DOSSIER SÉCURITÉ IT

Pourquoi votre entreprise est-elle aussi une cible et comment barrer la route aux pirates ?

BUSINESS

TABLE DES MATIÈRES

“Aujourd’hui, chaque aspect de votre infrastructure IT nécessite sa propre protection”

Jusqu’il y a quelques années, tout ce dont votre entreprise avait besoin se trouvait en local, au sein du réseau de l’entreprise. Aujourd’hui, on se tourne vers le cloud pour de plus en plus de fonctionnalités. Le modèle classique, selon lequel un pare-feu de nouvelle génération pouvait tout protéger, ne suffit plus.

Chaque partie de votre infrastructure IT nécessite sa propre solution : votre réseau et votre centre de données, mais aussi vos terminaux (smartphones, ordinateurs portables…), vos applications web (Office 365, Skype…), votre cloud, votre réseau IoT. Une protection efficace doit plus que jamais se composer de plusieurs couches.

La sécurisation des terminaux, des applications web, du cloud et de l’IoT n’est, bien sûr, pas neuve. Mais vu le contexte actuel, elle ne fait que gagner en importance. Au travers de ce dossier, nos spécialistes de la sécurisation espèrent vous en convaincre.

Martine Tempels
Senior Vice President
Telenet Business

7 tendances en matière de sécurité IT

01

Les menaces sont plus avancées

Les menaces auxquelles votre entreprise est confrontée gagnent en complexité. Prenez les logiciels malveillants : ils se modifient sans cesse, de sorte qu'ils peuvent échapper aux systèmes traditionnels destinés à les détecter. Un fait d'autant plus alarmant que les pirates consacrent de plus en plus de temps à leurs attaques, comme l'illustre le social engineering.

02

Le nombre d'attaques DDoS augmente

Autre tendance qui se dessine de plus en plus clairement : la multiplication des attaques DDoS. La nouveauté réside dans le changement de source : on utilise de plus en plus des appareils IoT (internet des objets) – insuffisamment protégés. Logique : plus les appareils connectés à internet sont nombreux, plus les pirates peuvent les utiliser.

03

La sécurité adopte l'intelligence artificielle

Les solutions de sécurisation gagnent en intelligence. Elles utilisent de plus en plus des techniques telles que l'apprentissage automatique et profond. Elles sont en mesure de collecter des données, d'en tirer des leçons et, dès lors, de s'améliorer constamment. Conclusion : la gestion des menaces sur la base de l'intelligence artificielle n'est plus une lointaine utopie.

04

La prévention seule ne suffit pas

La sécurité IT mettait autrefois l'accent sur la prévention. Une approche qui ne suffit plus vu la complexité croissante des attaques. Aujourd'hui, on accorde de plus en plus d'attention à la détection. Les systèmes de détection identifient les comportements qui s'écartent du comportement normal et interviennent en conséquence.

05

La demande de services gérés augmente

Les entreprises belges se tournent de plus en plus vers le cloud public pour leur infrastructure et leurs applications. Ces modèles hybrides complexifient fortement la sécurisation. Les entreprises se rendent compte qu'il est devenu compliqué de disposer de l'expertise nécessaire en interne – et de la conserver. Elles font, dès lors, de plus en plus souvent appel à un spécialiste pour gérer leur infrastructure.

06

Le périmètre de sécurité ne suffit plus

Les tendances telles que le télétravail gomment de plus en plus le lien avec le réseau de l'entreprise. La sécurisation doit donc changer de cible : là où il suffisait autrefois de sécuriser le périmètre – l'enveloppe IT –, il faut désormais aussi protéger les terminaux et les applications web. À l'image d'un oignon, la meilleure des protections se compose de diverses couches.

07

La sécurité IT devient la priorité de tous

Alors que les actifs sont de plus en plus souvent digitaux, la gouvernance, la gestion du risque et la conformité gagnent en importance. L'emblématique triade CIA (confidentialité, intégrité et disponibilité) de la business continuity doit être placée en tête de liste des priorités des entreprises. A fortiori au vu de l'entrée en vigueur du RGPD et de l'importance croissante de la politique de sécurité.

01

La sécurité IT : pour les entreprises, il est moins une

De plus en plus d'actifs digitaux

Des données des clients aux résultats R&D, en passant par les informations salariales… Les entreprises collectent et traitent une foule de données sensibles au format digital. Elles sont, par conséquent, plus vulnérables que jamais. Un incident IT peut avoir un impact considérable : perte de données, détérioration de l'image, voire immobilisation totale.

Une nouvelle manière de travailler

Les travailleurs modernes sont en ligne 24 h/24, utilisent les dernières technologies et attendent la même convivialité dans la sphère professionnelle. « À défaut, ils apportent leur appareil personnel ou utilisent leurs propres applications », explique Eric De Smedt, Security Manager chez Telenet. « Bien que le BYOD (Bring Your Own Device) et le shadow IT ne soient pas neufs, les managers IT restent confrontés à des défis de taille. Ils doivent sécuriser l'ensemble des données de l'entreprise tout en instaurant un équilibre avec la convivialité. »

LE SHADOW IT, LA LIGNE DE DÉSIR DE L'IT

Le shadow IT désigne l'ensemble du matériel et des logiciels mis en œuvre au sein d'une entreprise **sans que le département IT les contrôle ou en ait connaissance.** Il constitue la ligne de désir de l'infrastructure IT : les travailleurs préfèrent aller au plus court qu'emprunter les voies officielles sécurisées si celles-ci sont plus escarpées.

> Le grand défi des managers IT actuels ? Sécuriser l'ensemble des données de l'entreprise, tout un instaurant un équilibre avec la convivialité.
>
> ERIC DE SMEDT
> CYBER SECURITY MANAGER CHEZ TELENET

> De nombreuses entreprises pensent, à tort, qu'elles sont automatiquement protégées dans le cloud public. Or c'est la responsabilité de tous.

ERIC DE SMEDT
CYBER SECURITY MANAGER CHEZ TELENET

L'infrastructure IT dans le cloud public

De plus en plus d'entreprises se tournent vers le cloud public pour leur infrastructure et/ou leurs applications. Selon Eric, une idée fausse circule à ce sujet : « De nombreuses entreprises pensent qu'elles sont automatiquement protégées dans le cloud public. Ce n'est vrai que dans une certaine mesure. Les fournisseurs de services cloud ne protègent pas les applications ou l'accès à leurs serveurs. Or ces serveurs sont totalement ouverts sur internet, et accessibles à tous. La sécurisation d'un cloud public relève, dès lors, de la responsabilité de tous. En tant que client, vous devez déterminer vous-même le dispositif de sécurisation que vous activez et le prix que vous êtes prêt à payer. »

LES 3 COUCHES DU **CLOUD PUBLIC**

IaaS:
Infrastructure as a Service, par exemple le stockage des données et la puissance de calcul

PaaS:
Platform as a Service, par exemple une solution de base de données

SaaS:
Software as a Service, par exemple Office 365

La vulnérabilité de l'internet des objets

De plus en plus d'appareils sont connectés à internet : des caméras IP aux capteurs qui analysent la qualité de l'air, en passant par les capteurs d'aide au stationnement. Il y a néanmoins un problème : la sécurisation n'était pas une priorité lors du développement de nombreux appareils IoT. Eric : « Les mots de passe par défaut de bon nombre de ces appareils circulent en ligne. Les entreprises qui ne modifient pas les mots de passe sont des cibles faciles. Si le piratage d'un capteur d'aide au stationnement ne représente, certes, pas un danger, sachez qu'une seule commande permet au pirate d'intercepter l'ensemble du trafic réseau. »

L'évolution constante des menaces

« Tant que ça marche, je ne touche à rien », se disent les managers IT. « Mais ce n'est pas la bonne approche », insiste Eric. « En matière de sécurité IT, on n'en a jamais fini. Il ne suffit pas de mettre en place une infrastructure de sécurité : il faut l'actualiser constamment. Des failles sont découvertes régulièrement, que les WannaCry, Spectre, Meltdown et autres logiciels malveillants se font un plaisir d'exploiter. La gestion des correctifs constitue donc un aspect crucial de la sécurité IT. »

LORGNER VOS VOISINS

Certains sites web permettent de s'inviter au cœur des entreprises belges. Leurs caméras de surveillance IP ont pu être piratées, car ces entreprises n'avaient **jamais modifié le mot de passe par défaut.** Les criminels peuvent même aller encore plus loin et désactiver les caméras au moment de l'effraction.

CYBER SECURITY COALITION

Le monde universitaire, les institutions publiques et les entreprises partagent leurs expériences et leurs incidents en matière de sécurité au sein de la Cyber Security Coalition. L'objectif va au-delà des secteurs et de la concurrence : les membres veulent apprendre les uns des autres afin de pouvoir agir plus efficacement contre la cybercriminalité.

Le RGPD entrera en vigueur le 25 mai 2018. Toute entreprise qui traite les données de citoyens européens devra avoir une politique documentée en matière de vie privée et de sécurité.

ISABELLE GHISLAIN
PRIVACY MANAGER CHEZ TELENET

Un cadre juridique plus strict

Que faire en cas de piratage ? Qu'advient-il si un de vos travailleurs laisse échapper des informations ? Êtes-vous responsable ? Risquez-vous une amende ? Isabelle Ghislain, Privacy Manager chez Telenet, lève le voile sur le volet juridique.

Législation belge

« Nous pouvons déduire du droit de la responsabilité que chaque entreprise doit appliquer une politique de protection adéquate », explique Isabelle. « Avec la **Cyber Security Strategy,** le gouvernement belge tend à mettre en place une approche globale de la sécurité digitale. Mais il existe peu d'informations sur la manière d'implémenter concrètement la stratégie. »

Par ailleurs, il existe d'autres lois. « Les exploitants d'une infrastructure critique sont soumis à la **loi pour les infrastructures critiques.** Et dès que les entreprises traitent des données à caractère personnel, la **loi relative à la protection de la vie privée** s'applique. Elle définit la manière de traiter ces données et les mesures à prendre pour les protéger suffisamment. »

Législation européenne

Le **Règlement général sur la protection des données (RGPD)** entrera en vigueur le 25 mai 2018. « Il s'appliquera à toutes les entreprises qui traitent les données de citoyens européens », précise Isabelle. « Le RGPD les obligera notamment à dresser un inventaire de leurs données et à protéger ces données en prenant les mesures techniques et organisationnelles adéquates. Les entreprises devront aussi avoir une politique documentée en matière de vie privée et de sécurité. Et dans la mesure où les entreprises seront tenues de communiquer à leur commission locale de protection de la vie privée – et, dans certains cas, aux personnes concernées – tout incident relatif à la protection de la vie privée, elles devront aussi élaborer des procédures ad hoc pour déceler et signaler les fuites de données. »

Outre le RGPD, citons également le **Network and Information Security Directive (NISD).** Isabelle : « Cette directive vise à combler le fossé entre les États membres de l'UE à l'aide d'une approche concrète et uniforme en matière de cybersécurité. La NISD doit encore être transposée en droit belge. »

LE **RGPD** EN QUELQUES MOTS

Sanctions possibles

La Commission Vie privée aura le droit d'imposer des **amendes** susceptibles d'être très salées, selon la nature de l'incident : jusqu'à 4 % du chiffre d'affaires mondial ou 20 millions d'euros, en fonction du montant le plus élevé des deux.

Recommandations clés

Vu le montant élevé des amendes – et les dégâts potentiels en termes d'image –, les entreprises ont tout intérêt à se conformer au RGPD. Voici donc quelques recommandations à ne pas perdre de vue.

- Dressez un **inventaire** de vos données et expliquez pourquoi et comment vous traitez les données.
- Rédigez un **avis de confidentialité** clair pour informer les personnes dont vous conservez les données.
- Prenez des **mesures de sécurité** pour protéger vos données : cryptage, pseudonymisation…
- Élaborez une **politique claire en matière de vie privée et de sécurité** et dispensez une formation à vos collaborateurs.
- Mettez au point des procédures destinées à **identifier les fuites de données** et à les signaler, par exemple des audits réguliers.

LA SÉCURITÉ IT NE FAIT QUE GAGNER EN IMPORTANCE

Ce contexte professionnel souligne clairement l'importance croissante de la sécurité IT. Mieux vaut aussi savoir d'où proviennent les menaces potentielles.

Lisez le chapitre 2
pour en savoir plus à ce propos.

02

Les pirates visent les entreprises de diverses manières

01

Logiciels malveillants

Un logiciel malveillant est un logiciel qui vise à accéder à des systèmes informatiques et à les perturber ou à dérober des informations confidentielles. Il prend l'apparence d'un programme ou d'un fichier ordinaire, mais renferme des fonctions cachées qui permettent aux pirates d'accéder par l'extérieur à l'ordinateur contaminé. Détail surprenant : il se modifie sans cesse pour échapper aux systèmes de sécurisation traditionnels.

02

Rançongiciels

Un rançongiciel est un outil de chantage qui utilise des logiciels malveillants. Il chiffre l'ordinateur contaminé ou les données qu'il contient et demande à l'utilisateur de verser une rançon pour libérer l'ordinateur ou les données. L'utilisateur ne paie pas dans les délais ? La clé de décryptage n'est pas libérée et l'ordinateur ou les données restent inutilisables. Épargnez-vous bien des tracas et sauvegardez régulièrement vos données (précieuses).

WANNACRY

La plus vaste attaque par rançongiciel a eu lieu le 12 mai 2017. WannaCry est parvenu à bloquer plus de 230.000 ordinateurs Windows dans 150 pays. Parmi les victimes : le National Health Service britannique, l'entreprise de transport FedEx et l'entreprise ferroviaire allemande Deutsche Bahn.

230.000

PLUS DE 230.000 ORDINATEURS ONT ÉTÉ CONTAMINÉS

300 $

300 $ DE RANÇON ÉTAIENT DEMANDÉS PAR ORDINATEUR CONTAMINÉ

98%

98 % DES ORDINATEURS CONTAMINÉS TOURNAIENT SOUS WINDOWS

59

LE PATCH CONTRE LA FAILLE ÉTAIT DÉJÀ DISPONIBLE 59 JOURS AVANT L'ATTAQUE

03

Attaques DDoS

Une attaque DDoS (Distributed Denial of Service) rend indisponible l'infrastructure internet d'une entreprise – les sites web, les serveurs de messagerie, etc. Comme les années précédentes, le nombre, la portée et la complexité des attaques DDoS ont encore augmenté cette année. La nouveauté réside dans la source des attaques : les appareils IoT sont de plus en plus utilisés pour lancer des attaques.

TROIS TYPES **D'ATTAQUES DDOS**

01

D'attaque volumétrique

En cas d'attaque volumétrique, le pirate inonde votre infrastructure d'un énorme flux de données, de sorte à épuiser totalement la bande passante disponible.

02

D'attaque applicative

En cas d'attaque applicative, le pirate vise une application ou un serveur en particulier, qui n'est pas en mesure de traiter la quantité de données et tombe en panne.

03

D'attaque protocolaire

En cas d'attaque protocolaire, le pirate envoie des paquets de réseau qui ne répondent pas aux normes d'internet et font ralentir, voire planter les serveurs.

DDoS, l'arme (pas si) secrète des joueurs

Le moindre raté peut suffire. C'est pourquoi les joueurs se lancent de plus en plus souvent des attaques DDoS. Cela n'a rien d'étonnant : la location d'un botnet pour un quart d'heure ne coûte que 20 dollars.

04

Botnets

Partout dans le monde, des ordinateurs et d'autres appareils sont contaminés à l'insu de leurs utilisateurs. Ensemble, ils forment un botnet : un réseau pouvant être piloté à partir d'un point de commande central, par exemple pour mener une attaque DDoS. Les ordinateurs et appareils de botnet nuisent également à l'entreprise, car ils utilisent beaucoup de bande passante et ralentissent considérablement le réseau.

05

Erreurs de programmation

On détecte constamment des failles dans les logiciels. Toute personne ayant connaissance de ces failles peut les exploiter. C'est pourquoi le fournisseur développe et commercialise au plus vite un correctif qui vise à améliorer le logiciel. Mais tant que les entreprises n'ont pas installé ce patch, elles restent vulnérables. Cela n'a pas échappé aux pirates : leurs attaques ciblent de plus en plus souvent les applications web.

MIRAI, LE BOTNET IOT

L'un des pires botnets ayant jamais existé était composé d'appareils IoT. Mirai a pris le contrôle de caméras IP et d'autres appareils « intelligents » simplement en utilisant **les mots de passe par défaut.** En lançant une attaque ciblée sur le service DNS Dyn, Mirai est parvenu à paralyser des parties de l'internet, notamment Twitter et Spotify.

HAUSSE DE

69 %

DES ATTAQUES VISANT DES APPLICATIONS WEB

Selon une étude d'Akamai, le nombre d'attaques visant des applications web a augmenté de 69 % entre le 3e trimestre 2016 et le 3e trimestre 2017.

D'après l'Open Web Application Survey Project (OWASP), les risques les plus courants sont des erreurs d'injection, des échecs d'authentification et des fuites de données.

06

Trafic SSL

Une foule d'applications et de sites web utilisent le protocole de cryptage SSL afin d'empêcher des tiers d'intercepter leur trafic. Ce certificat SSL donne aux entreprises et aux internautes l'impression que la con-nexion est sécurisée. Pourtant, les pirates sont de plus en plus en mesure de contourner cette protection SSL – par exemple à l'aide du principe « man-in-the-middle ». Certains dissimulent même leur logiciel malveillant dans le trafic SSL.

07

Shadow IT

Bien qu'il soit en grande partie sans danger et qu'il stimule la productivité et l'innovation dans de nom-breux cas, le shadow IT s'accompagne d'une multitude d'inconvénients. Il est particulièrement complexe d'en garantir la continuité et la sécurité. Les fuites d'infor-mations résultent souvent d'initiatives que le manager IT n'avait pas approuvées ou dont il n'avait même pas connaissance.

08

Prise de conscience insuffisante

La sécurité IT n'a rien de simple au sein d'une en-treprise, tant pour le niveau C – budget insuffisant, absence de politique uniforme – que pour les travail-leurs. Tous peuvent involontairement occasionner des risques en matière de sécurité (faire entrer un logiciel malveillant en utilisant une clé USB infectée, par exemple). La sensibilisation, à tous les niveaux, est donc la première mesure à déployer pour mettre correctement la sécurité IT en pratique.

MAN-IN-THE-MIDDLE

Un internaute qui saisit une adresse web va généralement se rendre sur l'adresse http. **Le pirate intervient juste avant la sécurisation de la connexion.** Au lieu d'établir une connexion sécurisée avec le serveur du site web, l'internaute se connecte au serveur web du pirate.

FAITES ATTENTION AU **TRAFIC SSL**

Peu d'entreprises décryptent leur trafic SSL pour l'analyser dans le tunnel SSL. Elles considèrent trop souvent le trafic SSL comme sécurisé. Elles n'appliquent alors leurs **politiques que sur le trafic non SSL.**

09

Phishing

L'humain est et reste le maillon faible dans la chaîne de sécurité IT. Les e-mails de phishing sont souvent si mal rédigés qu'il apparaît clairement qu'il s'agit de falsifications. Mais ils portent tout de même leurs fruits. Ils sont, en effet, envoyés à des millions de personnes et il y aura toujours des internautes pour cliquer sur les liens sans se poser de questions.

10

Spear phishing

Le spear phishing est la déclinaison ciblée du phishing : il s'agit de falsifications parfaites ciblant des personnes spécifiques. Elles sont tellement bien réalisées qu'on n'y voit pratiquement que du feu. Cette technique prend la forme d'un e-mail qui semble provenir d'un collègue, d'une entreprise avec laquelle vous collaborez ou d'un candidat.

VOUS TROUVEREZ MON CV **CI-JOINT**

Les fichiers PDF sont le moyen par excellence de dissimuler une attaque de spear phishing. Ils sont omniprésents, semblent inoffensifs, mais recèlent une foule **de possibilités de dissimuler un code.** Un pirate n'a parfois rien d'autre à faire que d'envoyer un « CV » au format PDF. Si un collaborateur RH ouvre le PDF, le logiciel malveillant est installé et la voie est libre pour le pirate.

LE DANGER EST PARTOUT

Les pirates font preuve de plus en plus d'ingéniosité. Les menaces et les attaques viennent de tous les côtés. Mieux vaut donc protéger votre entreprise de plusieurs manières.

Découvrez tous les détails dans le chapitre 3.

03

Les attaques plus intelligentes nécessitent de nouvelles solutions de sécurisation

Verrouiller les portes et les fenêtres

« Rien ne sert de verrouiller votre porte d'entrée si la porte de derrière et les fenêtres sont grandes ouvertes. » La métaphore de Glyn Jones, Service Manager chez Telenet, ne pourrait pas être plus éloquente. Aujourd'hui, plus que jamais, la sécurité IT doit se composer de plusieurs couches.
Glyn : « Il ne suffit plus de sécuriser le périmètre. Toutes les composantes – réseau, centre de données, terminaux, applications web, cloud, réseau IoT – nécessitent une protection spécifique. C'est évidemment vous qui décidez jusqu'où aller. C'est à l'entreprise de mettre en balance l'investissement qu'elle souhaite/peut consentir et les risques qu'elle est prête à courir. »

Ce n'est pas une science exacte

« Les entreprises peuvent implémenter une bonne sécurisation à chaque niveau, mais ne pas parvenir à élaborer de bonnes politiques », met en garde Glyn. « Les entreprises doivent évaluer le rapport risque/bénéfice. Vous pouvez configurer un pare-feu de manière très rigoureuse, mais perdre en productivité. Ou votre politique peut être ouverte à tel point que vous ramenez la fonction de votre pare-feu à celle d'un routeur amélioré. » Telenet vous aide, certes, dans la définition et l'optimisation des politiques, mais c'est toujours le client qui en assume la responsabilité finale. « Nous faisons office de serrurier : nous pouvons poser une serrure efficace, mais c'est le client qui choisit le nombre de clés qu'il fait reproduire », conclut Glyn.

Vous trouverez, à la page suivante, un graphique qui compare l'ancienne approche de la sécurité IT et la nouvelle vision, plus moderne.

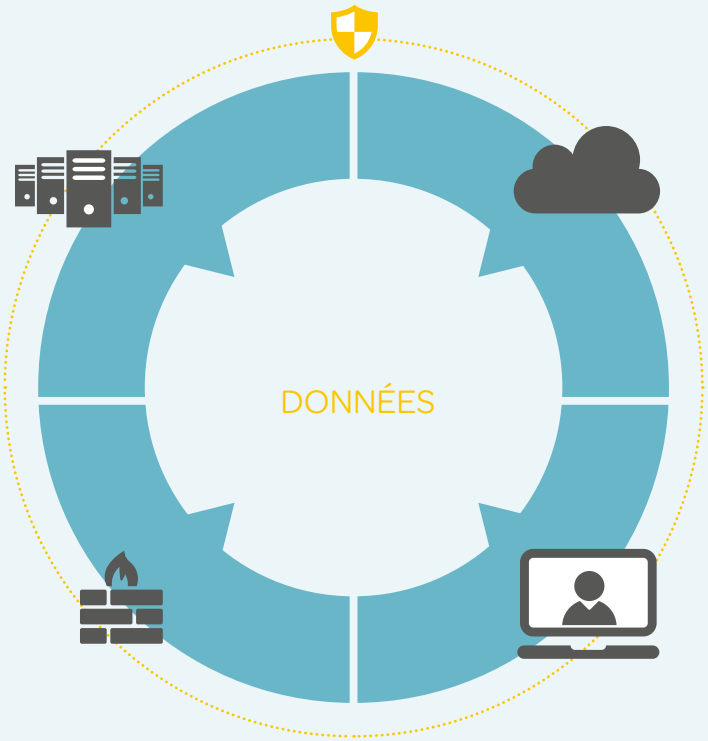
« Le réseau, le centre de données, les terminaux, les applications web, le cloud et l'IoT nécessitent une protection spécifique. »

GLYN JONES
SERVICE MANAGER CHEZ TELENET

AVANT

LA SÉCURITÉ IT : COMPARABLE À UN **BONBON**

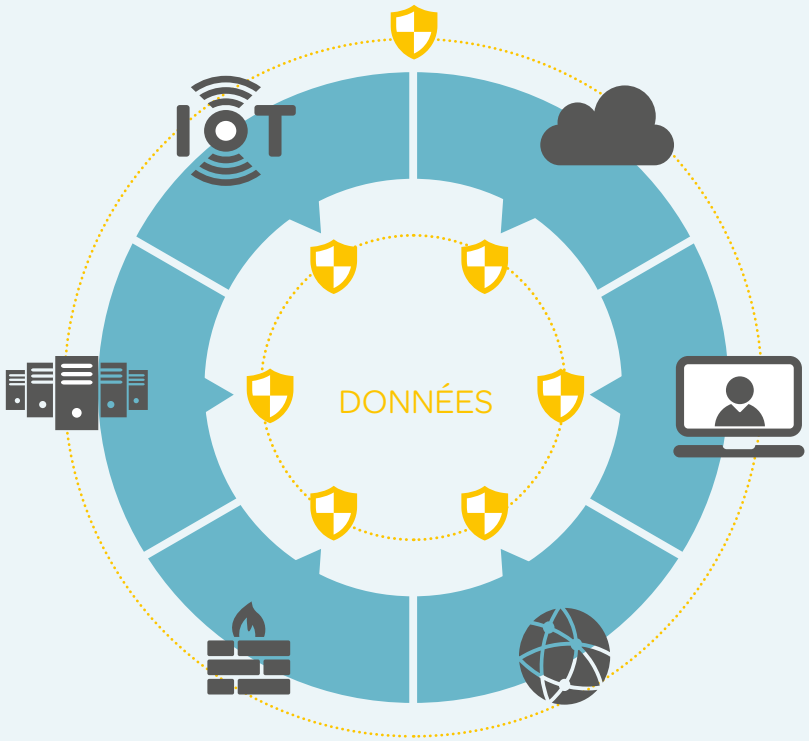
Dur à l'extérieur et mou à l'intérieur



AUJOURD'HUI

LA SÉCURITÉ IT : COMPARABLE À UN **OIGNON**

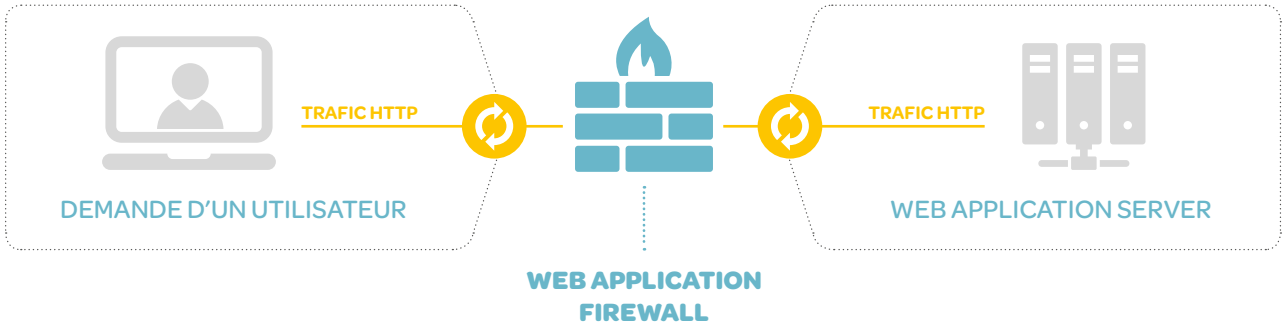
Elle présente plusieurs couches



Sécurisation des applications web

La sécurisation des applications web n'est pas neuve. « Mais à l'heure où les entreprises en utilisent de plus en plus, elle gagne en importance », explique Kris Bogaerts, Principal Security Consultant chez Telenet. Il envisage la sécurisation des applications web comme une combinaison de mesures. « Pour commencer, un web application firewall (WAF) peut vous éviter bien des ennuis. Il filtre le trafic http au départ et à destination de l'application. Il procède sur la base de signatures. S'il décèle une tentative d'exploitation d'une faille, il la corrige virtuellement. Ce processus va généralement plus vite que si vous corrigiez ou modifiiez l'application web vous-même. »

Un WAF présente l'avantage de pouvoir appliquer des profils de sécurité. Kris : « Des profils adaptés vous permettent de définir différentes mesures pour différentes applications web. C'est essentiel, car il n'y a pas deux applications identiques. » La réputation IP est un autre élément clé. Kris : « De nombreuses attaques sont menées par des botnets et des organisations criminelles. Sur la base d'une liste noire, vous pouvez bloquer automatiquement des adresses IP qui ont mauvaise réputation, avant même qu'elles aient l'occasion de tenter quoi que ce soit. » Enfin, Kris insiste sur l'importance de tester constamment les applications : « Les applications web évoluent, du nouveau code vient s'ajouter en permanence. Il faut donc tester et évaluer régulièrement les applications. »



Si un web application firewall peut vous éviter bien des ennuis, la sécurisation des applications web relève malgré tout d'une combinaison de mesures.

KRIS BOGAERTS
PRINCIPAL SECURITY CONSULTANT CHEZ TELENET

La sécurisation des terminaux s'effectue désormais dans le cloud et comprend trois grands volets : prevention, detection et response.

WILLEM JANSSENS
SECURITY CONSULTANT CHEZ TELENET

Protection des terminaux

Quand on évoque la protection des terminaux, on pense aux ordinateurs de bureau et aux portables classiques. Willem Janssens, Security Consultant chez Telenet, estime néanmoins que la sécurisation des terminaux va beaucoup plus loin : des serveurs aux appareils IoT, en passant par les smartphones et les tablettes. Willem : « La sécurisation des terminaux a fortement évolué, ces deux dernières années. Là où l'administration s'effectuait autrefois au départ d'un serveur local, elle est aujourd'hui basée dans le cloud. Et là où on se concentrait presque uniquement sur la prévention, on accorde désormais de l'attention à la prévention, à la détection et à la récupération. »

UNE NOUVELLE APPROCHE, **POUR PLUS D'AVANTAGES**

SÉCURISATION CLASSIQUE
SERVEUR LOCAL

SÉCURISATION MODERNE
BASÉE DANS LE CLOUD

La sécurisation classique des terminaux était gérée au départ d'un serveur local. Aujourd'hui, tout s'effectue depuis une plateforme basée dans le cloud. Ce changement présente plusieurs avantages : vous ne devez **plus assurer la maintenance** d'un serveur et vous conservez un niveau de protection maximal, même si le terminal se trouve à l'extérieur du réseau de l'entreprise. Là où on se concentrait autrefois essentiellement sur Windows, les nouvelles technologies sont aussi capables de **protéger les systèmes d'exploitation macOS et Linux.** Vous pouvez, en outre, surveiller tous vos terminaux sur **un tableau de bord clair.**

EN DÉTAIL : LES **3 VOLETS** DE LA **SÉCURISATION DES TERMINAUX** À L'HEURE ACTUELLE

PREVENTION

BLOQUER LES LOGICIELS MALVEILLANTS

Les solutions de sécurisation des terminaux utilisaient autrefois des signatures pour bloquer les logiciels malveillants. Elles reposent aujourd'hui sur la **modélisation prédictive.** Des dizaines de milliers de caractéristiques sont compilées dans un modèle prédictif sur la base de l'apprentissage automatique. Ce modèle compare chaque fichier aux caractéristiques et connaît les mauvaises combinaisons de caractéristiques. Il est donc en mesure de reconnaître et de bloquer le logiciel malveillant, **même s'il ne l'a jamais rencontré auparavant.**

DETECTION

BLOQUER LES CAUSES DES COMPORTEMENTS ANORMAUX

Les logiciels malveillants sont de plus en plus sophistiqués. Même avec un modèle prédictif, les solutions de sécurisation des terminaux ne peuvent pas tout régler. Il faudrait qu'elles puissent aussi **détecter les attaques** pour lesquelles aucune prévention n'était possible. Pour ce faire, elles examinent le comportement des terminaux : si un appareil présente un **comportement anormal,** la solution cherche et bloque la cause. Vu la complexité actuelle, la couche de détection a considérablement gagné en importance ces dernières années.

RESPONSE

PROCÉDER À UNE ANALYSE ET UN NETTOYAGE AUTOMATIQUES

Lorsque la solution de sécurisation des terminaux a arrêté un logiciel malveillant, vous voulez forcément connaître tous les tenants et aboutissants et **réparer les éventuels dommages.** Il se peut qu'un logiciel malveillant ait placé des scripts sur le terminal ou qu'un rançongiciel ait chiffré des fichiers. Les solutions actuelles de sécurisation des terminaux permettent de supprimer, en quelques clics, toutes les modifications apportées par les logiciels malveillants. Vous pouvez même réparer les dommages causés à vos données par le chiffrement.

En plus de modifier l'infrastructure IT typique, le cloud a un impact sur la méthode de sécurisation.

SERGE EGO
SECURITY MANAGER CHEZ TELENET

Sécurisation du cloud

De plus en plus d'entreprises se tournent vers le cloud. « Alors qu'elles privilégiaient auparavant un cloud privé, elles s'orientent désormais vers un cloud public », précise Serge Ego, Security Manager chez Telenet. Résultat : un changement de l'infrastructure IT typique, mais aussi de la méthode de sécurisation. Serge : « On ne peut pas mettre en place de pare-feu physiques dans un cloud public. C'est pourquoi nous associons des techniques de virtualisation et de segmentation existantes à de nouvelles techniques telles que les CASB. Ces Cloud Access Security Brokers constituent des solutions SaaS idéales. »

Techniques de virtualisation

La virtualisation dans les centres de données physiques ne date bien sûr pas d'hier. Nous utilisons désormais aussi les techniques destinées à contrôler le trafic dans des environnements virtuels pour sécuriser l'accès aux applications publiques basées dans le cloud.

Segmentation

Tout comme en présence d'un cloud privé, la communication de votre réseau local vers le cloud public doit être extrêmement bien protégée, par exemple via un chiffrement. La segmentation reste essentielle. Elle empêche les pirates d'accéder aux différents segments de votre infrastructure IT et fait en sorte qu'une attaque ne contamine pas l'ensemble de votre environnement. Le Software Defined Networking vous permet, en outre, de tout automatiser.

Gestion des identités

Les Cloud Access Security Brokers, ou CASB, contrôl-ent et analysent le contenu du trafic et le comportement de vos collaborateurs dans le cloud. En cartographiant le trafic cloud, ils contribuent à lutter contre l'usurpation d'identité. Les solutions d'authentification intelligente sécurisent, en outre, l'accès de manière conviviale.

SECURITY AS A SERVICE

LA SÉCURISATION AU DÉPART DU CLOUD

Nous sommes en pleine évolution vers le cloud. La sécurité IT s'effectuera, elle aussi, de plus en plus par ce biais. « Le client n'a plus besoin d'exécuter de logiciels de sécurité en local », explique Serge. « L'ensemble du matériel est chez le fournisseur de réseau, le filtrage s'effectue sur son backbone. Il surveille constamment le trafic au départ, à destination et au sein de vos plateformes, systèmes, réseaux, appareils et applications. Vous obtenez un aperçu en temps réel des menaces et des éventuelles attaques, mais vous ne devez pas intervenir vous-même. » La SaaS offre un modèle particulièrement intéressant aux PME. Serge : « Elles peuvent utiliser leurs applications en toute sécurité sans se préoccuper de la sécurisation. Qui plus est, Telenet peut facilement proposer une solution complète, connectivité comprise. Nous pouvons même établir une connexion privée vers votre (vos) fournisseur(s) de cloud public, totalement dissociée de l'internet public de nos autres clients. »

SECURITY AS A SERVICE : TOUR D'HORIZON **DES AVANTAGES**

- Vous avez besoin de **moins de connaissances techniques** en interne.
- Vous disposez d'un **tableau de bord** pour tout suivre et analyser.
- Vous avez le choix parmi **les meilleurs fournisseurs de sécurité** du marché.

> La SaaS est particulièrement intéressante pour les PME. Celles-ci peuvent utiliser leurs applications en toute sécurité sans se préoccuper de la sécurisation.

SERGE EGO
SECURITY MANAGER CHEZ TELENET

La segmentation du réseau en sections cantonne les risques et les effets d'une attaque à une seule section.

PATRICK LECLUYSE
MANAGER PROFESSIONAL SERVICES CHEZ TELENET

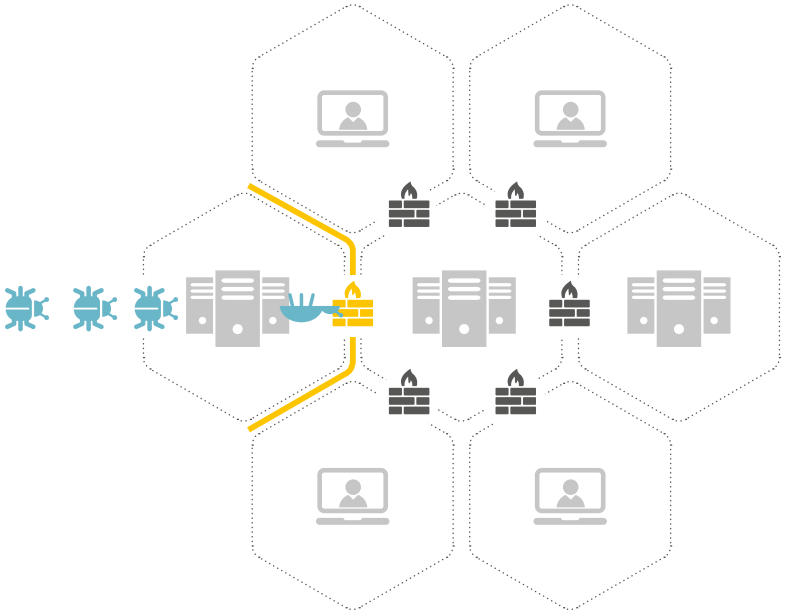
Sécurisation du réseau et du centre de données

Réseaux

En raison de leur complexité accrue, les réseaux sont beaucoup plus vulnérables qu'avant. « La segmentation du réseau apporte une réponse à ce défi », remarque Patrick Lecluyse, Manager Professional Services chez Telenet. « Elle divise le réseau en plusieurs sections. Les liaisons entre ces différentes sections sont contrôlées par le biais d'un pare-feu. Ainsi, les risques et les effets d'une attaque sur le réseau se limitent à une seule section et non à l'ensemble du réseau. »

Centres de données

Dans les centres de données, on surveillait et on sécurisait autrefois surtout le trafic nord-sud – le trafic entre les clients et le serveur. Maintenant que le trafic entre les serveurs gagne en importance, nous devons imposer une politique afférente. Patrick : « Dans le cadre de ce que l'on appelle le trafic ouest-est, il importe de définir précisément ce qui est autorisé et ce qui ne l'est pas. Outre un pare-feu physique, vous avez aussi besoin de pare-feu au sein de l'environnement virtualisé pour appliquer une politique entre serveurs. »



Sécurisation de l'internet des objets

Sécuriser les appareils IoT n'est pas une sinécure. Bart Van den Branden, Business Development Manager IoT chez Telenet : « Comment obtenir des mises à jour de plusieurs Mb sur un appareil qui a justement été conçu pour utiliser un minimum de bande passante – quelques Kb tout au plus ? Ou comment chiffrer des données sur un appareil censé consommer le moins possible de batterie alors que le chiffrement nécessite une puissance de calcul considérable ? »

« La sécurisation IoT comporte deux volets », poursuit Bart. « Nous pouvons, d'une part, **aider les entreprises qui développent des applications IoT.** En collaboration avec nos partenaires, nous prenons alors en charge la conception et l'implémentation d'une plateforme IoT sécurisée : celle avec laquelle les appareils IoT communiquent. Nous réfléchissons à la manière de sécuriser le firmware et les appareils IoT, nous participons au codage et nous nous demandons comment crypter et protéger les données dans le cloud. »

« Nous pouvons, d'autre part, **aider les utilisateurs de l'internet des objets** », poursuit Bart. « Nous ne pouvons évidemment pas purement et simplement modifier le firmware existant, mais nous pouvons contribuer à limiter les risques. Pensez à la segmentation, qui consiste à séparer le réseau IoT du reste du réseau. Nous pouvons aussi procéder à des tests d'intrusion et passer les protocoles IoT au crible. De quoi identifier les problèmes potentiels. L'application est mal sécurisée ? Il incombe alors à l'utilisateur de choisir de continuer à l'utiliser ou non. Nous donnons aussi des conseils lors du choix d'une nouvelle application 100 % sûre. »

> Nous ne pouvons évidemment pas purement et simplement modifier le firmware existant, mais nous pouvons contribuer à limiter les risques.

BART VAN DEN BRANDEN
BUSINESS DEVELOPMENT MANAGER IOT CHEZ TELENET

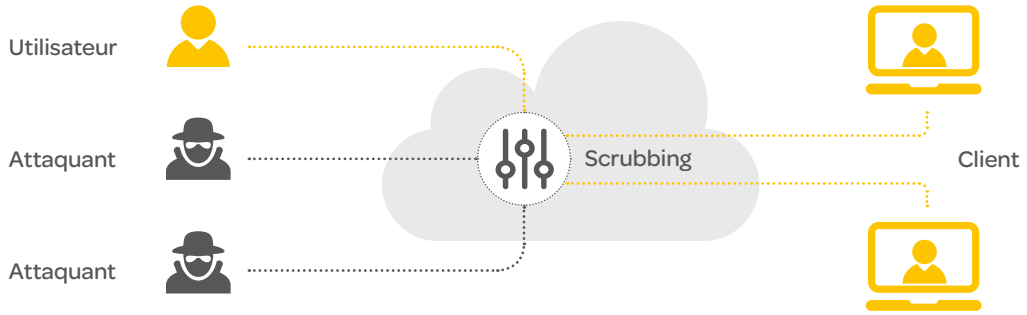
À présent que les appareils IoT sont ajoutés aux botnets, la protection contre les attaques volumétriques gagne en importance.

NICO VANDEVOORT
SECURITY PRESALES CONSULTANT CHEZ TELENET

Sécurisation DDoS

Les attaques DDoS peuvent miner la position des entreprises à différents niveaux : en envoyant un flux important de données vers leur infrastructure, en ciblant des applications spécifiques ou en envoyant des paquets de réseau malveillants. « Nous conseillons donc aux entreprises de se prémunir contre ces trois types d'attaques », explique Nico Vandevoort, Security Pre-sales Consultant chez Telenet.

Il existe plusieurs solutions pour contrer les attaques DDoS : des solutions « sur site » aux solutions « dans le cloud ». Nico : « Alors qu'une solution sur site protégera les entreprises des attaques applicatives et protocolaires, une solution anti-DDoS sur notre connectivité et dans le cloud préviendra les attaques volumétriques. Maintenant que les appareils IoT sont ajoutés aux botnets, la protection contre les attaques volumétriques gagne particulièrement en importance. La solution dans le cloud peut, par exemple, traiter les attaques DDoS jusqu'à 4,5 Tbps. »



ANTI-DDOS

ANTI-DDOS SUR NOTRE PROPRE CONNECTIVITÉ

Pour mieux vous protéger des attaques volumétriques, nous avons lancé notre propre solution anti-DDoS. Les attaques sont typiquement contrées sur notre réseau, avant même de vous atteindre. Résultat : votre bande passante n'est jamais en danger.

Nous surveillons et analysons le trafic de votre réseau

Telenet surveille et analyse le trafic de votre réseau en continu à l'aide d'un système de gestion anti-DDoS. Après dépassement des limites configurées, ce système identifie automatiquement les attaques DDoS volumétriques types. Comment ? Notamment sur la base d'un intelligence feed DDoS à l'aide des empreintes actuelles des attaques et d'une liste de botnets.

Nous filtrons automatiquement le trafic suspect

Lors d'une attaque, le trafic de votre réseau est acheminé vers une infrastructure de scrubbing. Le scrub-bing vise à filtrer l'attaque DDoS et à transférer vers votre réseau uniquement le trafic sûr. Le tout sans que vous vous en aperceviez, car l'attaque n'impacte pas votre réseau.

LA SÉCURITÉ IT NÉCESSITE UNE VISION CLAIRE

Les nouvelles menaces et les nouvelles solutions nécessitent une vision globale en matière de sécurité. Envie de découvrir l'approche de Telenet Security

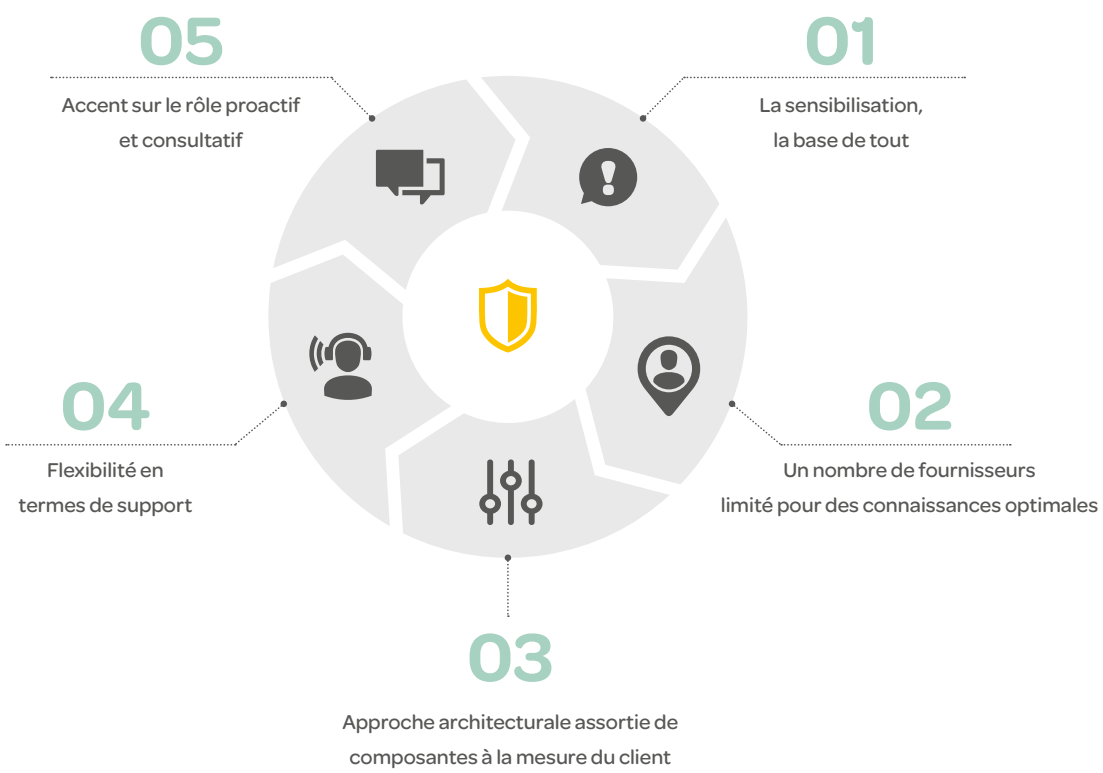
Le chapitre 4 vous la présente en détail.

04

L'approche de Telenet : le cycle de vie de la sécurisation en guise de principe de base

NOTRE APPROCHE

LA SÉCURISATION : UN PROCESSUS CONSTANT



Cycle de vie de la sécurisation

L'approche de Telenet Security repose sur le « cycle de vie de la sécurisation ». La sécurisation est un processus constant. Ce processus commence par une évaluation ou un audit de votre situation actuelle ainsi qu'une analyse de vos besoins. Nous concevons et implémentons la meilleure architecture sur la base de cet audit. Le monitoring et le réalignement jouent, par ailleurs, un rôle clé dans le maintien du niveau de sécurité.

Là où nous nous contentions principalement d'implémenter des solutions par le passé, nous participons désormais à la réflexion avec le client.

LORE MATTELAER
SECURITY COMPETENCE MANAGER CHEZ TELENET

01
La sensibilisation, la base de tout

Nous sommes convaincus que tout commence par la sensibilisation. « Il est essentiel de susciter une prise de conscience », affirme Lore Mattelaer, Security Competence Manager chez Telenet. « Nous avons mis ce rôle consultatif sur le devant de la scène ces dernières années. Là où nous nous contentions principalement d'implémenter des solutions par le passé, nous participons désormais à la réflexion avec le client. »

Le **pentesting** est le point de départ idéal pour une sécurisation plus efficace. Telenet collabore avec Toreon dans ce domaine. Lore : « Forte de son expertise et de son indépendance, cette entreprise se classe parmi les meilleures de Belgique en matière de piratage éthique. Ses experts certifiés ne sont liés à aucun produit, fournisseur ou opérateur télécom. Sa franchise est absolue. »

Alors que le pentesting est utilisé comme seul baromètre dans la plupart des cas, le **Vulnerability Management** est la méthode d'assessment la plus constante et la plus automatisée. Lore : « Dans ce cadre, la difficulté réside davantage dans le suivi constant et actif (le fait de patcher) que dans la surveillance. C'est pourquoi nous faisons confiance à NVISO. L'entreprise dispose de toutes les compétences nécessaires pour interpréter correctement le rapport et pour le transposer dans une approche GRC (gouvernance, gestion du risque et conformité) concrète. »

EN PRATIQUE | SECURITY CONSULTANCY

Security Consultancy est la dénomination commune utilisée pour désigner nos services spécialisés en matière de sensibilisation.

Security Check-up

Un Security Check-up identifie votre utilisation du réseau et votre statut de sécurité.

- Vision claire du trafic de votre réseau
- Rapport détaillé du statut de sécurité, assorti de points d'action
- Aucune connaissance préalable de votre infrastructure nécessaire

Security Pentesting | en collaboration avec Toreon

Avec le service Security Pentesting, nous faisons tester votre infrastructure par un pirate éthique. L'objectif est de mettre en lumière les faiblesses de votre sécurité et de les

- Garantie de qualité grâce à la certification CEH (Certified Ethical Hacker)
- Aperçu clair de vos failles de sécurité
- Techniques et outils similaires à ceux des pirates malveillants, mais sans danger pour vos données

Security Policy Optimisation

Avec Security Policy Optimisation, nous analysons les manières d'optimiser votre politique en matière de pare-feu.

- Analyses structurées, aucune action manuelle
- Détection des règles non utilisées, doubles, contradictoires et dangereuses dans votre politique
- Même outil que pour les certificats ISO, SOX et autres

Vulnerability Management | en collaboration avec NVISO

Forme d'assessment par laquelle votre infrastructure IT est systématiquement examinée afin d'identifier les failles à temps.

- Nexpose de Rapid7 comme scanner de la vulnérabilité
- Vision claire de votre situation grâce à des tableaux de bord conviviaux et des rapports clairs
- Accompagnement dans le cadre de l'interprétation des rapports et l'exécution des points d'action

Security Assessment

Nous analysons votre infrastructure actuelle et formulons des recommandations pour une protection optimale.

- Garantie de qualité grâce à la certification CISA (Certified Information Systems Auditor)
- Rapport détaillé sur l'état de votre infrastructure de sécurité, assorti de recommandations concrètes
- Point de départ idéal pour optimiser votre environnement de sécurité

En limitant notre offre aux technologies les plus performantes du marché, nous sommes réellement en mesure de nous spécialiser.

ANDRIES DE LOMBAERDE
PRINCIPAL SECURITY CONSULTANT CHEZ TELENET

02
Un nombre de fournisseurs limité pour des connaissances optimales

Telenet Security ne promeut aucun produit, mais établit des partenariats en fonction des besoins des clients. Andries De Lombaerde, Principal Security Consultant chez Telenet : « En limitant notre offre aux technologies les plus performantes du marché, nous sommes réellement en mesure de nous spécialiser. Nos connaissances représentent donc notre principale plus-value par rapport aux autres intégrateurs. »

Le degré des partenariats en est la plus belle preuve : partenaire 4 Stars de Check Point, partenaire Diamond de Palo Alto Networks et partenaire Gold de F5. Andries Lombaerde : « Ces partenariats nous permettent de réellement défier les fournisseurs et de poursuivre notre collaboration en matière de technologie afin qu'elle réponde au mieux aux souhaits de nos clients. Nous organisons régulièrement des réunions au cours desquelles nos partenaires nous dévoilent les nouvelles fonctionnalités ou les nouveaux outils à venir. Nous profitons, quant à nous, de l'occasion pour partager notre expérience du terrain. Nous abordons les points en suspens, les problèmes que nous rencontrons avec les clients et les limites des produits. Il est tenu compte des remarques et du feed-back. Il se crée une véritable interaction : ils peaufinent leurs produits ou en développent même de nouveaux sur la base de notre input. »

EN PRATIQUE

PARTENARIATS À L'HONNEUR

Nous collaborons avec trois fournisseurs de premier plan : Check Point, Palo Alto Networks en F5. Le consultant en technologie Gartner place chaque année Check Point et Palo Alto Networks parmi les leaders dans son « Magic Quadrant for Enterprise Firewalls ».

Partenaire Gold de F5

Telenet est partenaire Gold de F5, spécialiste réputé pour la mise à disposition particulièrement rapide et efficace d'applications, surtout via le Load Balancing. F5 compte aussi parmi les acteurs phares de la sécurité. Les Application Delivery Controllers (ADC) BIG-IP vous permettent d'optimiser aussi bien la vitesse que la protection et la disponibilité de diverses applications.

« Telenet a très bonne réputation sur le marché. Forte de ses riches connaissances techniques, elle parvient parfaitement à convertir notre portefeuille en valeur ajoutée pour le client. »

JOZEF VAN ROYEN
CHANNEL ACCOUNT MANAGER BELUX CHEZ F5

Partenaire 4 Stars de Check Point

Telenet est partenaire 4 Stars de Check Point Software Technologies, l'un des leaders du marché en firewalling de nouvelle génération. Outre un contrôle avancé de l'identité et des applications, les solutions de Check Point offrent une foule de possibilités de virtualisation. En 2015, Telenet a été nommé Best Performing Partner.

« En s'adaptant rapidement et facilement à nos dernières technologies et aux certifications afférentes, Telenet démontre chaque fois ses connaissances et son professionnalisme. »

PIERRICK VAN DEN ABEELE
SALES MANAGER BELUX CHEZ CHECK POINT

Partenaire Diamond de Palo Alto Networks

Palo Alto Networks a développé le premier pare-feu de nouvelle génération avec un moteur hautes performances basé sur une architecture Single Pass. L'entreprise propose aujourd'hui des solutions de sécurisation ultramodernes et intégrées. Telenet est partenaire Diamond avec le statut d'élite ASC (Authorized Support Centers) et a décroché le prestigieux « Excellence in Support EMEA Award » de Palo Alto.

« Telenet est le seul partenaire de Belgique à posséder ce statut d'élite ASC pour le support en matière de sécurité. »

LUC VERVOORT
DIRECTOR EMEA STRATEGIC ALLIANCES CHEZ PALO ALTO NETWORKS

Nous élaborons avec vous l'architecture adéquate, identifient les composantes de sécurité les plus appropriées et les implémentent.

BRUNO GYSELS
SECURITY CONSULTANT CHEZ TELENET

03
Approche architecturale assortie de composantes à la mesure du client

Nous sommes convaincus que la sécurisation ne se limite pas aux produits. Nous optons résolument pour une approche architecturale et non pour des solutions techniques « ad hoc » qui, dans le meilleur des cas, ne font que résoudre temporairement les problèmes.

Bruno Gysels, Security Consultant chez Telenet : « Compte tenu de la complexité actuelle de la sécurisation des informations, un fournisseur de sécurité n'est plus en mesure de proposer à lui seul une solution globale. Pour malgré tout pouvoir offrir une protection entièrement intégrée, nous collaborons avec différents partenaires technologiques. Nous élaborons avec vous l'architecture adéquate, identifions les composantes de sécurité les plus appropriées et les implémentons. Nous ne nous limitons ainsi pas au périmètre, mais nous veillons aussi à la sécurisation des terminaux, des serveurs web, des centres de données et des solutions anti-DDoS, entre autres. »

EN PRATIQUE | SECURITY IMPLEMENTATION

Nous développons une architecture, choisissons le matériel et les logiciels et implémentons cette architecture de sécurisation dans votre entreprise. Nous vous conseillons aussi quant à l'utilisation et la sensibilisation de vos collaborateurs.

Nous faisons uniquement appel aux meilleurs parten-aires technologiques et installons les composantes de sécurité les plus adaptées, et ce, sur la base de l'expérience de nos experts. Selon votre situation, votre infrastructure de protection peut comporter les compo-santes et technologies suivantes :

Composantes	Partenaires technologiques
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

Notre helpdesk de sécurité ne dispose pas de la première ligne habituelle. Les clients sont d'emblée mis en contact avec un ingénieur certifié.

BJORN DESANDER
MANAGER SERVICE DESK SECURITY CHEZ TELENET

04
Flexibilité en termes de support

Les clients de Telenet Security bénéficient d'une flexibilité sans égal en matière de support. « Libre à eux de décider s'ils souhaitent un support ou pas et, si oui, à quel niveau. Ils peuvent, en outre, nous en confier entièrement la gestion », explique Brice Mees, Security Services Operations Manager chez Telenet.

Les clients qui optent pour **Security Support** ont le choix : soit pendant les heures de bureau, soit 24 h/24. « En cas de question ou de problème, ils peuvent contacter directement nos spécialistes », précise Bjorn Desander, Manager Service Desk Security chez Telenet. « Notre helpdesk de sécurité ne dispose pas de la "première ligne" habituelle. Les clients sont d'emblée mis en contact avec un ingénieur certifié. Un véritable avantage pour les clients, mais aussi pour les vendeurs. Nous sommes plus qu'une simple boîte aux lettres : nous : nous résolvons la plupart des incidents sans impliquer le vendeur. »

Les clients nous confient de plus en plus souvent la gestion de leur infrastructure IT. Brice : « Nos **Managed Security Services** sont modulaires : ils reposent sur un service standard assorti d'une «shopping list» de services supplémentaires au choix. Dans le cadre du service standard, nous actualisons votre infrastructure et votre Service Manager vous fait un rapport tous les trois mois. Si ce service n'est pas assez poussé, vous pouvez y ajouter d'autres services. D'ailleurs, nous gérons non seulement votre infrastructure, mais aussi votre politique en matière de sécurité. Si vous souhaitez pouvoir apporter vous-même certaines modifications à votre politique, vous pouvez opter pour Change Management. Nous examinerons vos adaptations et vous pourrez dormir sur vos deux oreilles. »

EN PRATIQUE | SECURITY SUPPORT ET MANAGED SECURITY

Dans le cadre de Security Support, nous vous apportons une assistance technique et assurons la gestion des licences.
Si vous optez pour Managed Security, vous nous confiez la gestion, le suivi et l'optimisation de votre sécurisation.

Security Support

Business Hours Support

- Telenet Security Desk comme point de contact
- Jours ouvrables de 8 h 30 à 17 h 30

24/7 Support

- Extension du Business Hours Support
- 24/7

Managed Security

STANDARD

Services de sécurité inclus

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

MODULAR

Services de sécurité supplémentaires possibles

- + Change Management par technologie
- + IPS Policy Management par appareil
- + Premium Monitoring par appareil
- + Premium Reporting par appareil
- + Premium Service Management par client

Tous nos experts peuvent parfaitement participer aux réflexions du client et le guider vers un environnement de protection optimal.

BRICE MEES
SECURITY SERVICES OPERATIONS MANAGER
CHEZ TELENET

05
Accent sur le rôle proactif et consultatif

La sécurité IT est particulièrement délicate, complexe et extrêmement évolutive. Pour rester en phase avec cette évolution, vous pouvez périodiquement compter sur les experts en sécurité de Telenet Security.

Brice Mees : « Tous nos experts possèdent au moins 5 ans d'expérience sur le terrain. Ils peuvent dès lors parfaitement participer aux réflexions du client et le guider vers un environnement de protection optimal. L'expertise revêt une importance cruciale à nos yeux, c'est pourquoi nous investissons énormément dans les formations au sein de l'équipe Security. Résultat : les connaissances et les certifications de nos experts sont toujours à jour. Notre équipe ne connaît d'ailleurs qu'une faible rotation, ce qui nous permet de garantir une certaine continuité aux clients.

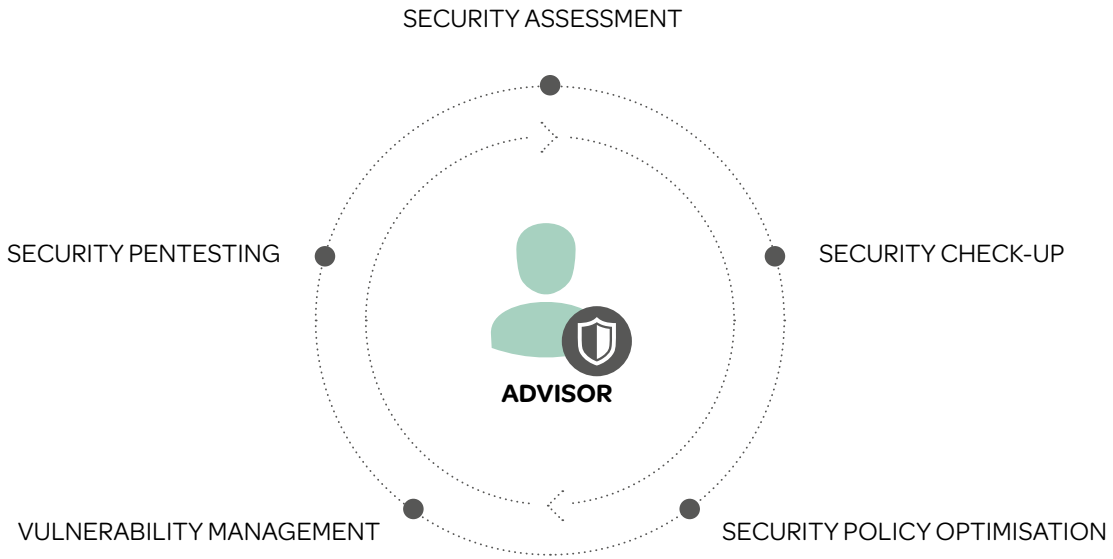
Brice considère le Trusted Security Advisor comme le pivot central du cycle de vie de sécurité du client : « Il signale par exemple les nouvelles versions et fonctionnalités de manière proactive, et donne de précieux conseils quant aux performances actuelles, à la maîtrise et à la sécurisation. Il peut, par ailleurs, coacher des profils spécifiques, apporter son aide en matière de gestion du changement et valider l'implémentation des grandes transformations. »

EN PRATIQUE | TRUSTED SECURITY ADVISOR

Le Trusted Security Advisor est le pivot central du cycle de vie de votre sécurité. Il peut parfaitement participer aux réflexions de votre entreprise et vous guider vers un environnement de protection optimal. »

Vous pouvez aussi, au besoin, faire appel aux experts en sécurité de manière périodique.

- Meilleure harmonisation de votre environnement de sécurité et des besoins de votre entreprise
- Réponse plus rapide et appropriée à l'évolution effrénée des défis de sécurité
- Meilleur accompagnement et meilleur soutien de votre équipe de sécurité IT



CHAPITRE 05

Comment s'y prennent Colruyt, Rossel et Partena ?

Telenet protège Colruyt Group contre les attaques DDoS

Colruyt est de plus en plus souvent la cible d'attaques DDoS. « Inutile de vous dire que 20 minutes d'immobilisation coûtent très cher », explique Wim Derijnck, Teammanager Network Solutions chez Colruyt. C'est pourquoi Colruyt a opté pour le système anti-DDoS de Telenet. En exfiltrant certaines données sur son réseau, Telenet peut alors distinguer ce type d'attaques du trafic légitime. Le système anti-DDoS isole le trafic malveillant : notre réseau est ainsi épargné. Les coûts de cette solution de protection ne représentent qu'une fraction de son rendement potentiel. »

« Les coûts d'une solution anti-DDoS ne représentent qu'une fraction de son rendement potentiel. »

WIM DERIJNCK
TEAMMANAGER NETWORK SOLUTIONS CHEZ COLRUYT

Rossel poursuit sa « métamorphose média » en toute sécurité

Informations confidentielles des journalistes, données personnelles des lecteurs… La protection des données trône en tête de liste des priorités du groupe média Rossel. « Personne ne doit pouvoir entrer dans notre système », insiste David De Geyter, IT & Security Manager chez Rossel. « La solution proposée par Telenet ne se limitait pas à un simple «pare-feu». Elle instaurait un partenariat solide. Les connaissances de Telenet nous apportent un atout majeur : Telenet cerne parfaitement nos besoins, nos exigences et nos attentes. »

« La solution de sécurisation de Telenet ne se limite pas à un simple «pare-feu» ; elle instaure un partenariat solide. »

DAVID DE GEYTER
IT & SECURITY MANAGER CHEZ ROSSEL

Partena opte pour la protection à deux niveaux de Telenet

Chez Partena, pas moins de 1.600 collaborateurs traitent des données confidentielles au quotidien. Pour la sécurisation, l'entreprise a opté pour deux technologies proposées par Telenet. Franky Goethals, Manager Infrastructure & Security chez Partena : « Les deux systèmes sont tout à fait complémentaires et le web application firewall est parfaitement adapté à nos applications web. Pour nous permettre de bien cerner les enjeux, Telenet a d'ailleurs effectué un Security Check-up gratuit. Ce rapport nous a permis de justifier un investissement de cette ampleur. »

« Pour nous permettre de bien cerner les enjeux, Telenet a effectué un Security Check-up gratuit. »

FRANKY GOETHALS
MANAGER INFRASTRUCTURE & SECURITY CHEZ PARTENA

ENVIE DE DÉCOUVRIR LE TÉMOIGNAGE D'AUTRES CLIENTS ?

Colruyt Group, Rossel et Partena ne sont pas les seuls clients satisfaits de nos solutions de sécurité. Envie de connaître l'avis d'autres clients ? Consultez tous les témoignages sur notre site web.

telenet.be/temoignages

En savoir plus

telenet.be/security
0800 66 066

BUSINESS