DOSSIER IT-SECURITY

Waarom ook uw bedrijf een doelwit is en hoe u hackers buitenhoudt

NEXTEL
you're always one step ahead

BUSINESS

INHOUD

Vandaag heeft elk onderdeel van uw IT-infrastructuur zijn eigen bescherming nodig

Tot enkele jaren geleden stond alles wat u als bedrijf nodig had lokaal, in het bedrijfsnetwerk. Tegenwoordig trekken we voor steeds meer functionaliteiten de cloud in. Het klassieke model, waarbij een next generation firewall alles kan beschermen, voldoet niet meer.

Vandaag heeft élk onderdeel van uw IT-infrastructuur bescherming nodig. Niet alleen uw netwerk en datacenter, maar ook uw endpoints zoals smartphones en laptops, uw webapplicaties zoals Office 365 en Skype, uw cloud, uw IoT-netwerk. Goede beveiliging bestaat, meer dan ooit, uit meerdere lagen.

Helemaal nieuw zijn endpoint-, webapplicatie-, cloud- en IoT-beveiliging natuurlijk niet. Maar in het huidige klimaat, winnen ze alleen maar aan belang. Met dit dossier hopen onze security-experts u daarvan te overtuigen.

Martine Tempels
Senior Vice President
Telenet Business

7 trends op vlak van IT-security

01

Bedreigingen worden geavanceerder

De bedreigingen waarmee u als bedrijf geconfronteerd wordt, nemen alsmaar toe in complexiteit. Malware bijvoorbeeld omzeilt traditionele antimalwaresystemen door zichzelf constant aan te passen. Even verontrustend is dat hackers meer tijd steken in hun aanvallen. Social engineering is daar een mooi voorbeeld van.

02

Het aantal DDoS-aanvallen neemt toe

Een andere trend, die zich jaar na jaar blijft aftekenen, is de stijging van het aantal DDoS-aanvallen. Wel nieuw is dat de bron verandert: steeds meer worden – onvoldoende beveiligde – Internet of Things-toestellen ingezet. Niet onlogisch: hoe meer toestellen met het internet verbonden worden, hoe meer hackers er gebruik van kunnen maken.

03

Security omarmt artificial intelligence

Beveiligingsoplossingen worden steeds intelligenter. Meer en meer maken ze gebruik van technieken als machine- en deep learning. Ze zijn in staat data te verzamelen, eruit te leren en zichzelf zo constant te verbeteren. Hun beveiliging wordt dus alsmaar beter. Bedreigingen aanpakken op basis van een artificial intelligence komt zo een stap dichterbij.

04

Preventie alleen is niet voldoende

Vroeger lag de focus van IT-security puur op preventie. De stijgende complexiteit van aanvallen zorgt ervoor dat die aanpak alleen niet meer voldoet. Tegenwoordig wordt er dan ook meer aandacht geschonken aan detectie. Detectiesystemen zullen elk gedrag
dat afwijkt van standaardgedrag opsporen en gepast ingrijpen.

05

De vraag naar managed services stijgt

Belgische bedrijven trekken meer en meer naar de public cloud voor hun infrastructuur en toepassingen. Die hybride modellen maken beveiliging heel complex. Bedrijven merken dat de nodige expertise in huis hebben en houden moeilijk geworden is. Ze vragen dan ook steeds meer een gespecialiseerde partij om hun infrastructuur te beheren.

06

Perimeterbeveiliging volstaat niet meer

Trends als thuiswerken maken dat de link met het bedrijfsnetwerk steeds vaker verdwijnt. De beveiligingsfocus moet dus veranderen: vroeger volstond het om de perimeter – de buitenkant – te beveiligen, nu moeten ook endpoints en webapplicaties beschermd worden. Want de beste beveiliging bestaat, net als een ajuin, uit meerdere lagen.

07

IT-security wordt voor iedereen prioritair

Nu assets steeds vaker digitaal zijn, winnen governance, risk management en compliancy enorm aan belang. De fameuze CIA van business continuity (confidentiality, integrity en availability) moet hoog op de prioriteitenlijst van bedrijven staan. Zeker nu de GDPR in werking treedt en het securitybeleid alleen maar aan belang wint.

01

IT-security: voor bedrijven is het vijf voor twaalf

Meer en meer digitale assets

Klantengegevens, looninformatie, R&D-resultaten... Bedrijven verzamelen en verwerken heel wat gevoelige data digitaal. Dat maakt ze kwetsbaarder dan ooit.
De impact van één IT-incident kan enorm zijn: van dataverlies over imagoschade tot volledige downtime.

Een nieuwe manier van werken

Werknemers vandaag zijn 24/7 online, gebruiken de nieuwste snufjes en verwachten hetzelfde gebruiksgemak in hun werkomgeving. Is dat niet het geval, dan brengen ze wel hun eigen toestel mee, of werken ze met hun eigen applicaties. BYOD (Bring Your Own Device) en Shadow IT zijn verre van nieuw, maar blijven IT-managers wel voor enorme uitdagingen stellen. Het is hun taak om ervoor te zorgen dat alle bedrijfsdata veilig zijn, maar tegelijk moeten ze een evenwicht vinden met gebruiksgemak.

SHADOW IT, DE OLIFANTENPAADJES VAN IT

Shadow IT is alle soft- en hardware die binnen een bedrijf gebruikt wordt, zonder dat de IT-afdeling er controle over heeft of zelfs weet van heeft. Het zijn de olifantenpaadjes van de IT-infrastructuur: werknemers nemen de kortste weg als die minder omslachtig is dan de officiële – veilige – weg.

De grootste misvatting van organisaties die in de publieke cloud werken? Dat ze zelf geen beveiliging moeten opzetten.

SERGE EGO, SECURITY MANAGER BIJ TELENET

IT-infrastructuur in de public cloud

Steeds meer bedrijven trekken naar de public cloud voor hun infrastructuur en/of applicaties. Er heerst daar één grote misvatting rond. Veel bedrijven denken dat ze automatisch beschermd zijn in de public cloud. Maar dat klopt maar tot op zekere hoogte.

Zo bieden cloudproviders geen applicatie- of toegangsbeveiliging naar hun servers. Terwijl die servers wel open en bloot op het internet staan en voor iedereen toegankelijk zijn. Beveiliging van een public cloud is dan ook een gedeelde verantwoordelijkheid. Als klant moet u zelf beslissen welke beveiliging u activeert en wat u daarvoor wilt betalen.

DE 3 LAGEN VAN DE **PUBLIC CLOUD**

IaaS:
Infrastructure as a service, zoals dataopslag en processorkracht
PaaS:
Platform as a Service, zoals een database-oplossing
SaaS:
Software as a Service, zoals Office 365

Het kwetsbare Internet of Things

Steeds meer apparaten zijn met het internet verbonden: van IP-camera's over parkeersensoren tot sensoren die de luchtkwaliteit meten. Hét probleem: bij de ontwikkeling van veel Internet of Things-apparaten was beveiliging geen prioriteit. Van veel van die toestellen circuleren de standaardpaswoorden online. Bedrijven die de paswoorden niet wijzigen, zijn dus een makkelijk slachtoffer. Een gehackte parkeersensor lijkt misschien onschuldig, maar vergeet niet dat de hacker met één commando al het achterliggende netwerkverkeer kan onderscheppen.

De constante evolutie van bedreigingen

'Zolang de boel draait, blijf ik eraf', hoor je IT-managers denken. Maar zo werkt het niet. Met IT-security bent u nóóit klaar. Een security-infrastructuur neerpoten is niet voldoende, ze moet ook up-to-date gehouden worden. Met de regelmaat van de klok worden er kwetsbaarheden ontdekt en de WannaCrys, Spectres en Meltdowns van deze wereld maken daar al te graag gebruik van. Patchmanagement is dan ook een onmisbaar onderdeel van IT-security.

GLUREN BIJ DE BUREN

Via bepaalde websites is het mogelijk om binnen te kijken bij Belgische bedrijven. Hun IP-bewakingscamera's konden gehackt worden, omdat de bedrijven het standaardpaswoord nooit wijzigden. Criminelen kunnen zelfs een stap verder gaan en de camera's uitschakelen op het moment dat ze inbreken.

CYBER SECURITY COALITION

De academische wereld, overheidsinstellingen en bedrijven delen in de Cyber Security Coalition hun security-ervaringen en -incidenten. Het doel overstijgt sectoren en concurrentie: de leden willen van elkaar leren om krachtiger te kunnen optreden tegen cybercrime.

Op 25 mei 2018 treedt de GDPR in werking. Elk bedrijf dat data van Europese burgers verwerkt, moet een gedocumenteerd privacy- en securitybeleid hebben.

ISABELLE GHISLAIN
PRIVACY MANAGER BIJ TELENET

Een strenger juridisch kader

Wat als u gehackt wordt? Wat als een van uw werknemers gegevens lekt? Bent u dan verantwoordelijk? Riskeert u een boete? Isabelle Ghislain, Privacy Manager bij Telenet, belicht kort de juridische kant.

Belgische wetgeving

"Uit het aansprakelijkheidsrecht kunnen we afleiden dat elk bedrijf een adequaat beveiligingsbeleid moet hebben", start Isabelle. "Met de **Cyber Security Strategy** streeft de Belgische overheid naar een integrale aanpak rond digitale veiligheid. Maar er is weinig informatie over hoe dat concreet geïmplementeerd moet worden."

Daarnaast gelden er bijkomende wetten. "Voor exploitanten van een kritieke infrastructuur is er de **Wet voor kritieke infrastructuren**. En van zodra bedrijven persoonsgegevens verwerken, geldt de **Privacywet**. Die bepaalt hoe ze met die gegevens moeten omgaan en welke maatregelen ze moeten nemen om de gegevens voldoende te beschermen."

Europese wetgeving

Op 25 mei 2018 treedt de **General Data Protection Regulation (GDPR)** in werking. "Voor alle bedrijven die data van Europese burgers verwerken", weet Isabelle. "De GDPR verplicht hen onder meer een inventaris van hun data op te maken en die data met passende technische en organisatiorische maatregelen te beveiligen. Ze moeten ook een gedocumenteerd privacy- en securitybeleid hebben. En omdat de bedrijven verplicht zijn om privacy-incidenten aan hun lokale privacycommissie te melden – en in sommige gevallen ook aan de betrokkenen – moeten ze ook de nodige procedures ontwikkelen om datalekken op te sporen en te melden."

Naast de GDPR zit ook de **Network and Information Security Directive (NISD)** eraan te komen. Isabelle: "Die richtlijn tracht de kloof tussen de Europese lidstaten te dichten met een uniforme en concrete beveiligingsaanpak voor cybersecurity. De NISD moet wel nog in Belgische wetgeving omgezet worden."

DE **GDPR** IN EEN NOTENDOP

Mogelijke sancties

De Privacycommissie kan **boetes** opleggen die, afhankelijk van de aard van het incident, kunnen oplopen tot 4 procent van de wereldwijde omzet óf 20 miljoen euro – wat het hoogste bedrag van de twee is.

Sleutelaanbevelingen

Gezien de hoge boetes – en de mogelijke imagoschade – is het voor bedrijven enorm belangrijk om in regel te zijn met de GDPR. Hieronder vindt u alvast enkele sleutelaanbevelingen:

- Maak een **inventaris** van uw data op en houd bij waarom en hoe u de data verwerkt
- Stel een duidelijke **privacy notice** op om de personen van wie u data bijhoudt te informeren
- Tref **veiligheidsmaatregelen** om uw data te beschermen: encryptie, pseudonimisering…
- Werk een **duidelijk privacy- en securitybeleid** uit en voorzie training voor uw medewerkers
- Ontwikkel procedures om **datalekken** op te sporen en te melden, zoals regelmatige audits

IT-SECURITY WORDT ALLEEN MAAR BELANGRIJKER

Als deze bedrijfscontext íets duidelijk maakt, is het wel dat IT-security aan belang wint. U weet dus ook maar beter waar de mogelijke bedreigingen liggen.

Meer daarover in hoofdstuk 2

02

Hackers nemen bedrijven op allerlei manieren in het vizier

01

Malware

Malware, kort voor malicious software, is software die gebruikt wordt om toegang te krijgen tot computersystemen en ze te verstoren of gevoelige informatie te stelen. Ze lijken op gewone programma's of bestanden, maar bevatten verborgen functies waarmee hackers van buitenaf toegang krijgen tot de besmette computers. Opvallend detail: malware past zichzelf aan om onder de radar van de traditionele beveiliging te blijven.

02

Ransomware

Ransomware is een chantagemethode op basis van malware. Het encrypteert de besmette computer of gegevens die erop staan en vraagt de gebruiker losgeld te betalen om de computer of de gegevens weer vrij te geven. Betaalt de gebruiker niet binnen de bepaalde periode, dan wordt de decryptiesleutel niet vrijgegeven en de computer of data onbruikbaar. Door geregeld back-ups te maken van (kostbare) data kunnen bedrijven zich al veel leed besparen.

WANNACRY

De grootste ransomware-aanval ooit vond plaats op 12 mei 2017. WannaCry wist meer dan 230.000 Windows-computers in 150 landen te blokkeren. Onder de slachtoffers, niet de minste: de Britse National Health Service, transportbedrijf FedEx en de Duitse spoorwegmaatschappij Deutsche Bahn.

230.000

MEER DAN 230.000 COMPUTERS IN 150 LANDEN WERDEN BESMET

$ 300

PER BESMETTE COMPUTER WERD ER $ 300 LOSGELD GEVRAAGD

98%

98% VAN DE BESMETTE COMPUTERS DRAAIDE OP WINDOWS

59

DE PATCH VOOR DE KWETSBAARHEID WAS AL 59 DAGEN VÓÓR DE AANVAL BESCHIKBAAR

03

DDoS-aanvallen

Een DDoS-aanval (Distributed Denial of Service) zorgt ervoor dat de internetinfrastructuur van een bedrijf – webservers, mailservers enz. – onbeschikbaar wordt. Net als de voorbije jaren, steeg ook dit jaar het aantal, de omvang en de complexiteit van DDoS-aanvallen. Nieuw is de bron van de aanvallen: steeds meer worden Internet of Things-toestellen ingezet om aanvallen te lanceren.

DRIE SOORTEN **DDOS-AANVALLEN**

01

Volumetrische aanval

Bij een volumetrische aanval overspoelt de hacker uw infrastructuur met een enorme hoeveelheid data, waardoor uw bandbreedte volledig opgebruikt wordt.

02

Applicatieve aanval

Bij een applicatieve aanval valt de hacker heel gericht een applicatie of server aan, die de hoeveelheid data niet kan verwerken en uitvalt.

03

Protocolaanval

Bij een protocolaanval stuurt de hacker netwerkpakketten die niet aan de internetstandaarden voldoen, waardoor servers vertragen en zelfs crashen.

DDoS, het (niet zo) geheime wapen van gamers

Elke kleine hapering kan volstaan. Daarom lanceren gamers steeds vaker DDoS-aanvallen op elkaar. Verwonderlijk is dat niet eens: voor 20 dollar huur je al een kwartier een botnet.

04

Botnets

Overal ter wereld zijn computers en andere toestellen besmet zonder dat hun gebruikers er weet van hebben. Samen vormen ze een botnet: een netwerk dat vanuit een centraal commandopunt aangestuurd kan worden, bijvoorbeeld om een DDoS-aanval te lanceren. Botnetcomputers- en toestellen zijn nadelig voor een bedrijf, omdat ze veel bandbreedte gebruiken en een netwerk aanzienlijk vertragen.

05

Programmeerfouten

Er worden voortdurend kwetsbaarheden ontdekt in software. Iedereen die op de hoogte is van zo'n kwetsbaarheid, kan ze uitbuiten. Daarom ontwikkelt en verdeelt de softwareleverancier zo snel mogelijk een patch die de software verbetert. Maar zolang bedrijven die patch niet geïnstalleerd hebben, blijven ze kwetsbaar. Dat is ook hackers niet ontgaan: bij hun aanvallen viseren ze steeds meer webapplicaties.

MIRAI, HET IOT-BOTNET

Een van de grootste botnets ooit bestond uit IoT-toestellen. Mirai kreeg IP-camera's en andere 'slimme' toestellen in zijn macht door er simpelweg **standaardwachtwoorden** op los te laten. Met een gerichte aanval op DNS-dienst Dyn slaagde Mirai erin delen van het internet, waaronder Twitter en Spotify, even plat te leggen.

69%

MEER AANVALLEN OP WEBAPPLICATIES

Onderzoek van Akamai toont aan dat het aantal aanvallen op webapplicaties tussen Q3 2016 en Q3 2017 met 69% toenam.

Volgens het Open Web Application Security Project (OWASP) zijn de meest voorkomende risico's injectiefouten, falende authenticatie en datalekken.

06

SSL-verkeer

Veel applicaties en websites gebruiken SSL-encryptie, zodat hun verkeer niet door anderen 'af te luisteren' is. Zo'n SSL-certificaat geeft de bedrijven en surfers de indruk dat de verbinding veilig is, maar vaak weten hackers de SSL-beveiliging te omzeilen – bijvoorbeeld via het 'man-in-the-middle'-principe – of gebruiken ze zelf SSL-verkeer om malware in te verbergen.

07

Shadow IT

Hoewel het voor een groot deel onschuldig is en in veel gevallen net de productiviteit en innovatie stimuleert, kleven er heel wat nadelen aan Shadow IT. De continuïteit en vooral veiligheid zijn moeilijk te waarborgen. Datalekken zijn vaak het gevolg van initiatieven waar de IT-manager nooit zijn goedkeuring voor gaf of zelfs geen weet van had.

08

Onvoldoende awareness

IT-security is vaak geen sinecure binnen bedrijven. Dat geldt zowel voor het C-level – onvoldoende budget vrijmaken, geen uniform beleid uittekenen – als voor werknemers. Zij kunnen ongewild beveiligingsrisico's veroorzaken, zoals malware binnenhalen door een geïnfecteerde usb-stick te gebruiken. Bewustwording, op alle niveaus, is dan ook de eerste stap om IT-security goed in de praktijk te brengen.

MAN-IN-THE-MIDDLE

Een surfer die een webadres ingeeft, gaat meestal eerst naar het http-adres. De hacker komt ertussen op **het moment dat de http in https verandert**.
In plaats van een veilige verbinding met de server van de website te maken, verbindt de surfer met de webserver van de hacker.

SSL-VERKEER, MINDER VEILIG DAN U DENKT

Er zijn heel weinig bedrijven die hun SSL-verkeer decrypteren om het in de SSL-tunnel te inspecteren. Ze gaan er nog al te vaak van uit dat SSL-verkeer veilig is, waardoor ze hun **policies enkel toepassen op niet-SSL-verkeer.**

09

Phishing

De mens is en blijft de zwakste schakel als het op IT-beveiliging aankomt. Hoewel phishingmails vaak zo slecht gemaakt zijn dat het zichtbaar om vervalsingen gaat, werpen ze voor criminelen toch vruchten af. Ze worden naar miljoenen mensen gestuurd en er zijn er altijd die op de links klikken zonder er zich veel vragen bij te stellen.

10

Spear phishing

Spear phishing is de doelgerichte vorm van phishing: perfecte vervalsingen gericht aan specifieke personen, zo goed gemaakt dat ze nauwelijks als vervalsing te herkennen zijn. Het is een e-mail die afkomstig lijkt te zijn van een 'collega', van een 'onderneming waarmee u samenwerkt' of van een 'sollicitant'.

ALS **BIJLAGE** VINDT U MIJN CV

Pdf-bestanden zijn hét geschikte middel voor spear phishing. Ze zijn alomtegenwoordig, lijken onschuldig, maar hebben veel **mogelijkheden om code in te verbergen**. Een hacker hoeft soms niets meer te doen dan een 'cv' als pdf op te sturen. Opent een HR-medewerker de pdf, dan wordt er malware geïnstalleerd en heeft de hacker vrij spel.

GEVAAR LOERT OM ELKE HOEK

Hackers gaan steeds slimmer te werk, bedreigingen en aanvallen komen werkelijk van overal. U beschermt uw bedrijf dan ook best op verschillende manieren.

In hoofdstuk 3 leest u er alles over

03

Slimmere aanvallen vragen om nieuwe beveiligingsoplossingen

Ramen en deuren op slot

Het heeft weinig zin uw voordeur volledig te vergrendelen, als uw achterdeur en ramen wagenwijd openstaan. De metafoor die niet duidelijker kan zijn. Vandaag, meer dan ooit, moet IT-beveiliging uit meerdere lagen bestaan.
Het volstaat niet meer om de perimeter te beveiligen. Alles – netwerk, datacenter, endpoints, webapplicaties, de cloud, een IoT-netwerk – heeft zijn eigen specifieke beveiliging nodig. Hoever bedrijven daarin gaan, blijft uiteraard hun keuze. Het is aan hen om de afweging te maken tussen de investering die ze willen of kunnen doen en de risico's die ze willen lopen.

Geen exacte wetenschap

Bedrijven kunnen op elk niveau de juiste beveiliging implementeren, maar de mist ingaan bij het instellen van de policies. Bedrijven moeten de risico's tegen de opportuniteiten afwegen. U kan een firewall zeer strikt configureren, maar dan boet u in aan productiviteit. Of uw policy kan zó open zijn dat uw firewall een veredelde router wordt. Telenet helpt uiteraard om policies te definiëren en te optimaliseren, maar de klant blijft wel de eindverantwoordelijke.
Telenet is de slotenmaker: we kunnen een goed slot plaatsen, maar de klant beslist hoeveel sleutels hij laat bijmaken.

Op de volgende pagina zetten we de oude benadering van IT-security grafisch tegenover de nieuwe, moderne visie.

VROEGER

IT-BEVEILIGING ALS EEN **SNOEPJE**

Hard aan de buitenkant, zacht aan de binnenkant

VANDAAG

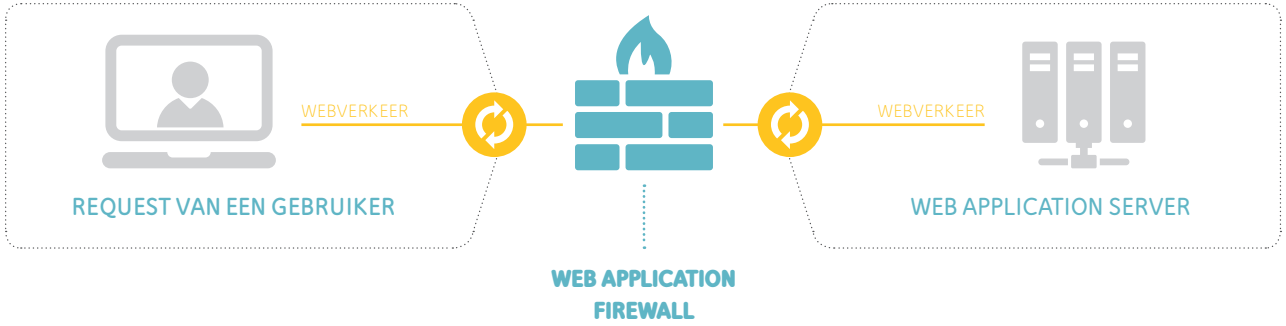
IT-BEVEILIGING ALS EEN **AJUIN**

Opgebouwd uit verschillende lagen

Webapplicatiebeveiliging

Webapplicatiebeveiliging is niet nieuw. "Maar nu bedrijven steeds meer webapplicaties gebruiken, wint het aan belang", zegt Kris Bogaerts, Principal Security Consultant bij Telenet. Hij ziet webapplicatiebeveiliging als een combinatie van maatregelen. "Om te beginnen kan een web application firewall (WAF) veel onheil voorkomen. Zo'n WAF filtert het http-verkeer van en naar de applicatie. Hij doet dat op basis van actuele signatures. Ontdekt hij een poging om een kwetsbaarheid uit te buiten, dan zal hij die virtueel patchen. Meestal gaat dit sneller dan de webapplicatie zelf patchen of wijzigen."

Een meerwaarde van een WAF is dat hij securityprofielen kan toepassen. Kris: "Met aangepaste securityprofielen kan u verschillende maatregelen instellen voor verschillende webapplicaties. Heel belangrijk, want elke applicatie is anders." Ook IP-reputatie is een belangrijk onderdeel van de beveiliging. Kris: "Veel aanvallen worden door botnets en criminele organisaties uitgevoerd. Op basis van een black list kan u IP-adressen met een slechte reputatie automatisch blokkeren, nog vóór ze iets kunnen proberen." Tot slot hamert hij op het blijven testen van de applicaties: "Webapplicaties veranderen, er komt constant nieuwe code bij. Ze moeten dan ook regelmatig getest en geëvalueerd worden."



Een web application firewall kan veel onheil voorkomen, maar webapplicatiebeveiliging is vooral een combinatie van maatregelen.

KRIS BOGAERTS
PRINCIPAL SECURITY CONSULTANT BIJ TELENET

De nieuwste endpointbeveiliging gebeurt vanuit de cloud en bestaat uit drie grote luiken: prevention, detection en response.

WILLEM JANSSENS
SECURITY CONSULTANT BIJ TELENET

Endpointbeveiliging

Bij endpointbeveiliging denken we klassiek aan desk- en laptops. Maar volgens Willem Janssens, Security Consultant bij Telenet, gaat endpointbeveiliging veel verder: van servers over smartphones en tablets tot zelfs IoT-toestellen. Willem: "De laatste twee jaar is endpointbeveiliging enorm geëvolueerd. Vroeger gebeurde het beheer vanop een lokale server, nu vanuit de cloud. Vroeger werd er zo goed als alleen op preventie gefocust, nu zowel op preventie, detectie als herstel."

NIEUWE AANPAK, **MÉÉR VOORDELEN**

KLASSIEKE ENDPOINTBEVEILIGING
LOKALE SERVER

MODERNE ENDPOINTBEVEILIGING
CLOUDPLATFORM

Klassieke endpointbeveiliging werd vanop een lokale server beheerd. Nu gebeurt het vanuit een cloudplatform. Dat heeft enkele voordelen. U hoeft **geen server meer te onderhouden** én het beschermingsniveau blijft maximaal, ook al bevindt het endpoint zich buiten het bedrijfsnetwerk. Waar er vroeger vooral op Windows gefocust werd, kunnen de nieuwste technologieën nu **ook macOS- en Linux-besturingssystemen** beschermen. Bovendien kan u al uw endpoints in **één overzichtelijk dashboard** monitoren.

IN DETAIL: DE **3 LUIKEN** VAN MODERNE **ENDPOINTBEVEILIGING**

PREVENTION

MALWARE TEGENHOUDEN

Vroeger vertrouwden endpointbeveiligingsoplossingen op signatures om malware tegen te houden. Nu werken ze op basis van **predictive modeling.** Door middel van machine learning worden tienduizenden karakteristieken in een predictive model verzameld. Dat model toetst elk bestand aan de karakteristieken af en weet welke combinaties van karakteristieken slecht zijn.
Zo kan het malware herkennen en stoppen, óók als het die malware **voordien nog nooit gezien** heeft.

DETECTION

NIET-STANDAARD GEDRAG STOPPEN

Malware wordt steeds gesofisticeerder. Zelfs met predictive modeling kunnen endpointbeveiligings-oplossingen niet álles oppikken. Ze moeten dus ook **aanvallen kunnen detecteren** waarvoor preventie niet mogelijk was. Daarvoor gaan ze naar het gedrag van de endpoints kijken: als een toestel zich **abnormaal gedraagt**, zoekt en stopt de endpointbeveiligingsoplossing de oorzaak. Gezien de huidige complexiteit heeft de detectielaag het laatste jaar enorm aan belang gewonnen.

RESPONSE

AUTOMATISCH ANALYSEREN EN OPKUISEN

Als de endpointbeveiligingsoplossing malware heeft kunnen stoppen, dan wilt u automatisch het hele malwareverhaal kennen én de **eventuele schade kunnen terugdraaien.** Malware kan bijvoorbeeld scripts op het endpoint geplaatst hebben, ransom-ware kan bestanden geëncrypteerd hebben. Met de endpointbeveiligingsoplossingen van vandaag kan u alle aanpassingen die de malware veroorzaakt heeft in enkele muisklikken opkuisen. Zelfs schade aan uw data door encryptie kan teruggedraaid worden.

De cloud verandert niet alleen de typische IT-infrastructuur, maar heeft ook impact op de manier van beveiligen.

SERGE EGO
SECURITY MANAGER BIJ TELENET

Cloudbeveiliging

Steeds meer bedrijven trekken naar de cloud. “En waar ze in eerste instantie nog voor een private cloud kozen, zien we nu de vlucht vooruit naar de public cloud”, zegt Serge Ego, Security Manager bij Telenet. Dat verandert niet alleen de typische IT-infrastructuur, maar ook de manier van beveiligen. Serge: “In een public cloud kunnen we uiteraard geen fysieke firewalls gaan neerpoten. Daarom combineren we bestaande virtualisatie- en segmentatietechnieken met nieuwe technieken als CASB’s. Zo’n Cloud Access Security Brokers zijn ideaal voor SaaS-oplossingen.”

Virtualisatietechnieken

Virtualisatie binnen fysieke datacenters bestaat uiteraard al een tijdje. De bestaande technieken om het verkeer in virtuele omgevingen te controleren, gebruiken we nu ook om de toegang tot de publieke applicaties in de cloud te beveiligen.

Segmentatie

Net als bij een private cloud, moet de communicatie van uw lokale netwerk naar uw public cloud extra beveiligd worden, bijvoorbeeld via encryptie. Segmentatie blijft enorm belangrijk. Zo kunnen hackers niet zomaar doorstoten naar de verschillende segmenten van uw IT-infrastructuur en kan een aanval niet uw hele omgeving besmetten. Met Software Defined Networking kan u bovendien alles op een geautomatiseerde manier organiseren.

Identity management

Cloud Access Security Brokers of CASB’s controleren en analyseren de inhoud van het verkeer en het gedrag van uw medewerkers in de cloud. Ze brengen het cloudverkeer in kaart en helpen zo identiteitsdiefstal tegen te gaan. Daarnaast zorgen slimme authenticatieoplossingen op een gebruiksvriendelijke manier voor een beveiligde toegang.

SECURITY AS A SERVICE

BEVEILIGING VANUIT DE CLOUD

De evolutie richting cloud is in volle opmars. Ook IT-beveiliging zal steeds meer vanuit de cloud gebeuren. "Als klant hebt u dan geen beveiligingssoftware meer lokaal draaien", legt Serge uit. "Alle hardware staat bij de netwerkprovider, de filtering gebeurt op hun backbone. Zij monitoren continu het verkeer van, naar en binnen uw platformen, systemen, netwerken, toestellen en applicaties. U krijgt realtime inzicht in de bedreigingen en eventuele aanvallen, maar hoeft zelf niet in te grijpen."

Security as a Service is zeker voor kmo's een zeer interessant model. Serge: "Ze kunnen hun applicaties veilig gebruiken, zonder van de beveiliging te moeten wakker liggen. Bovendien kan Telenet makkelijk een totaaloplossing bieden, in combinatie met connectiviteit. We kunnen zelfs een private verbinding naar uw public cloud provider(s) leggen, volledig gescheiden van het publieke internet en van onze andere klanten."

SECURITY AS A SERVICE: DE **VOORDELEN** OP EEN RIJTJE

- Veel **minder technische kennis** in huis nodig
- **Dashboard** om alles te monitoren en analyseren
- Keuze uit de **beste security vendors** op de markt

> Security as a Service is zeker voor kmo's interessant. Ze kunnen hun applicaties veilig gebruiken, zonder van de beveiliging te moeten wakker liggen.
>
> SERGE EGO
> SECURITY MANAGER BIJ TELENET

Door een netwerk in secties op te delen, worden de risico's en effecten van een aanval telkens tot één sectie beperkt.

PATRICK LECLUYSE
MANAGER PROFESSIONAL SERVICES BIJ TELENET

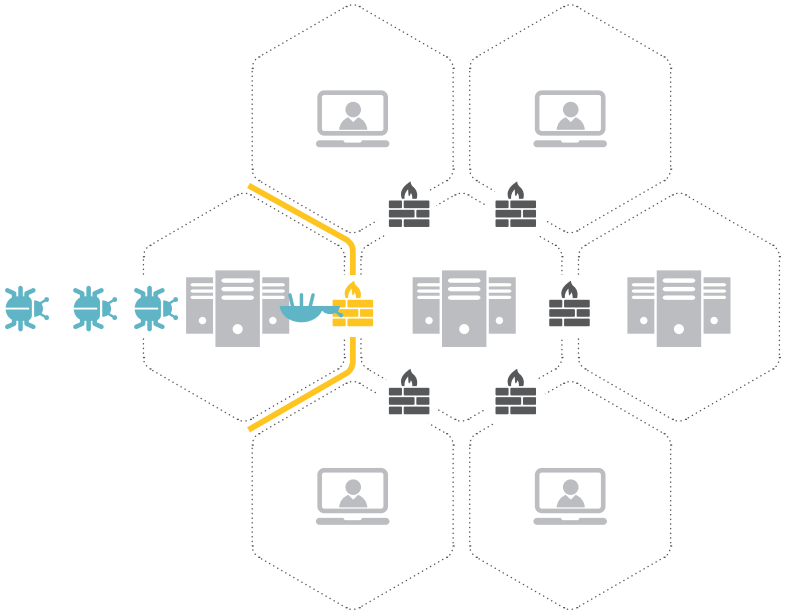
Netwerk- en datacenterbeveiliging

Netwerken

Netwerken zijn door hun toegenomen complexiteit veel kwetsbaarder geworden. "Netwerksegmentatie komt aan die uitdaging tegemoet", zegt Patrick Lecluyse Manager Professional Services bij Telenet. "Het netwerk wordt in verschillende secties opgedeeld en de verbindingen tussen de secties door een firewall gecontroleerd. Zo worden de risico's en effecten van een aanval op het netwerk beperkt tot één sectie en komt niet het hele netwerk in gevaar."

Datacenters

In datacenters werd vroeger vooral het noord-zuidverkeer – tussen clients en de server – geïnspecteerd en beveiligd. Nu ook de trafiek tussen servers onderling toeneemt, moet er ook daar een beleid afgedwongen worden. Patrick: "Bij dat zogenaamde oost-westverkeer moet er expliciet gedefinieerd worden wat wel mag en wat niet. Naast een fysieke firewall, hebt u dus ook firewalls binnen de gevirtualiseerde omgeving nodig om een beleid tussen servers onderling af te dwingen."



Internet of Things-beveiliging

IoT-toestellen beveiligen is een hele uitdaging. Bart Van den Branden, Business Development Manager IoT bij Telenet: "Hoe krijg je updates van enkele Mb tot bij een toestel, dat net ontworpen is om met zo weinig mogelijk bandbreedte – hooguit een paar kb – te communiceren? Of hoe ga je data encrypteren bij een toestel dat zo weinig mogelijk batterij moet verbruiken? Terwijl encryptie net veel processorkracht vraagt."

"Als we spreken over IoT-beveiliging, dan zijn er twee luiken", zegt Bart. "Enerzijds kunnen we **bedrijven helpen die IoT-toepassingen ontwikkele**n. Samen met partners staan we dan in voor het design en de implementatie van een beveiligd IoT-platform, het platform waarmee de IoT-toestellen communiceren. We denken mee over hoe we de firmware en de IoT-toestellen kunnen beveiligen, we helpen bij het coderen en we kijken hoe we de data kunnen encrypteren en beschermen in de cloud."

"Anderzijds kunnen we ook **IoT-gebruikers helpen**", gaat Bart verder. "Uiteraard kunnen we bestaande firmware niet zomaar aanpassen, maar we kunnen de risico's wel helpen beperken. Denk aan segmentatie, waarbij we het IoT-netwerk afschermen van de rest van het netwerk. We kunnen ook een penetration test doen en de IoT-protocollen onder de loep nemen. Zo zien we waar de mogelijke pijnpunten liggen. Blijkt de toepassing niet veilig, dan is het aan de gebruiker om ze te blijven gebruiken of niet. We kunnen ook adviseren bij de keuze van een nieuwe, veilige toepassing."

Bestaande firmware kunnen we uiteraard niet zomaar aanpassen, maar we kunnen de risico's wel helpen beperken.

BART VAN DEN BRANDEN
BUSINESS DEVELOPMENT MANAGER IOT BIJ TELENET

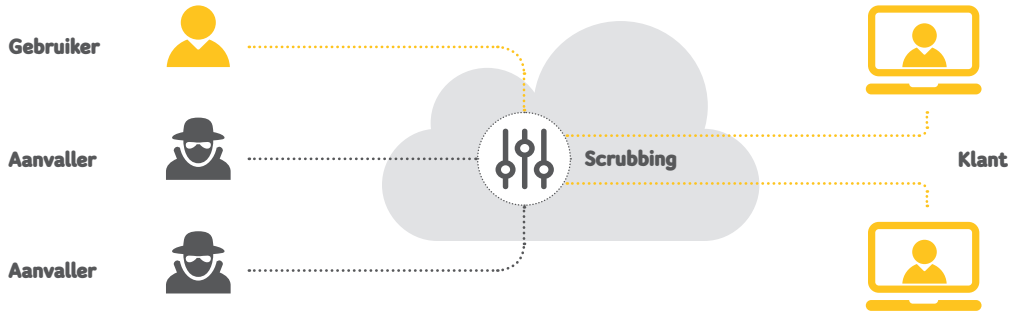
Nu ook IoT-toestellen aan botnets toegevoegd worden, wordt bescherming tegen volumetrische aanvallen heel belangrijk.

NICO VANDEVOORT
SECURITY PRESALES CONSULTANT BIJ TELENET

DDoS-beveiliging

DDoS-aanvallen kunnen bedrijven onderuit halen door een enorme vloed aan data naar hun infrastructuur te sturen, door specifieke applicaties te viseren of door foute netwerkpakketten te versturen. "We raden bedrijven dan ook aan zich tegen de drie soorten aanvallen te beschermen", zegt Nico Vandevoort, Security Presales Consultant bij Telenet.

Er zijn verschillende oplossingen om DDoS-aanvallen tegen te gaan: van oplossingen on site tot in de cloud. Nico: "Een on site-oplossing zal bedrijven tegen applicatieve en protocolaanvallen beschermen. De anti-DDoS-oplossing op onze eigen connectiviteit en in de cloud beschermt u dan weer tegen volumetrische aanvallen. Nu ook IoT-toestellen aan botnets toegevoegd worden, wint vooral bescherming tegen volumetrische aanvallen aan belang. De oplossing in de cloud kan bijvoorbeeld DDoS-aanvallen tot 4,5 Tbps verwerken."



ANTI-DDOS

ANTI-DDOS OP EIGEN CONNECTIVITEIT

Om u beter te beschermen tegen volumetrische aanvallen, lanceerden we onze eigen anti-DDoS-oplossing. Typisch is dat de aanvallen tegengehouden worden op ons netwerk, nog vóór ze u kunnen bereiken. Uw bandbreedte komt dus nooit in gevaar.

We monitoren en analyseren uw netwerkverkeer

Telenet zal uw netwerkverkeer continu monitoren en analyseren met een anti-DDoS-managementsysteem. Dat systeem zal, na het overschrijden van de geconfigureerde drempels, automatisch de typische volumetrische DDoS-aanvallen detecteren. Dat gebeurt onder meer op basis van een DDoS intelligence feed met actuele fingerprints van aanvallen en een lijst van botnets.

We filteren het slechte verkeer er automatisch uit

Bij een aanval wordt al uw netwerkverkeer omgeleid naar een scrubbinginfrastructuur. De scrubbing zal de DDoS-aanval eruit filteren en alleen het goede verkeer naar uw netwerk doorsturen. Dat gebeurt zonder dat u er iets van merkt, want de aanval bereikt uw netwerk niet.

IT-SECURITY VRAAGT EEN DUIDELIJKE VISIE

Nieuwe bedreigingen en nieuwe oplossingen vragen een totaalvisie op security. Benieuwd naar de aanpak van Telenet Security?

Alle details in hoofdstuk 4

04

De Telenet-aanpak: security lifecycle als uitgangspunt

ONZE AANPAK

BEVEILIGING ALS CONTINU PROCES

Security lifecycle

De aanpak van Telenet Security is gebaseerd op de 'security lifecycle'. Beveiliging is een continu proces. Dat proces begint met een assessment of een audit van uw huidige situatie en het analyseren van
uw behoeften. Op basis van die audit tekenen we de beste architectuur uit en implementeren ze. Monitoring en bijsturing zijn essentiële onderdelen om de beveiliging op peil te houden.

Waar we vroeger vooral oplossingen implementeerden, denken we nu businessgewijs met de klant mee.

LORE MATTELAER
SECURITY COMPETENCE MANAGER BIJ TELENET

01
Alles start met bewustwording

We zijn ervan overtuigd dat alles start met bewustwording. “Awareness creëren is belangrijk”, zegt Lore Mattelaer, Security Competence Manager bij Telenet. “Die adviserende rol, daar zijn we de laatste jaren echt op gaan focussen. Waar we vroeger vooral oplossingen implementeerden, denken we nu businessgewijs met de klant mee.”

Pentesting is het ideale startpunt voor een efficiëntere beveiliging. Daarvoor werkt Telenet met Toreon samen. Lore: “Dankzij hun expertise en onafhankelijkheid, behoren ze tot de Belgische top in ethical hacking. Het zijn gecertificeerde experts die zich niet vastpinnen op producten, leveranciers of telecomproviders. Ze zeggen onverbloemd waar het op staat.”

Waar pentesting in de meeste gevallen als eenmalig ijkpunt gebruikt wordt, is **vulnerability management** de meer constante, geautomatiseerde manier van assessment. Lore: “De moeilijkheid daar ligt niet bij het monitoren, maar bij de constante, actieve opvolging ervan – het patchen. Daarvoor vertrouwen we op NVISO. Zij hebben alle competenties in huis om het rapport juist te interpreteren en het om te zetten in concrete governance, risk management en compliancy.”

IN DE PRAKTIJK | SECURITY CONSULTANCY

Security Consultancy is de verzamelnaam voor onze gespecialiseerde diensten om bewustwording te realiseren.

Security Check-up

Een Security Check-up brengt uw netwerkgebruik en de beveiligingsstatus in kaart.

- Duidelijk zicht op uw netwerkverkeer
- Uitgebreid rapport over de beveiligingsstatus met actiepunten
- Geen voorafgaande kennis van uw infrastructuur vereist

Security Pentesting | in samenwerking met Toreon

Met Security Pentesting laten we een ethical hacker uw infrastructuur testen om u op de zwakheden te wijzen en ze te verbeteren.

- Gegarandeerde kwaliteit dankzij CEH-certificatie (Certified Ethical Hacker)
- Duidelijk zicht op de kwetsbaarheden van uw beveiliging
- Dezelfde technieken en tools als malafide hackers, maar zonder gevaar voor uw data

Security Policy Optimalisatie

Met Security Policy Optimalisatie kijken we waar uw firewallpolicy beter kan.

- Gestructureerde analyses, geen manuele acties
- Detectie van ongebruikte, dubbele, tegenstrijdige en gevaarlijke regels in uw policy
- Dezelfde tool als voor ISO-, SOX- en andere certificaten

Vulnerability Management | in samenwerking met NVISO

Vorm van assessment waarbij uw IT-infrastructuur systematisch geïnspecteerd wordt om kwetsbaarheden vroegtijdig op te sporen.

- Nexpose van Rapid7 als vulnerability scanner
- Goed inzicht in uw stand van zaken via gebruiksvriendelijke dashboards en duidelijke rapporten
- Begeleiding bij de interpretatie van de rapporten en de uitvoering van de actiepunten

Security Assessment

We analyseren uw infrastructuur en geven u aanbevelingen voor een optimale bescherming.

- Gegarandeerde kwaliteit dankzij CISA-certificatie (Certified Information Systems Auditor)
- Uitgebreid rapport over de status van uw infrastructuur en met concrete aanbevelingen
- Ideaal startpunt voor een verbeterde beveiligingsomgeving

Door ons aanbod te beperken tot de allerbeste technologieën op de markt, kunnen we ons echt specialiseren.

ANDRIES DE LOMBAERDE
PRINCIPAL SECURITY CONSULTANT BIJ TELENET

02
Een beperkt aantal vendors voor de beste kennis

Telenet Security promoot geen producten, maar gaat partnerships aan in functie van wat klanten nodig hebben. Andries De Lombaerde, Principal Security Consultant bij Telenet: "Door ons aanbod te beperken tot de allerbeste technologieën op de markt, kunnen we ons echt specialiseren. Onze kennis is dan ook dé toegevoegde waarde ten opzichte van andere integratoren."

De graad van partnerships is daar het levende bewijs van: 4 Stars Partner van Check Point, Diamond Partner van Palo Alto Networks en Gold Partner van F5. Andries: "Die partnerships maken dat we de vendors echt kunnen challengen. Dat we samen kunnen verderwerken aan de technologie, zodat die beter gericht is op onze klanten. We hebben regelmatig meetings waarbij zij ons inlichten over nieuwe functionaliteiten die ze gaan implementeren of nieuwe tools die ze gaan uitbrengen en waarbij wij onze ervaring uit the field delen. We bespreken openstaande issues, zaken die we bij klanten tegenkomen, beperkingen van een bepaald product. Er wordt rekening gehouden met bemerkingen en feedback. Het is een wisselwerking: aan de hand van onze input gaan zij hun producten verder finetunen of zelfs nieuwe zaken ontwikkelen."

IN DE PRAKTIJK | **PARTNERSHIPS IN DE KIJKER**

De drie topvendors waarmee we samenwerken zijn Check Point, Palo Alto Networks en F5. Ieder jaar opnieuw plaatst technologieconsultant Gartner Check Point en Palo Alto Networks opnieuw bij de leiders in zijn 'Magic Quadrant for Enterprise Firewalls'.

Gold Partner van F5

Telenet is Gold Partner van F5, bekend als specialist in het sneller en beter ter beschikking stellen van applicaties, vooral via load balancing. Inmiddels is F5 ook een belangrijke speler in security. Met de BIG-IP Application Delivery Controllers (ADC's) kan u nu zowel de snelheid, de beveiliging als de beschikbaarheid van applicaties optimaliseren.

"Telenet heeft een uitstekende reputatie in de markt. Door hun uitgebreide technische kennis weten ze ons portfolio zeer goed te vertalen in toegevoegde waarde voor de klant."

JOZEF VAN ROYEN
CHANNEL ACCOUNT MANAGER BELUX BIJ F5

4 Stars Partner van Check Point

Telenet is 4 Stars Partner van Check Point Software Technologies, een van de marktleiders in Next Generation Firewalling. De oplossingen van Check Point bieden, naast geavanceerde identiteits- en applicatiecontrole, tal van virtualisatiemogelijkheden. In 2015 werd Telenet bekroond als Best Performing Partner.

"Door de snelle en vlotte adaptie aan onze nieuwste technologieën en de daarmee samengaande certificering, bewijst Telenet keer op keer zijn kennis en professionaliteit."

PIERRICK VAN DEN ABEELE
SALES MANAGER BELUX BIJ CHECK POINT

Diamond Partner van Palo Alto Networks

Palo Alto Networks ontwikkelde de eerste Next Generation Firewall met een hoogperformante single-pass engine. Het bedrijf biedt vandaag vooruitstrevende en geïntegreerde securityoplossingen. Telenet is Diamond Partner met ASC Elite Status (Authorized Support Centers) en wist Palo Alto's prestigieuze 'Excellence in Support EMEA Award' al in de wacht te slepen.

"Op vlak van security support heeft Telenet als enige partner in België de ASC Elite Status."

LUC VERVOORT
DIRECTOR EMEA STRATEGIC ALLIANCES BIJ PALO ALTO NETWORKS

We tekenen samen met u de gepaste architectuur uit, gaan na wat de meest geschikte beveiligings-componenten zijn en implementeren ze.

BRUNO GYSELS
SECURITY CONSULTANT BIJ TELENET

03

Architectuurbenadering met componenten op maat van de klant

We vinden dat beveiliging veel verder moet gaan dan louter producten. Wij kiezen resoluut voor een architectuurbenadering en niet voor technische ad-hocoplossingen die bedrijven, in het beste geval, alleen maar tijdelijk uit de problemen helpen.

Bruno Gysels, Security Consultant bij Telenet: "Gezien de huidige complexiteit van informatie-beveiliging, kan één securityleverancier niet langer een totaaloplossing aanbieden. Om u wél een volledig geïntegreerde beveiliging te kunnen bieden, werken wij met verschillende technologiepartners samen. We tekenen samen met u de gepaste architectuur uit, gaan na wat de meest geschikte beveiligingscomponenten zijn en implementeren ze. We beperken ons daarbij niet tot de perimeter, maar kijken ook naar de beveiliging van onder meer endpoints, webservers, datacenters en anti-DDoS-oplossingen."

IN DE PRAKTIJK | SECURITY IMPLEMENTATION

We tekenen een architectuur uit, kiezen de hard- en software en implementeren de beveiligingsarchitectuur in uw bedrijf. We voorzien ook advies voor het gebruik en de bewustmaking bij uw medewerkers.

We doen enkel een beroep op de beste technologiepartners en installeren de meest geschikte beveiligingscomponenten, gebaseerd op de ervaring van onze experts. Afhankelijk van uw situatie, kan uw beveiligingsinfrastructuur uit deze componenten en technologieën bestaan:

Componenten	Technologiepartners
Firewalls	› Check Point – Palo Alto Networks
Web Application Firewalls	› F5
Remote Access	› Check Point – Palo Alto Networks – Pulse Secure – F5
Link/Loadbalancers	› F5
Strong Authentication	› Vasco
Network Automation	› Infoblox
Firewall Optimalisation	› Algosec
Proxy Servers	› Zscaler – Symantec
Mail AntiVirus/AntiSpam	› Cisco Ironport – Barracuda Networks
Threat Prevention	› Check Point – Palo Alto Networks
Anti-DDoS	› Akamai – Telenet – Check Point – F5
Mobile Security	› MobileIron
Endpoint protection	› SentinelOne – Check Point – Palo Alto Networks
Vulnerability scanning	› Rapid7

Onze securityhelpdesk heeft niet de typische ‘eerste lijn’. Klanten komen direct bij een gecertificeerde engineer terecht.

BJORN DESANDER
MANAGER SERVICE DESK SECURITY BIJ TELENET

04
Flexibiliteit op vlak van ondersteuning

Op vlak van ondersteuning bestaat er veel flexibiliteit voor de klanten van Telenet Security. “Ze kunnen kiezen of ze al dan niet ondersteuning willen en zo ja, op welk niveau. Ze kunnen het beheer zelfs aan ons uitbesteden”, zegt Brice Mees, Security Services Operations Manager bij Telenet.

Klanten die voor **Security Support** kiezen, hebben de keuze: tijdens de kantooruren of 24/7. “Als ze vragen of problemen hebben, kunnen ze onze specialisten rechtstreeks contacteren”, zegt Bjorn Desander, Manager Service Desk Security bij Telenet. “Onze securityhelpdesk heeft niet de typische ‘eerste lijn’. Klanten komen direct bij een gecertificeerde engineer terecht. Dat wordt niet alleen door de klanten zelf geapprecieerd, ook door de vendors. We zijn meer dan een brievenbus, we lossen de meeste incidenten zelf op, zonder de vendor erbij te betrekken.”

Steeds vaker vragen klanten om het beheer van hun IT-infrastructuur over te nemen. Brice Mees, Security Services Operations Manager bij Telenet: “Onze **Managed Security Services** zijn modulair opgebouwd: één standaard service en een ‘shopping list’ aan mogelijke extra services. Bij de standaard service houden we uw infrastructuur up-to-date en komt uw Service Manager driemaandelijks rapporteren. Gaat dat niet ver genoeg, dan kan u makkelijk extra services toevoegen. We beheren trouwens niet alleen uw infrastructuur, maar ook uw security policy. Wilt u zelf bepaalde aanpassingen aan uw policy kunnen uitvoeren, dan kan u voor Change Management kiezen. Wij zullen uw aanpassingen dan nakijken, zo kan u op beide oren slapen.”

IN DE PRAKTIJK | SECURITY SUPPORT EN MANAGED SECURITY

Bij Security Support voorzien wij u van technische ondersteuning en staan we in voor het licentiebeheer. Kiest u voor Managed Security, dan besteedt u het beheer, de monitoring en de optimalisering van uw beveiliging aan ons uit.

Security Support

Business Hours Support

- Telenet Security Desk als Point of Contact
- Weekdagen van 8.30 uur tot 17.30 uur

24/7 Support

- Uitbreiding op de Business Hours Support
- 24/7

Managed Security

STANDARD

Inbegrepen security services

MODULAR

Mogelijke extra security services

- ✓ Persoonlijke Service Manager
- ✓ Release Management
- ✓ Standard Monitoring
- ✓ Standard Service Management
- ✓ Standard Reporting

- \+ Change Management per technologie
- \+ IPS Policy Management per toestel
- \+ Premium Monitoring per toestel
- \+ Premium Reporting per toestel
- \+ Premium Service Management per klant

Al onze experts kunnen perfect meedenken met de business van de klant en hem naar een optimale beveiligingsomgeving begeleiden.

BRICE MEES
SECURITY SERVICES OPERATIONS MANAGER
BIJ TELENET

05
Sterke focus op de proactieve, adviserende rol

IT-beveiliging is heel kritisch, complex en uiterst evolutief. Om als organisatie met deze evolutie mee te zijn, kan u op periodieke basis een beroep doen op de security experts van Telenet Security.

Brice Mees: "Al onze experts hebben minstens 5 jaar ervaring in the field, waardoor ze perfect kunnen meedenken met de business van de klant en hem naar een optimale beveiligingsomgeving kunnen begeleiden. Expertise vinden we enorm belangrijk, daarom investeren we binnen het Security-team veel in opleidingen. Zo zijn onze experts altijd up-to-date qua kennis en certificeringen. Dat maakt trouwens ook dat we binnen ons team heel weinig verloop hebben, wat onze continuïteit naar klanten uiteraard ten goede komt."

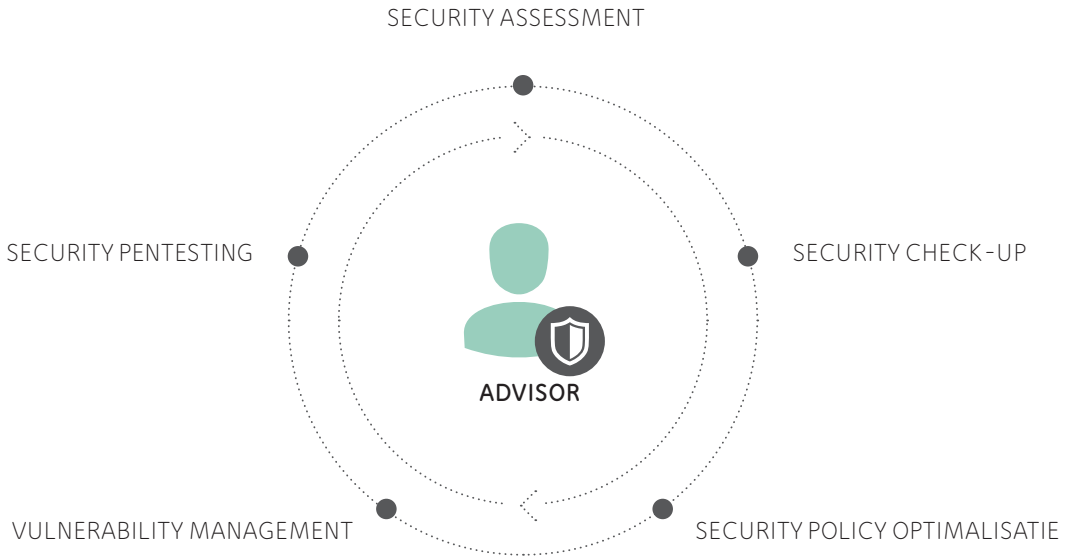
Brice ziet de Trusted Security Advisor als de centrale spil binnen de security lifecycle van de klant: "Hij zal bijvoorbeeld proactief nieuwe versies en functionaliteiten signaleren en advies geven over de huidige performantie, beheersbaarheid en beveiliging. Daarnaast kan hij ook helpen bij de coaching van specifieke profielen en change management, en de implementatie van grote veranderingen mee valideren."

IN DE PRAKTIJK | TRUSTED SECURITY ADVISOR

De Trusted Security Advisor is de centrale spil binnen uw security lifecycle. Hij kan perfect meedenken met uw business en zal u naar een optimale beveiligingsomgeving begeleiden.

U kan een beroep doen op security-experts, indien gewenst zelfs op periodieke basis.

- Betere afstemming van uw beveiligingsomgeving op de noden van uw bedrijf
- Sneller en adequater inspelen op snel veranderende beveiligingsuitdagingen
- Betere begeleiding en ondersteuning van uw eigen IT-beveiligingsteam



HOOFDSTUK 05

Hoe pakken **Colruyt, Rossel en Partena** het aan?

Telenet beschermt Colruyt Group tegen DDoS-aanvallen

Colruyt is steeds vaker het doelwit van DDoS-aanvallen. "Ik hoef je vast niet uit te leggen dat 20 minuten stilstand ons véél geld kost", zegt Wim Derijnck, Teammanager Network Solutions bij Colruyt. Daarom koos Colruyt voor het anti-DDoS-systeem van Telenet. "Door de data op hun netwerk te scrubben, kan Telenet DDoS-aanvallen onderscheiden van legitiem verkeer. Het anti-DDoS-systeem zuigt het malafide verkeer weg, waardoor ons netwerk gespaard blijft. De kost om ons met deze oplossing te beschermen, is slechts een fractie van de mogelijke opbrengst."

"De kost om ons met anti-DDoS te beschermen, is slechts een fractie van de mogelijke opbrengst."

WIM DERIJNCK
TEAMMANAGER NETWORK SOLUTIONS BIJ COLRUYT

Rossel zet zijn 'mediamorfose' in alle veiligheid voort

Vertrouwelijke informatie van journalisten, persoonlijke gegevens van lezers... Databeveiliging is een topprioriteit voor mediagroep Rossel. "Niemand mag ons systeem kunnen binnendringen", zegt David De Geyter, IT & Security Manager bij Rossel. "De oplossing die Telenet voorstelde, was dan ook meer dan 'zomaar een' firewall. Het was een hecht partnerschap. De kennis van Telenet is een enorme troef voor ons: ze voelen perfect onze behoeften, eisen en verwachtingen aan. Ze zijn even begaan met de beveiliging van onze gegevens als wijzelf."

"De beveiligingsoplossing van Telenet is meer dan 'zomaar een' firewall, het is een hecht partnerschap."

DAVID DE GEYTER
IT & SECURITY MANAGER BIJ ROSSEL

Partena kiest voor tweelaagsbeveiliging van Telenet

Bij Partena werken zo'n 1600 medewerkers dag in dag uit met confidentiële data. Voor de beveiliging vertrouwen ze op de combinatie van twee securitytechnologieën die Telenet voorstelde. Franky Goethals, Manager Infrastructure & Security bij Partena: "De technologieën vullen mekaar perfect aan en de inbegrepen web application firewall is ideaal voor onze webgebaseerde toepassingen. Om de nodige awareness te creëren, voerde Telenet trouwens gratis een Security Check-up uit. Dat heeft ons zeker geholpen om zo'n aanzienlijke investering te rechtvaardigen."

"Om de nodige awareness te creëren, voerde Telenet gratis een Security Check-up uit."

FRANKY GOETHALS
MANAGER INFRASTRUCTURE & SECURITY BIJ PARTENA

BENIEUWD NAAR ONZE ANDERE KLANTENVERHALEN?

Colruyt Group, Rossel en Partena zijn slechts een kleine greep uit onze tevreden securityklanten. Benieuwd naar wat andere klanten te vertellen hebben? U vindt alle klantenverhalen op onze website.

telenet.be/klantenverhalen

Meer info

telenet.be/security
0800 66 066

BUSINESS