LIVRE BLANC

Olfeo
La sécurité positive

Sécurisez intégralement vos accès web

Cybermenaces et sécurité du SI : les 7 règles fondamentales à respecter pour protéger votre organisation

80%
DES ENTREPRISES ONT CONSTATÉ AU MOINS UNE CYBERATTAQUE EN 2018 (1)

AURIEZ-VOUS ENVIE DE METTRE TOUS VOS ŒUFS DANS LE MÊME PANIER POUR PROTÉGER VOTRE SYSTÈME D'INFORMATION ?

(1) SOURCE : Baromètre de la Cybersécurité des entreprises du CESIN (www.cesin.fr)

SOMMAIRE

Olfeo
La sécurité positive

UN PRÉALABLE : DOCUMENTER, SUPERVISER ET AUDITER L'INFRASTRUCTURE

Pour se protéger efficacement contre les cybermenaces, **il est fondamental de bien connaître et de maîtriser son système d'information**.

La plupart des organisations maintiennent à jour des schémas d'architecture permettant de visualiser les différents réseaux, les ressources informatiques et la position des équipements de sécurité. Mais est-ce que cela permet de savoir pour autant ce qui est vraiment utilisé et ce qui l'est moins ? Est-ce que ces cartographies affichées aux murs de la DSI permettent de savoir où sont stockées précisément les données les plus sensibles et quelles seraient les failles que les cybercriminels pourraient exploiter ?

1

La supervision et l'analyse des logs doivent favoriser une meilleure prévention

Grâce aux fonctions de supervision des passerelles de sécurité web, il est possible de mieux analyser les différents flux réseau et donc les comportements des différentes ressources humaines et informatiques. Quels sont les domaines sollicités ? Quels sont les flux réseau réguliers facilement identifiables que des malwares pourraient chercher à détourner ? Où se situent les tentatives d'intrusion et/ou de connexion en échec ? Etc.

Ces informations permettent de mieux identifier d'éventuelles faiblesses dans l'architecture et de « rationaliser » le fonctionnement des différentes ressources composant le système d'information. Que l'on parle de « Shadow IT » ou de l'augmentation des applications métiers utilisées sans qu'elles aient été validées au préalable par la DSI, les flux réseau doivent absolument rester maîtrisés et donc filtrés. Par exemple, si certains composants sont susceptibles de ne pas être à jour alors qu'une faille vient d'être découverte, ils doivent pouvoir être isolés et désactivés rapidement. Pour autant, toutes les organisations n'ont pas encore de « stores » centralisés vérifiant les mises à jour et les diffusant de manière automatisée. Il est donc important d'avoir identifié au préalable ces ressources ou applicatifs à risque et de pouvoir les bloquer le cas échéant.

2

Pour ensuite adopter une démarche d'amélioration continue

En complément de la cartographie et de l'apport des outils de supervision, les services informatiques se sont depuis toujours organisés pour **disposer d'un référentiel exhaustif de leurs ressources (matériels, licences, etc.) anticipant les fins de maintenance de logiciels et/ou fins de durées de vie de certains matériels**. Elles intègrent ainsi dans le schéma directeur d'évolution du système d'information les changements et mises à jour nécessaires.

Si cet inventaire et l'anticipation des upgrades sont indispensables, **les DSI doivent désormais les compléter par une véritable démarche d'amélioration continue questionnant la pertinence des dispositifs de sécurité face à la sophistication croissante des cybermenaces et les changements de comportements**. L'efficacité des outils de protection d'hier ne sera peut-être plus la même quand on sait que 90% du trafic internet sera chiffré en HTTPS en 2020[2], que les objets connectés (IoT) souvent développés en open-source se généralisent sans qu'une dimension « security by design » soit garantie, que les hackers élaborent des algorithmes d'intelligence artificielle pour améliorer l'efficacité de leurs techniques de phishing et que leurs « wipers » sont de plus en plus destructeurs.

3

Et enfin auditer régulièrement le système d'information pour maintenir à jour la procédure de réaction à un incident

Mettre à jour et documenter l'architecture du système d'information est essentiel et il faut également intégrer une procédure claire à suivre en cas d'incident de sécurité, tant pour les équipes de la DSI que pour l'utilisateur final. Sur ce point, **l'enjeu se situe au niveau de la rapidité de la réponse : dès qu'un comportement suspect est détecté, les réactions doivent s'enchaîner immédiatement**.

La procédure de réaction doit par exemple prévoir clairement la déconnexion progressive des différentes zones réseaux à risque afin de les compartimenter et ainsi contenir l'éventuelle menace. **Pour parfaire la pertinence de cette procédure, l'audit régulier du système d'information voire la réalisation de tests d'intrusion préventifs sont particulièrement indiqués**. Ils peuvent par exemple prendre la forme de fausses campagnes de phishing auprès des utilisateurs pour identifier les comportements à risque et les sensibiliser davantage ou de mener des tests d'intrusion voire de détournement d'applicatifs métiers utilisés en interne mais non installés par la DSI.

(2) SOURCE : CA Security Council (CASC) 2019 Predictions: The Good, the Bad, and the Ugly

RÈGLE 1

SEGMENTER
LES DIFFÉRENTS RÉSEAUX : POSTES UTILISATEURS MAÎTRISÉS, INVITÉS, OBJETS SUR IP, SERVEURS...

La première règle de base bien connue pour protéger efficacement le réseau informatique de l'organisation est de le scinder en plusieurs zones différentes afin de pouvoir répartir les risques. En effet, ces zones seront interconnectées par des équipements de sécurité qui permettront de les cloisonner immédiatement dans le cas d'une attaque.

Leur création doit privilégier l'homogénéité des usages et des niveaux de sécurité attendus :

- Aucun équipement local ne doit accéder directement à internet, il doit impérativement passer par le serveur mandataire (le Proxy),
- Les postes non maîtrisés voulant accéder à internet doivent être redirigés vers un réseau à part, ne leur donnant pas accès au réseau local,
- Les réseaux doivent être segmentés selon la nature des différents serveurs : administration, infrastructures techniques, applicatifs métiers...
- Les postes de travail et/ou serveurs servant à l'administration doivent être sur un réseau totalement à part qui peut éventuellement être déconnecté d'internet ou utiliser une instance dédiée de la passerelle de sécurité web,
- Etc.

En complément de cette segmentation des différentes parties du réseau, **il faut compléter le filtrage d'IP des Firewalls par un filtrage sur l'ensemble des équipements faisant des requêtes vers internet (imprimantes, IoT, etc.).**

Le filtrage DNS est dans ce cas particulièrement indiqué puisqu'il permet de bloquer en amont tout appel d'un serveur et/ou domaine internet qui ne serait pas dans la liste préalablement autorisée. Cela suppose néanmoins d'avoir une base d'URL très riche, maintenue à jour régulièrement pour bénéficier d'un taux de reconnaissance du web élevé et ne pas bloquer les flux de manière abusive. **Le filtrage DNS est intéressant puisqu'il répond précisément à l'enjeu d'instantanéité de la cybersécurité.**

RÈGLE 2

SÉCURISER
LES ACCÈS END POINT

La deuxième règle également bien connue est de sécuriser les accès End Point puisque les utilisateurs finaux sont de plus en plus exposés aux malwares et tentatives de cyberattaques alors que leur maîtrise des bonnes pratiques de sécurité informatique est pour le moins variable.

Sécuriser les accès End Point prend différentes formes :

- Systématiser l'installation et la configuration d'anti-virus de postes en automatisant leur mise à jour,
- Contrôler l'ajout d'applications et d'extensions des navigateurs web sur les postes maîtrisés à ceux préalablement validés par la DSI,
- Restreindre les droits d'administration des postes de travail,
- Automatiser les sauvegardes des données des postes de travail,
- Etc.

Pour faciliter toutes ces opérations, **il est essentiel de centraliser la gestion des équipements informatiques afin d'homogénéiser les politiques de sécurité sur l'ensemble du parc informatique**. Si l'anti-virus de poste est indispensable, il n'est plus suffisant et tous les dispositifs doivent être pilotés de manière centralisée si l'on veut avoir une administration commune et homogène.

On peut ainsi recourir à un service d'annuaire, de CMDB (*Configuration Management Data Base*) voire de MDM (*Mobile Device Management*) mais il faut surtout prendre conscience que ce sont **les politiques de filtrage des flux internet qui sont aujourd'hui le 1er rempart face à la sophistication croissante des malwares** et qu'elles doivent être gérées de manière centralisée en priorité.

Autre exemple, même si les serveurs de messagerie sont aujourd'hui équipés d'anti-spams intégrant de plus en plus des anti-virus scannant les pièces jointes avant leur diffusion interne, c'est bien l'ouverture d'une pièce-jointe appelant une URL pouvant exécuter un code malveillant qui constitue une des menaces les plus courantes. **Tout l'enjeu pour que la sécurisation des accès End Point soit maximale réside donc aujourd'hui dans la qualité du filtrage internet.**

RÈGLE 3

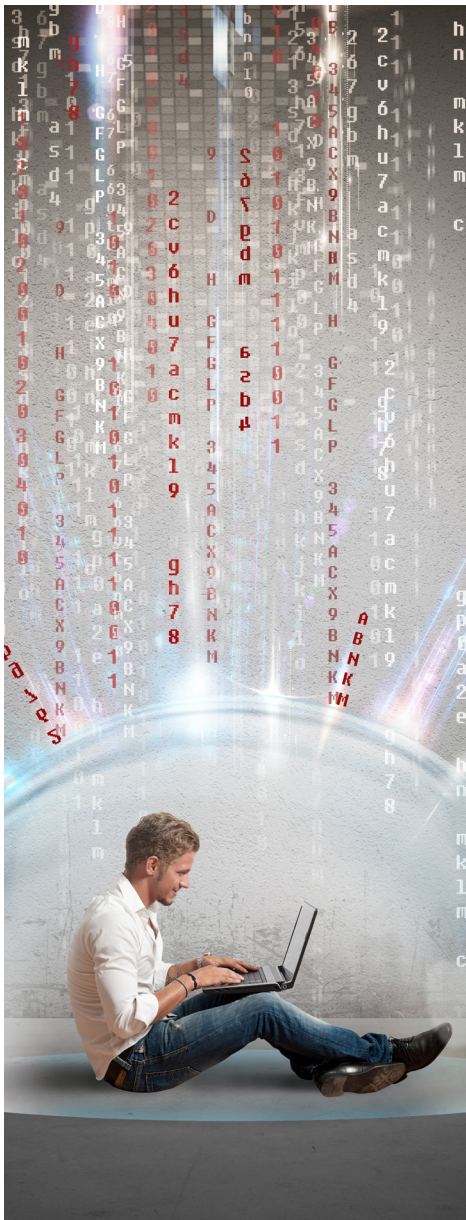
BIEN RÉPARTIR
LES RÔLES ENTRE LE FIREWALL ET LE PROXY

Le Firewall est le premier équipement de sécurité indispensable pour protéger le réseau informatique d'une organisation, c'est pourquoi il n'est plus possible de continuer à lui ajouter systématiquement de nouveaux traitements à supporter : déchiffrement des flux HTTPS, anti-virus web, filtrage internet, etc.

Face à la recrudescence des attaques, **la bonne pratique en matière de protection du système d'information a toujours été de répartir les services de cybersécurité sur plusieurs équipements distincts afin de constituer une chaîne de sécurité web complète**. Il est donc vivement conseillé d'ajouter un Proxy autonome en complément du Firewall qui va venir renforcer son efficacité et lui permettre de se concentrer pleinement sur ses prérogatives d'autorisation d'entrées/sorties des flux réseau, internes ou externes, ouverts (internet) ou protégés (VPN), et ne plus tomber dans l'erreur de tout lui faire supporter. Le Proxy assurera quant à lui sa mission complémentaire de contrôle, d'optimisation et de filtrage des flux web de l'organisation.

En matière de cybersécurité, il est donc vital de ne plus « mettre tous ses œufs dans le même panier ».

Si l'on prend l'exemple du déchiffrement HTTPS, 90% des flux web seront chiffrés d'ici 2020 et si cela repose sur la fonction Firewall de l'UTM, cela consommera énormément de ressources et dégradera inévitablement ses performances (une étude NSS Labs a mis en évidence que cette dégradation pouvait représenter jusqu'à 74%[3]). Or, **un point-clé sur lequel la DSI ne peut déroger en matière de cybersécurité c'est bien la haute-disponibilité tout comme l'évolutivité des équipements utilisés**. Quand on sait que l'utilisation de la bande passante augmente de 10 à 20% chaque année[3] et que les attaques DDOS destinées à faire tomber le Firewall sont de plus en plus fréquentes, ces opérations doivent absolument être confiées au Proxy autonome qui pourra plus facilement être virtualisé et ainsi augmenter ses capacités de traitement si cela était nécessaire.



(3) SOURCE : NSS Labs, John W. Pirc, Significant SSL performance loss leaves much room for improvement

RÈGLE 4

FAIRE LES BONS CHOIX
EN MATIÈRE DE FILTRAGE

L'enjeu de filtrage prend aujourd'hui de plus en plus d'ampleur comme nous l'avons vu dans les trois règles précédentes. **Filtrer l'intégralité du trafic réseau pour bloquer les accès vers des sites malveillants est un des principaux facteurs clés dans la protection du système d'information.**

Toute connexion vers internet, qu'elle provienne d'un poste de travail ou autre, doit donc transiter par le Proxy qui sera en charge de réaliser les opérations de filtrage et de déchiffrement HTTPS qui pose quant à lui des questions de conformité légale et de confidentialité des données personnelles déchiffrées.

Sur ce point, **rappelons d'abord que disposer de logs nominatifs sur l'utilisation d'internet par les utilisateurs est une obligation légale**. Le Proxy autonome permet de gérer et de maîtriser des politiques et catégories de filtrage d'une grande finesse par utilisateur ou groupes d'utilisateurs. Il est donc préférable qu'il soit à la fois en charge de l'identification de l'utilisateur et du filtrage de son trafic internet.

La qualité de la base qui sera utilisée et sa conformité légale et culturelle au contexte français sont également déterminants. La granularité du filtrage, la reconnaissance de sous-domaines interdits, les catégories de filtrage conformes au cadre législatif local assurent à la DSI une protection juridique maximale. Rappelons à ce propos que la responsabilité civile et pénale de l'ensemble des acteurs de l'entreprise peut être engagée en cas d'accès par des collaborateurs à des sites illicites au regard du droit français.

Il restera enfin à choisir entre liste noire (blocage de sites malveillants déjà connus) et liste blanche (blocage des sites inconnus le temps qu'ils soient classifiés). Pour cela, le taux de reconnaissance du web dans la base de données d'URL sera déterminant pour permettre un fonctionnement en liste blanche, considéré comme le niveau « suprême » de sécurité web, mais exigeant qu'un minimum de 98% des sites internet visités par vos utilisateurs soient reconnus pour garantir un confort d'utilisation optimal.

RÈGLE 5

SÉCURISER LES NOUVEAUX USAGES NOMADES

Les politiques de sécurité du système d'information sont souvent plus compliquées à appliquer en situation de mobilité où la DSI ne peut maîtriser tous les équipements utilisés. **Or, le nomadisme ne cesse d'augmenter** : télétravail, déplacements professionnels, etc. Il est donc important d'améliorer la sécurité des postes de travail en situation de nomadisme car si les protections End Point comme l'anti-virus restent indispensables, elles ne suffisent plus pour bénéficier du même niveau de sécurité réseau.

La première réponse est de recourir à une connexion VPN qui peut prendre différentes formes :

- **Le Full VPN** : le poste de travail nomade se connecte au réseau de l'organisation, il bénéficie alors des mêmes niveaux de protection mais ne peut plus accéder à des ressources locales, comme une imprimante par exemple.
- **Le Split VPN** : ce mode hybride permet d'accéder à deux réseaux en même temps (le réseau local de la personne en situation de mobilité et celui de l'organisation) mais il est moins sécurisé et certainement moins apprécié des DSI.

Ensuite, **si l'on veut reproduire les mêmes règles et niveaux de sécurité que l'on soit sur le réseau local ou en situation de mobilité, il convient d'ajouter des agents nomades**. Pour cela, il faut piloter de manière centralisée tous les équipements informatiques afin de pouvoir distribuer automatiquement des politiques de sécurité dédiées.

L'agent nomade installé sur le poste de travail en situation de mobilité se connectera soit au serveur Proxy de l'organisation soit vers un serveur mandataire déporté qui permettra d'assurer la continuité du service de filtrage en dehors de l'entreprise. La richesse de la base de données et les fonctions de déchiffrement HTTPS apporteront ainsi les mêmes garanties que le poste soit connecté au réseau local ou à un réseau externe quel qu'il soit.

RÈGLE 6

MAÎTRISER
LA GESTION DES IDENTITÉS ET DES DROITS D'ACCÈS

La vie du système d'information est ponctuée des arrivées et départs des collaborateurs, qui bénéficient de droits d'accès selon la nature de leurs missions. En revanche, il n'est pas rare de constater qu'un collaborateur ayant changé de fonction bénéficie encore des droits d'accès liés à son poste précédent, ou que le compte d'un collaborateur ayant quitté l'entreprise reste ouvert quelques semaines après son départ.

Cela représente un risque majeur pour les organisations quand on sait que les cybercriminels cherchent d'abord à récupérer des codes d'authentification et des données personnelles sur les utilisateurs pour s'en servir à des fins d'intrusion, physique et/ou numérique.

Il est donc essentiel de maîtriser parfaitement la gestion des identités et des accès :

- Constituer un référentiel exhaustif pour identifier individuellement toutes les personnes (internes et externes) connectées au système d'information et les droits d'accès dont elles bénéficient et le maintenir à jour continuellement,
- Définir puis automatiser des procédures claires gérant les arrivées, les changements de postes et les départs des collaborateurs (par exemple, le compte d'un utilisateur quittant l'entreprise est automatiquement désactivé et archivé le jour de son départ puis supprimé après une certaine période),
- Vérifier que les droits d'accès aux « zones sensibles » du système d'information soient régulièrement audités pour éviter qu'un utilisateur ne conserve un accès s'il n'est pas réellement indispensable à l'exercice de ses fonctions,
- Superviser et filtrer de manière continue les flux réseau des comptes dits « à privilège ».

Il y a trop souvent des « passe-droits » dans les organisations qui perdurent au-delà du raisonnable. **Tracer, contenir et maintenir les droits de tous les utilisateurs du système d'information est primordial mais il faut pour cela être en mesure d'authentifier chaque personne derrière tous les flux et ne pas se contenter de l'identification de l'IP.**

RÈGLE 7

RÉPONDRE
AU NOUVEL ENJEU D'INTERACTION EN TEMPS RÉEL AVEC LES UTILISATEURS

Comme nous le disions, l'enjeu en matière de cybersécurité se situe dans l'instantanéité de la réponse. Or, les utilisateurs finaux sont de plus en plus la cible des cybercriminels qui comptent sur leur inattention ou leur méconnaissance des risques informatiques pour arriver à leurs fins. L'ingénierie sociale des cybermenaces, notamment à travers les techniques de phishing, s'est généralisée et professionnalisée ces dernières années.

La dernière règle fondamentale pour protéger le système d'information est donc d**'inclure l'utilisateur final comme un maillon essentiel de la chaîne de sécurité web**. Pour cela, il faut les sensibiliser aux bonnes pratiques de sécurité informatique mais plutôt qu'une formation ponctuelle dont ils ne retiendraient pas tout, **c'est plutôt en temps réel que cette pédagogie doit désormais être délivrée**.

Le problème n'est plus entre la chaise et le clavier : les messages anxiogènes sont mal perçus par les utilisateurs finaux et ne fonctionnent pas. **Pour créer une culture de la sécurité positive, il est indispensable de valoriser l'utilisateur et d'interagir avec lui de manière qualitative** en lui diffusant des messages pertinents et adaptés au contexte de ses usages. Pour cela, **le Proxy qui filtre un flux internet vers un site non autorisé peut devenir un véritable outil de dialogue en temps réel en affichant une page de blocage contenant des messages ou des vidéos de sensibilisation personnalisés et explicites** afin que l'utilisateur comprenne la nature du risque auquel il expose l'organisation. Olfeo enrichit cette démarche en proposant une solution de formation à la sécurité des collaborateurs à travers l'accès à des parcours de vidéos pédagogiques et saynètes avec **quizz pour tester les connaissances et le passage de certification**.

L'accélération de la transformation digitale et la sophistication croissante des malwares vont augmenter l'exposition des utilisateurs finaux aux cybercriminels dans les années à venir. **Il est donc essentiel que le modèle OSI (*Open Systems Interconnection*) des organisations intègre une nouvelle couche liée au facteur humain afin de sensibiliser et responsabiliser chaque personne en temps réel.**

OLFEO,
LA PASSERELLE DE SÉCURITÉ WEB DISRUPTIVE
BASÉE SUR UNE VISION À 360°.

Olfeo est leader français de la sécurité web.

Nous accompagnons depuis **plus de 16 ans** les **entreprises exigeantes** dans la sécurisation de leur flux web. Grâce à notre **connaissance** extrêmement fine des **besoins des organisations françaises**, nous avons développé une passerelle de sécurité web disruptive, basée sur une **vision globale**, et **pas uniquement technologique**.

Notre passerelle de sécurité web, basée sur une infrastructure Proxy inclut les fonctions suivantes :

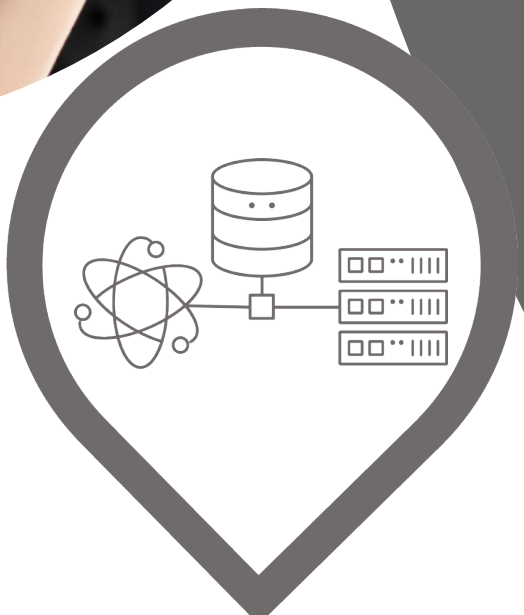
- Filtrage web
- Proxy avancé & déchiffrement HTTPS
- Antivirus web
- Filtrage DNS
- Nomadisme
- Campus
- Portail Public
- Filtrage protocolaire

Sensibilisez l'utilisateur final au sein de la solution Olfeo, avec :

- Le coaching, et l'envoi de rapports personnalisés à chaque collaborateur
- La diffusion de la charte informatique auprès de vos équipes
- L'affichage de messages de sensibilisation contextuels lors de navigation web
- Une expérience utilisateur fluide, à juste mesure
- L'envoi de mails contenant des vidéos pédagogiques sur la sécurité

Pour en savoir plus, téléchargez nos cas d'usages et avis d'experts Cybersécurité

TÉLÉCHARGER



Olfeo

CONTACTEZ-NOUS

- 4 rue de Ventadour
  75001 Paris
  +33(0) 969 390 999

contact@olfeo.com

www.olfeo.com