werken er naar schatting voor uw bedrijf/ organisatie wereldwijd?"



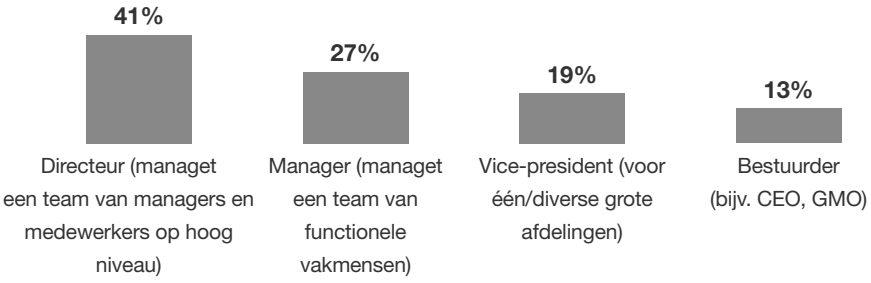
"Wat is volgens uw beste schatting de jaarlijkse omzet van uw organisatie (USD)?" (N = 861)



"Voor de aankoopbeslissingen op het vlak van technologie en services die u het meest beïnvloeden, willen wij graag weten hoeveel werknemers of leden van het personeelsbestand van uw organisatie er direct bij zijn betrokken?"



"Welke functie beschrijft het beste uw positie in uw organisatie?"



Basis: 887 zakelijke en IT-beleidsmakers die betrokken zijn bij de besluitvorming voor de aanschaf van laptops, computers en andere apparaten
Bron: een onderzoek uitgevoerd door Forrester Consulting namens Dell, maart 2019

FORRESTER®

Bijlage C

VOETNOTEN

[1] Bron: “Transform The Employee Experience To Drive Business Performance,” Forrester Research, Inc., February 12, 2018.

[2] Bron: James K. Harter, Frank L. Schmidt, and Theodore L. Hayes, “Business-Unit-Level Relationship Between Employee Satisfaction, Employee Engagement, and Business Outcomes: A Meta-Analysis,” Journal of Applied Psychology, April 2002 (http://www.factorhappiness.at/downloads/quellen/s17_harter.pdf).