Telenet Security Whitepaper

Plus de sécurité pour faire des affaires et collaborer sur internet

Business

150 000

Chaque jour en Europe, près de 150 000 ordinateurs sont contaminés par un virus.

290 miljard

Symantec estime le préjudice engendré par la cybercriminalité mondiale à 290 milliards d'euros par an.

18%

Il ressort de l'enquête Eurobaromètre sur la cybercriminalité que 18 % des internautes hésitent davantage à faire des achats sur internet en raison d'inquiétudes concernant la cyberprotection.

1/4

D'après Eurostat, un quart seulement des entreprises disposent d'une politique claire en matière de protection ICT.

Source : europa.eu - mars 2014

Plus de sécurité pour faire des affaires et collaborer sur internet

Sommaire

Introduction

Saisissez les opportunités gérez les risques

Avec une connexion internet performante, rapide et fiable, vous pouvez collaborer plus efficacement et explorer de nouvelles méthodes commerciales. Chez Telenet nous sommes sur la brèche jour après jour pour vous offrir le meilleur accès au web. Nous sommes également attentifs aux risques mettant votre connectivité – et donc le bon fonctionnement de votre entreprise – en péril.

Internet nous confronte à des menaces telles que le vol de données, la violation de la vie privée, les virus et les campagnes diffamatoires. La plupart des entrepreneurs sont conscients de ces dangers et de la nécessité d'une protection efficace. Mais ils ne savent pas toujours comment intégrer une telle protection. C'est notamment ici que Telenet a un rôle à jouer. Nous mettons notre expertise et nos solutions à votre disposition pour limiter et même éliminer les risques.

« Chaque entreprise est désormais vulnérable sur internet, quelle que soit son ampleur ou son activité. »

Martine Tempels, Senior Vice-President,
Telenet Business

Ainsi, votre entreprise pourra exploiter pleinement les opportunités offertes par internet. Ce Livre Blanc vous donne un aperçu des risques encourus, décrit les solutions et produits existants, et montre comment les entreprises gèrent leur protection en pratique.

Dans la première partie, Xavier Mertens, Principal Security Consultant, passe en revue les menaces dont il vaut mieux tenir compte ainsi que les aspects à ne surtout pas négliger en matière de protection. Dans la seconde partie, nous nous penchons sur l'aide apportée par Telenet pour la protection de votre connectivité et de vos données. La troisième partie porte sur quelques technologies de sécurisation. Enfin, diverses études de cas vous montrent comment nous travaillons, quelles solutions concrètes nous avons réalisées, et quel en est le résultat.

Nous espérons que ces informations contribueront à une utilisation plus sûre d'internet dans votre organisation. Elles s'adressent à toutes les entreprises car chacune d'entre elles est désormais vulnérable sur internet, quelle que soit son ampleur ou son activité. Ce document ne peut, certes, pas apporter une réponse exhaustive à toutes vos questions concrètes. C'est impossible. Votre Account Manager chez Telenet et nos spécialistes en sécurité pourront néanmoins approfondir vos besoins spécifiques.

Nous serons ravis de pouvoir vous être utiles.

Martine Tempels
Senior Vice-President
Telenet Business

« Aujourd'hui, chaque entreprise est une cible potentielle »

« La sécurité est trop souvent l'apanage des spécialistes. Elle doit devenir plus accessible à l'utilisateur final », déclare Xavier Mertens, Principal Security Consultant. D'après lui, c'est l'humain le maillon faible dans la chaîne de sécurité et il faut redoubler d'efforts pour mettre un terme aux actes malveillants. Car voici la mauvaise nouvelle : ils ne cessent de croître.

Xavier Mertens : « Pour l'équipe de CERT.be (*Cyber Emergency Team belge*), la situation tend à s'aggraver. Cette évolution négative se confirme d'ailleurs au niveau international. Ainsi, le *Data Breach Investigations Report* a examiné plus de 47. 000 incidents de sécurité à l'échelle mondiale et sa conclusion est sans appel : aujourd'hui, chaque entreprise est une cible potentielle. Le rapport indique également une forte hausse de la rapidité et de l'ingéniosité des criminels. Il est toutefois surprenant de constater que pour 78 % des intrusions relevées, il n'a pas fallu de connaissances pointues ni de ressources particulières pour pénétrer les systèmes d'une entreprise. Le rapport précise en outre que dans 84 % des cas, les criminels avaient atteint leur cible en quelques minutes à peine. Les entreprises n'accordent pas encore une priorité suffisante à la protection de leurs données - sans doute en raison des coûts y afférents, qu'elles ne veulent pas consentir. Pourtant, les conséquences d'un seul incident peuvent s'avérer catastrophiques, tant pour le fonctionnement de l'entreprise que pour sa situation financière et son image. Le facteur temps y joue également un rôle. À titre d'exemple, les entreprises confrontées à une forte pression concurrentielle misent résolument sur le développement de nouveaux produits, reléguant les impératifs de sécurisation au second plan. »

Plus de confort, plus de risques

« La situation est d'autant plus alarmante que l''Internet of Things' est en plein essor : de plus en plus d'objets et de machines sont connectés via internet, ce qui leur permet d'échanger des informations entre eux ou avec des gens. Cette évolution est fantastique en soi. Ainsi, votre smartphone vous permet de régler votre chauffage central à distance via l'internet mobile. Une solution pratique mais ce type de connexion peut aussi faire l'objet d'abus. Pensez, par exemple, aux photocopieuses d'entreprises. De nos jours, elles ont toutes une adresse IP. Les criminels peuvent atteindre votre réseau d'entreprise via ces machines et consulter les données de la mémoire tampon. Si vous avez copié des données sensibles, vous vous les ferez subtiliser sans même vous en rendre compte. »

Ne négligez pas la sécurité en cas d'outsourcing

« Les criminels tentent d'atteindre des sociétés via leurs partenaires. Votre entreprise peut donc s'avérer une cible intéressante, non pas en elle-même, mais parce que vous faites des affaires avec une autre entreprise. Les entreprises technologiques fournissant des services sur un VPN via un *accès distant* constituent dès lors une proie privilégiée. Si vous travaillez vous-même avec des fournisseurs IT externes, assurez-vous de toujours bien savoir où vos données se trouvent, comment leur accès est régulé et quelles personnes sont impliquées. Si vous contrôlez tout correctement, il n'y a pas de raison de paniquer. Le *Data Breach Investigations Report* précise que les nouvelles applications telles que le *cloud computing* n'entraînent pas de risques accrus. Que du contraire. La plupart des intrusions transitent toujours, apparemment, par des ordinateurs portables, des ordinateurs de bureaux et des serveurs classiques. »

Les humains demeurent le maillon faible

« Le piratage de machines représente encore un risque important mais un autre problème en expansion rapide est le phishing. Il s'agit de la falsification de vrais sites web et e-mails afin de voler des informations sensibles, comme des numéros de cartes de crédit ou des données de connexion. Le phishing est en plein essor car les gens continuent à cliquer sur les liens et boutons sans trop se poser de questions. D'un côté, il y a les e-mails de phishing, tellement mal rédigés que la plupart des gens se rendent compte qu'il s'agit de falsifications. Mais comme ces e-mails sont envoyés à des millions de personnes, ils obtiennent tout de même des résultats. Il suffit que quelques destinataires crédules se laissent duper. Une tendance plus inquiétante pour les entreprises est celle du *spear phishing* : d'excellentes falsifications ciblant des personnes spécifiques. Elles sont tellement bien réalisées qu'on n'y voit quasi que du feu. Vous pensez avoir affaire à un véritable e-mail d'un véritable collègue. Ces e-mails sont souvent le fruit de plusieurs mois de préparation. Les programmes de sensibilisation sont très importants pour rendre les collaborateurs attentifs à ce type de risque. Ils doivent également savoir que de nos jours, les criminels sévissent via des sites de réseaux sociaux et des call centers. »

« Votre entreprise peut s'avérer une cible intéressante, non pas en elle-même, mais parce que vous faites des affaires avec une autre entreprise. »

Xavier Mertens, Principal Security Consultant

La sensibilisation du personnel à la problématique peut rapidement renforcer la sécurité au sein de l'entreprise. Ceux qui ne prennent pas d'initiatives finiront par y être incités par le législateur. Ainsi, le Parlement européen a lancé l'année dernière une nouvelle *Directive sur la protection des données* qui, une fois convertie en législation, obligera les entreprises à signaler les *violations de données à caractère personnel*. La Commission Vie privée pourra aussi imposer des amendes, ce qui n'est pas encore le cas. Une telle amende impliquera non seulement une sanction financière, mais elle entachera aussi la réputation d'une entreprise.

Dangers fréquents

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 pour envoyer des spams, propager des virus, faire transiter des données en douce ou lancer des attaques sur des systèmes informatiques. Les ordinateurs d'un botnet nuisent également à l'entreprise contaminée car ils utilisent de la bande passante et peuvent ralentir un réseau. Vous pouvez en outre être considéré comme juridiquement responsable si vos ordinateurs sont impliqués dans un crime.

Attaques DDoS

Les botnets sont souvent utilisés pour mener des attaques DDoS (Distributed Denial-of-Service attacks, attaques distribuées par déni de service). Lors de DDoS, les ordinateurs du botnet se connectent en même temps à un serveur (web). Vu le nombre considérable de connexions simultanées, ce serveur plante ou devient inaccessible. De telles attaques peuvent paralyser des systèmes d'entreprises et d'institutions publiques.

Phishing

Le phishing est une forme de social engineering où des gens sont attirés vers un faux site (bancaire), souvent par e-mail. Les utilisateurs dupés sont alors invités à introduire leurs données de connexion, un numéro de carte de crédit ou d'autres données sensibles.

Chevaux de Troie

Un cheval de Troie ressemble à un programme ou fichier ordinaire, mais contient des fonctions cachées permettant l'accès à l'ordinateur infecté depuis l'extérieur. Souvent envoyés en pièce jointe à un e-mail, les chevaux de Troie sont utilisés pour collecter des adresses e-mail ou accéder à un compte bancaire. Il ne faut pas confondre un cheval de Troie avec un virus, qui endommage un ordinateur, ou un ver, qui se propage d'ordinateur en ordinateur.

Xavier Mertens *est Principal Security Consultant. Il se spécialise depuis 2006 dans les Security Assessments et audits, l'architecture de la protection et le Security Monitoring. À l'instar des autres experts en sécurité de Telenet, il affine ses connaissances en permanence. Xavier a ainsi décroché de nombreux certificats agréés à l'échelon international en matière de sécurité.* ***Suivez Xavier sur blog.rootshell.be***

La sécurité selon Telenet

01 La sécurité : un processus continu

Comment protégez-vous votre connectivité, vos données et vos systèmes ? Il n'y a hélas pas de réponse simple et univoque à cette question. Chaque entreprise est unique. Et aucun produit n'offre une sécurisation parfaitement sur mesure. Notre approche est donc très différente de celle des 'product resellers'.

En voici les 7 principaux atouts :

1 Approche orientée-processsus

Telenet voit la sécurisation comme un processus continu. Ce processus commence par une évaluation ou un audit de votre situation actuelle ainsi que l'analyse de vos besoins. Le suivi et le réalignement y jouent un rôle essentiel.

2 Approche architecturale

Nous sommes persuadés que la sécurisation doit viser bien davantage que de purs produits. Nous optons résolument pour une approche 'architecturale' et non pour des solutions techniques 'ad hoc' qui, dans le meilleur des cas, ne vous apporteront qu'une aide temporaire.

3 Partenariats en toute indépendance

Nous ne faisons pas la promotion de produits mais établissons des partenariats en fonction des besoins de nos clients. Ainsi, nous sommes les premiers en Europe à avoir opté pour Palo Alto Networks, et les seuls en Belgique à disposer du plus haut niveau de partenariat chez Palo Alto Networks et Check Point. Ce sont les leaders du Magic Quadrant de Gartner pour les pare-feu d'entreprises. Notre partenariat avec ces deux acteurs démontre l'excellence de notre expertise, l'ampleur de notre installed base et l'efficacité de notre back-to-back support.

4 Pragmatisme

Outre le 'firewalling', Telenet planche sur des dossiers liés à l'application delivery control, au MDM, etc. Nous travaillons avec pragmatisme, compte tenu de ce qui importe vraiment pour votre environnement. Nos consultants techniques vous aident à assimiler les nouveautés. Ils effectuent des tests dans notre labo, essaient de nouvelles versions et suivent les évolutions technologiques de diverses autres manières.

5 Connaissances et expérience poussées

Nous détenons depuis 1998 les connaissances et l'expérience requises pour l'intégration et l'optimisation d'une architecture de sécurisation complexe. Notre Security Competence Center compte plus de 30 spécialistes chevronnés en matière de produits, technologies et processus d'entreprises.

6 Collaboration ouverte

Une grande partie de nos clients gèrent leurs solutions eux-mêmes. Nous assurons leur formation, prodiguons des conseils et partageons notre expertise lors de réunions fréquentes. Ceux qui préfèrent les services administrés ('managed services') peuvent également compter sur un contact technique attitré. Nous communiquons régulièrement et vous tenons informé via une solide documentation, par exemple.

7 Confort

Les entreprises souhaitant des services administrés ont le choix entre différents SLA (Service Level Agreements). Tout peut être réglé pour vous : modernisation, 'policy clean-up', gestion des licences, documentation, rapportage, changements, etc. Si un alignement s'avère nécessaire à l'un ou l'autre niveau, nous spécifions les points d'action requis. Les services administrés sont particulièrement intéressants pour les PME, entre autres parce qu'elles n'ont généralement pas les connaissances et l'infrastructure requises pour organiser leur sécurisation elles-mêmes. Dans le cas de services administrés, votre entreprise utilise des appareils installés chez Telenet ou nous gérons à votre place les appareils de votre entreprise.

« Avant, il fallait quasiment un diplôme universitaire pour établir une connexion VPN sécurisée. À présent, tout s'effectue en parfaite transparence pour nos utilisateurs. »

Bart Colson, VP IT Operations chez Telenet

« La sécurité est avant tout une question de business, elle démarre avec le relevé des principaux risques en la matière. »

Eric De Smedt, Manager Cyber Security chez Telenet

02 De la politique de sécurité à sa mise en œuvre

Telenet ne se contente pas de proposer des produits de sécurisation tels que Check Point et Palo Alto Networks : elle en fait elle-même usage. Bart Colson, VP IT Operations chez Telenet et Eric De Smedt, Manager Cyber Security, parlent de leur approche.

« *La mise en œuvre* de la sécurisation relève de l'IT, mais la sécurité est avant tout une question de business », souligne Eric De Smedt. « La sécurisation démarre avec le relevé des risques liés au business, à commencer par les plus importants. La politique de sécurité qui en découle au plus haut niveau est une politique gestionnelle encore peu pertinente sur le plan de l'IT. Vous allez la proposer aux différentes entités de votre organisation et ainsi la peaufiner sous la forme d'exigences. Vous établirez ensuite des normes de contrôle et déterminerez le mode de vérification du respect de cette politique. Bien entendu, vous devrez tester votre environnement en permanence, par exemple via des analyses de vulnérabilité. »

Connexion transparente

Operations, le département de Bart Colson, transpose les politiques et directives de Cybersecurity en solutions techniques. « L'année dernière, nous avons révisé notre infrastructure dans sa globalité et implémenté Palo Alto Networks. Toute notre communauté d'utilisateurs, qui compte quelque 3.000 personnes, déborde d'enthousiasme envers la migration vers le nouveau système. Avant, il fallait quasiment un diplôme universitaire pour établir une connexion VPN sécurisée. À présent, cette opération s'effectue de manière transparente en arrière-plan, que vous travailliez à la maison, dans un hôtel ou au bureau. Si votre PC passe en mode de veille, vous serez tout de même directement connecté lors de la réactivation. Cette simplicité d'utilisation et ce transfert transparent vers Palo Alto Networks s'appuient sur un travail de fourmis dans le back-office. Un système tel que Palo Alto Networks exige une configuration minutieuse, ce qui implique des opérations fort complexes. »

Détection anticipée

Bart Colson : « Grâce à Palo Alto Networks, nous savons mieux qui fait quoi et à quel endroit. Nous ne nous contentons plus de gérer les droits d'un utilisateur. Nous pouvons, par exemple, aborder des problèmes de façon anticipée, vu que le système va signaler les comportements anormaux. Et pour cela, nous ne sommes pas obligés d'indiquer nous-mêmes au préalable ce qui est 'anormal'. Le système le fait à notre place. C'est très important car les dangers actuels sont tellement nombreux qu'il est impossible de tous les définir et évaluer à l'avance. À présent, s'il se passe quelque chose, nous sommes directement avertis et pouvons tout de suite intervenir. »

Modèle progressif

Eric De Smedt : « Pour nous, la sécurité revêt une importance cruciale. Nous appliquons la norme internationale ISO 27001/2 et, en tant qu'entreprise cotée en Bourse avec un actionnaire principal américain, devons également satisfaire à la réglementation SOX américaine. Mais vous pouvez toujours suivre notre approche progressive même si vous ne voulez ou pouvez pas satisfaire à ces normes draconiennes. Il faut d'abord définir la stratégie puis chercher des solutions. N'oubliez pas non plus qu'un environnement complexe est plus difficile à sécuriser. Il est donc toujours intéressant de réduire la complexité. »

Prêt pour l'IPv6 ?

Maintenant que le manque d'adresses IPv4 se fait de plus en plus ressentir, Telenet consacre une attention explicite à l'IPv6. Nous mettons tout en œuvre pour que vous puissiez faire face à l'évolution vers ce nouveau protocole.

Les concepts et produits que nous proposons à nos clients tiennent tous compte de l'IPv6 et nos consultants maîtrisent bien ce domaine. N'hésitez pas à leur demander des explications et des conseils.

« Grâce à Palo Alto Networks, nous savonsmieux qui fait quoi. »

Bart Colson, VP IT Operations chez Telenet

De l'identification à la protection contre les DDoS

Grâce au rachat de C-CURE, Telenet peut s'appuyer sur une expertise en matière de sécurisation qui remonte à 1998. Pour l'heure, nous disposons de 15 Security Engineers certifiés parfaitement à l'aise dans un vaste éventail de technologies liées à la sécurité. Telenet travaille notamment avec Check Point, Palo Alto Networks, F5 et d'autres produits de pointe. Bref tour d'horizon...

Check Point

Telenet est partenaire Platinum de Check Point Software Technologies, l'un des leaders en firewalling de nouvelle génération. En plus d'un contrôle sophistiqué en matière d'identité et d'applications, les solutions de Check Point offrent de nombreuses possibilités de virtualisation. Vous pouvez en outre adapter la sécurisation de votre environnement à vos besoins spécifiques via des 'software blades' : des 'lames logicielles' modulaires qui s'installent et se configurent rapidement.

Caractéristiques

- Contrôle de l'identité
- Contrôle de l'application
- Système de prévention des intrusions (Intrusion Prevention System, IPS)
- Filtrage d'URL
- Antivirus
- Antibot
- Émulation des menaces (Threat Emulation)
- Accès mobile sécurisé aux applications de l'entreprise via un portail SSL et un SSL VPN
- Pare-feu virtuel intégré (VSX)
- Génération de rapports détaillés avec SmartEvent/SmartReporter
- Options de redondance (Clustering) pour la passerelle et la gestion

Avantages

- Approche structurée de la politique de sécurité
- Compatible avec diverses plates-formes
- Excellente gestion centrale
- Protection puissante contre les logiciels malveillants (‘malwares’)

Nouveautés de Check Point R77

- Threat Emulation Blade avec protection contre les menaces ‘Zero-Day’ et inconnues, analyse du comportement hostile en bac à sable (‘Sandbox’), et partage des constatations via ThreatCloud
- Compliance Blade
- Moteur HyperSPECT aux performances optimisées

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 ultramodernes intégrées pour la sécurité. En 2013, le consultant en technologie Gartner a donc de nouveau classé Palo Alto Networks parmi les leaders de son ‘Magic Quadrant for Enterprise Firewalls’. Telenet est partenaire Platinum de Palo Alto Networks et Palo Alto Networks Authorized Training Center.

Caractéristiques

- Contrôle de l’identité
- Contrôle de l’application
- Système de prévention des intrusions (Intrusion Prevention System, IPS)
- Filtrage d’URL
- Antivirus
- Anti-spyware
- Protection WildFire contre les logiciels malveillants de type ‘Zero-Day’
- GlobalProtect
- VPN IPSec
- Virtualisation
- Options de redondance (Clustering) pour la passerelle et la gestion

Avantages

- Politique simple avec sécurité basée sur les applications (‘Application Based Security’)
- Plates-formes multiples (50 Mbits/s à 20 Gbits/s)
- Multi-plate-forme OS uniforme
- Gestion basée sur le web
- Gestion des rapports à la demande
- Modèle de licence simple

Nouveautés de Palo Alto Networks 6.0

- Améliorations liées à la technologie Wildfire (nouveaux types de fichiers et système d’exploitation)
- Pare-feu VM-Series sur Citrix SDX
- Pare-feu VM-Series NSX Edition

Palo Alto Networks Authorized Training Center

Telenet est aussi Palo Alto Networks Authorized Training Center. Nous organisons notamment une formation normalisée de trois jours sur la sécurité pour les utilisateurs de Palo Alto Networks. Vous pouvez également découvrir les possibilités de Palo Alto Networks sans engagement lors d'un atelier Ultimate Test Drive axé sur la pratique.

F5 BIG-IP

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

Quelques modules disponibles sur les ADC de F5 :

- **BIG-IP Local Traffic Manager (LTM)** améliore votre efficacité opérationnelle et garantit les performances de votre réseau, y compris en période de pointe. Utilisez LTM pour protéger vos applications critiques, réduire les temps d'arrêt, accélérer vos activités et effectuer des tâches telles que le Load Balancing et l'Offloading.
- **BIG-IP Access Policy Manager (APM)** permet l'authentification et l'identification unique ('Single Sign-on'), indépendamment du lieu et de l'appareil. APM consolide les fonctionnalités telles que l'accès distant, la gestion de l'accès web et le VDI, tout en simplifiant la gestion des politiques d'accès. Votre infrastructure devient ainsi moins complexe, d'où une réduction des coûts.

« Check Point convient particulièrement pour la gestion de nombreux pare-feu et services à grande échelle. »

Andries De Lombaerde, Senior Security Consultant chez Telenet

- **BIG-IP Application Security Manager (ASM)** inclut un pare-feu certifié pour une sécurité optimale des applications web basées sur une politique. Utilisez cette application pour une visibilité accrue, pour l'analyse des menaces et pour la conformité. ASM est une solution flexible, performante et évolutive.
- **BIG-IP Global Traffic Manager (GTM)** envoie automatiquement les utilisateurs vers l'environnement physique, virtuel ou cloud le plus proche ou le plus performant. GTM protège votre infrastructure DNS contre les attaques DDoS et offre une solution DNSSEC complète en temps réel qui vous protège contre les intrusions.

Caractéristiques

LTM

- Accélération et optimisation d'applications
- Analyse en temps réel
- Load Balancing
- Accélération et offloading SSL
- Mise en œuvre simple du protocole
- Optimisation du protocole
- Sécurisation efficace
- Contrôle adapté
- Flexibilité virtuelle et liée au cloud
- Performances et évolutivité importantes

GTM

- Performances et sécurisation DNS élevées
- Mise en cache et résolution DNS
- Sécurisation DNSSEC intégrale
- Global Server Load Balancing
- Contrôle permanent
- Application Health Monitoring
- Routage fondé sur l'emplacement

ASM

- Protection avancée
- Prévention du webscraping
- Sensibilisation et protection liées à la session
- Pare-feu XML intégré
- Protection des données et cloaking
- Corrélation des transgressions et regroupement des incidents
- Mises à jour automatiques des signatures d'attaque
- Contrôle basé sur la géolocalisation et la réputation

APM

- Convient pour IPv6
- Support pour serveur AAA
- Intégration aisée
- Identification unique (Single Sign-on, SSO)
- Sécurisation efficace
- Realtime Access Health Data

Nouveautés de BIG-IP

BIG-IP 11.3

- SSL forward proxy
- ICAP services
- Network HSM
- Unified logging framework

Big-IP 11.4

- Avec attribution flexible
- iApps
- Analytics

Big-IP 11.5

- iControl REST Interface
- Nouvelles fonctionnalités anti-DDOS sur ASM
- APM Secure Web Gateway

« Chez Palo Alto Networks, l'inspection des applications est toujours active. »

Bruno Gysels, Security Consultant chez Telenet

Infoblox

Solution destinée à la gestion centrale d'adresses IP ainsi que du DNS et du DHCP à partir de l'IPAM (IP Addres Management), Infoblox vous permet de contrôler toutes les adresses IP au sein de votre organisation. Son service DNS offre une sécurité DNSSEC et DNS Firewall. Infoblox est totalement prêt pour IPv6, qu'il prend en charge.

Pulse Secure Access

Avec Pulse Secure Access, vous offrez à vos utilisateurs mobiles un accès sécurisé à un réseau d'entreprise via une authentification sur tout dispositif orienté-web. Cette solution combine la protection SSL, le contrôle des accès basé sur des normes et la création de politiques sur mesure.

Cisco Ironport

Cisco Ironport est une solution axée sur l'envoi et la réception sécurisés d'e-mails avec un système d'exploitation dédié. Ses fonctionnalités antispam et antivirus sont très puissantes. Vous contrôlez les e-mails entrants sur la base de la réputation IP, vous bénéficiez d'un support SPF et DomainKey, et vous pouvez effectuer des contrôles de sécurité Sophos. Cisco Ironport intègre un tableau de bord complet et adaptable pour le suivi de toutes les activités liées à la messagerie.

Solutions contre les attaques DDoS

Telenet propose différentes solutions pour protéger votre entreprise contre les attaques DDoS (Distributed Denial-of-Service attacks) :

- Prolexic ('nettoyage dans le cloud')
- Dispositif anti-DDoS de Checkpoint
- Dispositif Arbor Networks Pravail
- Fonctions anti-DDoS de F5 Big IP.

BlueCoat

BlueCoat vous offre une architecture de plate-forme proxy évolutive pour sécuriser la communication web et accélérer la distribution des applications. ProxySG vous permet de vérifier de manière flexible et minutieuse si le contenu, les utilisateurs, les applications et les protocoles sont conformes à vos politiques.

MobileIron

MobileIron vous permet de gérer tous vos appareils, applications et documents mobiles de façon centralisée. Vous pouvez ainsi déterminer quelles applications peuvent être utilisées par un collaborateur et quelles données doivent être cryptées. En cas de perte ou de vol, vous pouvez effacer vos apps et données à distance de façon sélective.

« Nous constatons que de grandes entreprises établissant un VPN pour une multitude de petits sièges y ajoutent souvent notre Secured Internet Breakout. »

Bart Van den Branden, Product Manager Security chez Telenet

Telenet Secured Internet Breakout et SSL VPN

Fort de plusieurs années d'expérience en matière de sécurité, Telenet a également développé quelques produits dans ce domaine. Secured Internet Breakout est un pare-feu de nouvelle génération orienté-applications pour les entreprises disposant d'un VPN. « Nous constatons que e grandes entreprises établissant un nouveau VPN pour une multitude de petits sièges y ajoutent souvent notre Secured Internet Breakout, » déclare Bart Van den Branden, Product Manager Security. Cette solution offre une protection totale contre les intrusions, vols, virus et logiciels malveillants. Elle est proposée en tant que service administré et donc gérée par Telenet même. En complétant Secured Internet Breakout de SSL VPN, les utilisateurs mobiles peuvent également accéder au réseau de leur entreprise aisément et en toute sécurité. La sécurisation s'effectue par authentification de l'utilisateur via un token et par cryptage des données.

Belgian Cyber Security Guide

La fin de l'année dernière a vu la publication du tout premier Belgian Cyber Security Guide, une initiative lancée entre autres par la FEB, les Chambres du Commerce, EY et Microsoft. Ce guide comporte des recommandations, une auto-évaluation de sécurité, des études de cas et une vue d'ensemble des principaux cadres et adresses de contact liés à la sécurité. D'après ce guide, voici les 10 'must-do' en matière de sécurité :

01 Sensibilisez et formez les utilisateurs
02 Tenez les systèmes à jour
03 Protégez vos informations
04 Protégez les appareils mobiles
05 Ne donnez accès aux informations que si c'est nécessaire
06 Imposez des règles pour une utilisation sûre d'internet
07 Utilisez des mots de passe efficaces et conservez-les de manière sûre
08 Réalisez des back-ups de vos données et informations d'entreprise, et contrôlez-les
09 Abordez les virus et autres logiciels malveillants de façon hiérarchisée
10 Optez pour la prévention, détectez les problèmes et réagissez

« Telenet nous a proposé un concept exhaustif. »

Rik Van Oost, ICT Manager de l'AZ Sint-Blasius

Nouveau pare-feu à l'AZ Sint-Blasius

Voici quelques années, l'AZ Sint-Blasius a entamé la rénovation à grande échelle de son infrastructure IT. La capacité du réseau interne a été élargie et tous les télétravailleurs ont bénéficié d'une meilleure connexion. L'ancien pare-feu a également été reconsidéré. Rik Van Oost, ICT Manager : « Notre pare-feu avait 6 à 7 ans. Dans le domaine de la sécurité, c'est un âge 'vénérable', voire digne d'un 'traitement palliatif'. Il tournait sur un serveur unique et commençait à devenir un véritable goulet d'étranglement. Nous nous sommes donc mis en quête d'une nouvelle solution et avons abouti chez Telenet. »

Comme dans d'autres hôpitaux comparables, le département IT de l'AZ Sint-Blasius est relativement modeste. L'établissement cherchait donc un partenaire proposant une approche exhaustive. « Une entreprise capable de gérer les logiciels, le matériel, le support et la migration », explique Rik Van Oost. « En interne, nous n'avons ni le temps, ni les connaissances pour tenir à jour un pare-feu et assurer nous-mêmes son suivi. Nous sommes désormais épaulés sur ce plan par Telenet, qui nous a proposé un concept exhaustif. »

Concept exhaustif

Rik Van Oost : « Telenet nous aide via des révisions régulières et veille à la cohérence des règles de notre pare-feu. Il peut aussi contrôler le pare-feu proactivement 24 heures sur 24, ce qui nous est impossible avec nos effectifs limités. Nous avons d'abord examiné ensemble ce dont nous disposions, puis introduit le nouveau matériel, repris la configuration de l'ancien pare-feu, reconsidéré et rationalisé les règles et enfin, nous avons opéré la transition. Comme nous utilisons la 'Klinisch Werkstation' (KWS, station de travail clinique) de l'UZ Gasthuisberg et sommes reliés à son campus par fibre optique, nous devions aussi tenir compte de ses exigences en matière de sécurité. »

Utilisateurs à domicile

Rik Van Oost : « S'il restait auparavant quelques îlots non contrôlés par notre ancien pare-feu, tout le trafic transite désormais par nos nouveaux pare-feu. Nous disposons à présent d'une protection uniforme pour tout le monde sans défaillances, sans intrusion de l'extérieur et avec un meilleur temps de réaction. De même, nous faisons travailler nos 120 médecins indépendants et actifs à leur domicile via le nouveau pare-feu. » Fréderic Vannieuwenhuyse, Coordinateur IT : « Notre nouvelle protection est entièrement redondante, avec deux pare-feu de Check Point. Comme nous n'avons aucun contrôle sur les ordinateurs des utilisateurs à domicile, il y a encore quelques problèmes de compatibilité sur ce plan mais ils devraient être résolus avec l'introduction de la lame logicielle Mobile Access Software Blade de Check Point. »

Procédures

Fréderic Vannieuwenhuyse : « Telenet a formé deux de nos collaborateurs à la gestion du pare-feu. Mais la gestion à plus grande échelle, comme les mises à jour et le rapportage, reste entre les mains de Telenet. » Maintenant que le pare-feu tourne bien, l'AZ Sint-Blasius peut se concentrer sur le peaufinage des procédures. Rik Van Oost : « Les pouvoirs publics nous imposent beaucoup d'exigences concernant la communication à l'intérieur comme à l'extérieur de l'hôpital. Vu la liaison avec diverses mutualités, la Banque-Carrefour, etc., nous sommes obligés de formaliser encore davantage notre politique en matière de sécurité. Cette formalisation des procédures est également importante pour que notre hôpital obtienne l'accréditation JCI. Nous devons pouvoir démontrer que nous sommes capables de voir à tout moment qui a accès à quels éléments. »

L'Algemeen Ziekenhuis Sint-Blasius de Termonde, dont les racines remontent à 1202, est un centre moderne pour une aide médicale de haute qualité. Cet hôpital se caractérise par son innovation audacieuse, son orientation-patient et son excellence dans des techniques mini-invasives. La direction a élaboré une vision d'avenir stratégique basée sur les valeurs-clés Sécurité, Information, Confort, Qualité clinique et Rapidité. L'hôpital compte 446 lits, répartis sur les campus de Termonde et Zele. Chaque jour, plus de 1.100 personnes s'investissent corps et âme pour prodiguer les meilleurs soins aux patients.

« La gestion à plus grande échelle, comme les mises à jour et le rapportage, reste entre les mains de Telenet. »

Fréderic Vannieuwenhuyse, Coordinateur IT de l'AZ Sint-Blasius

« Comme l'IT ne fait pas partie de notre 'core business', nous préférons confier la sécurité de notre environnement à une entreprise telle que Telenet. »

Frank De Winter, CEO et Directeur IT d'Arista

Arista : en sécurité dans le cloud

De grandes organisations qui ont tout mis sur le cloud ? Il y en a. Arista, un service externe de prévention et de protection au travail, en fait partie. Son cloud privé contient 800.000 dossiers médicaux et est utilisé par ses 250 collaborateurs. « Si vous intégrez tout dans le cloud comme nous, la sécurité devient essentielle », déclare Frank De Winter, CEO et Directeur IT d'Arista.

La décision d'adopter le cloud, Arista l'a prise lorsqu'elle est devenue autonome. Frank De Winter : « Avant, nous collaborions et partagions notre infrastructure avec HDP. Lorsque nous sommes devenus autonomes, ce n'était plus possible. Nous aurions pu entamer un processus de migration mais son impact était difficile à évaluer. Les migrations sont coûteuses et risquées. Leur époque est désormais révolue, car le cloud permet de créer plus facilement un nouvel environnement en parallèle de l'ancien. C'est une solution plus rapide et économique que la migration. »

Maintenir la distinction entre gestion et sécurité

Frank De Winter : « Toute notre infrastructure ERP se trouve sur le cloud. Comme il s'agit d'un environnement partagé, un contrôle indépendant est crucial. Voilà pourquoi nous avons choisi, en plus de notre partenaire pour le centre de données, un second partenaire pour la sécurité. Si vous confiez les deux au même fournisseur, vous perdez une part de contrôle. Pour bien régir la sécurité d'un environnement tel que le nôtre, seules deux entreprises entrent en ligne de compte en Belgique. Telenet est l'une d'elles. Elle peut livrer et installer le matériel adéquat, possède une connaissance approfondie de l'infrastructure réseau, comprend la problématique du cloud, etc.

C'est une expertise en sécurité que l'on ne trouve quasi nulle part ailleurs. Nous ne pourrions jamais nous en charger nous-mêmes. Comme l'IT ne fait pas partie de notre 'core business', nous préférons confier la sécurité de notre environnement à une entreprise telle que Telenet. Elle nous offre une protection sous la forme de services administrés. La simplicité même. »

Pourquoi Telenet ?

Le choix de Telenet n'a pas été motivé que par son expertise et son savoir-faire. Frank De Winter : « La façon de travailler a également joué un rôle. Le service-desk de Telenet compte parmi les meilleurs de Belgique. Et Telenet offre également la capacité requise. En trois mois de temps, nous devions passer du 'néant' à une architecture ERP complète sur le cloud. Dans pareil cas, on a besoin de partenaires aux épaules solides. Nous avons atteint nos objectifs avec Telenet. »

ARISTA

Frank De Winter est CEO et directeur IT d'Arista, un service externe de prévention et de protection au travail. Cette organisation effectue des examens médicaux, conseille les entreprises en matière de gestion des risques et apporte une assistance psychologique aux travailleurs.

« Avec Telenet, la collaboration a toujours été très enrichissante, basée sur la confiance et la proactivité. »

Bruno Delcourt, responsable du Service Réseaux & Voix de l'Université de Namur

Un pare-feu sur mesure pour l'Université de Namur

L'Université de Namur compte aujourd'hui six facultés, soixante-deux laboratoires, environ six mille quatre-cents étudiants et un millier de chercheurs. De nos jours, l'usager de l'Université ne peut plus se passer des outils informatiques, fixes et mobiles. « L'institution doit continuellement adapter ses infrastructures et technologies », nous explique Bruno Delcourt, responsable du Service Réseaux & Voix de l'Université de Namur.

« Par rapport à une dizaine d'années en arrière, les gros changements sont d'abord l'évolution des comportements et pratiques des utilisateurs, qui ne se contentent plus de consulter leur boîte e-mail. Ensuite, le nombre d'utilisateurs a explosé ! De même que le nombre d'appareils mobiles pouvant se connecter au réseau. Si l'on compte 2 ou 3 appareils par usager, on arrive à 13 à 18.000 appareils, qui vont potentiellement pouvoir se connecter au réseau de l'Université... En plus, les étudiants veulent également accéder à leurs données, partout et tout le temps. », explique Bruno Delcourt. « Nous avons changé de solution parce que nous sentions que des attentes n'étaient plus rencontrées. C'était le momentum ! Il était important d'aller au-delà des simples mesures de contrôle des ports. », précise-t-il.

Une question de confiance

« Pour que tout fonctionne, il faut bien entendu un bon produit au départ, mais ce n'est pas suffisant ! Il faut que le partenaire ait du répondant. Cela fait partie des éléments garantissant le succès. » En effet, Bruno Delcourt a pu apprécier la qualité et la richesse des échanges avec les spécialistes de Telenet Security, sur les plans technique et commercial, tout au long de

l'utilisation de la solution précédente. D'autres éléments ont fini de le convaincre : l'installation sur mesure du nouveau pare-feu, de nouvelle génération (next-gen) Palo Alto Networks, et la formation à son utilisation, sur site.

Un processus continu

Sécuriser un réseau informatique est un processus continu, qui dépasse de loin les caractéristiques techniques d'un outil très performant. « Un des gros challenges était de mettre en place une infrastructure et des mesures, qui tiennent compte de l'hétérogénéité des profils et des besoins, et qui protègent au mieux toutes les personnes, en leur imposant le moins de contraintes possibles. », commente Bruno Delcourt. Faciliter la disponibilité des ressources, en trouvant le juste équilibre, entre respect de la liberté individuelle et contrainte-contrôle, pour le bien de la communauté.

Monitoring et reporting

Un monitoring et un reporting détaillés, par la solution Palo Alto Networks, permettent d'offrir plus de transparence, grâce à des « analyses assez riches, qui vérifient que les mesures mises en place fonctionnent correctement. » Pour Bruno Delcourt, le reporting est également très bien fait : « bien souvent, des captures d'écran suffisent ; je n'ai pas de travail de présentation à fournir en plus. Les non-spécialistes les comprennent facilement ! Nous gagnons donc beaucoup de temps ! »

Des actions et analyses plus fines

Le pare-feu next-gen Palo Alto Networks autorise maintenant des actions plus précises en matière de sécurisation. Il fournit des analyses beaucoup plus fines : elles indiquent les nouvelles tendances sur le réseau et permettent de prévenir les menaces potentielles. « On comprend mieux encore les changements apportés par le nouveau firewall, en prenant l'exemple d'une ville fortifiée du Moyen-Âge, qui aurait évolué vers une ville plus moderne, plus ouverte, mais néanmoins avec un contrôle efficace », explique Bruno Delcourt. En outre, le pare-feu synchronise également au mieux les informations avec les autres systèmes et bases de données, développés en interne à l'Université. « Grâce à lui, c'est tout le réseau de l'Université de Namur qui a gagné en puissance globale et en souplesse ! », reconnaît Bruno Delcourt.

Un feed-back positif

« Le feed-back des utilisateurs est positif parce que le système est resté assez transparent. On continue d'offrir une protection, sans trop perturber l'expérience des utilisateurs vis-à-vis d'Internet. Moins ils perçoivent les solutions de sécurité et plus nous sommes contents ! », se réjouit Bruno Delcourt. « Avec les interfaces intuitives de Palo Alto Networks, il est assez simple et facile de définir des zones réseau différentes, chacune avec des mesures de sécurité particulières. On peut même confier certaines interventions aux autres membres de l'équipe, qui n'y travaillent pas régulièrement. »

Résultats et évolutions

Les résultats obtenus ont été conformes aux attentes de l'Université. L'installation du nouveau firewall Palo Alto Networks et son intégration avec les outils existants se sont déroulées sans incident. Les différents profils utilisateurs ont gagné en confort et souplesse d'utilisation. De son côté, l'équipe de Bruno Delcourt a pu, elle aussi, se perfectionner. La nouvelle structure est ouverte et évolutive : « les lignes de conduite pourront rester viables pour les 3 à 5 ans à venir. Nous mettons donc en place les fondations d'un système, pour construire des choses solides », conclut Bruno Delcourt.

« Les lignes de communication directes avec Telenet sont la pierre angulaire de notre relation de confiance. »

Louis Mahy, CIO de Record Bank

Record Bank booste l'efficacité et la sécurité de ses agents

Dans le cadre de la promotion de ses produits et services, Record Bank fait confiance à un vaste réseau d'agents indépendants. Ceux-ci restent en contact avec les sièges locaux de la banque grâce à un réseau WAN à base coax. « L'association de la technologie IP-VPN et de Secured Internet Breakout de Telenet permet à nos agents de créer et de gérer les dossiers clients en ligne rapidement et en toute sécurité », explique Louis Mahy, CIO de Record Bank.

Record Bank résulte de la fusion de quatre entités : Sodefina, De Vaderlandsche Spaarbank, SEFB Record Bank et Dipo. Au cours de la période 2001-2006, Record Bank a ensuite racheté quatre autres banques d'épargne. Tout en étant le deuxième réseau de détail d'ING, Record Bank a réussi à tirer parti de la crise bancaire de 2008. En effet, depuis 2008, le volume des dépôts est passé de 8 à 14 milliards d'euros.

Des services en ligne pour le réseau d'agents

Ce succès s'explique notamment par son modèle différent de sa maison-mère et basé sur un réseau d'agents et courtiers indépendants. Les trois sièges, situés à Evere, Liège et Gand, comptant 700 collaborateurs internes au total, apportent leur soutien à un réseau de 700 agents et 300 courtiers indépendants. Ceux-ci font appel aux experts de la banque, pour promouvoir le compte gratuit, l'attrayante offre épargne, les crédits logements, crédits auto et prêts personnels. « Nous voulons nous profiler comme le meilleur choix pour le particulier et le commerçant local qui souhaitent utiliser des services bancaires de manière simple, sûre et transparente », explique Louis Mahy, CIO. « En tant que département IT, notre principal défi est de proposer des services en ligne dans notre réseau et de contribuer ainsi à préserver l'équilibre entre la rapide croissance de l'Internet avec ses services bancaires directs et le rôle de conseil de notre réseau d'agents indépendants. »

Dissocier le réseau de l'Internet

« L'informatique moderne a considérablement étendu les solutions numériques dans le secteur bancaire», souligne Louis Mahy. Loin de freiner cette évolution, l'informatique doit s'adapter au changement de mentalité, selon lui. « Aujourd'hui, nous sommes confrontés aux applications mobiles. Comme nous disposons depuis plusieurs années d'un 'Core Banking System', un système unique de services bancaires, nous pouvons nous appuyer sur cette plateforme pour desservir de nombreux canaux de distribution et intégrer sans délai de nouvelles tendances comme l'utilisation d'équipements personnels. »

Le département IT a commencé par étudier notre réseau d'agents. « Le système de connexions sécurisées VPN via Internet avec un réseau ADSL classique commençait à dater et la nécessité de plus hauts débits imposait une nouvelle approche », précise Louis Mahy. « Nous voulions rendre notre réseau plus performant et moins dépendant de l'Internet et nous devions aussi faire migrer les terminaux de paiement vers notre propre réseau. Dans ce cas également, nous n'étions pas partisans d'utiliser l'Internet. » La solution proposée par Telenet a séduit d'emblée Louis Mahy : un réseau WAN à base coax reposant sur un backbone MPLS IP-VPN. « L'accès au réseau Telenet n'est pas influencé par la distance et offre un débit garanti. En outre, la solution est gage de souplesse et d'extension : nous pouvons paramétrer un débit minimum de départ pour chaque site et, au besoin, mettre à niveau la connexion sans intervention sur site. »

« Avec Secured Internet Breakout, Telenet a également proposé la solution de sécurisation idéale », poursuit Louis Mahy. Telenet a conçu ce pare-feu de nouvelle génération spécialement pour les entreprises disposant d'un VPN. « Grâce à Secured Internet Breakout, nous gérons le trafic internet de tous nos agents à l'aide d'une seule solution. Nous leur offrons donc un accès sécurisé aux applications en ligne dont ils ont besoin. »

Dans les rares cas où il n'était pas possible d'installer une connexion coaxiale, Louis Mahy a opté pour une connexion VDSL/ADSL2 toujours gérée par Telenet. « En cas de dérangement prolongé de la connexion d'une agence, l'agent peut utiliser une 'valise 3G ' de secours automatique qui lui procure instantanément une connexion 3G sans fil. »

Une réalisation rapide et irréprochable

Les 700 agents ont été raccordés au réseau en six mois. « Le déploiement s'est parfaitement déroulé, on voit que Telenet maîtrise totalement son domaine. Telenet met un point d'honneur à respecter les délais. Au plus fort de l'opération, nous avons réalisé jusqu'à 50 raccordements par semaine. » Louis Mahy s'est dit impressionné par la vitesse de Telenet dans l'exécution du contrat mais aussi dans la fourniture de rapports. « La gestion de projet est excellente. Par ailleurs, les rapports directs entre l'équipe account et la direction de l'entreprise accélèrent la prise de décision et favorisent la souplesse de l'exécution. Les accords en matière de qualité du service (SLA) sont en outre confortés par un suivi rigoureux et l'intervention locale rapide de techniciens expérimentés. Lors d'une visite d'un client de référence de Telenet, nous avions eu des échos positifs sur l'approche de Telenet. Il avait dit vrai. »

Record
recordbank.be

En tant que filiale d'ING, Record Bank se concentre sur le marché belge de l'offre bancaire de base. Sa mission est dès lors d'offrir une réponse aux besoins financiers des particuliers, indépendants et petites entreprises. Avec 12 milliards d'euros de prêts en cours, Record Bank représente 7% du marché hypothécaire belge. Avec sa banque-mère ING, ils visent la première place en matière de prêts à tempérament. Quelque 800.000 clients ont déjà ouvert environ 1 million de comptes auprès de Record Bank. Parmi les 350.000 comptes courants avec cartes bancaires gratuites, ils sont près de 200.000 à utiliser régulièrement l'application Internet Banking.

Plus de sécurité pour faire des affaires et collaborer sur internet

Telenet vous aide à optimiser vos affaires sur internet et veille à ce que vos employés puissent collaborer en toute fluidité via vos systèmes digitaux. Mais nous tenons aussi à vous offrir une sécurité totale. Voilà pourquoi nous avons développé des solutions de sécurisation spécifiques pour les PME au budget limité, et nous disposons de spécialistes capables de résoudre les problématiques de sécurité les plus complexes des grandes entreprises. Découvrez dans ce Livre Blanc pourquoi la sécurisation est si importante et comment nous pouvons vous aider. Telenet est parfaitement à l'aise dans de nombreux domaines tels que le firewalling, les systèmes antispam et antivirus, la détection de logiciels malveillants, les tests d'intrusion, l'audit, le Vulnerability Scanning, etc.

0800 66 066
telenet.be/business

Business

E.R. : Telenet n.v., Liersesteenweg 4, 2800 Malines Version juillet 2015.