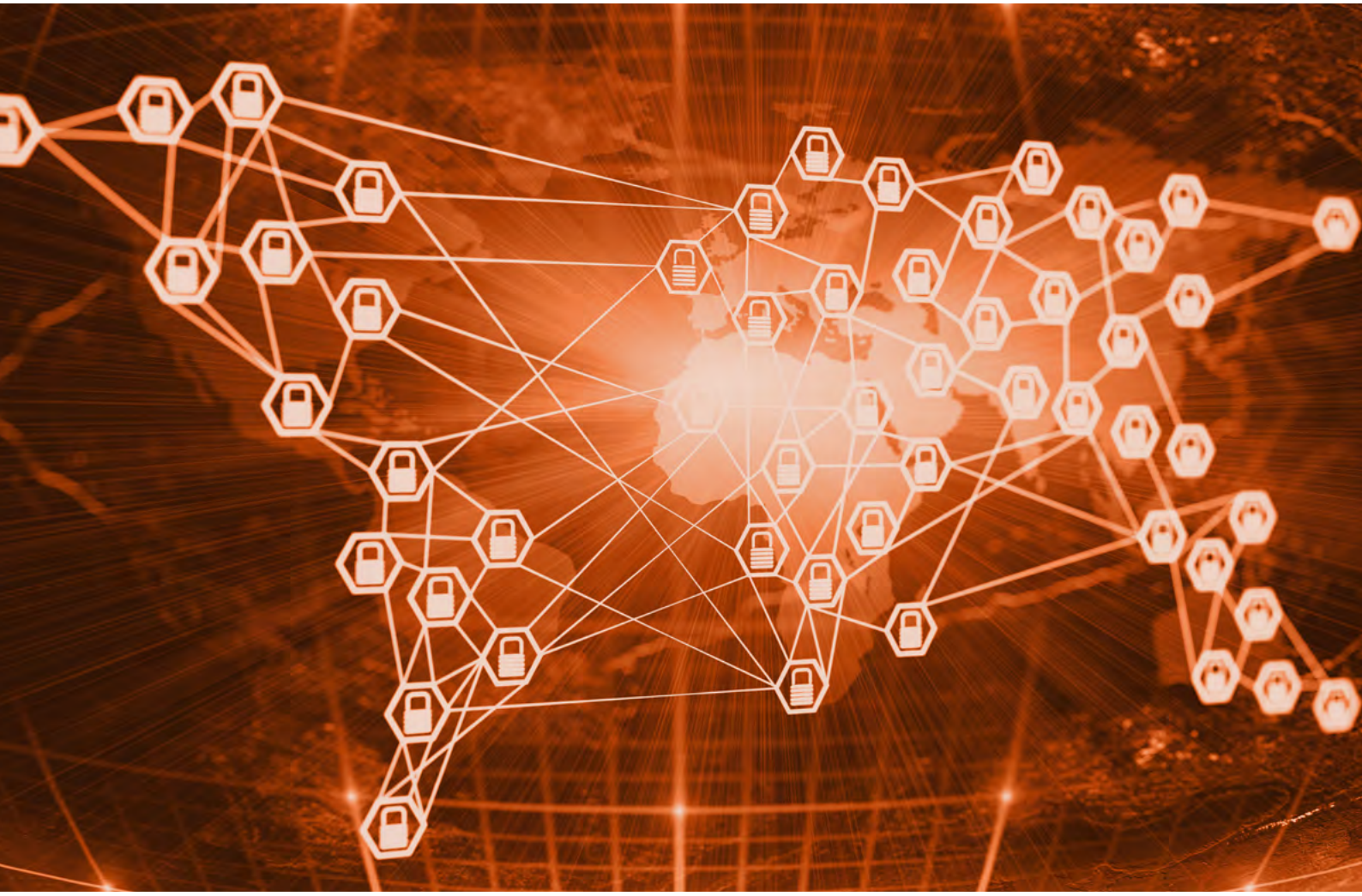
REPENSEZ VOTRE APPROCHE EN MATIÈRE DE CYBERSÉCURITÉ

Pourquoi les leaders de la sécurité sont désormais contraints de faire face aux principales menaces de sécurité



Le paysage de cybermenace continue de croître et d'évoluer. Cybersecurity Ventures prévoit que la cybersécurité deviendra un business de mille milliards de dollars entre 2017 et 2021.[1] Plus inquiétant encore, le coût du cybercrime devrait correspondre à plus de 6000 milliards de dollars dans le même temps.

Malgré des technologies de cybersécurité nouvelles et évoluées, les professionnels de l'informatique ne sont pas confiants. Ils sont 75 % à avoir craint d'être la cible de cyberattaques l'année dernière et rien ne laisse penser que ce pourcentage diminuera en 2017.[2] Cela n'a rien de surprenant puisqu'ils sont près de la moitié à croire qu'ils ne sont plus en mesure d'identifier les activités malveillantes transitant par leurs réseaux et 86 % signalent que leur fonction de cybersécurité n'est pas conforme aux besoins organisationnels.[3]

Une partie du problème réside dans l'empreinte numérique des entreprises qui ne cesse de s'étendre. Par exemple, la quantité de données générées double tous les deux ans.[4] La protection de toutes ces données (fixes ou en transit) constitue un défi significatif. La surface des réseaux d'entreprise connait également une expansion rapide. De nouveaux appareils sont introduits tandis que les dispositifs existants qui n'étaient pas encore connectés au réseau le deviennent. Enfin, les employés utilisent en moyenne au minimum trois périphériques pour exécuter leurs activités professionnelles. Enfin, 40 % des entreprises indiquent posséder une politique BYOD tandis que le paysage des menaces devient de plus en plus menaçant.[5]

Dans un livre blanc récent, Fortinet a identifié cinq domaines de cybermenace qui font aujourd'hui courir des risques aux entreprises:[6]

- L'adoption du cloud
- L'internet des objets
- Le ransomware
- Le chiffrement SSL (Secure Sockets Layer)
- Le manque de professionnels de la cybersécurité

LA SÉCURITÉ DANS LE CLOUD

L'ADOPTION DU CLOUD

Malgré le bruit et les discussions autour du cloud computing, il ne dépasse toujours pas 15 % des dépenses informatiques totales. Cela signifie que l'adoption du cloud ne fait que commencer. Le marché mondial du cloud augmente de 22 % par an, et a représenté plus de 146 milliards de dollars cette année,[7] et devrait dépasser 50 % des budgets informatiques d'ici 2019.[8]

Les modes de prestation de services varient indépendamment du modèle de cloud, la plupart des entreprises adoptant de nombreux services : SaaS (software as a service), PaaS (platform as a service) et IaaS (infrastructure as a service). Une nouvelle vague d'adoption est certainement en cours : d'ici 2020, 92 % des charges de travail seront traitées dans le cloud contre 8 % par des datacenters traditionnels.[9]

Le cloud comprend le cloud privé, le cloud public et des offres hybrides. Des recherches ont mis en avant que le cloud public connaît une croissance plus rapide que le cloud privé ; les charges de travail sur le cloud public devraient atteindre 68 % d'ici à 2020 (contre 49 % maximum l'an dernier). Cela résulte principalement de l'adoption des applications basées sur le SaaS qui augmente substantiellement la quantité de données conservées dans le cloud public, ainsi que la quantité de données échangées entre différents systèmes et applications.

MOTIFS CONDUISANT À L'ADOPTION DU CLOUD

Qu'est-ce qui conduit à cette adoption du cloud ? Les gérants de d'entreprises citent principalement les facteurs suivants :[12]

- La disponibilité, 46 %
- La réduction des coûts, 41 %
- Une évolutivité plus flexible, 36 %
- Une complexité réduite, 14 %
- La conformité à la réglementation, 13 %

Le résultat cumulé de ces facteurs fait que ces entreprises bénéficient d'une efficacité concurrentielle accrue en s'appuyant sur les opportunités offertes par le cloud. Et comme le cloud s'impose, de nombreuses entreprises qui ne l'adoptent pas ne pourront plus être concurrentielles.

PROBLÈMES INHÉRENTS À LA SÉCURITÉ DANS LE CLOUD

La gestion de la sécurité et de la conformité sur ces services de cloud disparates (publics, privés ou hybrides) constitue un défi. Paradoxalement, même si 64 % des professionnels de l'informatique croient que le cloud est plus sécurisé que ne peut l'être une infrastructure locale, ils considèrent malgré tout la sécurité comme le principal défi à relever quand il s'agit du cloud.[13]

La future adoption des applications reposant sur le SaaS et la transmission des données de et vers le cloud arrivent en haut de la liste des préoccupations. Mais d'autres facteurs accroissent également les inquiétudes en matière de sécurité. Ainsi, la hausse du nombre d'applications reposant sur le SaaS entraîne l'augmentation des interdépendances entre elles.

3/4 Les des professionnels de l'informatique craignent que leur entreprise ne soit victime d'une **cyberattaque** l'année prochaine

86 % des professionnels de l'informatique pensent que leur fonction de cybersécurité **ne** satisfait pas les exigences de leur entreprise

DONNÉES STOCKÉES DANS LE CLOUD[10]

- E-mail, 44 %
- Données sur les clients, 32 %
- Données commerciales et marketing, 31 %
- Données sur les employés, 30 %
- Contrats, factures, commandes, 26 %
- Données financières d'entreprise, 19 %
- Propriété intellectuelle, 18 %

OCCUPÉS À ÉLABORER DES CLOUDS[11]

% de responsables informatiques signalant être occupés à élaborer des…

- Clouds publics, 32 %
- Clouds privés, 38 %
- Clouds hybrides, 59 %

BARRIÈRES DE SÉCURITÉ POUR PASSER AU CLOUD[15]

- Problèmes de sécurité, 53 % (contre 45 % l'an dernier)
- Conformité à la réglementation, 42 % (contre 29 % l'an dernier)
- Risques de perte de données, 40 %

DevOps cherche à intégrer le « développement, les opérations informatiques, la sécurité et l'assurance qualité sous une seule égide automatisée ». Dans ce cadre, il introduit de nouveau défis et de nouvelles opportunités en matière de sécurité. DevOps intervenant principalement sur le cloud, les entreprises doivent développer de nouvelles manières d'intégrer la sécurité à la boucle perpétuelle de planification, codage, test, déploiement, fonctionnement et surveillance.[14]

L'IoT

CROISSANCE DE L'IoT[16]

La croissance de l'Internet des objets (IoT) est rapide et forte. De nombreux segments industriels connaissent une hausse de 50 % par an du nombre d'appareils IoT connectés au réseau. Les prévisions sont presque infinies. IHS prévoit que le marché de l'IoT doublera pour atteindre 30,7 milliards d'appareils d'ici 2020 et 75,4 milliards d'ici 2025 ![17] Les prévisions de recettes sont également impressionnantes. Elles sont estimées à 300 milliards de dollars d'ici 2020 avec un impact sur l'économie mondiale de 1,9 mille milliards de dollars.[18]

Sur certains segments industriels, les appareils IoT entraînent des transformations. Prenons la santé par exemple. Dans ce secteur, les appareils IoT peuvent améliorer les soins apportés aux patients tout en optimisant l'efficacité. Les médecins peuvent assurer une surveillance en temps réel des patients lorsqu'ils rentrent chez eux. Le transport et la distribution constituent un autre segment industriel où l'IoT fait toute la différence. Les entreprises de transport peuvent assurer un suivi et un contrôle complets, du carburant et de la consommation des véhicules aux conteneurs de livraison.

LES DÉFIS EN MATIÈRE DE SÉCURITÉ DE L'IoT

Les appareils IoT pourraient davantage s'imposer dans la vie des gens (IoT utilisateur final) et dans celle des entreprises (IoT industriel) que les smartphones. Les problèmes de sécurité sont amplifiés à cause de l'utilisation qui est faite de ces appareils IoT, tant en termes de données qu'ils transmettent que des systèmes qu'ils contrôlent et auxquels ils ont accès. Et comme les appareils IoT se multiplient, les risques de sécurité connexes augmentent.

Les appareils IoT sont plus fragiles que de nombreuses autres connexions réseau face aux attaques malveillantes car ils n'ont pas été conçus ou fabriqués en tenant compte de la sécurité et possèdent donc un niveau d'authentification et d'autorisation faible. De plus, la vaste majorité des appareils IoT ne disposent pas d'interface graphique de sorte qu'il est impossible d'installer les logiciels de sécurité habituellement utilisés pour bloquer les logiciels malveillants.

L'IoT automobile est un secteur jouissant d'une croissance et d'opportunités significatives. Son taux de croissance annuel composé est estimé à 22 % d'ici 2025.[20] Cependant, la prolifération de véhicules connectés à l'IoT offrira aux cybercriminels une surface d'attaque nettement supérieure et pourra avoir des perspectives catastrophiques.[21]

Certains piratages IoT de véhicules « intelligents » peuvent n'être coûteux qu'en temps et en argent via une attaque par ransomware exigeant le paiement d'une rançon pour déverrouiller le véhicule, réactiver un système de divertissement ou de navigation ou récupérer des données personnelles confidentielles volées. Dans d'autres cas, les conséquences peuvent être bien plus désastreuses comme la perte du contrôle des freins, du moteur ou de la direction avec un risque d'accident mortel.

Pour ce qui est des utilisateurs finaux, , les appareils IoT ont accès à leurs informations personnelles sur la santé, les finances, l'éducation, le domicile, etc. Dans les entreprises, les appareils IoT ont accès aux opérations de fabrication et de chaîne d'approvisionnement, aux systèmes de soins, aux infrastructures stratégiques et à d'autres systèmes. L'introduction d'un logiciel malveillant dans ces systèmes peut occasionner des ramifications substantielles. Les individus peuvent perdre des informations personnelles hautement confidentielles tandis que les entreprises peuvent subir des pannes systèmes suite à une attaque par déni de service, et perdre des données. Dans certains cas, la panne d'une infrastructure stratégique des systèmes SCADA (supervisory control and data acquisition) qui surveillent des barrages, des systèmes de transport, des produits alimentaires et des réseaux électriques, notamment, peut non seulement faire perdre des millions de dollars mais également mettre des vies en danger.[22]

PRINCIPALES APPLICATIONS SAAS

Actuellement déployées	Application SaaS	Déploiement prévu
41 %	Microsoft Office 365	20 %
27 %	Salesforce	7 %
24 %	Microsoft Exchange	11 %
20 %	Google Apps	6 %
17 %	Dropbox	5 %
15 %	ServiceNow	5 %
14 %	Box	4 %
9 %	Workday	4 %
8 %	Aucune	5 %
7 %	SuccessFactors	3 %

CROISSANCE INDUSTRIELLE DE L'IoT[19]

- Énergie et services publics, 58 %
- Surveillance du domicile, 50 %
- Transport et distribution, 49 %
- Municipalités intelligentes (gouvernement), 43 %
- Agriculture, 33 %
- Santé et pharmacie, 26 %

RISQUES DE SÉCURITÉ CONCERNANT L'IoT[23]

1. *Vulnérabilités en matière de sécurité.* Appareils livrés avec des logiciels obsolètes ou devenant obsolètes au fil du temps.
2. *Communications peu fiables.* Communications non chiffrées et fuites de données.
3. *Fuites de données.* Elles peuvent se produire entre les appareils et à partir du cloud.
4. *Infection par un logiciel malveillant.* Un logiciel malveillant peut infiltrer les appareils IoT, interrompre leur fonctionnement et compromettre les données qu'ils contiennent.
5. *Interruption de service.* La perte de disponibilité ou de connectivité peut dégrader la sécurité des services et exposer des systèmes, comme les systèmes d'alarme domestiques, accroissant ainsi les risques.

RANSOMWARE

Les attaques par ransomware ont plus que doublé l'année dernière pour atteindre jusqu'à 4 000 attaques par jour touchant en moyenne 30 000 à 50 000 appareils par mois. Le montant des rançons payées l'an passé a été multiplié par 35 (soit une hausse vertigineuse de 24 millions de dollars à 850 millions de dollars). Le montant des demandes de rançon a également augmenté, passant en moyenne de 294 dollars en 2015 à 679 dollars l'année dernière. Enfin, il est probable que le nombre réel d'attaques par ransomware soit sensiblement supérieur aux signalements déclarés par moins d'un quart des entreprises.[24]

Les attaques par ransomware se transforment également et sont de plus en plus automatisées du fait de la disponibilité et de l'accessibilité des services automatiques de logiciel malveillant comme les RaaS (ransomware as a service), la location de botnets et les services de harponnage. Les ransomwares traditionnels se sont généralement attaqués aux données des entreprises en chiffrant et en verrouillant les fichiers jusqu'au paiement d'une rançon. Cependant, avec l'émergence de l'IoT, une nouvelle tendance s'est développée afin de cibler les systèmes de commande des véhicules, des chaînes de montage et des systèmes d'alimentation. Le verrouillage du système d'amorçage sous-jacent rend les appareils inopérants en l'absence d'une possibilité de restauration à partir de sauvegardes ou du paiement de la rançon par le propriétaire.

L'impact des ransomwares ne réside pas seulement dans le paiement de la rançon mais également dans les répercussions sur les opérations commerciales. Les temps d'arrêt peuvent se traduire en pertes financières, en incidence environnementale voire même en décès. L'an dernier, par exemple, 63 % des entreprises ont signalé qu'une attaque par ransomware a entraîné une indisponibilité opérationnelle et 48 % qu'il en a résulté une perte matérielle ou de données.[25] Comme le piratage concerne fréquemment des données confidentielles à haute valeur ajoutée, les cybercriminels menacent de plus en plus de divulguer ces informations.

DIFFUSION DES RANSOMWARES[26]

- Liens transmis par e-mail, 31 %
- Pièces jointes d'un e-mail, 28 %
- Pièces jointes d'un site Web, 24 %
- Sources inconnues, 9 %
- Réseaux sociaux, 4 %
- Applications commerciales, 1 %

CHIFFREMENT SSL

HAUSSE DU TRAFIC SSL

Le trafic SSL représente entre 35 et 50 % du trafic réseau aujourd'hui[27] et il continue de croître au rythme de 20 % par an.[28] Les sites Web reposent de plus en plus sur le protocole HTTPS par défaut, mais il reste encore beaucoup à faire dans ce domaine. Au fur et à mesure que ces sites adopteront le protocole HTTPS, le pourcentage global de trafic SSL augmentera.[29] L'adoption du cloud est une autre explication de cette hausse. En effet, les entreprises cherchent à protéger leurs données lors de leur transit de et vers le cloud. Les applications SaaS comme Salesforce, Dropbox et Microsoft Office 365 accordent une importance centrale à la confidentialité et à l'activation du chiffrement SSL sur leurs plateformes.

Les entreprises de divers segments industriels doivent chiffrer certains types de données sensibles en transit à l'aide du chiffrement SSL (Secure Sockets Layer) pour se conformer à la réglementation, notamment la norme PCI-DSS (Payment Card Industry Data Security Standard) et la loi HIPAA (Health Information Portability and Accountability Act).

DÉFIS INHÉRENTS AU CHIFFREMENT SSL

Cependant, le chiffrement SSL est à double tranchant. Les cybercriminels ont l'habitude de cacher leur logiciel malveillant et leur ransomware aux solutions de sécurité traditionnelles afin de franchir les défenses des entreprises. De plus, ils utilisent également le chiffrement SSL pour chiffrer leurs communications avec les systèmes de commande et de contrôle. Les systèmes de détection des intrusions (IDS) et les systèmes de prévention des intrusions (IPS) sont élaborés pour faire confiance au trafic chiffré, et par la même, dans l'incapacité de détecter les ransomwares. Comme le chiffrement, tout acteur bon ou mauvais confondu, se complexifie et compte de plus en plus de cryptogrammes, le déchiffrement devient une nécessité. Et comme les cybercriminels utilisent généralement les cryptogrammes les plus avancés pour chiffrer leurs logiciels malveillants, la prise en charge de cryptogrammes imposés par l'industrie devient cruciale pour procéder au déchiffrement.

Qu'en résulte-t-il ? 90 % des DSI indiquent avoir été confrontés ou être confrontés à une attaque réseau au moyen du chiffrement SSL et 87 % précisent que leurs systèmes de protection sont moins efficaces aujourd'hui du fait que les cybercriminels utilisent le chiffrement pour masquer leurs attaques.[30]

Le chiffrement SSL peut également avoir un impact sur les performances du réseau tout en complexifiant la gestion de la sécurité du réseau. Les systèmes d'inspection du trafic et de déchiffrement SSL peuvent accroitre la latence du réseau, voire même interrompre les opérations commerciales. En outre, le chiffrement SSL peut complexifier la gestion de la sécurité du réseau par l'introduction de matériel, de logiciels, de politiques de sécurité et de flux de travail supplémentaires.

Il est toutefois possible de ne pas compromettre les performances. Pour ne pas compromettre les performances du réseau, par exemple, un chiffrement SSL avec fonction de prévention contre les menaces peut être utilisé. Les entreprises peuvent ainsi déchiffrer et identifier si le texte en clair est un logiciel malveillant sans que cela n'ait d'incidence sur les performances.

MANQUE DE PROFESSIONNELS DE CYBERSÉCURITÉ

La complexification de la gestion de la sécurité est un problème pour de nombreuses entreprises. Près de 40 % des entreprises indiquent disposer d'au moins 5 solutions de sécurité.[31] La difficulté de gestion de ce patchwork de solutions augmente chaque fois qu'une solution individuelle supplémentaire vient s'ajouter. Aussi, 40 % des entreprises décident-elles de ne pas mettre leur réseau à niveau.[32]

OÙ UTILISER LE DÉCHIFFREMENT ET L'INSPECTION SSL

- Messagerie
- Navigateur Web (site Web et réseaux sociaux)
- Applications SaaS
- Applications commerciales personnalisées

UTILISATION DU CHIFFREMENT SSL PAR LES CYBERCRIMINELS

1. *Dissimulation de l'infection initiale.* Les cybercriminels chiffrent leurs logiciels malveillants et les envoient via un port approuvé. Les utilisateurs cliquent sur les liens intégrés qui les renvoient sur des sites contenant la charge malveillante ou sur un fichier joint. Heartbleed constitue un exemple de ce type d'attaque. Ce bug de sécurité dans la bibliothèque de cryptographie d'OpenSSL a été largement utilisé pour l'implémentation de SSL. Il est possible de pirater et d'infecter des systèmes via un serveur ou un client et entraîner une validation erronée de la mise en œuvre de l'extension Transport Layer Security (TLS).
2. *Dissimulation des commandes et des contrôles.* Certaines familles de logiciels malveillants utilisent le chiffrement pour cacher les communications relatives aux commandes et aux contrôles.
3. *Dissimulation de l'exfiltration des données.* De nombreuses familles de logiciels malveillants utilisent également le chiffrement pour cacher les informations réseau comme les mots de passe et les informations volées (par exemple, les comptes bancaires, etc.).

Trouver des professionnels de la sécurité informatique qui maîtrisent la mise en œuvre et la gestion de ces solutions n'est pas chose aisée. Voici le dilemme : il y a une pénurie de professionnels de la sécurité informatique. D'après les estimations, il en manque environ un million aujourd'hui. En outre, bien que les conseils de direction reconnaissent l'importance de la sécurité et mandatent des initiatives de formation d'un plus grand nombre d'informaticiens spécialisés dans la sécurité, cette pénurie devrait continuer d'augmenter pour atteindre 1,5 million dans le monde entier d'ici 2020.[33]

Les responsables informatiques sont conscients du problème : près des deux tiers mentionnent la sécurité informatique comme étant la principale compétence de recrutement de leurs équipes (la deuxième compétence étant le développement de logiciels avec 18 %).[34] Les trois quarts croient qu'ils seront confrontés à davantage de menaces de sécurité dans les cinq prochaines années à cause d'une pénurie de professionnels de la sécurité informatique. Enfin, plus de la moitié accorde une priorité absolue au recrutement de professionnels de la sécurité informatique dotés de compétences ou de connaissances spécialisées.[35]

Tous ces facteurs ont une incidence sur l'entreprise. Plus de la moitié des responsables informatiques indiquent que la pénurie en personnel de cybersécurité a augmenté la charge de travail du personnel existant, 35 % ont fait des compromis pour combler les postes avec les compétences et l'expérience appropriées et, encore 35 % déclarent que leurs équipes n'ont pas pu apprendre à utiliser ou exploiter pleinement leurs technologies de sécurité. Plus effrayant encore, plus de la moitié révèle que son entreprise a subi au moins un événement de cybersécurité pouvant être imputé au manque de formation à la sécurité et de ressources en personnel qualifié.[36]

Profil le plus demandé	Profil le plus difficile à trouver
Sécurité du cloud, 51 %	Sécurité dans le cloud, 32 %
Technologies de sécurité informatique, 47 %	Technologies de sécurité informatique, 29 %
Big Data/analyse des données, 37 %	Architecture de la sécurité, 26 %
Sécurité des applications, 30 %	Piratage/test de pénétration, 26 %
Piratage/test de pénétration, 30 %	Sécurité des applications, 22 %

PÉNURIE EN COMPÉTENCES DE CYBERSÉCURITÉ

Le taux de croissance annuel composé (CAGR) des professionnels de la sécurité informatique est d'environ 10 % quand le nombre de nouveaux professionnels de la sécurité informatique n'augmente que de 5,6 %.[38]

RÉPARTITION DU PERSONNEL DE SÉCURITÉ INFORMATIQUE[39]

- Recours à des employés à temps plein, 52 %
- Recours à des sous-traitants uniquement, 15 %
- Mixte des deux, 33 %

CHOISIR PARMI LES DIFFÉRENTES OPTIONS DE SÉCURITÉ À VOTRE DISPOSITION

Suivre le rythme de l'évolution et des avancées continues du paysage de menaces n'est pas une entreprise facile. Les cinq domaines de cybersécurité mentionnés ci-dessus compliquent considérablement le travail des responsables de la sécurité informatique lorsqu'il s'agit de protéger leurs réseaux et leurs données.

Les entreprises ont le choix entre trois architectures principales de sécurité :

SOLUTIONS DE SÉCURITÉ SPÉCIFIQUES

La première consiste à acquérir des solutions spécifiques qui répondent à des besoins précis en matière de cybersécurité. Toutefois, avec l'évolution et la transformation de la cybersécurité, ce modèle pose des problèmes d'inefficacité, d'interruptions, voire même de failles.[40] Voici les défis associés aux solutions spécifiques :

1. Gestion et personnel

La mise en œuvre et l'administration de chaque solution spécifique constitue une tâche isolée des autres. Près de 50 % des entreprises indiquent posséder au moins cinq solutions de sécurité opérationnelles, ce qui peut rapidement poser des problèmes substantiels avec un impact conséquent sur le personnel en charge de la cybersécurité au sein de l'entreprise (nécessité de rechercher, recruter et fidéliser du personnel et conserver ce personnel formé sur chacune des différentes solutions).

2. Gestion désagrégée de la politique

Il est difficile d'intégrer des solutions spécifiques disparates et de les faire communiquer entre elles. En outre, les entreprises informatiques ne peuvent pas développer de politiques universelles afin de gérer la sécurité sur le plan supérieur. Elles doivent créer des politiques propres à chaque solution spécifique et gérer chaque ensemble séparément, créant ainsi des failles de sécurité que les cybercriminels peuvent exploiter.

3. Manque d'intégration

L'intégration de chaque solution spécifique est une tâche qui demande du temps sans être jamais totalement achevée. De plus, il est difficile (voire parfois impossible) d'intégrer chaque solution spécifique à d'autres technologies tierces. Enfin, chaque fois qu'une nouvelle solution spécifique est introduite, le personnel informatique doit retracer les étapes d'intégration antérieures.

4. Visibilité partielle du fait d'un fonctionnement en silos

Avec des solutions spécifiques, les équipes de sécurité informatiques n'ont aucune visibilité sur l'intégralité de l'entreprise. Chaque solution spécifique offre une visibilité mais à l'échelle de son silo uniquement. Une fois de plus, il en résulte des inefficacités et de potentielles faiblesses en termes de sécurité.

5. Intelligence à courte vue

Un environnement de cybersécurité robuste exploite tous les éléments pour concevoir un tout plus résistant. Cependant, les équipes de sécurité informatique ne peuvent pas partager les informations sur les menaces entre différentes solutions spécifiques. Elles ne disposent pas d'une vue complète sur les données ni du partage des informations collaboratives à l'échelle de la surface d'attaque.

6. Performances

Les solutions spécifiques sont exécutées sur du matériel (appliances ou serveurs propriétaires) reposant sur des processeurs locaux qui manquent de capacité de traitement haute performance, d'où des goulets d'étranglement et une lenteur des réseaux et des applications. Tout cela a une incidence sur la productivité de l'utilisateur final et l'efficacité opérationnelle.

LES PLATEFORMES DE SÉCURITÉ

Le nombre de points d'entrée est considérablement plus important aujourd'hui qu'il y a seulement quelques années. Les entreprises doivent se protéger au niveau de douzaines, voire de centaines, de points d'entrée différents du fait de l'utilisation des services de cloud et de divers appareils, ainsi que des travailleurs mobiles. La sécurité ne s'arrête pas à la protection du périmètre. Les entreprises doivent également protéger leurs datacenters, leurs succursales, les applications dans le cloud et les sites partenaires, notamment.

Des solutions reposant sur une plateforme ont émergé pour satisfaire cette prolifération du paysage de cybersécurité. Mais, comme elles sont implantées sur un élément de sécurité spécifique (firewalls, terminaux, etc.), les composants supplémentaires que ces fournisseurs ajoutent sur leur plateforme constituent un ensemble d'outils et non une solution homogène.[41] Voici les inconvénients des solutions reposant sur une plateforme :

1. Console centralisée

Les plateformes de sécurité connectent les différents éléments en leur sein par le biais d'une console de gestion centralisée. Il en résulte des délais qui ralentissent les communications et la collaboration entre les différents composants de la plateforme. Cela a une incidence sur la capacité de l'entreprise à réagir aux menaces comme les attaques zero-day.

2. Performances

Les solutions reposant sur une plateforme souffrent des mêmes problèmes de performances que les solutions spécifiques. Le matériel des plateformes dépend des appliances et repose sur des processeurs locaux qui ne sont pas conçus pour satisfaire les seules exigences de la cybersécurité. Les entreprises doivent généralement acheter du matériel supplémentaire (exécuté à partir de processeurs locaux) auprès du fournisseur de la plateforme de sécurité pour atteindre le niveau de performance dont elles ont besoin.

3. Évolutivité et agilité

La cybersécurité constitue un environnement dynamique qui change rapidement. Les solutions reposant sur une plateforme peuvent évoluer pour répondre à de nouveaux besoins par le biais du remplacement de l'équipement existant par du matériel plus récent et plus performant ou par l'ajout de nouveaux appareils et dispositifs. Il en résulte toutefois des coûts supplémentaires et une trop grande lenteur pour réagir aux pics de trafic réseau et à l'émergence de nouvelles cybermenaces, notamment.

4. Zones d'ombre et failles de sécurité

Chaque fois que plusieurs produits sont combinés sous une même égide, des zones d'ombre et des failles de sécurité sont associées en rapport avec l'intégration ou l'absence de fonctionnalités. Les cybercriminels peuvent en tirer profit pour infiltrer votre réseau. Avec la croissance des appareils d'IoT et l'utilisation du chiffrement SSL pour dissimuler les menaces entrantes et sortantes, le risque de zones d'ombre et de failles de sécurité augmente. Les solutions reposant sur une plateforme, avec tout le matériel ajouté, manquent d'agilité et d'envergure d'intégration et d'automatisation pour contrecarrer ces menaces.

5. Manque de visibilité

Les différents produits constituant la solution reposant sur une plateforme possèdent probablement des tableaux de bord distincts notamment dans le domaine de la collecte des données et des mécanismes de création de rapport. Certaines entreprises tentent d'agréger ces informations manuellement mais cette tâche est longue, fastidieuse et certainement pas exécutée en temps réel. Or, sans transparence ni visibilité en temps réel à l'échelle de son réseau, une entreprise ne dispose pas de toutes les informations requises pour prendre des décisions de manière proactive en matière de cybersécurité. Cela est pourtant crucial alors que les attaques zero-day tendent à devenir la norme.

6. Intégration tierce

Les produits individuels de la plateforme de sécurité possèdent leurs propres API et interfaces, ce qui complique la connexion et l'intégration de solutions tierces. Les entreprises se trouvent soudain confrontées aux mêmes défis qu'un fonctionnement en silos propre aux solutions spécifiques.

SECURITY FABRIC

Une nouvelle alternative aux solutions ci-dessus repose sur une Security Fabric. Toutes les solutions de sécurité au sein de cette Security Fabric sont disponibles en tout point de l'environnement en temps réel, des IoT au cloud. Voici certains avantages clés d'une Security Fabric :

1. Communication en temps réel

La Security Fabric intègre en toute transparence les divers éléments présents dans l'environnement tout en permettant aux entreprises informatiques d'y ajouter des produits tiers. Tous les produits communiquent en temps réel entre eux, facilitant ainsi l'information collaborative.

2. Protection de l'intégralité de la surface d'attaque

Contrairement aux solutions spécifiques qui ne couvrent qu'une partie de la surface d'attaque, la Security Fabric est globale. Sa couverture comprend le cloud, les applications, le réseau, les points d'accès, les terminaux et les appareils IoT. Il en résulte une visibilité transparente et une posture plus robuste face aux menaces.

3. Incidence sur les performances et l'infrastructure

Tandis que les solutions spécifiques et reposant sur une plateforme utilisent des processeurs locaux, la Security Fabric exploite des processeurs de sécurité avancés spécifiquement conçus pour répondre aux exigences de la cybersécurité. La Security Fabric s'appuie également sur un traitement matériel utilisant un chemin d'accès parallèle afin d'optimiser les performances en termes de débit tout en s'adaptant aux hausses de trafic SSL chiffré. Des listes blanches robustes permettent aux entreprises de laisser passer le trafic connu tout en concentrant les ressources de traitement sur les menaces inconnues.

4. Réponses automatiques et dynamiques

La Security Fabric comprend des technologies lui permettant d'identifier les menaces connues et inconnues à l'aide de technologies comme les listes blanches et le sandboxing. Cette réponse totalement intégrée aux menaces et aux attaques est intégralement coordonnée entre chaque solution appartenant à la Security Fabric.

LES CINQ ÉLÉMENTS À RETENIR SUR LA SECURITY FABRIC

Si l'on reconnaît les avantages de la Security Fabric par rapport aux solutions spécifiques traditionnelles et aux solutions reposant sur une plateforme, dans quelle mesure la Security Fabric est-elle intéressante pour les cinq menaces de cybersécurité émergentes identifiées ?

LE CLOUD

L'émergence du cloud exige des entreprises l'ajout de solutions spécifiques supplémentaires, et des fournisseurs, la mise à disposition de nouvelles solutions sur leurs plateformes. Il en résulte toutefois des problèmes d'intégration et la nécessité de davantage former le personnel. De plus, il reste des zones d'ombre et des failles que les cybercriminels peuvent exploiter pour s'infiltrer. La Security Fabric constitue une meilleure option en intégrant les applications dans le cloud dans un environnement élargi sous l'égide de politiques de sécurité et de conformité universelles offrant une visibilité transparente à l'échelle de la surface d'attaque.

L'IoT

La croissance rapide des appareils IoT crée des menaces hautement pernicieuses. La capacité d'ajouter ces appareils en toute transparence à la structure de sécurité offre aux entreprises une plus grande agilité pour contrer les menaces potentielles. Les entreprises qui comptent sur des solutions spécifiques, doivent en ajouter une nouvelle pour protéger leurs appareils IoT. Si elles utilisent une solution reposant sur une plateforme, elles peuvent devoir faire appel à leur fournisseur pour ajouter d'autres composants avant d'être protégées.

La généralisation du déploiement des appareils IoT complique la mise en place d'une visibilité et d'une gestion transparentes globales. De nombreuses solutions spécifiques ou reposant sur une plateforme sont tout simplement incapables d'intégrer ces appareils (y compris les contrôles d'accès et la réponse aux incidents) à une gestion centralisée. De même, l'évolutivité (de plus en plus d'appareils IoT étant connectés au réseau) devient un problème pour les solutions spécifiques ou reposant sur une plateforme. Au contraire, une Security Fabric peut intégrer tous les points d'accès disparates d'un réseau (terminaux, applications, cloud et appareils IoT) indépendamment de leur distribution, dans une solution de bout en bout qui couvre toutes les différentes surfaces d'attaque.

RANSOMWARES

Les entreprises qui souhaitent bloquer les attaques par ransomware ont besoin d'une Security Fabric pour couvrir les différents canaux de propagation utilisés par les cybercriminels pour s'infiltrer : liens et pièces jointes par e-mail, pièces jointes sur les sites Web, applications commerciales, réseaux sociaux et même appareils IoT. Si les entreprises informatiques doivent rester vigilantes sur les menaces entrantes, il en va de même sur les menaces sortantes. Les entreprises utilisant une Security Fabric peuvent également surveiller les communications sortantes pour détecter les communications de commandes et contrôles chiffrés par un ransomware, ainsi que les fichiers piratés verrouillés avec une clé de chiffrement privée. La Security Fabric utilise le partage local automatique des informations sur les menaces pour interrompre les communications de commandes et de contrôles, la propagation latérale des infections et l'infection au stade zéro (avant sa propagation aux autres utilisateurs et terminaux).

LE CHIFFREMENT SSL

Le chiffrement SSL constitue un outil important des boîtes à outils de sécurité informatique car il permet aux entreprises de protéger des informations hautement sensibles et confidentielles. Malheureusement, cet outil est tout aussi stratégique pour les cybercriminels qui utilisent le chiffrement pour accéder aux informations et dissimuler leur vol de données ou le piratage par ransomware. Contrairement aux solutions spécifiques ou reposant sur une plateforme, une Security Fabric est en mesure d'offrir des processus d'inspection et de déchiffrement SSL haute performance et hautement intégrés pour les communications entrantes et sortantes à l'échelle du spectre d'attaque.

LA PÉNURIE EN PERSONNEL DE CYBERSÉCURITÉ

Les professionnels de la cybersécurité sont en sous-nombre et les entreprises ne peuvent pas recruter autant de professionnels de la sécurité informatique qu'elles le voudraient. Les cybermenaces étant de plus en plus nombreuses et virulentes et les architectures de sécurité étant de plus en plus complexes, la Security Fabric constitue une alternative convaincante par rapport aux solutions spécifiques ou reposant sur une plateforme pour lesquelles le personnel de cybersécurité doit être formé tout en maîtrisant plusieurs composants de produits et de solutions. Plus précisément, tous les aspects de la sécurité sont imbriqués dans une Security Fabric offrant une vision centralisée et transparente qui permet aux entreprises de ne pas embaucher de spécialistes de la sécurité informatique tout en offrant au personnel de cybersécurité existant une prise en charge évolutive d'un paysage de sécurité en constante évolution et croissance.

[1] « Cybersecurity Market Report », Cybersecurity Ventures, décembre 2016.

[2] « The State of Cybersecurity: Implications for 2016 », ISACA and RSA, février 2016.

[3] « Path to Cyber Resilience: Sense, Resist, React », 19th Global Information Security Survey, EY, décembre 2016.

[4] « The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things », IDC, avril 2014.

[5] « BYOD and Mobile Security », Crowd Research Partners, 2016.

[6] « A Security Leader's Definitive Guide to the Threat Landscape », Fortinet, février 2017.

[7] Clint Boulton, « 6 Trends That Will Shape Cloud Computing in 2017 », CIO.com, 2 novembre 2016.

[8] Fredric Paul, « Cloud to Consume Almost Half of IT Infrastructure Sales by 2019 », Network World, 7 juillet 2015.

[9] Joe McKendrick, « With Internet of Things and Big Data, 92% of Everything We Do Will Be in the Cloud », Forbes, 13 novembre 2016.

[10] « Cloud Security: 2016 Spotlight Report », LinkedIn Security Group, 2016.

[11] Ibid.

[12] « Cloud Security: 2016 Spotlight Report », LinkedIn Security Group, 2016.

[13] Sarah Patrick, « Security and the Cloud: Trends in Enterprise Cloud Computing », Clutch, 3 mars 2016.

[14] Doug Drinkwater, « Is DevOps the Holy Grail for Information Security? » CSO.com, 4 mars 2016.

[15] « Security and the Cloud », Clutch.

[16] « Cloud Security: 2016 Spotlight Report ».

[17] Louis Columbus, « Roundup of Internet of Things Forecasts and Market Estimates, 2016 », Forbes.com, 27 novembre 2016.

[18] Gil Press, « Internet of Things by the Numbers: Market Estimates and Forecasts », Forbes, 22 août 2014.

[19] « State of the Market: Internet of Things 2016: Accelerating Innovation, Productivity, and Value », Verizon, décembre 2016.

[20] Andrew Meola, « Automotive Industry Trends: IoT Connected Smart Cars & Vehicles », Business Insider, 20 décembre 2016.

[21] « Motor Vehicles Increasingly Vulnerable to Remote Exploits », Federal Bureau of Investigation, 16 mars 2016.

[22] Ed Nugent, « SCADA Cybersecurity in the Age of the Internet of Things », Control Engineering, 30 août 2016.

[23] « Internet of Things (IoT) Security and Privacy Recommendations », BITAG, novembre 2016.

[24] Minal Khatri, « Ransomware Statistics – Growth of Ransomware in 2016 », Systweak, 25 août 2016.

[25] « State of the Channel Ransomware Report 2016 », Datto, 2016.

[26] « Non-Malware Attacks and Ransomware Take Center Stage in 2016 », Carbon Black Threat Report, 2016.

[27] See, e.g., J. Michael Butler, « SANS Institute InfoSec Reading Room: Finding Hidden Threats by Decrypting SSL », novembre 2013 ; Johnnie Konstantas, « SSL Encryption: Keep Your Head in the Game », Security Week, 15 mars 2016.

[28] Butler, « SANS Institute InfoSec ».

[29] Brian Barrett, « Most Top Websites Still Don't Use a Basic Security Feature », WIRED, 17 mars 2016.

[30] Jai Vijayan, « When Encryption Becomes the Enemy's Best Friend », Dark Reading, 5 mars 2016.

[31] « Top Networking and Security Challenges in the Enterprise: Planned Network Investments in 2017 », Global Industry Report, CATO, novembre 2016.

[32] « Protecting Your Organization in a Talent-Scare Market: Information Security », Experis, 2015.

[33] Michael Suby, et al., « The 2015 (ISC)2 Global Information Security Workforce Study », Frost & Sullivan, 2015.

[34] « Emerging Cyberthreats Report 2016 », Georgia Tech Cyber Security Summit, Institute for Information Security & Privacy, 2016.

[35] Suby, « The 2015 (ICS)2 Global Information Security Workforce Study ».

[36] Jon Oltsik, « Through the Eyes of Cyber Security Professionals: Annual Research Report (Part II) », ESG and ISSA, décembre 2016.

[37] « Cybersecurity: Protecting Your Future, Early Adopters Win », Robert Half, 2016.

[38] « Protecting Your Organization in a Talent-Scare Market: Information Security », Experis, 2015.

[39] « Protecting Your Organization », Experis.

[40] Francisco Ordillano, « Security Fabric, Expertly Tailored to Fit Your Organisation », InfosecPartners, 14 septembre 2016.

[41] Zeus Kerravala, « Cybersecurity Fabric vs. a Security Platform: Fabric Wins », Network World, 16 novembre 2016.

SIÈGE SOCIAL INTERNATIONAL
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
États-Unis
Tél. : +1.408.235.7700
www.fortinet.com/sales

SUCCURSALE EMEA
905 rue Albert Einstein
06560 Valbonne
France
Tél. : +33.4.8987.0500

SUCCURSALE APAC
300 Beach Road 20-01
The Concourse
Singapour 199555
Tél. : +65.6513.3730

AMÉRIQUE LATINE — SIÈGE SOCIAL
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tél. : +1.954.368.9990

TOUR ATLANTIQUE
11ème étage,
1 place de la Pyramide
92911 Paris La
Défense Cedex
France
Ventes: +33-1-8003-1655

58160-A-0-FR

15 février 2017