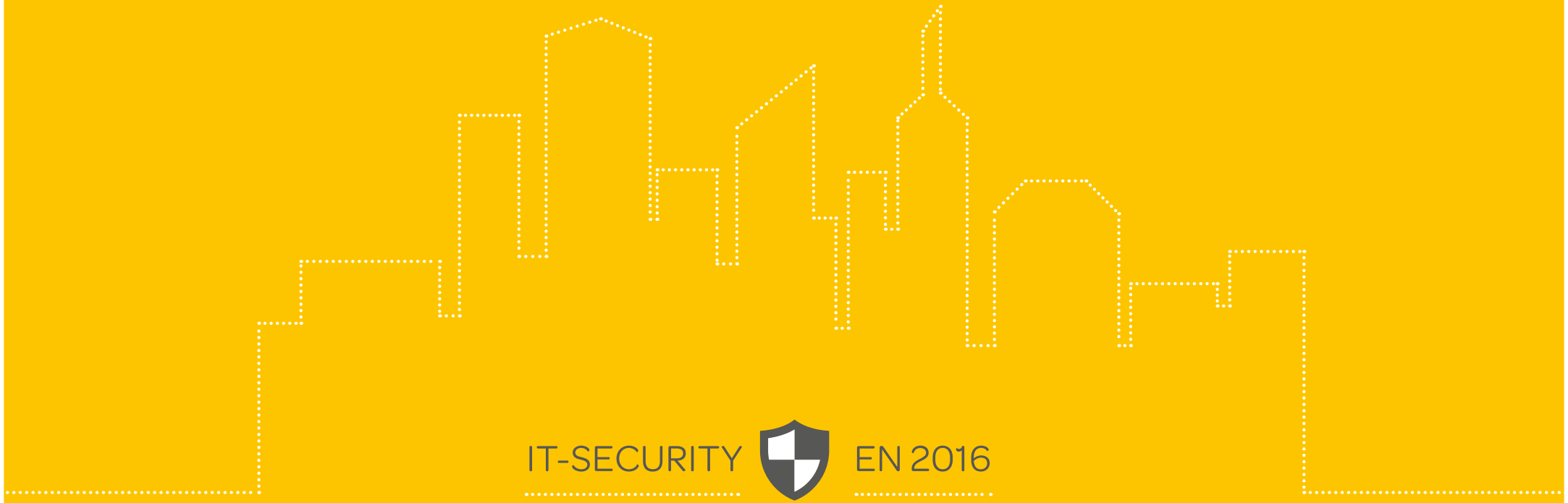
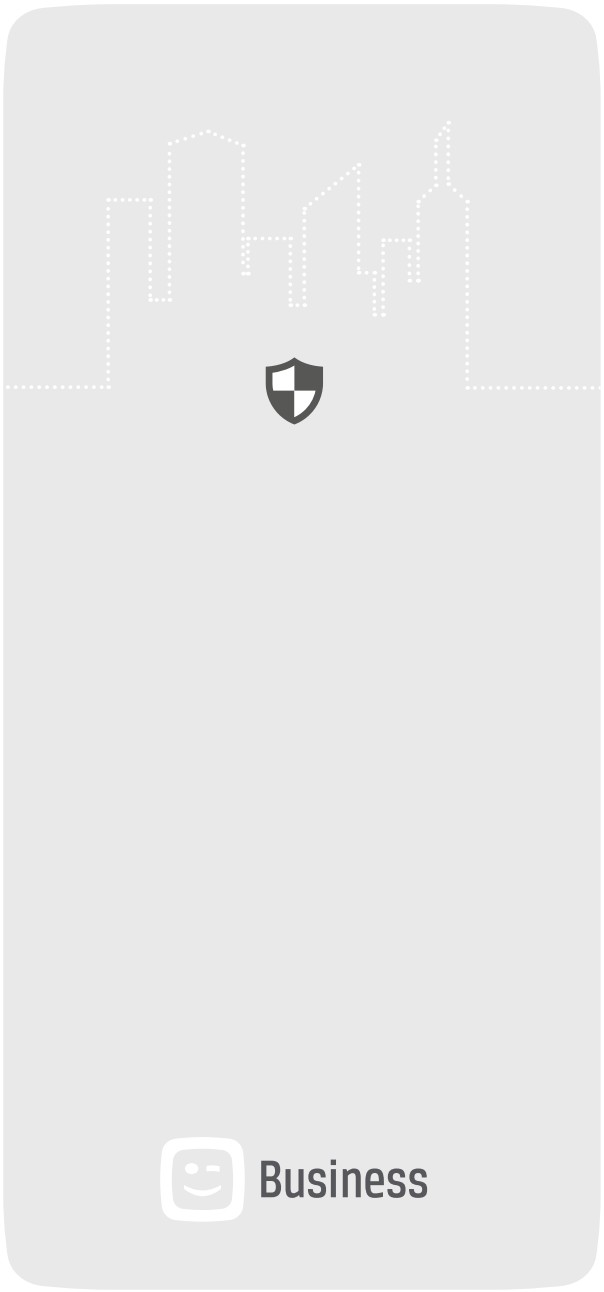
Business



IT-SECURITY EN 2016

Plus que jamais au cœur de toute entreprise



AVANT-PROPOS

« La sécurité IT s'apparente à une assurance. Vous n'en voyez pas l'utilité, jusqu'à ce qu'un grave problème se pose. »

Incendie, vol, accident du travail... En tant qu'entreprise, vous connaissez certainement la valeur d'une bonne assurance. Verser la prime n'est certes pas une partie de plaisir, mais vous serez sans aucun doute ravi d'être assuré en cas de problème.

Il en va de même pour la sécurité IT. L'investissement se justifie parfois difficilement, mais les conséquences d'un piratage, d'une attaque DDoS ou d'un rançongiciel peuvent être désastreuses. Tant pour le fonctionnement de l'entreprise ou votre situation financière que pour votre image.

Bien que nous sachions tous qu'il vaut mieux prévenir que guérir, la sécurité IT survient encore trop souvent en réponse à un problème ou une situation. La plupart des entreprises attendent trop longtemps avant d'investir dans une sécurité adaptée.

Avec ce dossier, nous espérons vous convaincre qu'agir de manière proactive peut vous éviter bien des frais et des soucis. Que la sécurité IT n'est plus l'affaire du département informatique, mais bien l'affaire de toute l'entreprise. Nos spécialistes restituent pour vous le contexte, identifient les menaces de l'année 2016 et y confrontent notre approche de la sécurité.

Bonne lecture.

Martine Tempels
Senior Vice President – Telenet Business

EXECUTIVE SUMMARY

7 tendances en matière de sécurité IT

1

De la réactivité à la **proactivité**

Si nous observons les tendances en termes de sécurité IT, l'émergence d'une approche proactive est probablement la plus marquée. Auparavant, nous réagissions souvent à la suite d'un incident, mais la situation est tout autre aujourd'hui. Plus la technologie et l'approche des intégrateurs sont proactives, plus elles durent dans le temps. Dans le cadre de la business continuity, les entreprises sont de plus en plus nombreuses à adopter une approche proactive.

2

Les menaces sont **plus avancées**

Si les menaces auxquelles votre entreprise est confrontée se multiplient, elles gagnent aussi en complexité. Saviez-vous que 27 % des logiciels malveillants ont été conçus en 2015 ? Et qu'ils peuvent désormais échapper aux systèmes traditionnels destinés à les détecter ? Un fait d'autant plus alarmant que le trafic SSL – jusqu'il y a peu une référence en termes de sécurité – est plus susceptible d'être piraté et que les pirates agissent par le biais de la technique du social engineering et utilisent les outils pratiques pus ingénieusement que jamais.

3

Les technologies évoluent

Les menaces sont pointues, mais elles ne sont fort heureusement pas les seules à l'être ; les technologies et les solutions des développeurs de produits le sont aussi. Bien que les logiciels malveillants les plus récents se déclinent sous de multiples formes, ils reposent toujours sur une vingtaine de « techniques d'exploitation ». Les dernières technologies de protection n'identifient donc plus les logiciels malveillants sur la base de signatures, mais sur la base de leur comportement.

4

Le nombre d'**attaques DDoS** augmente

Une autre tendance se dessine très clairement : l'essor des attaques DDoS. Elles surviennent de plus en plus souvent, gagnent en intensité et sont orchestrées d'une manière plus intelligente. Pas moins de 602 GB de données ont été envoyés par seconde lors de la plus rude attaque DDoS mesurée jusqu'à présent. Les attaques DDoS se composent souvent de plusieurs types d'attaque et/ou sont uniquement utilisées à des fins de diversion pour d'autres attaques.

5

La durée de vie du matériel diminue

Les nouvelles menaces écourtent la durée de vie du matériel de sécurité. Nous attendons, par exemple, bien plus des pare-feu qu'il y a cinq ans. Ils présentent de nouvelles fonctionnalités comme le sandboxing, l'antivirus ou les Intrusion Prevention Systems (IPS) et gèrent un trafic plus important, car ils doivent désormais aussi examiner le trafic SSL. Alors que nous achetions auparavant les pare-feu avec une marge de croissance d'environ 10 à 20 %, ce pourcentage n'est plus suffisant aujourd'hui.

6

Le périmètre de sécurité ne suffit plus

Il suffisait autrefois de sécuriser l'enveloppe IT pour « construire un rempart de protection autour de l'entreprise ». Aujourd'hui, les menaces émanent de plus en plus de l'intérieur. Les infrastructures internes doivent dès lors aussi faire l'objet d'une protection accrue. Le trafic nord-sud (entre les clients et les serveurs) et le trafic est-ouest (entre les serveurs) doivent tous deux être examinés et sécurisés. À l'image d'un oignon, la meilleure des protections se compose de diverses couches.

7

La sécurité IT devient **la priorité** de tous

Alors que les actifs clés de l'entreprise 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. D'autant plus que la législation afférente se durcit. Fin 2015, nous avons ainsi franchi les premières étapes vers une politique de sécurité IT unifiée et uniforme en Europe.

Découvrez les défis auxquels le contexte professionnel de 2016 confronte chaque entreprise.

CHAPITRE 1

« Le shadow IT ne date pas d'hier, mais il a connu une croissance exponentielle avec l'essor de la génération Y et du cloud. »

Lore Mattelaer
Security Business Development Manager chez Telenet

CHAPITRE 01

Le défi d'un nouveau contexte professionnel

Actifs et entreprises : de plus en plus digitaux

Les données clés de l'entreprise sont de plus en plus souvent digitales. Chaque entreprise collecte et traite des documents et des données au format digital : des données des clients aux résultats R&D, en passant par les informations salariales. Ce nouveau contexte s'accompagne d'une foule de risques. Résultat : les entreprises sont plus vulnérables que jamais. Un incident IT peut avoir un impact considérable : détérioration de l'image, passage des clients à la concurrence, perte de données ou baisse du chiffre d'affaires, car les données sont hors service ou inaccessibles pendant un certain temps.

Une nouvelle génération de travailleurs

La génération Y – personnes nées entre 1980 et 2000 – détermine de plus en plus le rythme du marché et du lieu de travail. Elle modifie les règles du jeu. Cette première génération de digital natives impacte le monde professionnel. « L'arrivée de la génération Y a modifié le rôle du manager IT et lui a donné plus d'importance. », explique Andrew Turner, Product Manager chez Telenet. « Nous attendons de plus en plus d'un manager IT qu'il participe à la réflexion avec l'entreprise et trouve des solutions de manière proactive et non plus réactive. »

La génération Y est toujours connectée, dispose des technologies les plus récentes, utilise les dernières applications et en attend de même de son environnement de travail. Cette évolution diversifie la nature des attaques dirigées contre les entreprises. Andrew Turner ajoute : « Nous laissons de plus en plus de portes ouvertes. Non seulement, car nous utilisons davantage d'outils sur notre lieu de travail, mais surtout, car la génération Y ne se préoccupe pas (ou très peu) de la sécurité. Son seul souci est de travailler avec des appareils et des applications rapides et conviviaux. »

Le shadow IT, la ligne de désir de l'IT

Le cloud offre désormais une alternative à presque chaque application professionnelle. « Mieux encore : elles sont installées et opérationnelles en seulement quelques clics. Il est bien plus simple de partager des fichiers avec Dropbox qu'avec SharePoint. Répondre à un message via Yammer est bien plus rapide que par e-mail. Et pourquoi utiliser le système CRM complexe de l'entreprise alors que Salesforces offre une solution beaucoup plus simple ? » fait remarquer Lore Mattelaer, Security Business Development Manager chez Telenet.

« Le shadow IT ne date pas d'hier, mais il a connu une croissance exponentielle avec l'essor de la génération Y », poursuit Lore Mattelaer. Le shadow IT désigne tous les logiciels et le matériel mis en œuvre au sein de l'entreprise, mais en dehors du département IT. Et d'ajouter : « Ils n'ont donc pas reçu d'approbation officielle. Le shadow IT constitue la ligne de désir de l'infrastructure IT de l'entreprise : les travailleurs préfèrent marcher sur la pelouse – plus pratique et efficace – que sur les sentiers officiels sécurisés, mais souvent escarpés. »

Ces sentiers tracés en dehors des voies bétonnées placent le manager IT face à un défi de taille, explique Lore Mattelaer : « Son objectif est de veiller à la sécurité des appareils et des données de l'entreprise. Mais comment y parvenir si les travailleurs utilisent des logiciels et du matériel dont il n'a pas connaissance ? »

Vers un cadre légal clair et unifié

Que faire en cas d'attaque ? Qu'advient-il si un de vos travailleurs laisse échapper des informations ? Qui en assume la responsabilité ? Êtes-vous soumis à l'obligation d'information ? Risquez-vous une amende ? Isabelle Ghislain, Legal Counsel chez Telenet, lève le voile sur le cadre légal.

« En Europe, la cybersécurité fait débat », commence Isabelle Ghislain. « Bien que les États membres reconnaissent qu'il s'agit là d'une priorité, leur approche manque considérablement de cohérence. La cybersécurité est, à leurs yeux, une préoccupation nationale. Il en résulte des différences significatives dans la politique, le cadre légal et les capacités opérationnelles. »

EN RÉSUMÉ

Réglementation pertinente en Belgique
– Loi pour les infrastructures critiques
– Cyber Security Strategy
– Loi relative à la protection de la vie privée

Réglementation pertinente en Europe
– Network and Information Security Directive *(NISD)*
– General Data Protection Regulation *(GDPR)*

BELGIQUE

Loi pour les infrastructures critiques

En Belgique, nous partons du principe que chaque « acteur professionnel du marché » doit appliquer une politique de protection adéquate. Isabelle : « Nous pouvons interpréter les dispositions du droit général de la responsabilité comme une "obligation générale de protection". Certains secteurs tels que ceux de l'énergie, des transports, des finances et des télécoms sont soumis à la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques. Dans la mesure où ils exploitent ce type d'infrastructure, ils sont légalement tenus de désigner un point de contact en matière de sécurité et d'élaborer un plan de sécurité minimal incluant du matériel interne et des mesures organisationnelles. »

Cyber Security Strategy

En 2012, le gouvernement belge a aussi mis sur pied une stratégie nationale en matière de cybersécurité. : la Cyber Security Strategy. « Le gouvernement s'emploie par ce biais à adopter une approche globale de la sécurité digitale. Mais, même en 2016, il existe peu d'informations sur la manière d'implémenter concrètement la stratégie », explique Isabelle Ghislain.

Loi relative à la protection de la vie privée

Une réglementation supplémentaire s'applique à toutes les entreprises qui traitent des données à caractère personnel. Isabelle Ghislain précise : « Les consommateurs n'en sont pas toujours conscients, mais ils partagent des informations personnelles presque chaque jour : lorsqu'ils demandent une carte de fidélité, qu'ils s'inscrivent à un cours ou participent à un concours, par exemple. Dans la mesure où le consommateur n'a généralement aucun contrôle sur ce qu'il advient de ces données, une loi qui définit la manière dont les entreprises doivent traiter ces données a vu le jour en 1992 : la loi relative à la protection de la vie privée. »

Cette loi impose la prise de mesures (de sécurité) supplémentaires pour protéger suffisamment les données personnelles. Isabelle Ghislain ajoute : « La liste des privacy requirements est longue, mais réalisable. Les traitements doivent être enregistrés auprès de la Commission de la protection de la vie privée et les droits de la personne concernée doivent être respectés. Les données doivent, par ailleurs, toujours être parfaitement à jour, supprimées en temps opportun, traitées aux fins légales prévues et uniquement accessibles aux personnes autorisées. »

EUROPE

Network and Information Security Directive *(NISD)*

En ce qui concerne les entreprises qui ne traitent pas de données à caractère personnel, la protection des données est souvent basée sur le concept de goodwill : elles se protègent des conséquences néfastes comme une détérioration de l'image ou une perte de chiffre d'affaires. Isabelle Ghislain attend toutefois un degré de sensibilisation accru : « Les choses bougent beaucoup au niveau européen. La directive Network and Information Security a vu le jour fin 2015. Elle vise à combler le fossé entre les États membres à l'aide d'une approche concrète et uniforme des mesures de sécurité. L'implémentation de cette directive en Belgique est actuellement en préparation. »

General Data Protection Regulation *(GDPR)*

La General Data Protection Regulation entrera, par ailleurs, en vigueur au printemps 2018. « La nouvelle GDPR présentera quelques nouveautés », explique Isabelle Ghislain. « Toute entreprise qui traite les données des citoyens européens sera tenue de communiquer aux autorités nationales les incidents en termes de protection de la vie privée. Cette obligation, à laquelle seul le secteur des télécoms est soumis en Belgique, s'ouvrira alors à tous les secteurs. L'arrivée de la GDPR s'accompagnera de sanctions inédites. La Commission Vie privée aura le droit d'imposer des amendes susceptibles d'être très salées, selon la nature de l'incident. Autre point important : nous attendons des entreprises qu'elles prennent la balle au bond et prévoient une politique étayée de protection de la vie privée et de sécurité. »

ROUND UP

INVESTIR DANS LA SÉCURITÉ, C'EST INVESTIR DANS LA CONTINUITÉ

Alors que le cadre juridique se durcit, il est évident que la sécurité IT gagne en intérêt. Dans le cadre de la business continuity, mieux vaut savoir d'où proviennent les menaces et identifier les niveaux de votre entreprise à sécuriser.
Lisez le prochain chapitre pour en savoir plus à ce propos.

CHAPITRE 2

« La clé d'une sécurité optimale est une conception claire et conforme à votre politique de sécurité. »

Glyn Jones
Service Manager chez Telenet

CHAPITRE 02

- Les menaces se multiplient et gagnent en complexité
- La sécurité évolue pour répondre à cette complexité

Les nouvelles menaces nécessitent de nouvelles formes de sécurité

Les menaces
se multiplient et gagnent en complexité

Les menaces et les attaques proviennent de partout. De nombreuses entreprises pensent être une cible sans intérêt, mais rien n'est moins vrai. Aujourd'hui, chaque entreprise est une cible potentielle. Premièrement, les attaques ne visent pas toujours une entreprise spécifique, mais elles sont le fruit du hasard. Les pirates peuvent, par exemple, aléatoirement identifier vos failles et s'introduire dans votre entreprise en raison d'un manque de protection. Deuxièmement, une entreprise piratée n'est souvent qu'un intermédiaire pour atteindre la cible finale. Les pirates ne sont pas toujours intéressés par vos données, mais par celles de vos clients ou d'autres entreprises avec lesquelles vous collaborez. Vous n'en restez pas moins la victime de l'attaque.

Vous trouverez ci-dessous un aperçu des menaces les plus courantes pour les entreprises.

Logiciels malveillants

Un logiciel malveillant est un logiciel qui vise à perturber les systèmes informatiques, dérober des informations confidentielles ou accéder aux systèmes informatiques privés. Il prend souvent l'apparence d'un programme ou d'un fichier ordinaire, mais renferme des fonctions cachées qui permettent d'accéder par l'extérieur à l'ordinateur contaminé. Un constat surprenant : pas moins de 27 % des logiciels malveillants ont été créés en 2015. Ils se modifient, par ailleurs, sans cesse. Les systèmes de protection contre les logiciels malveillants, qui identifient le logiciel malveillant sur la base de signatures connues, ne sont alors plus capables de reconnaître le nouveau logiciel malveillant.

Rançongiciels

Un rançongiciel est un outil de chantage qui utilise des logiciels malveillants. Le rançongiciel paralyse l'ordinateur contaminé ou les données qu'il contient et demande ensuite à l'utilisateur de verser une rançon pour libérer l'ordinateur ou les données. Le rançongiciel impose souvent une date limite et utilise un puissant cryptage pour paralyser le système ou les données. L'entreprise ne paie pas dans les délais – généralement par le biais d'un mode de paiement intraçable comme BitCoin ? La clé de décryptage n'est pas libérée et les données ou le système restent inutilisables. Épargnez-vous bien des tracas et sauvegardez régulièrement vos données (précieuses).

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. 10 % des entreprises belges ont déjà fait l'objet d'une attaque DDoS. Ces attaques se déclinent sous plusieurs formes. En cas d'attaques volumétriques, un énorme flux de données inonde votre infrastructure, de sorte à épuiser totalement la bande passante disponible. Les attaques applicatives sont plus subtiles et visent une application ou un serveur en particulier. La cible n'est alors pas en mesure de traiter la quantité de données et tombe en panne. Les attaques protocolaires piratent quant à elles les protocoles de réseau. En envoyant des paquets de réseau qui ne répondent pas aux normes d'internet, elles font ralentir et planter les serveurs.

En 2015, les attaques DDoS ont continué d'augmenter : tant en nombre et en volume qu'en complexité. Là où il s'agissait autrefois souvent d'activisme ou de vandalisme, il s'agit aujourd'hui plus régulièrement d'extorsion. Plus d'un quart des attaques rapportées concernent un volume de plus de 100 Gbps. Pas moins de 602 Gbps ont été envoyés lors de la plus rude attaque DDoS mesurée jusqu'à présent. Ces attaques gagnent, en outre, en complexité : les entreprises doivent souvent faire face à des attaques combinées. Lors de ce type d'attaque, les attaques volumétriques, applicatives et protocolaires alternent dans le temps.

LE SAVIEZ-VOUS ?

27%

des logiciels malveillants ont été conçus en 2015. Ils se modifient, par ailleurs, sans cesse, de sorte qu'ils peuvent échapper aux systèmes traditionnels destinés à les détecter.

10%

des entreprises belges ont déjà fait l'objet d'une attaque DDoS.
L'ampleur des attaques ne cesse, en outre, d'augmenter.

Botnets

Partout dans le monde, des ordinateurs sont contaminés à l'insu de leurs utilisateurs. Bon nombre d'entre eux forment un botnet, c'est-à-dire un réseau pouvant être piloté à partir d'un point de commande central. On utilise souvent des botnets pour mener des attaques DDoS. Les ordinateurs de botnet nuisent également à l'entreprise, car ils utilisent beaucoup de bande passante et peuvent ralentir considérablement le réseau.

Bugs de logiciels

On détecte constamment des failles dans les logiciels. Une fois cette (ces) faiblesse(s) identifiée(s), le fournisseur développe et commercialise au plus vite un patch qui vise à améliorer le logiciel. Les entreprises ne l'installent pas (dans l'immédiat) ? Elles sont alors vulnérables. Toute personne ayant connaissance de ces failles peut facilement les exploiter.

Trafic SSL

Les applications et les sites web utilisent souvent le protocole de cryptage SSL afin d'éviter le piratage du flux de données de l'application ou du site web. Ce certificat SSL modifie l'adresse de la barre d'adresse de http en https et donne aux internautes l'impression que la connexion au site web est sécurisée. Dans la mesure où de plus en plus d'applications web sont basées sur le trafic SSL, la bande passante des entreprises en contient de plus en plus, de 20 à 30 % jusqu'à 40 à 50 %.

Nous constatons avec surprise que les pirates sont toujours davantage en mesure de contourner cette protection SSL. Notamment à l'aide du principe « man-in-the-middle ». Un internaute qui saisit une adresse web va généralement se rendre sur l'adresse http avant de cliquer sur le site https. C'est à ce moment – juste avant la sécurisation de la connexion - que le pirate intervient et relie l'internaute au serveur web qu'il contrôle. Cette connexion est sécurisée aux yeux de l'internaute et du serveur, mais le pirate peut intercepter leur trafic.

Les pirates dissimulent, par ailleurs, de plus en plus souvent leur logiciel malveillant dans le trafic SSL. Il passe alors inaperçu, car peu d'entreprises décryptent leur trafic SSL pour l'analyser dans le tunnel SSL. Le principal danger du trafic SSL réside dans le fait que les entreprises le considèrent trop souvent comme sécurisé. Elles n'appliquent alors leurs politiques que sur le trafic non SSL.

Shadow IT

Bien qu'il soit en grande partie sans danger et qu'il stimule la productivité et l'innovation dans de nombreux 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'informations résultent souvent d'initiatives que le manager IT n'avait pas approuvées ou dont il n'avait même pas connaissance. Les dommages surviennent souvent en raison du non-respect des exigences et de la mise en œuvre de nouveaux processus qui ne se conforment pas aux règles existantes. Le shadow IT fait partie de ces éléments que la majorité des managers IT préfèrent ne pas voir dans leur organisation.

LE SAVIEZ-VOUS ?

HTTPS

Les entreprises considèrent trop souvent le trafic SSL comme sécurisé. Elles n'appliquent alors leurs politiques que sur le trafic non SSL.

Les collaborateurs de l'entreprise

L'humain est le maillon faible dans la chaîne de sécurité IT. Cette fragilité se traduit même à plusieurs niveaux au sein d'une entreprise. Le niveau C comprend des menaces, car la sécurité IT n'est généralement pas une priorité. Libérer un budget à allouer à la sécurité n'est pas une sinécure : les entreprises n'en tirent aucun bénéfice financier, mais la sécurité peut les empêcher de perdre gros. Et si elles ont déjà prévu un budget en ce sens, elles manquent souvent d'une politique uniforme : les données confidentielles ne sont pas identifiées et il n'existe aucune politique établissant ce qu'une entreprise autorise et interdit.

Et cela ne se limite pas à l'élaboration de la politique ; la vraie difficulté réside dans sa mise en pratique. Les travailleurs créent souvent – involontairement – des risques de sécurité pour l'entreprise. C'est notamment le cas lorsqu'ils se rendent sur des sites web malveillants ou qu'ils utilisent une clé USB contaminée. Le phishing (hameçonnage) connaît un essor considérable, car les internautes ont tendance à cliquer sur des liens sans se poser de questions. Les mots de passe représentent aussi un point d'entrée évident pour les pirates. Même si les travailleurs utilisent un réseau sécurisé, voler un mot de passe est un jeu d'enfant. Les pirates peuvent attirer les travailleurs sur une copie d'une page web et découvrir les mots de passe sans même impliquer de logiciels malveillants. La sensibilisation est la seule manière d'attirer l'attention des travailleurs sur ce type de risque.

Social engineering

Le social engineering, ou social hacking, réunit l'ensemble des techniques par lesquelles les pirates trompent les internautes et les invitent à effectuer des opérations ou à fournir des informations. La forme la plus courante de social engineering est sans aucun doute le phishing (hameçonnage). 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, car ils sont envoyés à des millions de personnes.

L'ingéniosité croissance avec laquelle les criminels procèdent est alarmante pour les entreprises. Le spear phishing est la déclinaison ciblée du phishing : des falsifications parfaites ciblant des personnes spécifiques. Elles sont tellement bien réalisées qu'on n'y voit pratiquement que du feu. Cette technique prend notamment la forme d'un e-mail qui semble provenir d'un collègue ou d'une entreprise avec laquelle vous collaborez. Ces e-mails sont souvent le fruit d'une préparation minutieuse, comme la recherche de l'organigramme de l'entreprise.

En parallèle, il peut tout aussi bien s'agir d'e-mails envoyés par un inconnu. Les collaborateurs RH reçoivent souvent des CV qu'ils doivent ensuite ouvrir et étudier. Il suffit aux pirates de sélectionner une offre d'emploi et de rédiger un CV correspondant, sur la base d'un profil LinkedIn public. Un collaborateur RH ouvre le fichier ? Le logiciel malveillant est alors installé et permet aux pirates d'accéder au réseau, aux données financières, aux données R&D, etc.

LE SAVIEZ-VOUS ?

Le format PDF est le moyen par excellence de dissimuler une attaque : omniprésent, inoffensif, mais avec une foule de possibilités de dissimuler un code.

La sécurité
évolue pour répondre à cette complexité

On compare parfois la sécurité IT à un bonbon : dur à l'extérieur et mou à l'intérieur. L'extérieur – ou le périmètre – est bien protégé, notamment avec les pare-feu et le système de surveillance, mais à l'intérieur – infrastructures internes –, les mesures de sécurisation se limitent au strict nécessaire.

« Aujourd'hui, la sécurité ne se limite pas au périmètre », explique Patrick Lecluyse, Manager Professional Services chez Telenet. « Vous pouvez tout à fait sécuriser la porte d'entrée, mais laisser la porte de derrière ouverte.
La protection idéale s'apparente à la structure d'un oignon : elle présente plusieurs couches. Sécuriser le réseau, le centre de données, le cloud et les terminaux, c'est fermer toutes les portes, et pas seulement la porte d'entrée. Grâce à cette approche, l'intérieur du bonbon «difficile à croquer». »

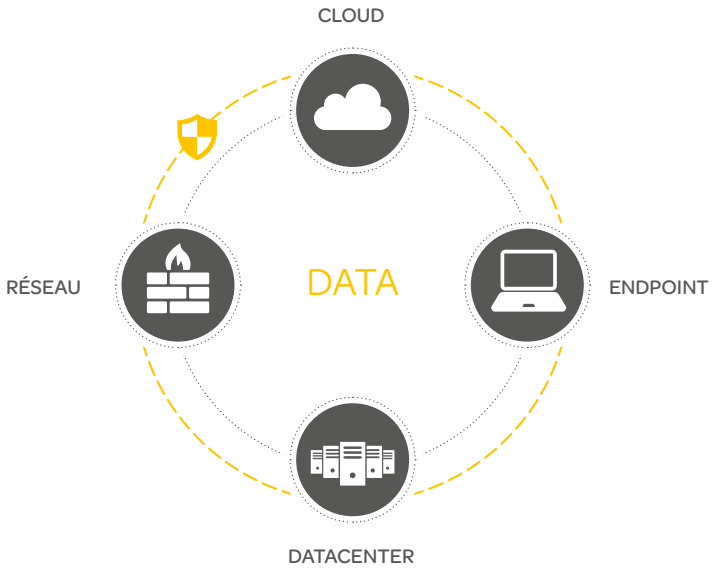
« La clé d'une sécurité optimale est une conception claire et conforme à votre politique de sécurité », affirme Glyn Jones, Service Manager chez Telenet. « Le client se focalise parfois sur le remplacement du matériel et non sur le renforcement de la sécurité. Le choix des solutions dépend bien sûr du type et de la taille de l'entreprise : un pare-feu sera déjà utile aux PME tandis que les entreprises actives en ligne doivent sécuriser leur réseau, mais aussi leurs applications et terminaux, et s'armer davantage contre les attaques DDoS. Nos consultants aident les clients à réfléchir de manière proactive à ce qu'ils doivent privilégier. »

Le graphique ci-dessous compare l'approche « à l'ancienne » et la vision moderne de la sécurité IT.

OLD SCHOOL

LA SÉCURITÉ IT EST COMPARABLE À UN BONBON

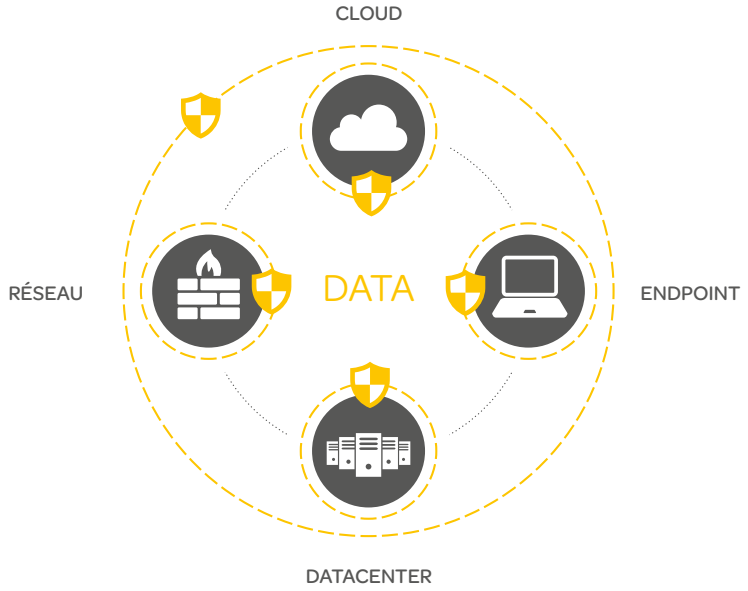
Dur à l'extérieur et mou à l'intérieur



NEW SCHOOL

LA SÉCURITÉ IT EST COMPARABLE À UN OIGNON

Elle présente plusieurs couches



Découvrez comment les technologies évoluent aux différents niveaux pour faire face aux menaces d'aujourd'hui.

Réseau

En raison de leur complexité accrue, de l'augmentation des applications personnelles et professionnelles, du comportement de l'utilisateur et des nouvelles menaces, les réseaux sont devenus beaucoup plus vulnérables ces dernières années. « La segmentation du réseau apporte une réponse à ces défis », remarque Nico Vandevoort, Security Presales Consultant chez Telenet. « La segmentation du réseau 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. »

« Les pare-feu de nouvelle génération empêchent, en outre, beaucoup de catastrophes », poursuit Nico Vandevoort. « Ils présentent de plus en plus de fonctionnalités pour sécuriser au mieux le réseau. Épinglons notamment le sandboxing et les Intrusion Prevention Systems (IPS). Le sandboxing vous permet d'examiner le comportement des fichiers suspects dans un environnement (cloud) distinct. Le fichier est envoyé à la sandbox où le comportement est simulé. On identifie des opérations suspectes ? Vous savez alors que quelque chose ne tourne pas rond. Les Intrusion Prevention Systems scrutent le trafic réseau afin de détecter une éventuelle activité malveillante et veillent à ce que les failles connues ne soient pas exploitées. »

Centre de données et cloud

Les nouvelles technologies de centre de données telles que le cloud computing ont radicalement transformé l'infrastructure IT type. Nico Vandevoort : « La sécurisation est aussi en pleine mutation. Dans les centres de données, il était, jusqu'il y a peu, essentiel de surveiller et de sécuriser 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 : ce que l'on appelle le trafic ouest-est définit précisément ce qui est autorisé et ce qui ne l'est pas. Là où un pare-feu physique suffisait autrefois à implémenter des politiques entre les clients et le centre de données, ce n'est plus le cas aujourd'hui. Pour appliquer une politique entre serveurs, vous avez aussi besoin de pare-feu au sein de l'environnement virtualisé. »

Terminaux

Pour se protéger des cyberattaques modernes, les entreprises doivent aussi envisager la sécurité des terminaux sous un nouvel angle. Kris Bogaerts, Security Consultant chez Telenet : « Cette tendance n'a pas échappé aux principaux fournisseurs. Ainsi, Palo Alto Networks et Check Point ont commercialisé deux systèmes, Palo Alto Traps et Check Point SandBlast Agent, qui visent à mieux sécuriser les terminaux. »

Ces deux technologies permettent aux entreprises de réagir de manière appropriée aux menaces actuelles et futures. Kris Bogaerts : « Palo Alto Traps propose une sécurisation de pointe des terminaux contre la plupart des menaces avancées. Il n'utilise plus une base de données de signatures – comme les antivirus traditionnels -, mais se concentre sur les techniques privilégiées des pirates. L'objectif de Traps est d'identifier les techniques d'attaque et de les neutraliser. Check Point SandBlast Agent adopte une autre approche : le système applique la fonctionnalité de passerelle existante aux terminaux. Il se focalise sur l'intégration entre la protection par la passerelle et le terminal. Outre une sécurisation proactive avec le sandboxing et la technique de threat extraction, SandBlast Agent fournit aussi une analyse des incidents de sécurité. »

Combinaison de niveaux

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. Une attaque DDoS peut, en outre, servir de diversion pour cacher une autre attaque. Alors qu'une attaque DDoS paralyse votre serveur de messagerie – et que vous portez toute votre attention sur ce problème –, les pirates peuvent, par exemple, dérober des données de clients.

Mieux vaut vous prémunir contre ces trois types d'attaques, car dans le pire des cas, vous pouvez être confronté à une combinaison de ces attaques. N'hésitez donc pas à conjuguer plusieurs solutions anti-DDoS.

La sécurité n'est pas une science exacte

En tant qu'entreprise, vous pouvez implémenter une bonne sécurisation à chaque niveau, mais ne pas parvenir à élaborer de bonnes politiques.

Glyn Jones : « 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. »

La politique de sécurité des entreprises doit les aider à identifier les risques qu'elles souhaitent prendre et ceux qu'elles vont couvrir. Glyn : « Elles peuvent, sur cette base, concevoir l'infrastructure de sécurité nécessaire. Telenet peut intervenir dans la définition et l'optimisation des règles du pare-feu, mais le client en assume toujours la responsabilité finale. Nous faisons office de serrurier ; c'est le client qui choisit le type de serrure qu'il pose sur sa porte et le nombre de clés qu'il fait reproduire. »

ROUND UP

LA SÉCURITÉ IT NÉCESSITE UNE VISION ET UNE APPROCHE CLAIRES

Un nouveau contexte, de nouvelles menaces et de nouvelles solutions nécessitent une vision globale claire en matière de sécurité. Découvrez l'évolution de l'approche de Telenet Security dans le chapitre suivant.

CHAPITRE 3

« Notre approche est basée sur le cycle de vie de la sécurisation. Dans ce cadre, nous nous concentrons sur trois piliers : la prévention, la détection et la récupération. »

Brice Mees
Security Services Operations Manager chez Telenet

CHAPITRE 03

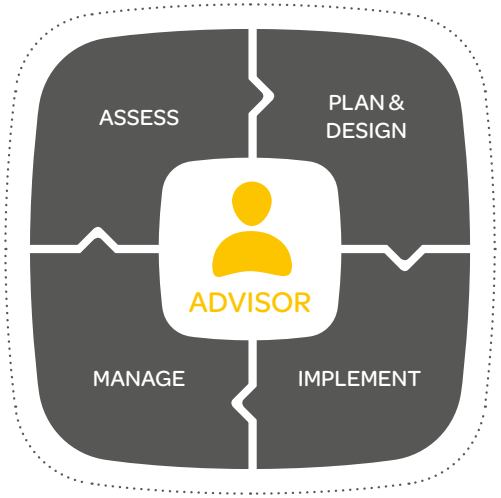
- La sensibilisation, la base de tout
- Un nombre de fournisseurs limité pour des connaissances optimales
- Approche architecturale assortie de composantes à la mesure du client
- Flexibilité en termes de support
- Accent sur le rôle proactif et consultatif
- La sécurité DDoS commence chez le fournisseur télécom

L'approche de Telenet Security

Le cycle de vie de la sécurisation
le principe de base d'une sécurisation constante

Telenet Security envisage la sécurisation comme un processus continu. 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.

Notre approche est basée sur le « cycle de vie de la sécurisation ». Nous nous concentrons constamment sur trois piliers : la prévention (prévention des menaces), la détection (identification des menaces) et la récupération (rétablissement post-menaces).



La sensibilisation, la base de tout

Nous sommes convaincus que tout commence par la sensibilisation. « Il est essentiel de susciter une prise de conscience chez le client », affirme Bart Van den Branden, Product Manager Security chez Telenet. « En termes de produit, Telenet était un intégrateur de sécurité classique jusqu'à il y a quelques années. Nous intégrions les composantes classiques dans le réseau : les pare-feu, les proxys, etc. Nous avons toutefois mis notre rôle consultatif sur le devant de la scène ces deux dernières années. Et cette mission consiste avant tout à sensibiliser nos clients. »

Le pentesting est le point de départ idéal pour une sécurisation plus efficace. Bart Van den Branden : « C'est pourquoi nous avons décidé de collaborer avec Toreon, qui se classe parmi les meilleures entreprises belges en matière de piratage éthique. Son expertise et son indépendance sont ses deux atouts majeurs. Elle n'est, en effet, liée à aucun produit, fournisseur ou opérateur télécom. Sa franchise est absolue. » Dieter Sarrazyn, Security Consultant & Managing Partner de Toreon, présente brièvement l'approche de l'entreprise. « Nous travaillons toujours de manière standardisée. Nous déterminons le périmètre du projet et composons, sur cette base, une équipe de pirates éthiques. Ces experts certifiés disposent d'au moins 15 ans d'expérience et sont spécialisés dans le piratage d'un domaine particulier, comme les réseaux ou les applications web. Après le pentest – qui se déroule via des outils (20 %) et manuellement (80 %) –, nous établissons un rapport assorti de recommandations que nous abordons avec Telenet et le client. »

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 automatisée. Bart Van den Branden : « En matière de Vulnerability Management, 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 Davinsi Labs. L'entreprise dispose de toutes les compétences nécessaires pour interpréter correctement le rapport, mais surtout pour le transposer dans une approche GRC (gouvernance, gestion du risque et conformité) concrète. Le Vulnerability Management représente donc aussi le tremplin idéal et le plus proactif vers une politique de sécurité claire et renforcée. »

« Nos partenariats avec Toreon et Davinsi Labs nous ont permis de renforcer considérablement notre portefeuille de produits dans le domaine de la sensibilisation. Là où nous nous contentions principalement d'implémenter des solutions par le passé, nous pouvons désormais participer à la réflexion avec le client », conclut Bart Van den Branden.

« Assessment » en pratique

EN PRATIQUE | SECURITY CONSULTANCY

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

Security Assessment

Avec 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

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 corriger.

- 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

L'élargissement des réseaux complique la politique de pare-feu. Avec Security Policy Optimisation, nous analysons les manières d'optimiser votre politique.

- 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 Davinsi Labs –

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 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

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 : « 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 Platinum de Palo Alto Networks et partenaire Gold de F5. Andries De 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 des 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. Une véritable interaction à la clé : ils peaufinent leurs produits ou en développent même de nouveaux sur la base de notre input. »

« Plan & design » en pratique

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.

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.

Partenaire Platinum avec le statut d'élite ASC 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. Aujourd'hui encore, l'entreprise continue à proposer des solutions de sécurisation ultra modernes et intégrées.

Telenet est partenaire Platinum et possède le statut d'élite ASC (Authorized Support Centers). Ce statut apporte des avantages supplémentaires à nos clients. Ils bénéficient, en effet, d'une remontée directe vers les Senior Support Experts de Palo Alto Networks.

La garantie d'expertise de Palo Alto Networks, la rapidité de réaction et la continuité du service ont déjà été récompensées par le prestigieux « Excellence in Support EMEA Award ».

Xavier Duyck,
Country Manager Belux chez
Check Point

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

Luc Vervoort,
Director EMEA Strategic Alliances
chez Palo Alto Networks

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

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.

Bart Van den Branden : « 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. Nos experts élaborent avec vous l'architecture adéquate, identifient les composantes de sécurité les plus appropriées et les implémentent. 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. »

« Implement » en pratique

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 partenaires 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 composantes 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	BlueCoat – F5
Mail AntiVirus/AntiSpam	Cisco Ironport – Barracuda Networks
Threat Prevention	Check Point – Palo Alto Networks – FireEye
Anti-DDoS	Akamai – Telenet – Check Point
Mobile Security	MobileIron
Endpoint protection	Check Point – Palo Alto Networks – Trend Micro
Vulnerability scanning	Rapid7

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.

Brice Mees, Security Services Operations Manager chez Telenet : « La majorité de nos clients gèrent leurs solutions eux-mêmes. Nous les formons, leur donnons des conseils et partageons notre expertise lors de réunions régulières. Certains points nécessitent d'être réajustés ? Nous identifions alors les points d'action requis. Dans le cadre de cette maintenance préventive, nous leur signalons par exemple qu'une technologie arrive en fin de vie ou qu'un patch ou une mise à jour va sortir. Le client peut ainsi procéder lui-même à ces changements. Il peut aussi nous confier leur mise en œuvre s'il le souhaite. »

Les clients qui désirent aller encore plus loin optent pour Security Support : soit pendant les heures de bureau, soit 24 h/24 et 7 jours/7. Ils peuvent ainsi contacter directement nos spécialistes en cas de questions ou de problèmes. Bjorn Desander, Manager Service Desk Security chez Telenet : « Notre helpdesk de sécurité ne dispose en effet pas de la "première ligne" habituelle. Les clients sont d'emblée mis en contact avec un ingénieur certifié capable de les aider. Un véritable avantage pour les clients, mais aussi pour les partenaires. Nous sommes plus qu'une simple boîte aux lettres : nous fournissons même le support de première et de deuxième ligne à nos meilleurs vendeurs. Nous résolvons ainsi la plupart des incidents sans impliquer le fournisseur. »

Nous proposons le service Managed Security aux clients qui souhaitent nous confier la gestion totale de leur architecture de protection. Brice Desander : « Avec Managed Security, nos spécialistes se chargent de la gestion de l'infrastructure, du monitoring et de l'optimisation de la protection. Les clients ont, à cet égard, le choix entre plusieurs niveaux de SLA (Service Level Agreement), d'une formule Basic à une formule Premium. »

« Manage » en pratique

EN PRATIQUE | SECURITY SUPPORT ET MANAGED SECURITY

Security Support

Support technique efficace assuré par des spécialistes de la sécurité certifiés et gestion efficace des licences comme garantie d'une protection continue.

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

Externalisation de la gestion de votre infrastructure, du monitoring et de l'optimisation de votre sécurité à nos spécialistes en la matière.

BASIC | Pack de base pour la maintenance de votre protection TIC

- Administration quotidienne de votre infrastructure par nos spécialistes
- Monitoring de la disponibilité
- Service Manager personnel
- Réunion annuelle pour examiner le fonctionnement et les résultats

STANDARD | Extension de Basic Managed Security, avec monitoring complet de la disponibilité et des performances

- Monitoring complet de la disponibilité et des performances
- Davantage de changements de configuration et de mises à jour logicielles
- Rapports trimestriels détaillés par votre Service Manager

PREMIUM | Extension de Standard Managed Security, avec une analyse continue de la situation et de l'évolution de votre sécurisation

- Analyse continue de la situation et de l'évolution de votre sécurisation
- Davantage de changements de configuration et de mises à jour logicielles
- Rapports mensuels détaillés par votre Service Manager

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. »

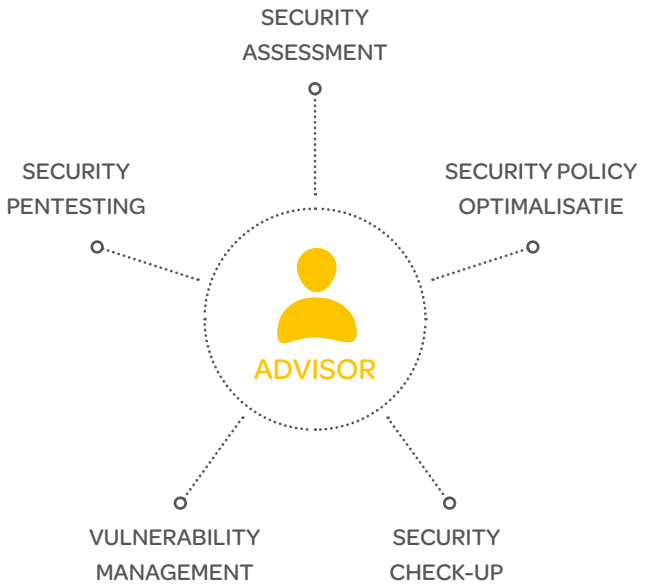
Brice considère le Trusted Security Advisor comme le pivot central du cycle de vie de sécurité du client : « Il signale par exemple les nouvelles versions et fonctionnalités de manière proactive, et donne de précieux conseils quant aux performances actuelles, à la maîtrise et à la sécurisation. Il peut,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

« Advice » en pratique

EN PRATIQUE | TRUSTED SECURITY ADVISOR

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



La sécurité DDoS commence chez le fournisseur télécom

Il existe plusieurs solutions pour contrer les attaques DDoS : des solutions « sur site » aux solutions « dans le cloud ». Chez Telenet Security, nous estimons que le fournisseur télécom a aussi son rôle à jouer.

Lore Mattelaer : « Compte tenu de la forte hausse des attaques DDoS, nous avons lancé la solution Anti-DDoS sur notre propre connectivité début 2016. Nous pouvons ainsi offrir à nos clients connectés une combinaison unique de trois technologies anti-DDoS, en collaboration avec nos partenaires technologiques. Alors qu'une solution sur site vous protégera généralement des attaques applicatives et protocolaires, une solution anti-DDoS sur notre connectivité et dans le cloud préviendra les attaques volumétriques. »

ANTI-DDOS SUR NOTRE PROPRE CONNECTIVITÉ

La solution anti-DDoS est disponible avec les produits internet Corporate Fibernet et iFiber de Telenet. Elle vous protège des attaques suivantes :

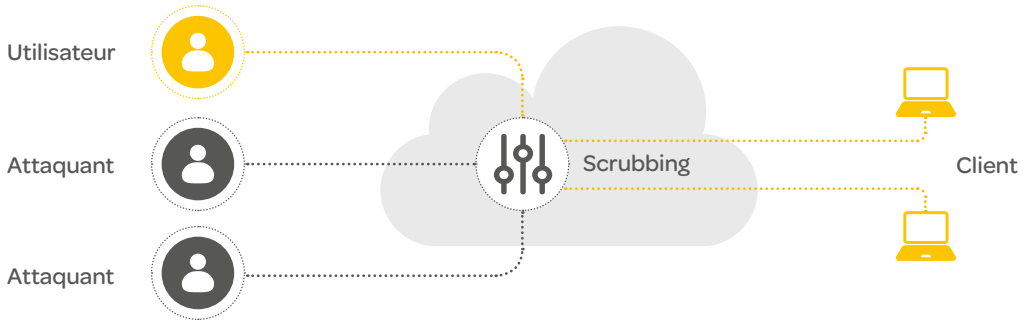
- paquets invalides : paquets qui ne répondent pas aux normes d'internet ;
- attaque par fragmentation, des fragments qui ne peuvent pas être réassemblés correctement ;
- imposants paquets NTP et DNS, typiquement utilisés lors des attaques DDoS par amplification ;
- charges et paquets sortants SSDP ;
- trafic d'appareils membres d'un botnet.

« Anti-DDoS » en pratique

EN PRATIQUE | ANTI-DDOS SUR NOTRE PROPRE CONNECTIVITÉ

Pour vous protéger au mieux des attaques volumétriques, nous lançons 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.

La solution anti-DDoS fonctionne en deux étapes



ÉTAPE 01

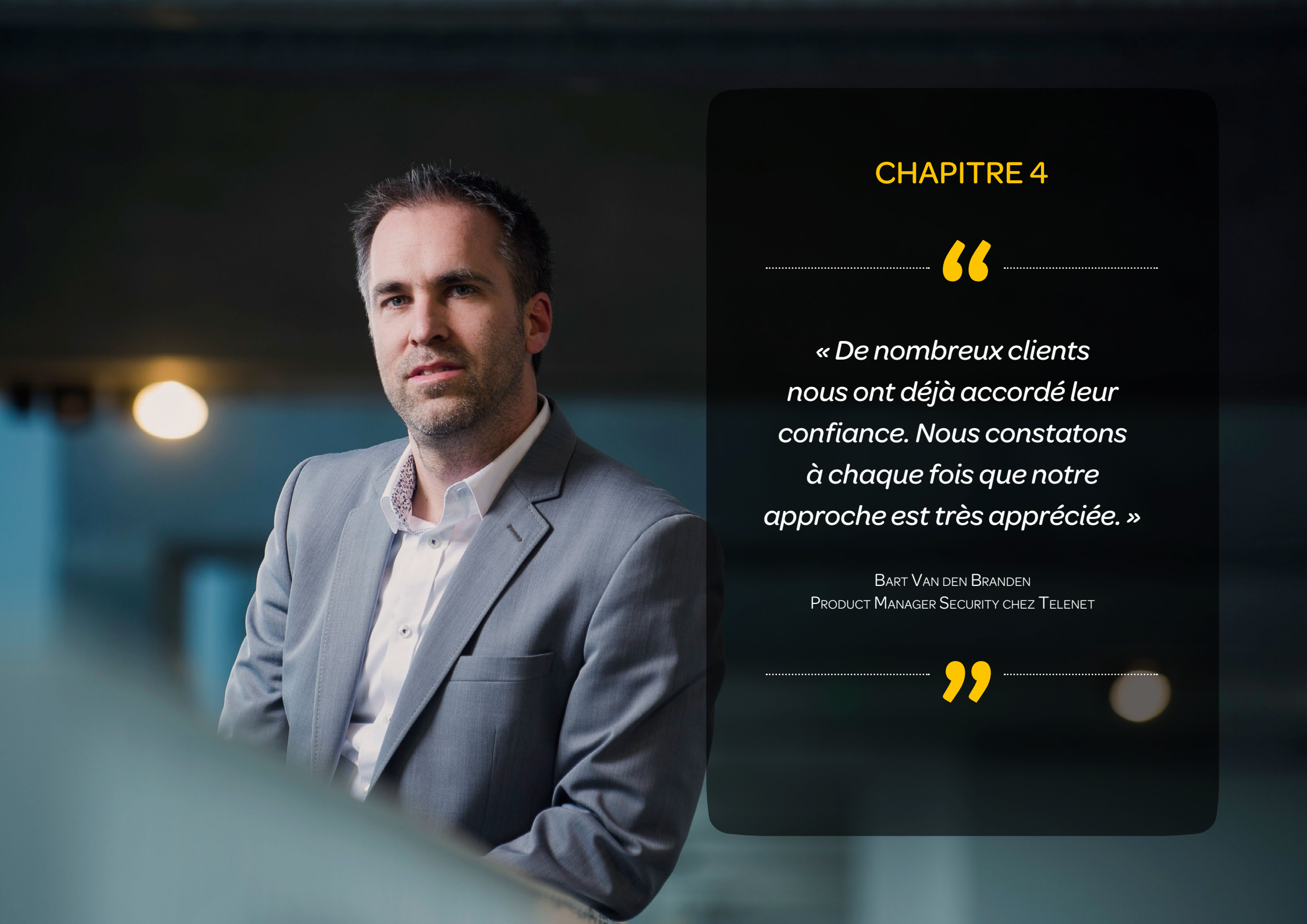
Nous surveillons et analysons en permanence le trafic de votre réseau

Telenet surveille et analyse le trafic de votre réseau en continu à l'aide d'un système de gestion anti-DDoS. Ce système permet d'identifier les attaques DDoS volumétriques types sur la base d'un intelligence feed DDoS à l'aide des empreintes actuelles des attaques et d'une liste de botnets.

ÉTAPE 02

Notre infrastructure de scrubbing filtre automatiquement le trafic suspect

Lors d'une attaque, le trafic de votre réseau est acheminé vers une infrastructure de scrubbing. Le scrubbing vise à filtrer l'attaque DDoS et à transférer vers votre réseau uniquement le trafic de réseau sûr. Le tout sans que vous vous en aperceviez : l'attaque n'impacte pas votre réseau. Votre bande passante n'est donc jamais en danger.



CHAPITRE 4

« De nombreux clients nous ont déjà accordé leur confiance. Nous constatons à chaque fois que notre approche est très appréciée. »

Bart Van den Branden
Product Manager Security chez Telenet

Partena opte pour la protection à deux niveaux de Telenet

« Une solution professionnelle de qualité garantit désormais la protection de nos données. »

Franky Goethals
Manager Infrastructure & Security – Partena

LE DÉFI

- Actualisation de l'infrastructure IT obsolète
- Protection optimale des données confidentielles des clients
- Limitation des coûts

LA SOLUTION

- Security Check-up
- Security Implementation : F5 et CheckPoint
- Managed Security

LES AVANTAGES

- Protection fiable et constamment à jour
- 24/7 Business Support
- Limitation des coûts grâce à l'externalisation de la gestion

Lisez le témoignage de Partena ››

KEYTRADE BANK

Telenet offre à Keytrade Bank une connectivité fiable et une sécurité infaillible

« L'association de deux technologies garantit un niveau de sécurité supérieur. »

Arnaud de Prelle
Head of IT Infrastructure – Keytrade Bank

LE DÉFI

- Nécessité d'une protection et d'une fiabilité absolues
- Problématique accrue des cyberattaques et des logiciels malveillants à l'échelle mondiale
- Partenaire qui dispose de connaissances approfondies en matière de sécurité

LA SOLUTION

- Check Point
- FireEye
- Conseils pour l'implémentation, la maintenance et l'évaluation

LES AVANTAGES

- Protection de bout en bout
- Assistance professionnelle rapide, 24/7
- Service personnalisé et réel engagement

Lisez le témoignage de Keytrade Bank ››

Nouveau pare-feu à l'AZ Sint-Blasius

« Telenet nous aide via des révisions régulières et veille à la cohérence des règles de notre pare-feu. »

Rik Van Oost
ICT-manager – AZ Sint-Blasius

LE DÉFI

- Actualisation de la sécurité
- Sécurité unique et uniforme pour l'ensemble du trafic
- Équipe IT réduite

LA SOLUTION

- Approche globale, du matériel à l'assistance
- Deux nouveaux pare-feu : Check Point
- Gestion assurée par Telenet

LES AVANTAGES

- Suivi permanent et évaluations régulières
- Temps de réaction amélioré
- Redondance totale

Lisez le témoignage de l'AZ Sint-Blasius ››

Business

EN SAVOIR PLUS

telenet.be/security 0800 66 066