Top 5 des pièges à éviter d'un chiffrement non maîtrisé

Tout chiffrer… Chiffrer les disques, chiffrer la donnée en mouvement, chiffrer les communications, chiffrer les flux

Plus qu'une bonne pratique, c'est aujourd'hui une nécessité dont les DSI ont bien conscience. Elles n'ignorent cependant pas que cette omniprésence des chiffrements - notamment dans les communications Internet et les échanges de données avec les services Cloud - est aussi porteuse de risques intrinsèques. L'objectif premier du chiffrement consiste à masquer la donnée et les flux pour protéger vos employés, vos clients, votre Business, et apporter de la confidentialité dans tous les échanges. Mais cette confidentialité peut se retourner contre l'entreprise parce qu'elle aveugle par la même occasion les sécurités mises en place pour protéger les utilisateurs et le savoir informationnel.

Il y a trois ans seulement, les flux chiffrés ne représentaient que 5% du trafic traversant l'infrastructure de l'entreprise. **En 2015, l'ARCEP estime que 50% des flux qui parcourent aujourd'hui l'entreprise sont chiffrés.**

Or, ce chiffrement de plus en plus systématique engendre un manque de visibilité sur les flux de données qui quittent l'entreprise ou qui y entrent. Ce risque potentiel ne doit pas être négligé parce que les flux SSL malveillants sont indiscernables des flux sains. Un tel chiffrement facilite aussi l'entrée des codes malveillants ainsi que la sortie d'information sans qu'on la perçoive. **Aujourd'hui, 80% des attaques exploitant SSL ou HTTPS ne sont pas détectées !**

Alertées par l'ANSSI, les DSI ont récemment pris conscience de ces risques. **Mais, nombreuses sont celles qui ignorent dans quel contexte, et comment, elles peuvent inspecter les flux chiffrés tout en respectant la confidentialité des échanges.**

Voici un TOP 5 des pièges à éviter et des mesures à prendre.

1. METTRE EN PLACE UNE POLITIQUE DE DÉCHIFFREMENT

Les entreprises doivent d'une manière ou d'une autre pouvoir retrouver de la visibilité et sécuriser les contenus avant qu'ils n'échappent ou ne pénètrent l'entreprise. Une opération vivement encouragée par l'ANSSI dans sa note technique « *Recommandations de sécurité concernant l'analyse des flux HTTPS* ».

Retrouver de la visibilité, c'est être à même d'inspecter les flux afin de vérifier qu'ils ne sont pas porteurs d'une menace sans pour autant compromettre la vie privée des collaborateurs. Cette visibilité ne doit pas être perçue comme une atteinte à la vie privée mais comme une protection des utilisateurs et de leurs données.

La CNIL reconnaît les besoins des entreprises en la matière et les invite à adopter les mesures de l'ANSSI. Elle rappelle que le déchiffrement SSL est parfaitement légitime tant que l'objectif poursuivi est uniquement l'amélioration de la sécurité de l'entreprise, de son système d'information et de ses utilisateurs. Ce déchiffrement doit se faire en toute transparence, en informant les collaborateurs, en limitant les traces conservées et en restreignant l'accès aux données déchiffrées.

Au-delà des solutions techniques, il est essentiel de mettre en place, avec les RH et les représentants du personnel, des politiques de bon usage du Web et des réseaux sociaux en tenant compte des impératifs de respect de la vie privée et de conformité aux réglementations en vigueur.

Les entreprises doivent aujourd'hui mettre en place une vraie politique de déchiffrement dans le même esprit que celle qu'elles ont déjà mise en place en matière d'accès à Internet et d'utilisation de l'email.

2. SAVOIR SE PRÉMUNIR DES MENACES MASQUÉES

Prenant conscience de la criticité des menaces cybercriminelles, les entreprises ont, ces dernières années, fortement investi pour bâtir une véritable infrastructure de sécurité avec des pare-feux, du sandboxing, des antivirus, du filtrage de spams et phishing, de la DLP (Data Leak Prevention). Mais, tout cet investissement, toute cette énergie déployée, toutes ces ressources, ne servent pourtant aujourd'hui qu'à inspecter 50% du trafic entrant et sortant de l'entreprise !

L'absence de visibilité qui découle du chiffrement des échanges a encouragé les cybercriminels à systématiquement chiffrer leurs applications et leurs flux malveillants afin d'œuvrer dans l'ombre et d'outrepasser la majorité des outils de sécurité réseau et des processus de contrôle mis en place. Le Gartner estime qu'en 2017 plus de la moitié des attaques menées sur les réseaux d'entreprise exploiteront une forme ou une autre de chiffrement de leurs activités malveillantes.

Pour lutter contre la prolifération de ces nouvelles menaces, les IT ont besoin de retrouver de la visibilité et s'assurer de pouvoir reconnaître et détecter les menaces qui se dissimulent derrière les trafics chiffrés. Ils ont besoin de pouvoir appliquer leurs outils d'analyses et de détection sur des flux préalablement déchiffrés.

La plupart des matériels et outils de sécurité dont disposent les DSI, intègrent - en général - des fonctions de déchiffrement SSL. Ces dernières sont, cependant, très rarement activées car leur mise en œuvre engendre un effondrement des performances (de l'ordre de 70 à 80% de performances en moins). Dès lors, il faudrait parfois doubler, voire tripler, les capacités matérielles ce qui n'est pas réaliste. En outre, leur activation et leur paramétrage sur chacun des éléments de sécurité est une opération délicate, difficile à maintenir dans le temps et bien peu optimale en matière d'administration.

Une autre approche doit donc être adoptée pour gérer efficacement, intelligemment et à moindre coût, ces trafics chiffrés...

3. APPRENDRE À GÉRER INTELLIGEMMENT LE TRAFIC CHIFFRÉ

Comme le confirment l'ANSSI et la CNIL, les entreprises peuvent et doivent déchiffrer les flux SSL, mais ne peuvent pas le faire n'importe comment.

Dans la pratique, tous les trafics ne doivent pas être déchiffrés. Il faut mettre en œuvre des solutions intelligentes et facilement administrables qui permettent de ne déchiffrer que ce qui mérite de l'être.

Allier le respect de la vie privée et la protection de l'infrastructure est un challenge qui peut être relevé à l'aide de solutions ETM (Encrypted Trafic Management) qui n'inspectent que des flux répondant à des stratégies préétablies par l'entreprise. Ces solutions techniques spécialisées sont d'un grand secours pour gérer le trafic chiffré en fonction des sites visités et des vulnérabilités connues. Elles permettent de limiter l'usage des flux déchiffrés aux uniques tâches de sécurité : filtres DLP, scan antivirus, tests des pièces attachées dans des environnements d'analyse automatisés (sandbox), etc. Elles satisfont, ainsi, aussi bien aux recommandations de l'ANSSI que de la CNIL.

4. LUTTER CONTRE LE SHADOW IT

Le Shadow IT est l'un des fléaux actuels. Poussés par une volonté de trouver très rapidement des solutions pratiques à leurs problèmes quotidiens ou ponctuels - au détriment de tout contrôle et de tout bon sens en matière de sécurité - les utilisateurs, mais aussi les développeurs, multiplient l'usage de services Web en dehors de toute approbation de la DSI. Un trafic souvent rendu encore plus obscur par l'utilisation de tunnels SSL qui masquent l'essentiel de l'usage.

Il est pourtant important pour les DSI de comprendre les usages faits de ces services afin de proposer aux utilisateurs des alternatives gérables/gérées par la DSI et respectant les contraintes réglementaires. Le déchiffrement permet de faire sortir ce Shadow IT de l'ombre...

5. NE PAS NÉGLIGER LES MENACES DE L'INTÉRIEUR

L'extraction d'informations confidentielles provient souvent de l'intérieur même des murs de l'entreprise. Une grande partie des fuites résultent d'actions des collaborateurs, dans la très grande majorité des cas, sans volonté de nuire à l'entreprise. Bien des utilisateurs utilisent des services Cloud, sans avoir conscience des risques, pour échanger des fichiers ou leur permettre de terminer des travaux en cours chez eux. Ils font confiance aux sécurités présentes dans l'entreprise et destinées à les protéger contre leurs propres erreurs, sans réaliser que le chiffrement de ces services rend aveugle ces protections. La généralisation du chiffrement handicape les capacités des entreprises à gouverner les données qui sortent de leur organisation et entraînent souvent un contournement des outils d'alertes ou de DLP (Data Leak Protection ou Protection contre la fuite de données) mis en place.

En outre, les malwares furtifs et autres APT (Advanced Persistant Threats) déjà présents dans l'infrastructure utilisent aussi des flux chiffrés pour masquer leurs activités malveillantes ce qui complexifie leur découverte.

Il est donc tout aussi essentiel de pouvoir retrouver de la visibilité sur les flux chiffrés qui quittent l'entreprise.

Au final, on retiendra que pour lutter contre les risques induits par un chiffrement de plus en plus omniprésent des flux entrants et sortants, les entreprises ne sont pas dénuées de solutions. Elles ont le droit et le devoir de retrouver de la visibilité en inspectant, à des fins de sécurité uniquement, le trafic chiffré. Il existe, sur le marché, des solutions spécifiquement pensées pour ces besoins. Certains spécialistes comme Blue Coat proposent des appliances ETM (Encrypted Trafic Management) de gestion des flux chiffrés. Ces dernières reposent sur deux concepts : retrouver de la visibilité SSL sans dégrader les performances et mettre en oeuvre une vraie politique de déchiffrement afin d'alimenter l'ensemble des outils de sécurité mis en place, tout en respectant les contraintes de confidentialité et de respect de la vie privée. Elles offrent des fonctionnalités avancées de contrôle des flux à déchiffrer, permettent de détecter des menaces jusqu'ici invisibles, et limitent les risques sur vos données, votre infrastructure et vos collaborateurs.

Réalisation éditoriale : Groupe IT Media www.ITMedia.fr – Conception graphique : Agence Com4Médias www.com4medias.com