Enterprise Strategy Group | Getting to the bigger truth.™

Livre blanc

Le chiffrement des réseaux et son impact sur la sécurité des entreprises

Par Jon Oltsik, analyste principal expert

Février 2015

Ce livre blanc d'ESG, a été réalisé à la demande de Blue Coat.
Il est distribué sous licence d'ESG.

Sommaire

Résumé analytique

Fin 2014, Enterprise Strategy Group (ESG) et Blue Coat Systems ont mené une étude collaborative auprès de 150 professionnels de l'informatique et de la sécurité des informations ayant des connaissances ou des responsabilités concernant le chiffrement du réseau et les contrôles, processus et politiques de sécurité associés appliqués dans leur entreprise.

Les participants à l'étude se trouvaient en Amérique du Nord et étaient employés dans des sociétés de tailles diverses : 18 % des participants travaillaient dans des entreprises moyennes de 500 à 999 employés, contre 82 % pour les grandes entreprises de plus de 1 000 employés. Divers segments de l'industrie et de l'administration étaient représentés, avec une participation plus importante pour les technologies de l'information (33 %), les services financiers (12 %), le secteur de la production (12 %), la vente au détail/en gros (11 %) et le secteur de la santé (9 %).

Ce projet de recherche était destiné à évaluer l'adoption de la technologie de chiffrement de réseau SSL/TLS ainsi que les pratiques en matière de sécurité des informations en vigueur pour crypter et inspecter le trafic chiffrer. D'après les données recueillies, les conclusions de ce livre blanc sont les suivantes :

- **Le chiffrement des réseaux est omniprésent et s'étend.** Aujourd'hui, de nombreuses entreprises (87 %) cryptent déjà au moins 25 % de l'ensemble de leur trafic réseau. De plus, 88 % des entreprises indiquent qu'à l'avenir, elles vont crypter un volume plus important du trafic réseau. Le chiffrement des réseaux est de plus en plus utilisé pour protéger la confidentialité des données et réduire le risque d'espionnage du réseau ou d'attaque de type « intermédiaire » (« man in the middle »).
- **Les entreprises déchiffrent et inspectent le trafic SSL/TLS pour des raisons de sécurité**. Alors que le chiffrement des réseaux peut protéger le trafic contre les oreilles indiscrètes, il constitue également un vecteur de menaces dans lequel les cybercriminels et les pirates informatiques peuvent s'engouffrer pour réaliser leurs activités malveillantes et contourner les contrôles de sécurité réseau existants. Conscientes de cette menace, 87 % des entreprises inspectent au moins une partie de leur trafic SSL/TLS dans le cadre de leurs opérations de sécurité réseau. Une fois ce trafic déchiffrer, les professionnels de la sécurité examinent les paquets du réseau afin de repérer, par exemple, les contenus malveillants provenant de sites sécurisés, les fichiers et/ou scripts cachés malveillants et les fuites de données sensibles. Il convient de noter que lorsque les entreprises inspectent le trafic SSL/TLS, elles ne le font peut-être pas à un niveau approprié permettant d'éviter les risques. Cela est particulièrement important car le cyber-risque va continuer à croître proportionnellement à l'augmentation de l'ensemble du trafic chiffrer.
- **Le déchiffrement et l'inspection SSL/TLS sont actuellement effectués de façon ciblée.** Les équipes de gestion de la sécurité et du réseau déchiffrent et inspectent le trafic SSL/TLS avec une myriade de technologies disparates telles que des pare-feux nouvelle génération, des équipements SSL/TLS et des services basés sur le cloud. Malheureusement, cette approche ciblée devient de plus en plus complexe et fastidieuse au fur et à mesure que le volume chiffrer sur les réseaux augmente. Dans le même temps, il semble que les temps changent. Les données d'ESG suggèrent également que 20 % des entreprises ont déjà établi une stratégie de déchiffrement et d'inspection SSL/TLS plus complète, alors que 66 % sont en train de mettre en œuvre une telle stratégie, envisagent de la mettre en place ou sont intéressées par ce type de stratégie pour une implémentation ultérieure. Ce type de stratégie de déchiffrement SSL/TLS holistique est vital, les approches ciblées actuelles ajoutant des frais généraux d'exploitation sans être en mesure d'évoluer pour faire face aux cyber-risques chiffrers émergeants.

Les données pointent, pour l'avenir, vers des stratégies de déchiffrement et d'inspection SSL/TLS à l'échelle de l'entreprise, mais à quoi ressemble ce type de stratégie ? Selon l'ESG, il sera mis en œuvre sous forme d'architecture en étoile, avec un « service » de déchiffrement à grande vitesse intégré sur l'ensemble du réseau qui va ensuite collecter, traiter et transférer le trafic du réseau en clair aux différents dispositifs de sécurité, ceux-ci pouvant approfondir son traitement et son analyse (analyses de sécurité, pare-feux, systèmes de prévention et de détection d'intrusions (IDS/IPS), équipements anti-malware/sandboxing, par exemple). Cela va non seulement

améliorer l'efficacité de la détection des incidents et la réaction à ceux-ci, mais aussi fournir une veille utilisable en temps réel pour automatiser la résolution des problèmes de sécurité réseau.

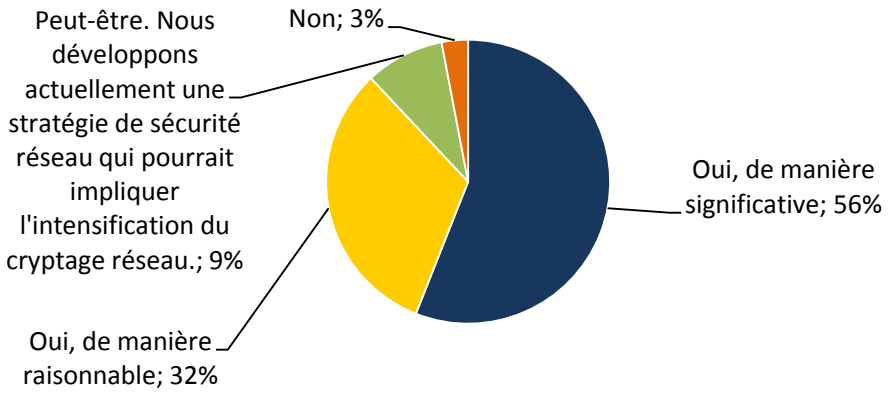
Chiffrement généralisé des réseaux

Le trafic chiffrer est devenu omniprésent dans la plupart des entreprises. Aujourd'hui, une grande majorité (87 %) des entreprises participant à l'étude cryptent au moins 25 % de l'ensemble de leur trafic réseau. De plus, certaines ont intégré le chiffrement du réseau à un niveau bien plus élevé : 25 % indiquent qu'elles cryptent déjà jusqu'à 75 % de leur trafic réseau !

Alors que le trafic chiffrer représente déjà un pourcentage significatif de l'ensemble des communications réseau, 56 % des entreprises déclarent que le volume de leur trafic réseau chiffrer va augmenter de façon significative au cours des 2 prochaines années, et 32 % pensent que ce volume va augmenter dans une certaine mesure sur la même période (voir la figure 1).

Figure 1. La part du trafic réseau chiffrer va augmenter dans la plupart des entreprises

Pensez-vous que le pourcentage du trafic réseau chiffré de votre entreprise augmentera au cours des 24 prochains mois ? (en pourcentage de réponses, N=150)



Source : Entreprise Strategy Group, 2015.

Pourquoi les entreprises augmentent-elles le chiffrement de leur réseau ? Les participants ont mis en avant plusieurs éléments :

- 42 % des entreprises intensifient le chiffrement de leur réseau car elles pensent que cela constitue une bonne pratique en matière de sécurité.
- 41 % des entreprises intensifient le chiffrement de leur réseau en raison d'une augmentation du trafic serveur à serveur (est-ouest) devant être protégé.
- 37 % des entreprises intensifient le chiffrement de leur réseau pour des motifs de conformité réglementaire.
- 33 % des entreprises intensifient le chiffrement de leur réseau (SSL/TLS, en particulier) pour une meilleure protection des applications Web développées en interne.

Chiffrement des réseaux et sécurité de l'information

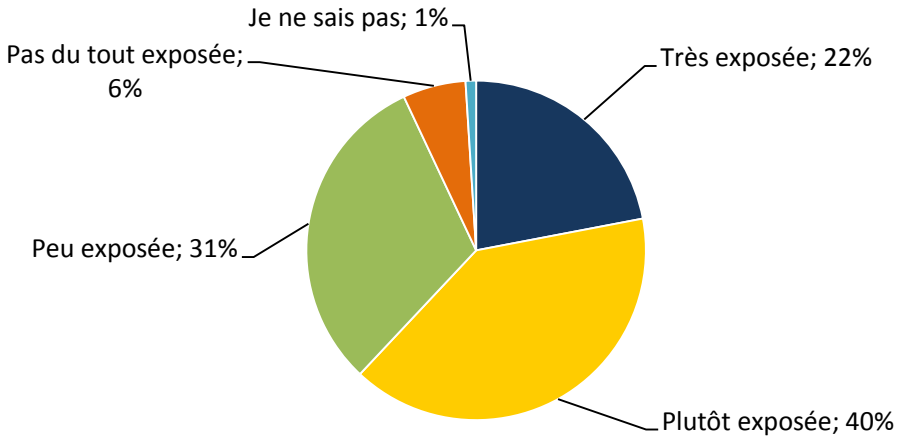
Le chiffrement des réseaux constitue une bonne pratique en matière de sécurité car cela protège la confidentialité du trafic réseau lors de son parcours de la source à la destination. Bien que cela puisse être bénéfique, les professionnels de la sécurité ont conscience que ce chiffrement peut également être utilisé pour des raisons

malveillantes. Les cybercriminels et les pirates informatiques peuvent utiliser les canaux chiffrers pour masquer des activités de reconnaissance, la distribution de logiciels malveillants et un trafic Commande-et-Contrôle (C&C ou C2) avec des sessions SSL/TLS anodines. En cryptant leurs actions malveillantes, les pirates informatiques parviennent à contourner les outils de sécurité réseau classiques utilisés pour le filtrage des paquets, l'inspection du trafic et la prévention/détection avancée des menaces qui peuvent uniquement scruter les paquets non chiffrers des réseaux. Le dilemme est également accentué par le fait que les menaces persistantes avancées (APT) utilisent de plus en plus les ports non standard (au-delà du Web/HTTPS sur le port TCP 443) pour infiltrer les entreprises et s'emparer des données propriétaires. De plus, les RSSI doivent être conscients que cette menace va uniquement augmenter au fur et à mesure de l'extension du chiffrement de l'ensemble du trafic réseau par les entreprises.

Ces dernières sont-elles vulnérables aux cyber-attaques qui utilisent le chiffrement des réseaux pour s'immiscer ? Les professionnels de l'informatique et de la sécurité qui ont participé à l'étude sont assurément convaincus que cela est le cas : 22 % indiquent que leur entreprise est extrêmement vulnérable à certains types de cyber-attaques utilisant le chiffrement SSL/TLS pour s'immiscer afin de contourner les contrôles de sécurité existants, et 40 % pensent que leur entreprise est vulnérable dans une certaine mesure à certains de ces types de cyber-attaques (voir la figure 2).

Figure 2. Les entreprises sont vulnérables aux cyber-attaques sur les canaux chiffrers

D'après vous, votre entreprise est-elle exposée à certains types de cyber-attaques (APT, exfiltration de données, menaces internes, etc.) qui utilisent le chiffrement SSL/TLS pour s'immiscer sur un réseau en déjouant les contrôles de sécurité en place ? (en pourcentage de réponses, N=150)



Source : Entreprise Strategy Group, 2015.

En raison de la menace représentée par le trafic SSL/TLS, la plupart des organisations indiquent qu'elles mettent activement en œuvre des contre-mesures de sécurité réseau. Une forte majorité (87 %) des entreprises ayant participé déchiffrent, puis inspectent, le trafic SSL/TLS pour détecter les signes d'une activité de reconnaissance, les logiciels malveillants, les communications Commande-et-Contrôle, etc. Parmi les autres entreprises, 8 % affirment qu'elles déploient des technologies de sécurité réseau appropriées qui leur permettent d'inspecter le trafic SSL/TLS au cours des 12 prochains mois. Les 5 % restants ne procèdent pas au déchiffrement/inspection du trafic SSL/TLS chiffrer, mais sont intéressées par cette méthode pour une période ultérieure.

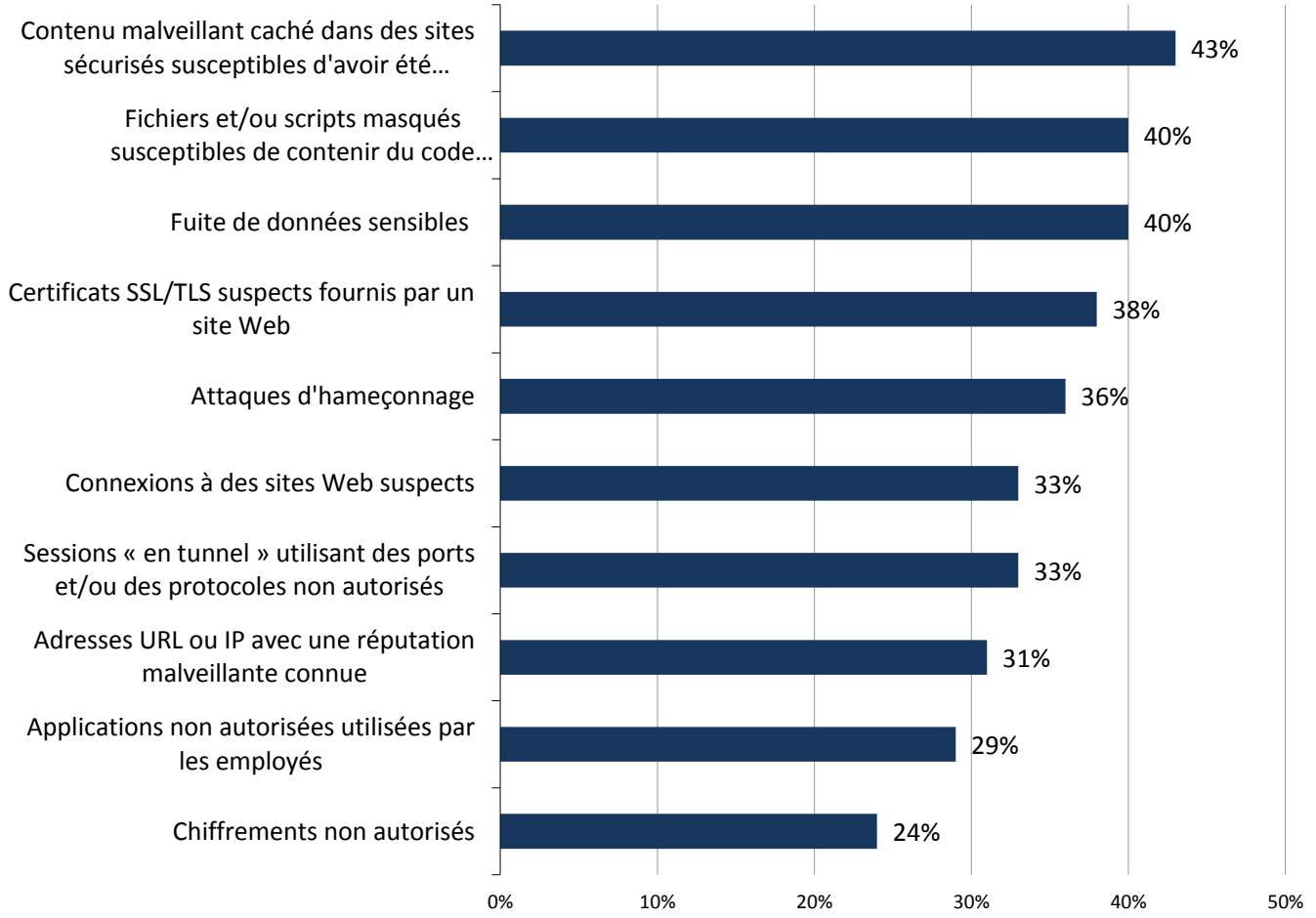
Les résultats de l'étude indiquent que le déchiffrement SSL/TLS est réalisé sur divers protocoles (HTTP, FTP, POP3, IMAP, etc.) avec de nombreux outils et technologies différents, notamment les pare-feux nouvelle génération, les services SaaS basés sur le cloud et les équipements de déchiffrement SSL/TLS dédiés. Les entreprises utilisent

également diverses technologies pour l'inspection du trafic telles que les passerelles de gestion des menaces Web, les passerelles antivirus et les outils légaux/d'analyse de la sécurité.

Mais qu'espèrent trouver les professionnels de la sécurité dans les sessions chiffrées ? 43 % recherchent des contenus malveillants intégrés dans des sites sécurisés qui ont pu être corrompus (technique du « point d'eau » ou waterholing), 40 % sont en quête de fichiers et/ou scripts cachés susceptibles de contenir un code suspect/malveillant, et 40 % surveillent le trafic SSL/TLS pour détecter toute fuite de données sensibles (voir la figure 3).

Figure 3. Menaces potentielles au sein du trafic chiffré

Concernant l'inspection du trafic SSL/TLS chiffré, quels types de menaces votre entreprise cible-t-elle ou envisage-t-elle de cibler ? (en pourcentage de réponses, N=150, plusieurs réponses possibles)



Source : Entreprise Strategy Group, 2015.

Défis de la sécurité réseau avec l'inspection/déchiffrement SSL/TLS

D'après l'étude d'ESG, les professionnels de la sécurité sont conscients de la menace que représente le trafic réseau chiffré et mettent en œuvre, de façon proactive, des contrôles de sécurité afin de réduire ce risque. En fait, 55 % des entreprises indiquent qu'à l'avenir, elles vont considérablement augmenter l'inspection/déchiffrement du trafic SSL/TLS, et 40 % vont l'accroître dans une certaine mesure.

Malgré leurs activités actuelles, le déchiffrement et l'inspection du trafic SSL/TLS ont créé un certain nombre de difficultés opérationnelles et techniques. Au cours des 5 dernières années, plusieurs entreprises ont progressivement augmenté le recours au trafic SSL/TLS dans les applications Web développées en interne et adopté des applications SaaS basées sur le cloud avec chiffrement des couches 5/6. Dans le même temps, les professionnels de la sécurité et des réseaux ont suivi le mouvement, en mettant en œuvre divers outils de déchiffrement et d'inspection du trafic SSL/TLS sur différents segments du réseau et plusieurs emplacements des réseaux des entreprises. Cette chaîne d'événements a abouti à une infrastructure désorganisée du déchiffrement et de l'inspection du trafic SSL/TLS, composée d'une variété de technologies et processus/procédures opérationnels. Cela peut expliquer le pourcentage élevé d'entreprises qui déchiffrent le trafic SSL/TLS pour des raisons de sécurité, même si cette activité est réalisée de façon ciblée et incomplète.

La gamme actuelle des méthodes de sécurité et de chiffrement des réseaux est illustrée dans les données de l'étude d'ESG. Lorsqu'il leur est demandé de décrire leur approche du déchiffrement et de l'inspection du trafic SSL/TLS pour des raisons de sécurité :

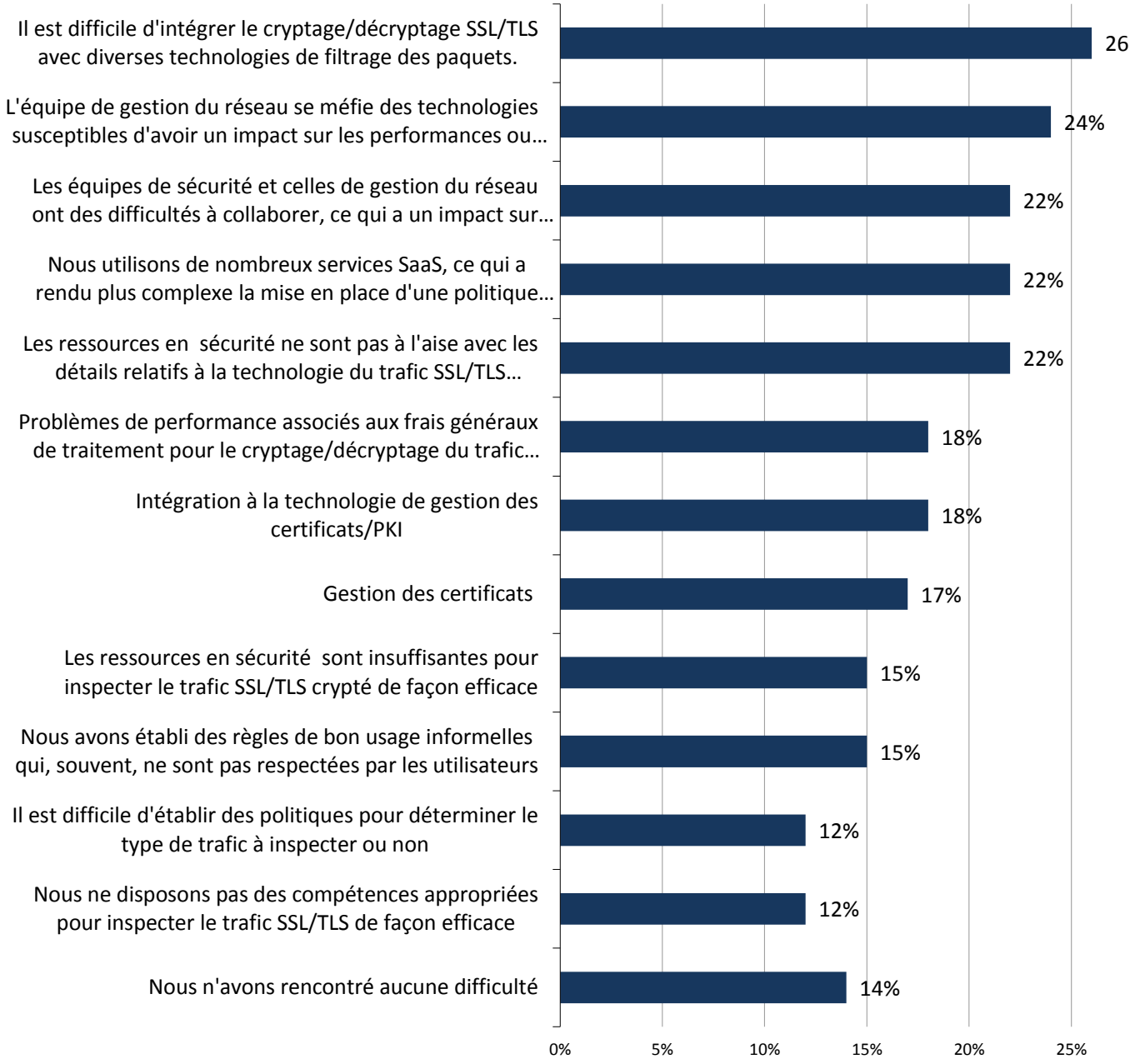
- 14 % des entreprises indiquent qu'elles inspectent le trafic SSL/TLS chiffré de manière ciblée en mettant en œuvre des technologies sur le réseau de façon ad-hoc et selon les besoins.
- 21 % des entreprises indiquent qu'elles inspectent actuellement le trafic SSL/TLS chiffré de manière ciblée en mettant en œuvre des technologies sur le réseau de façon ad-hoc et selon les besoins, mais qu'elles seraient intéressées, à l'avenir, par l'établissement d'une stratégie d'entreprise plus exhaustive.
- 21 % des entreprises indiquent qu'elles inspectent actuellement le trafic SSL/TLS chiffré de manière ciblée en mettant en œuvre des technologies sur le réseau de façon ad-hoc et selon les besoins, mais qu'elles prévoient d'établir, à l'avenir, une stratégie d'entreprise plus exhaustive.
- 24 % des entreprises indiquent qu'elles inspectent actuellement le trafic SSL/TLS chiffré de manière ciblée en mettant en œuvre des technologies sur le réseau de façon ad-hoc et selon les besoins, mais qu'elles sont en train de mettre en place une stratégie d'entreprise plus exhaustive pour une application ultérieure.
- Seules 20 % des entreprises indiquent qu'elles ont déjà mis en œuvre une stratégie d'entreprise exhaustive pour l'inspection du trafic SSL/TLS chiffré.

Les données cumulées illustrent clairement la règle des 80/20 : 80 % des entreprises déchiffrent/inspectent le trafic SSL/TLS de façon ciblée, contre seulement 20 % ayant une approche plus stratégique. Il est évident que cela va évoluer à l'avenir, 66 % des entreprises étant en cours d'implémentation d'une stratégie de déchiffrement/inspection du trafic SSL/TLS, envisagent de la mettre en place ou sont intéressées par ce type de stratégie.

Alors que cela est de bon augure pour l'avenir, de nombreuses entreprises font face à des difficultés croissantes avec le déchiffrement et l'inspection du trafic SSL/TLS actuels. Ces problèmes concernent l'organisation, les technologies, les processus et la confidentialité des données. Par exemple, 26 % des professionnels de la sécurité affirment qu'il est difficile d'intégrer des technologies de chiffrement/déchiffrement du trafic SSL/TLS avec une gamme de technologies de filtrage des paquets de sécurité du réseau, 24 % indiquent que l'équipe de gestion du réseau se méfie des technologies susceptibles d'avoir un impact/de perturber le réseau, et 22 % pointent des problèmes de collaboration entre les équipes de sécurité des informations (infosec) et celles de gestion du réseau au sein de leur entreprise (voir la figure 4).

Figure 4. Difficultés associées à l'inspection du trafic réseau chiffré

Parmi ces difficultés, le cas échéant, lesquelles votre entreprise a-t-elle rencontrées lors de l'inspection du trafic chiffré SSL/TLS ? (en pourcentage de réponses, N=130, trois réponses possibles)



Source : Entreprise Strategy Group, 2015.

À quoi ressemble la stratégie de déchiffrement et d'inspection SSL/TLS ?

L'étude d'ESG indique clairement que la plupart des entreprises vont uniquement augmenter le chiffrement de leur réseau et l'utilisation des technologies de déchiffrement et d'inspection du trafic SSL/TLS qui les accompagnent. De plus, la plupart des sociétés envisagent de créer à l'avenir une stratégie de déchiffrement SSL/TLS plus holistique et précisent que leurs approches ciblées actuelles ne fonctionnent pas.

Cela pose une question évidente : À quoi ressemblent une stratégie et une solution complètes de déchiffrement et d'inspection du trafic SSL/TLS ? ESG pense que ce type de stratégie de sécurité réseau se caractérise par les éléments suivants :

- **Des « services » de déchiffrement du trafic SSL/TLS spécifiques hautes performances.** Dans les mises en œuvre ciblées actuelles, les entreprises utilisent différentes technologies dispersées sur le réseau pour le déchiffrement du trafic SSL/TLS. Cela génère de nombreux frais généraux d'exploitation et peut aboutir à une mise en œuvre de proxys réseau complexe ainsi qu'à des problèmes de gestion des certificats SSL. Pour limiter ces difficultés, les entreprises sont en train de créer, ou sont susceptibles de créer, un « service » en étoile de déchiffrement du trafic SSL/TLS basé sur une technologie spécifique. Il est probable que la technologie de déchiffrement du trafic SSL/TLS sera basée sur une architecture logicielle comportant une fonctionnalité Commande-et-Contrôle centrale (gestion de la politique, gestion des certificats, gestion de la configuration, création de rapports, etc.) et une mise en œuvre distribuée. De plus, les véritables opérations de déchiffrement seront réalisées de différentes formes : équipements hautes performances pour le centre de données et/ou le cœur du réseau, équipements de petite taille ou virtuels pour les bureaux distants et équipements virtuels basés sur le cloud pour protéger les réseaux laaS, SaaS et PaaS.
- **Une intégration multicouche avec des outils de sécurité.** Une fois le trafic chiffrer, l'architecture de déchiffrement du trafic SSL/TLS va traiter et transférer ce dernier à plusieurs outils de sécurité (par exemple, pare-feu nouvelle génération, IDS/IPS, analyse de logiciels malveillants, analyses de sécurité, par exemple) pour une inspection du contenu plus approfondie. Cela va également ressembler à une architecture en étoile avec un service de déchiffrement du trafic SSL/TLS jouant le rôle de pont middleware centralisé. Cette approche préserve l'infrastructure de sécurité existante, tout en ajoutant une solution de gestion du trafic chiffrer évolutive et adaptable. Les outils d'analyse de sécurité, en particulier, vont inspecter le trafic individuellement pendant qu'un moteur d'analyse principal va corréler les menaces sur l'ensemble des services et outils d'analyse de sécurité du réseau.
- **Une résolution des problèmes automatisée.** Basées sur ce type de stratégie d'entreprise, l'inspection et le déchiffrement du trafic SSL/TLS seront coordonnées sur les réseaux et équipements haut débit avec des performances quasiment en temps réel. Ainsi, les RSSI devraient collaborer avec les ingénieurs et architectes réseau pour mettre en œuvre des contrôles de sécurité réseau automatisés sur le réseau. Lorsque la détection avancée des logiciels malveillants, l'analyse du réseau et les outils d'analyse au point de destination identifient un PC corrompu qui charge des fichiers chiffrers vers une adresse IP en Europe de l'Est avec un niveau de sécurité élevé, le réseau devrait être en mesure d'interrompre automatiquement cette connexion tout en créant des signatures IDS/IPS et des règles de pare-feu pour bloquer les activités similaires ultérieures.

L'architecture de déchiffrement et d'inspection du trafic SSL/TLS décrite ci-dessus va connaître une évolution symbiotique au fur et à mesure que les entreprises vont intégrer des technologies SDN (Software-Defined Networking) et NFV (Network Functions Virtualization) au cours des prochaines années. En effet, ces dernières rendent les fonctions du réseau programmables par le biais d'API logicielles standard. Lorsque le réseau détecte des paquets chiffrers, il peut être programmé pour créer un réseau VLAN dynamique pour acheminer le trafic vers un service de déchiffrement SSL/TLS. Une fois le déchiffrement effectué, le service SSL/TLS peut alors créer plusieurs réseaux VLAN dynamiques pour acheminer le trafic en clair vers différents équipements de sécurité, selon les besoins. Cela va considérablement simplifier le codage en dur des réseaux et faciliter la mise en œuvre d'une stratégie SSL/TLS à l'échelle de l'entreprise.

The Bigger Truth, la réalité du terrain

Les données présentées dans ce rapport sont habituelles pour les professionnels de la sécurité informatique et des informations. L'équipe informatique met en œuvre une nouvelle technologie que l'équipe de sécurité des informations est chargée de sécuriser. Il s'agit d'un processus fluide, avec différents processus, planifications d'adoption et technologies employés dans l'ensemble de l'entreprise. Les groupes informatiques et de sécurité collaborent pour équilibrer le maintien des activités par rapport à la gestion des risques, mais la diversité des personnes, processus et technologies mènent à une infrastructure chaotique difficile à gérer et contrôler.

Ce rapport indique que de nombreuses entreprises ont atteint ce point charnière précis. Elles augmentent le chiffrement du trafic de leur réseau pour protéger la confidentialité des données, ce qui induit un déchiffrement et une inspection du trafic SSL/TLS pour des raisons de sécurité. Bien qu'elles parviennent à faire face aux risques, ce processus est devenu extrêmement complexe et génère des frais généraux d'exploitation de plus en plus importants.

De nombreuses entreprises délaissant leurs méthodes de déchiffrement et d'inspection ciblées du trafic SSL/TLS pour une approche plus stratégique, il est raisonnable de supposer que les méthodes de déchiffrement et d'inspection du trafic SSL/TLS existantes deviennent chaque jour plus inefficaces et complexes. De plus, la plupart des entreprises envisageant de crypter davantage leur réseau, les RSSI ne devraient pas laisser leurs stratégies de déchiffrement et d'inspection du trafic SSL/TLS dépérir. Au contraire, ils devraient faire de la gestion du trafic chiffrer une priorité à court terme afin de pouvoir faire face à un trafic SSL chiffrer croissant et à des cyber-menaces dangereuses potentiellement masquées.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 (États-Unis) | Tél. : +1 508.482.0188 Télécopie : +1 508.482.0218 | www.esg-global.com