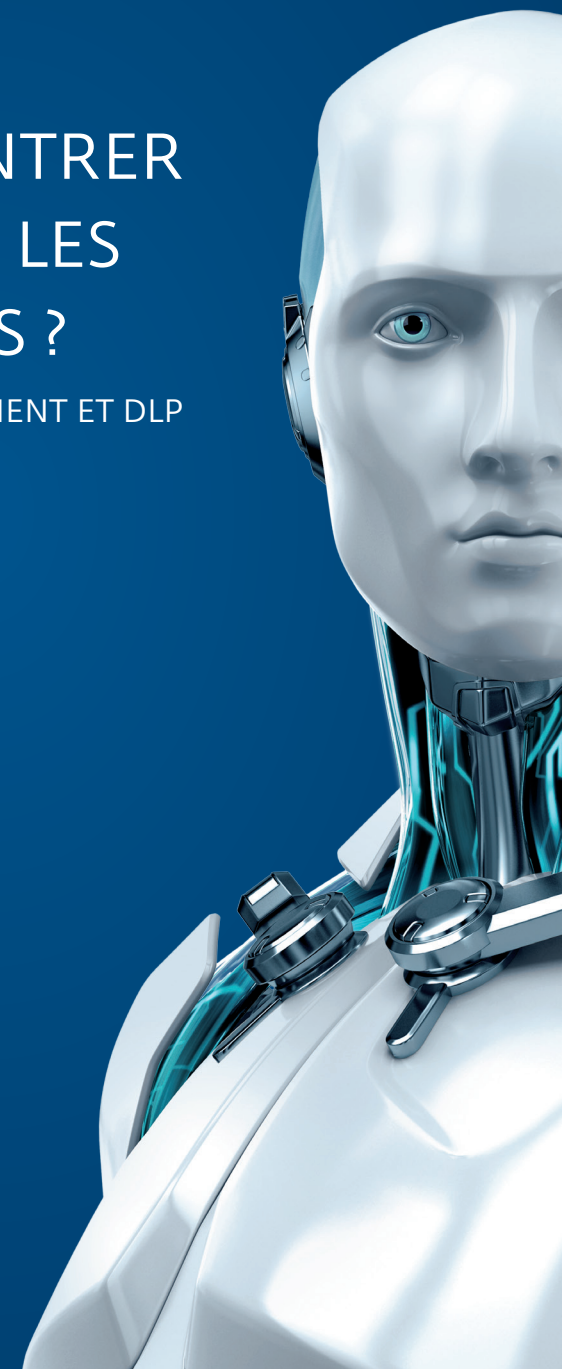
ENJOY SAFER TECHNOLOGY™

COMMENT CONTRER EFFICACEMENT LES RANSOMWARES ?

AUTHENTIFICATION, CHIFFREMENT ET DLP



En 2003, il y avait 500 millions d'adresses IP. En 2015, elles étaient 16 milliards et pour 2020, entre 50 et 80 milliards d'adresses IP (en intégrant les adresses des objets connectés - IoT) sont attendues. La multiplication des points d'entrée est inquiétante au vu de la facilité avec laquelle il est possible d'attaquer des entreprises en passant par les connexions extérieures de prestataires, services WEB, appareils mobiles...

En 2016, les ransomwares se propagent davantage via les courriers électroniques. En outre, 98 % des URL contenues dans les e-mails douteux redirigent la victime vers des sites contrôlés ou infectés par les cybercriminels qui hébergent des logiciels infectés présentés sous forme de fichiers exécutables. Une bonne part d'entre eux demande des « cyber-rançons ».

Ransomwares, nouveaux revenus pour les cyber-attaquants

Le modèle économique des codes employés par les cybercriminels a évolué. Longtemps, les pirates ont profité de leurs actions malveillantes pour dérober des identités et des données propres aux utilisateurs de cartes bancaires afin de les revendre sur des marchés clandestins du Deep Web. Mais sur ce marché aussi les prix connaissent des variations. Ces dernières années, le tarif des données détournées s'est effondré, passant de 25$ en 2011 à 6$ l'unité en 2016. Le business du ransomware s'est donc imposé face à celui de la revente de données. Ainsi, les codes malveillants qui chiffrent les données volées, acceptent de les déchiffrer grâce à une clé de déchiffrement à condition que la victime paye la rançon. Rentable et anonyme, ce type d'attaque cible particuliers comme entreprises. Selon les experts, les cybercriminels engrangent 30 millions de dollars par trimestre grâce au ransomware Cryptolocker. Le FBI a révélé récemment que les victimes de ransomwares aux Etats-Unis ont déclaré 209 millions de dollars de pertes au premier trimestre 2016, contre 24 millions pour l'ensemble de l'année 2015. Une variante, le ransomware Locky qui est l'un des plus connus, constitue un cas intéressant pour comprendre l'évolution des risques liés aux ransomwares. Rien qu'en 2016, le code a muté pour multiplier le nombre de victimes, passant de 3% de messages infectés en février à 17% en mars. Et ce n'est qu'un début : les performances des rançongiciels s'appuient sur de nombreux facteurs comme l'émergence de moyens de paiement anonymes de type Bitcoin, et le fort développement de la mobilité.

Les mobiles, future première cible

Un ransomware tel que Cryptolocker s'adapte aux outils et aux configurations de ses cibles. De plus en plus d'attaques visent directement les utilisateurs de mobiles. Un récent rapport livre des chiffres révélateurs sur l'année 2015 : les utilisateurs ont téléchargé plus de 2 milliards d'applications mobiles susceptibles de dérober des données personnelles via des ransomwares. **Les applications mobiles dangereuses affectent 2 entreprises sur 5.**

(lire : http://www.welivesecurity.com/wp-content/uploads/2016/02/Rise_of_Android_Ransomware.pdf)

Comment se protéger efficacement contre les ransomwares ?

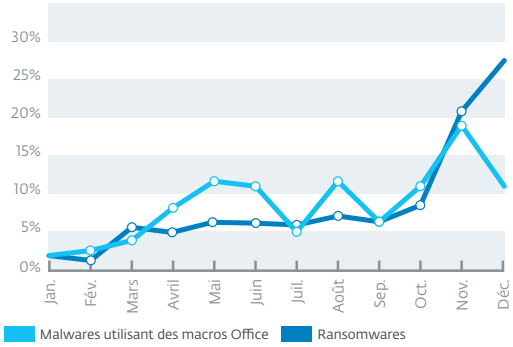
Plus de 50 variantes de ransomwares ont été répertoriées en 2016. La surface potentielle d'attaque s'étend rapidement. Idéalement, la stratégie la plus efficace contre les ransomwares – en plus d'une réelle politique de sauvegarde - consiste à anticiper leurs détections avant qu'ils ne pénètrent dans le système d'information de l'entreprise. Lorsqu'une alerte est déclenchée à propos d'une menace de type ransomware, il y a de forts risques que le chiffrement des données « prises en otage » ait débuté. Ce processus intervient généralement dans les minutes qui suivent la compromission initiale.

Plus de 50 variantes de ransomwares ont été répertoriées en 2016

Parmi les solutions de prévention, le principe de segmentation du réseau (à l'image de celle mise en place par les pompiers pour limiter l'extension d'un feu de forêt) s'avère utile. En cas d'attaque, seule une zone du réseau (forêt) est abandonnée aux malwares (feu). Il s'agit de contrôler l'accès à celui-ci, de faire barrage aux logiciels malveillants connus, et de détecter et faire obstacle aux malwares non identifiés. Les mécanismes de contrôle sur postes de travail peuvent se montrer particulièrement efficaces et ne doivent jamais être négligés.

Bien connaître les évolutions des dernières technologies utilisées par les campagnes de ransomwares permet de cerner la totalité des indicateurs de compromission (IOC) utilisés par ces logiciels malveillants. Ainsi, une fois le réseau infiltré, certains cyber-attaquants sélectionnent les données monnayables. Pour optimiser le tri, ils utilisent des codes malveillants dédiés à cette opération comme SamSa par exemple. Plus globalement, toutes les entreprises doivent aussi anticiper le vol de données en rendant inutilisables ces informations. Cette approche permet d'atténuer les conséquences financières, opérationnelles et l'image des organisations « cyber-victimes ».

Tendances mensuelles sur les ransomwares et les « macro malwares » en 2015



Source : FireEye 2016

Perte et vol de données, des milliards perdus : Les principaux résultats pour la France

32%

des entreprises ont fait l'objet d'un vol de données au cours des 12 derniers mois

72%

des professionnels de l'informatique doutent de pouvoir protéger leurs données si leur périmètre de sécurité venait à être compromis

81%

des professionnels de l'informatique pensent que les utilisateurs non autorisés seraient capables d'accéder au réseau voire, comme déclaré par 18% des interrogés, de l'infiltrer dans sa totalité.

Avec 1 e-mail sur 6 proposé sous la forme d'un spam contenant un code malveillant, le renforcement de la sécurité des e-mails devient un enjeu majeur pour les IT Managers en charge de la mise en place des politiques de sécurité.

Concernant les usurpations d'identités via les e-mails, IC3 (Internet Crime Center) entité rattachée au FBI, évalue leur augmentation à plus de 270% en 2015. Près de 80 pays en sont victimes et plus de 2 milliards de dollars de pertes ont été déplorées depuis fin 2013.

Étude Gémalto juin 2016 http://www2.gemalto.com/data-security-confidence-index/

Les leçons de « Panama Paper » : audit, patch, surveillance

L'affaire du Panama Paper a montré les faiblesses de la sécurité d'une entreprise de taille moyenne, mais dont les données des clients mondialement connus s'avèrent stratégiques puisqu'il s'agit d'un cabinet d'avocats international. Le cabinet visé ayant de grands clients institutionnels, il était de la responsabilité des dirigeants de faire auditer leurs services et ceux proposés par leurs fournisseurs. Les cyber-attaquants ont exploité sur les serveurs du cabinet des vulnérabilités connues mais non corrigées !

Rappelons une règle de base pour choisir de bons outils de sécurité : il faut toujours avoir conscience du modèle économique actuel : « si c'est gratuit ou pas cher, c'est vous et vos données qui seront exploités ».

« si c'est gratuit ou pas cher, c'est vous et vos données qui seront exploités »

Suite aux orientations de conformité réglementaire (voir ci-dessous) et de recommandations d'agences Européennes, le choix des grandes entreprises évolue et les solutions de sécurité d'éditeurs de confiance d'origine Européenne s'imposent de plus en plus auprès d'organisations stratégiques. ESET appartient à ce club confidentiel d'acteurs Européens de solutions et services de cyber-sécurité de haut niveau. Ses solutions sont reconnues pour leur efficacité et leurs performances et ses services sont réputés pour être très réactifs notamment pour contrer les vulnérabilités au moyen de patch.

Au-delà des équipements et applications, le choix de solutions de sécurité doit toujours comporter un volet « administration/threat intelligence ». Sauvegarder régulièrement les données et installer les mises à jour critiques constituent aussi les premiers réflexes contre l'attaque par ransomwares. Mettre en place des procédures de vérification du bon fonctionnement des solutions de sauvegarde s'avère aussi important que les sauvegardes elles-mêmes. Un autre niveau de sécurité consiste à tirer profit de tous les avantages de services de veille directement issus des laboratoires d'éditeurs reconnus et indépendants.

Règlement Général sur la Protection des Données et le Safe Harbor 2 : ce qu'il faut savoir

Connu sous l'appellation : Règlement général sur la protection des données (RGPD), le texte devrait entrer en vigueur courant 2016 et être applicable en 2018.

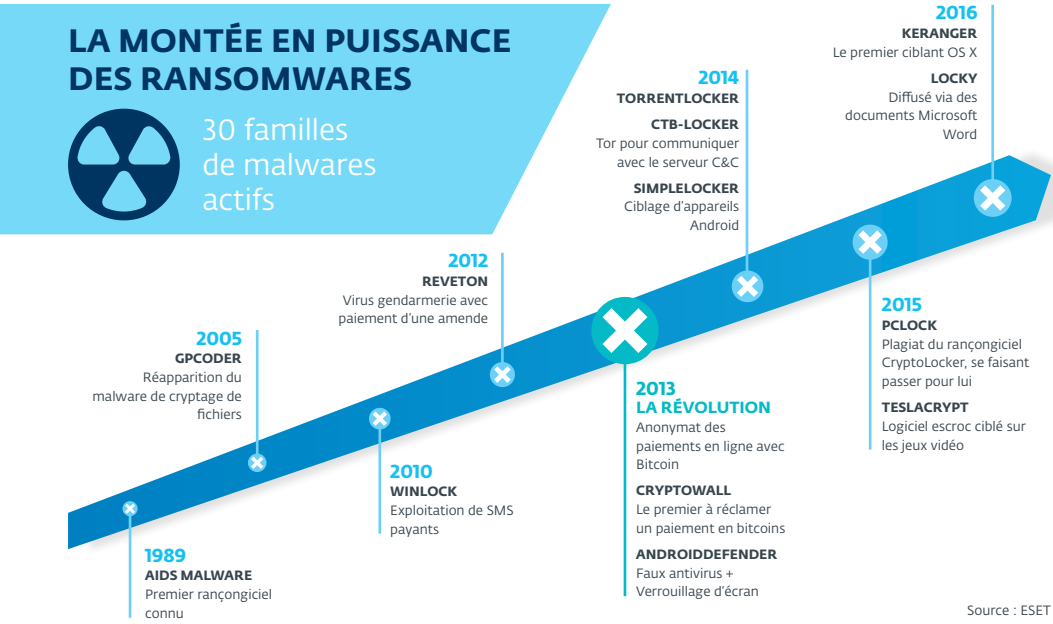
RGPD ou GDPR, ce texte récemment accepté par les pays membres de l'UE va avoir des conséquences importantes pour la mise en place de politiques de renforcement des procédures de protection des données pour l'ensemble des entreprises en activité dans les 28 pays de l'UE.

www.eset.com/fr/livres_blancs

Ransomwares : 200 millions de dollars en 2016

Les impacts financiers liés aux cyber-attaques alertent de plus en plus les directions générales. Le coût des ransomwares s'élevait à 25 millions de dollars en 2015. Il est estimé à 200 millions de dollars en 2016. Les noms de domaine créés pour les ransomwares sur le premier semestre 2015 ont été multipliés par 35 par rapport au quatrième semestre. Selon les éditeurs et opérateurs de services dédiés, l'augmentation du nombre de noms de domaine est généralement un signe avant-coureur d'attaques. Plus il y aura de rançons payées, plus il y aura d'attaques de ce type. Les cybercriminels peuvent se permettre d'augmenter le nombre de créations de noms de domaine DNS grâce aux revenus importants engendrés par les rançons. Des informations de cette nature restent souvent connues de prestataires spécialisés. Sur cette base, des services d'alertes sont proposés.

De leur côté, les groupes bancaires par exemple, consacrent « plusieurs centaines de millions d'euros chaque année » à la cybersécurité au niveau « services » pour identifier les failles de leurs systèmes, comprendre les mentalités des cyberattaquants, simuler des attaques et réaliser une veille « préventive ».

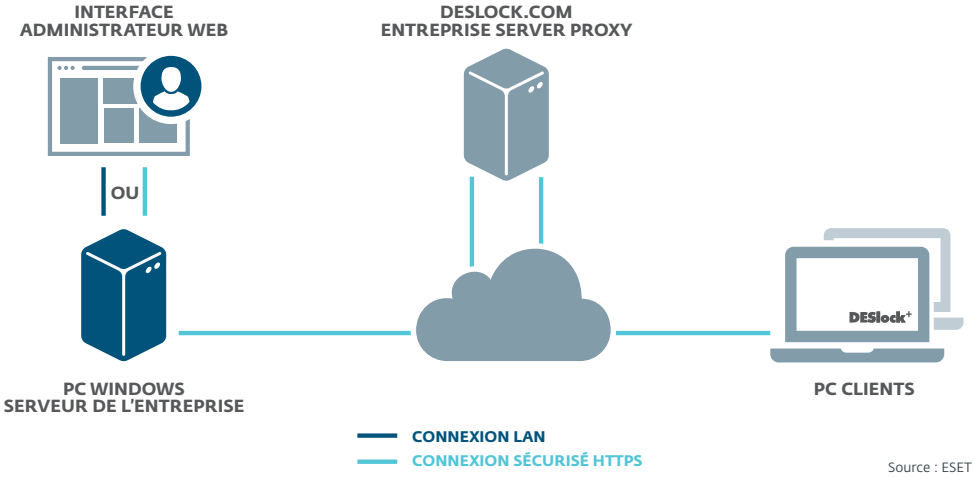


Source : ESET

Deux priorités face aux ransomwares : authentifier les accès et identifier les informations « critiques »

Une solution complète comme l'anti-ransomware d'ESET allant des serveurs de messagerie aux postes de travail, permet de détecter au niveau des e-mails si des ransomwares avec des droppers se trouvent en pièce jointe. En plus des terminaux où sont appliqués ces paramètres renforcés, les ingénieurs d'ESET ont effectué des tests qui démontrent que ces types de ransomwares n'ont aucune chance de chiffrer le système et le réseau.

Dans un autre cas (le ransomware TeslaCrypt) les équipes ESET ont rapidement créé un outil de déchiffrement gratuit capable de retrouver les fichiers infectés par toutes les variantes de ce ransomware. À ce sujet, la qualité d'investigation des laboratoires d'ESET s'effectue au plus haut niveau international. D'ailleurs, lors du récent test de Virus Bulletin qui testait 18 solutions complètes de sécurité e-mails pour les professionnels, ESET Mail Security pour Microsoft Exchange Server a atteint un taux de détection de spams de 99,999% sur les 177 000 spams envoyés. La solution d'ESET, 5ème éditeur mondial (Gartner 2015), détient pour la troisième fois consécutive la récompense VB Spam.



Source : ESET

ESET se distingue

Début 2016, un ransomware de dernière génération s'est propagé via des spams contenant des pièces jointes ou des liens vers des sites infectés. Le logiciel chiffrait les fichiers du système via un algorithme de type RSA-4096. La plupart des systèmes de chiffrement employés par les cybercriminels sont connus ce qui permet aux ingénieurs d'ESET de récupérer des fichiers chiffrés. Reste que cette approche nécessite le savoir-faire d'ingénieurs experts en cryptographie. Lors d'une récente attaque de ransomwares, les équipes d'ESET ont proposé une solution pour récupérer les données chiffrées, permettant ainsi de récupérer facilement les fichiers encodés en Base64.

Authentification : double et sans mémorisation de mot de passe

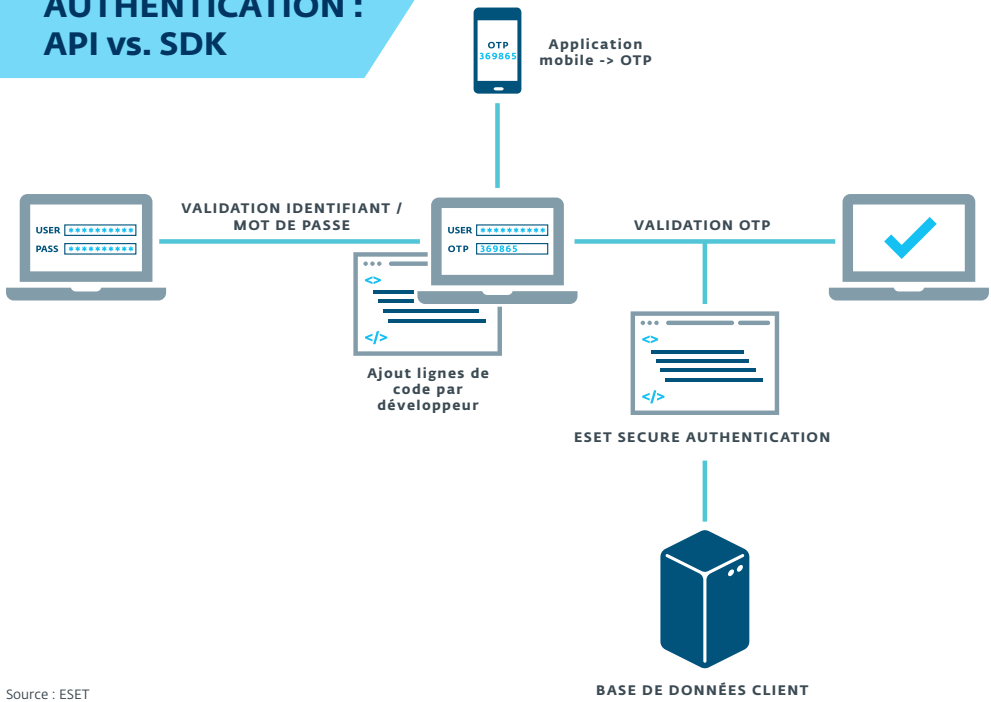
La sécurité informatique d'une société peut être mise à mal par les utilisateurs qui n'ont pas conscience de l'importance d'avoir des mots de passe différents pour chaque accès sécurisé. On remarque souvent le même schéma dans les entreprises, où les utilisateurs utilisent le même mot de passe pour un grand nombre de leur connexion. En général, ce mot de passe s'avère simple et court, d'où le risque important de voir sa sécurité informatique en défaut.

Que l'on soit fixe ou nomade, l'authentification à double facteur est la solution à adopter : une clé OTP (one time password) sur un poste de travail ou un téléphone mobile permet à l'utilisateur d'éviter de mémoriser plusieurs mots de passe.

Dans le cas du téléphone mobile, deux possibilités existent : soit l'appareil est un smartphone capable de stocker une application générant des mots de passe, soit il reçoit un SMS contenant un identifiant (Schéma 4).

De plus en plus de solutions d'authentification tentent de se passer du mot de passe personnel à mémoriser et toutes n'offrent pas la possibilité d'une double authentification. La solution d'ESET permet l'authentification à deux facteurs avec mot de passe à usage unique (2FA-OTP) lors de la connexion aux réseaux d'entreprise à travers le téléphone mobile des utilisateurs. Simple à mettre en œuvre, la solution ajoute une seconde couche de contrôle au processus d'authentification traditionnel composé de l'identifiant et du mot de passe. Selon les clients ESET, l'un des bénéfices de ce type d'approche est la simplicité d'utilisation et par voie de conséquence un gain de temps. Ce type d'authentification réduit les risques d'intrusion sur les messageries comme sur les réseaux privés. Afin d'optimiser la protection sur les infrastructures VPN, ce type d'approche séduit de plus en plus d'entreprises. Pour bon nombre de décideurs IT et Sécurité, il faut savoir s'affranchir de solutions packagées de certains éditeurs dont le métier est plus la gestion des infrastructures que la cyber-sécurité.

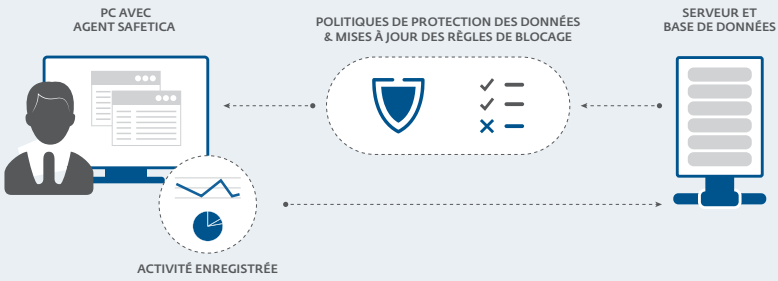
ESET SECURE AUTHENTICATION : API vs. SDK

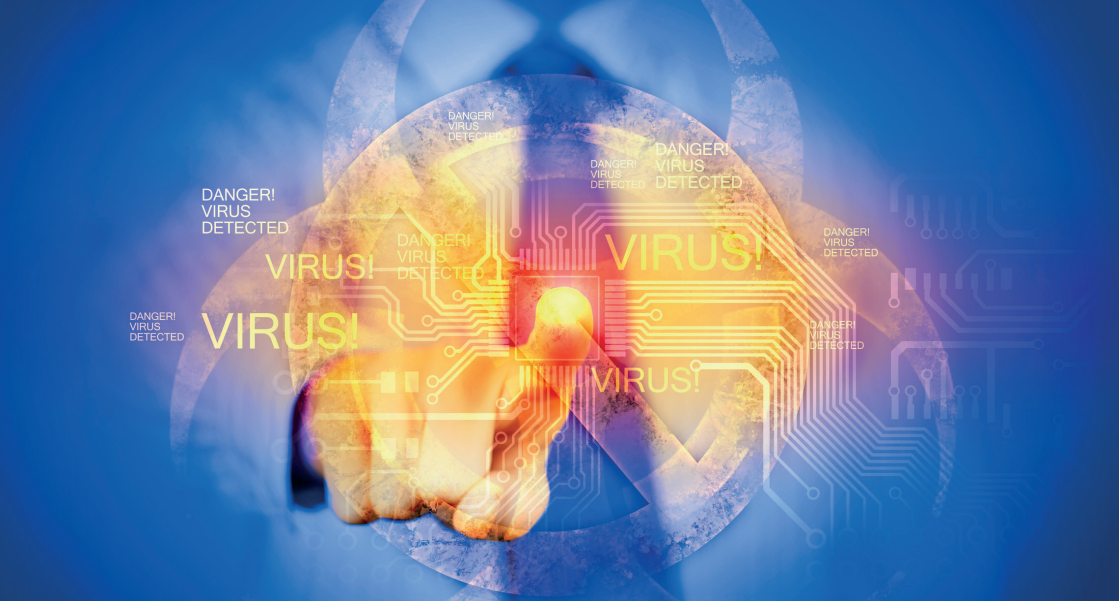


Source : ESET

DLP, une seconde génération de solutions simples et ergonomiques pour prévenir les fuites de données

Les données confidentielles doivent rester hébergées dans un bastion sécurisé, chiffrées avec un outil de confiance, et ne peuvent être consultables qu'à partir des appareils d'utilisateurs authentifiés. Ces informations critiques ou sensibles devront être suivies par des solutions de traçage de type DLP. Au-delà de leurs technologies, ces solutions doivent faire l'objet de services associés offerts par des prestataires de confiance. Éditeur Européen, ESET propose une solution et un accompagnement permettant d'atteindre simplement l'objectif fixé par la DLP.





Début juin 2016, Safetica (fournisseur reconnu de solutions de prévention dans la fuite de données) a rejoint la « Technology Alliance » d'ESET. Désormais, les clients ESET peuvent s'appuyer sur la suite Safetica DLP (Data Loss Prevention) pour identifier, tracer et réduire leurs fuites d'informations via certains indicateurs comme le comportement anormal d'un utilisateur. Selon Safetica, 63% des entreprises confrontées à un incident de sécurité estiment que d'anciens ou actuels employés en sont à l'origine. Safetica fournit une solution de prévention à part entière et propose également des rapports d'activité complets qui mettent en garde contre tout comportement suspect.

En 2015, l'enquête d'EY© portant sur la sécurité globale de l'information révèle que 56% des répondants définissent la prévention de perte de données comme une priorité haute et 33% comme une priorité moyenne pour leur entreprise au cours des 12 prochains mois. Via la solution de Safetica, ESET propose à toutes les entreprises un outil de prévention contre les fuites planifiées ou accidentelles de données, les actions malveillantes, les problèmes de productivité, les dangers BYOD etc...

En 2016, les cybermenaces se glissent davantage à différents endroits du système d'information ce qui nécessite d'avoir une protection multiple : protection du système de fichier, blocage de l'accès à la base du registre, filtrage des communications vers les serveurs C&C, protection des appareils mobiles et des applications partagées, des comportements des utilisateurs...

Une protection multiple doit être légère. ESET propose cette technologie principalement développée en assembleur et en langage C, ce qui est intéressant pour économiser les ressources CPU et la mémoire. Cette approche permet de descendre vers les couches les plus basses des OS sans en affecter les performances. Cette offre est systématiquement épaulée par les services support et les laboratoires d'ESET.

Les 10 recommandations du CESIN* face aux projets Cloud

01. Estimez la valeur des données que vous comptez externaliser ainsi que leur attractivité en termes de cybercriminalité

02. S'il s'agit de données sensibles voire stratégiques pour l'entreprise, faites valider par la direction générale le principe de leur externalisation

03. S'il s'agit de données sensibles voire stratégiques pour l'entreprise, faites valider par la direction générale le principe de leur externalisation

04. Adaptez vos exigences de sécurité dans le cahier des charges de votre appel d'offre en fonction du résultat du point 1

05. Effectuez une analyse de risque du projet en considérant les risques inhérents au cloud comme la localisation des données, les sujets de conformité et de maintien de la conformité, la ségrégation ou l'isolement des environnements et des données par rapport aux autres clients, la perte des données liée aux incidents fournisseur, l'usurpation d'identité démultipliée du fait d'une accessibilité des informations via le web, la malveillance ou erreur dans l'utilisation, etc. Sans oublier les risques plus directement liés à la production informatique : la réversibilité de la solution et la dépendance technologique au fournisseur, la perte de maîtrise du système d'information et enfin l'accessibilité et la disponibilité du service directement lié au lien Internet avec l'entreprise

06. Outre ces sujets, exigez un droit d'audit ou de test d'intrusion de la solution proposée

07. A la réception des offres, analysez les écarts entre les réponses et vos exigences

08. Négociez

09. Faites valider votre contrat par un juriste. Si vous êtes une entreprise française, ce contrat doit être rédigé en français et en droit français

10. Faites un audit ou un test d'intrusion avant démarrage du service (si cela est possible) et assurez-vous du maintien du niveau de sécurité de l'offre dans le temps

* CESIN : Club des experts de la sécurité de l'information et du numérique - www.cesin.fr

ENJOY SAFER TECHNOLOGY™

CONTACTEZ-NOUS

ESET France

Tel. + 33 (0)1 55 89 08 85

www.eset.com/fr

www.welivesecurity.com

Edition Août 2016