SOPHOS

# Liste des technologies, outils et tactiques pour une protection efficace du Web

Une stratégie de protection du Web efficace exige la mise en place de politiques pour réduire la surface d'attaque, d'outils et de technologies appropriés pour appliquer ces politiques et d'une protection pour bloquer les attaques à chaque niveau.

Nous vous invitons à créer les différentes politiques suivantes, basées sur les meilleures pratiques en la matière, et à expliquer à vos utilisateurs pourquoi elles sont importantes pour la sécurité de votre organisation.

## Liste des politiques à mettre en place pour une protection du Web efficace

### ☐ Navigation sécurisée

Bloquez les catégories indésirables et inappropriées pour réduire la surface d'attaque des menaces. Votre politique doit exclure au minimum les catégories suivantes :

- Adulte,Sexuellement explicite, nudité
- Proxies anonymes
- Activités criminelles, piratage
- Sites de jeux
- Drogues illégales, alcool et tabac
- Intolérance et haine
- Phishing, fraude, spam, spywares
- Mauvais goût et offensant
- Violence et armes

Vous pouvez contrôler d'autres catégories afin de préserver la productivité ou la bande passante.

### ☐ Mots de passe solides

Vous devriez appliquer des politiques pour créer des mots de passe efficaces, en suivant notamment ces conseils :

- Créez des mots de passe longs.
- Utilisez des chiffres, des symboles et des caractères avec minuscules et majuscules.
- N'utilisez pas de termes courants du dictionnaire.
- N'utilisez pas d'informations personnelles telles que votre nom de famille ou votre date de naissance
- Changez fréquemment vos mot de passe.
- Ne gardez pas de trace écrite de vos mots de passe.

### ☐ Contrôle des applications

Limitez au maximum le nombre de navigateurs Internet, d'applications et de plugins utilisés, en standardisant leur utilisation dans toute votre entreprise.

- Navigateur : Contentez-vous d'un seul navigateur prenant en charge l'API Safer Browsing de Google, tel que Google Chrome, Firefox, ou Apple Safari.
- Java : A moins que vous n'ayez besoin de Java pour des applications Web nécessaires à l'entreprise, désactivez-le, supprimez-le, ou limitez-le uniquement aux utilisateurs qui en ont besoin.
- Lecture PDF : Encore une fois, utilisez un logiciel de lecture PDF parmi les plus utilisés et maintenez les correctifs à jour.
- Lecteur média : Évitez les packs codecs et les modules "add-on" inutiles pour les lecteurs média. Si possible, tenez-vous en aux composants dont dispose déjà votre système d'exploitation et maintenez les correctifs à jour.
- Plug-ins, modules "add-on" et barres d'outils : Évitez les plug-ins et les barres d'outils inutiles.

### ☐ Gestion des correctifs

Assurez-vous que les applications suivantes disposent autant que possible de mises à jour automatiques et que les utilisateurs appliquent activement les mises à jour ou les correctifs au fur et mesure qu'ils sont disponibles.

- Navigateur Web
- Java
- Lecteur PDF
- Lecteur Flash

Pour appliquer vos politiques et garantir une protection contre les attaques Web les plus récentes, vous avez besoin des technologies et des outils suivants :

## Liste des outils et des technologies Web à vérifier

### ☐ Filtrage des URL

Pour appliquer votre politique sur la navigation sécurisée du Web, vous avez besoin d'un outil de filtrage des URL efficace. Recherchez une solution qui ne vous submerge pas de centaines de catégories, avec des exceptions de politiques simples. Votre solution doit permettre aux utilisateurs de soumettre facilement des requêtes à votre équipe informatique et de pouvoir les gérer en quelques clics.

### ☐ Filtrage des sites malveillants

Pour une protection contre les sites malveillants, assurez-vous d'avoir un filtrage sur réputation efficace. Optez pour une solution qui soit mise à jour en temps réel par le fournisseur grâce à des centres mondiaux d'analyse des menaces qui traquent en permanence les sites nouvellement infectés.

### ☐ Blocage des proxies anonymes

Surveillez les utilisateurs distants avec une technologie capable de bloquer les abus de proxies anonymes destinés à contourner le filtrage des URL. Choisissez une solution qui inclut à la fois le blocage des proxies anonymes et leur détection dynamique en temps réel afin de bloquer tous les proxies nouveaux, obscurs ou faits maison.

### ☐ Filtrage du spam

Assurez-vous que votre solution antispam utilise la dernière technologie pour bloquer les emails indésirables et inappropriés contenant des attaques de phishing et des liens malveillants - l'un des principaux points d'entrée des attaques modernes.

### ☐ Contrôle avancé des malwares sur le Web

L'ensemble de votre trafic Web doit être contrôlé par la technologie antimalware la plus avancée. Recherchez une solution capable de scanner tout le trafic (pas seulement les sites dangereux) sans impacter la latence ou les performances. Assurez-vous que votre solution utilise les toutes dernières technologies telles telle que l'émulation JavaScript pour détecter les menaces

### ☐ Contrôle HTTPS

Vous devez couvrir l'une des failles majeures dans votre protection Web à l'aide d'une solution qui analyse le trafic chiffré. Assurez-vous que la solution n'impacte pas les performances et que vous préservez la confidentialité de vos utilisateurs lorsqu'ils consultent des sites bancaires ou financiers.

### ☐ Détection « call home »

Dans le cas d'une infection, assurez-vous que votre solution puisse identifier les ordinateurs infectés sur le réseau par leurs requêtes d'URL connues de malwares.

### ☐ Protection hors site

Protégez les utilisateurs hors du réseau de l'entreprise en utilisant une solution qui offre une protection Web Endpoint ou un filtrage basé dans le Cloud. La protection du Web peut être intégrée à votre agent antivirus, réduisant ainsi les logiciels clients que vous avez besoin d'administrer et offrant une protection du Web sans backhauling, avec option de redirection pour un contrôle dans le Cloud. Recherchez une solution qui vous permette de gérer vos utilisateurs hors site avec la même console que vos utilisateurs sur le réseau.

### ☐ Mises à jour en temps réel

Assurez-vous que vos systèmes offrent des mises à jour live sans aucun délai. Des mises à jour toutes les heures ou tous les jours ne suffisent plus.

### ☐ Contrôle des applications

Appliquez vos politiques pour applications Web avec les bons outils pour empêcher les applications indésirables de s'installer ou d'être exécutées sur les systèmes d'extrémité. Bien que le filtrage au niveau des applications de la passerelle réseau puisse être utile pour la productivité et le contrôle de la bande passante, il est important d'appliquer le contrôle des applications au niveau des systèmes d'extrémité.

### ☐ Évaluation des correctifs

Simplifiez votre stratégie des correctifs avec une solution capable d'identifier et de classer par priorité les correctifs de sécurité pour votre logiciel client Web.

### ☐ Antivirus avec HIPS

Choisissez un agent antivirus pour systèmes d'extrémité avec système de prévention des intrusions sur l'hôte (HIPS) intégré. Recherchez une solution qui intègre les meilleures règles HIPS en la matière au lieu de vous efforcer de trouver tout seul les paramètres de protection contre les menaces les plus efficaces.

## Sophos Web Protection

Outre cette liste de technologies importantes, assurez-vous que vous êtes appuyé par un fournisseur en sécurité informatique qui s'engage à vous fournir la meilleure protection. Recherchez un éditeur disposant de centres d'analyse des menaces qui surveillent en permanence le web à la recherche des menaces les plus récentes et qui offrent des mises à jour instantanées aux menaces émergentes.

Enfin, en plus de garantir une protection efficace, choisissez une solution qui soit simple à déployer et à administrer. N'oublions pas qu'une sécurité simple est une meilleure sécurité.

Les cinq étapes d'une attaque de malware Web
Téléchargez maintenant

## Demandez un essai gratuit sur sophos.fr

Sophos Secure Web Gateway
Sophos EndUser Web Protection Suite

Équipe commerciale France :
Tél. : +33 (0)1 34 34 80 00
Courriel : info@sophos.fr



NP 10/13 NSG fr

SOPHOS