

Fiche à l'attention des **responsables de la sécurité des systèmes d'information**

## Sécuriser son environnement Windows

- Utiliser des **GPO** (Group Policy Object) pour **centraliser la gestion** des machines et des utilisateurs dans un environnement Active Directory
- **Appliquer** dans les meilleurs délais **les mises à jour Windows** sur les serveurs et les postes de travail (**Windows Server Update Services (WSUS)**) ainsi que pour les **logiciels tiers** (navigateurs, lecteurs multimédias [pdf, video, zip, ...], ...)
- Tenir à jour l'**antivirus** (différent de celui de la messagerie de préférence) ainsi que les bases de signatures
- Ne pas accorder les **droits d'administration locaux** à l'utilisateur du poste (si besoin, faire un compte séparé accessible par 'exécuter en tant que'). Un compte admin ne doit pas être utilisé pour naviguer sur Internet.

### Activer/Installer

- L'option<sup>1</sup> pour rendre visible les **extensions réelles** afin d'éviter les fichiers comme «Dernier\_film\_cinema.avi.exe» par exemple
- **Windows defender ASR pour bloquer l'exécution de fichiers** (Windows 10 > 1709 - règles de réduction de surface d'attaque)
- Une **politique de restriction d'exécution** type **applocker**<sup>2</sup> ou équivalent<sup>3</sup> (interdire l'exécution dans le répertoire utilisateur (c:\user) par exemple)
- **SYSMON**<sup>4</sup> pour **surveiller** et enregistrer des événements systèmes

### Sur le serveur de fichier

- FSRM pour contrôler les extensions de fichiers autorisées pour le stockage sur les partages de fichier type DFS.
- Le partage de fichiers en lecture seule

### Désactiver

- L'utilisation du protocole de partage de ressources **SMBv1** (Commande powershell: Set-SmbServerConfiguration -EnableSMB1Protocol \$false ), canal privilégié de propagation des maliciels
- Le service partage administratif (HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareWks=0), répertoires réseau partagés par défaut
- L'accès à Winrm ou Powershell à distance
- L'accès à distance à des comptes locaux
- Le stockage des mots de passe en clair
- L'ouverture automatique des objets à risque depuis l'explorateur 9 : ".ps1", ".hta", ".js", ".JSE", ".WSH", ".WSF", ".scf", ".scr", ".vbs", ".vbe" et ".pif
- Flash et Java si non nécessaires (voire désinstallation). Si Flash et Java sont nécessaires en interne alors il est possible d'avoir deux navigateurs (un interne avec java/flash et un externe sans).

## Office

Désactiver :

- **Macro**<sup>5</sup>
- **OLE object**<sup>6</sup>, protocole et système d'objets distribués permettant à des applications utilisant des formats différents de dialoguer
- **Object ActiveX** (Registre: DisableAllActiveX = 1), une des technologies du Component Object Model de Microsoft utilisées en programmation pour permettre le dialogue entre programmes
- **DDE et liens Excel** (Registre: AllowDDE = 0 & WorkbookLinkWarnings = 2 & DontUpdateLinks = 1)

## Adobe pdf

- Désactiver **Javascript** (Registre: bEnableJS = 0) ; les **fichiers intégrés** (Registre: bAllowOpenFile = 0 & bSecureOpenFile = 1)
- Activer la **protection** (Registre: bProtectedMode = 1 & iProtectedView = 1 & bEnhancedSecurityInBrowser = 1)

## Active Directory

### Accès à distance

- Activer le **mode restrictedAdmin** pour empêcher le stockage du hash en cas d'accès à distance<sup>7</sup>
- Utiliser les **comptes d'administration des contrôleurs de domaine** uniquement pour se connecter sur les contrôleurs de domaine
- **Auditer** régulièrement les comptes de service

### Comptes administrateurs locaux :

- Utiliser **LAPS** pour gérer automatiquement le mot de passe du compte « Administrateur » local de toutes les machines de votre domaine
- Mettre en place des mécanismes de **restriction d'authentification distante des comptes locaux** (en utilisant une GPO ainsi que le pare-feu local et l'UAC) pour filtrer les jetons d'accès privilégiés des comptes administrateurs locaux.

### Scripts de GPO :

- Ne pas stocker de mot de passe dans les scripts et privilégier l'authentification **Kerberos**, l'utilisation d'un compte de service, etc.

## Windows Attack Surface Reduction (ASR)<sup>8</sup>

*Objectif : mettre en place des règles concernant le comportement des fichiers. (uniquement sur Windows 10 et Windows server 2019.*

- Bloquer les **appels d'API Win32** à partir des macros Office
- Empêcher l'exécution des **fichiers exécutables** à moins qu'ils ne répondent à un critère de prévalence, d'âge ou de liste de confiance
- Bloquer les créations de processus provenant des commandes **PSEXEC** et **WMI** (permettant exécution de code à distance)
- Bloquer l'exécution de **scripts potentiellement obscurcis** et empêcher JavaScript ou VBScript de lancer le contenu exécutable téléchargé.

Les auteurs de logiciels malveillants utilisent l'obfuscation pour rendre le code malveillant plus difficile à lire, ce qui empêche un examen minutieux par les humains et les logiciels de sécurité.

- Empêcher toutes les applications Office (Word, Excel, PowerPoint, OneNote, Access, etc.) de créer des processus enfants, de créer du contenu exécutable, d'injecter du code dans d'autres processus.

## Réduction de l'exposition sur Internet et cloisonnement du réseau

- Mettre en place une **politique** stricte concernant les **accès à distance** (RDP et VPN), porte d'entrée privilégiée des attaquants
  - mettre en place un **VPN** pour la maintenance et le télétravail avec double authentification, filtrage GEOIP FR, limitation des comptes, et journalisation ;
- **Limiter l'exposition sur Internet au strict nécessaire** pour réduire le risque d'intrusion:
  - services à jour, filtrage fins, journalisation, utilisation de reverse proxy, de pare feu spécifiques aux services, aucun compte par défaut, limitation de la fuite d'informations techniques ...
- **Cloisonner** le système d'information avec des **firewalls** et/ou **ACL** (filtrage entre les différentes parties réduit au strict nécessaire) :
  - **poste** de travail: accès internet filtré (proxy web), pas de résolution DNS externe directe (gérée par le proxy web)
  - **imprimantes**: pas d'accès à internet
  - **serveur** (VM): pas d'accès à internet (sauf liste blanche, par exemple WSUS, dépôt linux interne, ...), pas de résolution DNS externe
  - **hyperviseur**: pas d'accès à internet, pas de résolution DNS externe
  - **Gisements de données** (bases de données, ...)
  - Serveurs physiques dédiés au stockage des **sauvegardes** ;
  - **VLAN administrateur**<sup>6</sup>
- **Protéger les interconnexions du réseau** avec internet :
  - **DMZ entrée** (services exposés sur internet): webmail + MX, VPN, partenaires, ...
  - **DMZ sortie** (vers internet): proxy web, résolveur DNS externe, smtp sortant...

Faire une **sensibilisation** à la prévention des attaques avec le kit mis à disposition par [cybermalveillance.gouv.fr](http://cybermalveillance.gouv.fr)

## Proxy web sortant

- Limiter les **ports de sortie** (443,80,21) et activer la **vérification des protocoles** : 80 uniquement pour HTTP, 443 pour TLS (interdire les tunnels qui n'utilisent pas TLS/SSL), 21 pour FTP
- Interdire les accès aux **catégories à risque** si votre proxy le permet, par exemple "remote access tool [RAT]"
- Mettre en place des **listes noires** : phishtank, urlhaus, <sup>17</sup> ...
- Interdire l'**accès par IP en direct** (sauf liste blanche)
- Interdire l'accès aux URL/IP malveillantes couramment utilisées dans le cadre d'attaques connues
- Interdire le **téléchargement de fichiers à risque** selon extension et mime-type (uniquement pour HTTP)
- Interdire le téléchargement de fichiers avec une **incohérence** entre le mime-type et l'extension (uniquement pour HTTP): exemple .gif avec un mime-type "text/plain"
- Si une politique de double navigateurs est en place (interne et externe), interdire l'**user-agent du navigateur interne** (celui qui contient flash, java, ...)
- Avoir des **logs enrichies** (referer, useragent, ...) et les analyser régulièrement pour identifier les trafics illégitimes.
- Conserver un **historique des configurations** pour avoir une trace de chaque modification et pouvoir les comprendre plus tard (possibilité d'utiliser git). Par exemple : pourquoi une adresse est en liste blanche/noire ?
- Mettre en place un **captcha sur les nouveaux domaines** contactés pour la première fois

## Messagerie

- Analyser les **protections** en place avec *l'outil ANS de test de messagerie* <sup>10</sup> / Auditer la visibilité du SI sur Internet
- Interdire les **pièces jointes à risque** (blocage sur mime-type, extension, macros venant d'Internet <sup>9</sup>...)
- Mettre en place **l'analyse d'URL** contenue dans les courriels avec les bases: phishtank & urlhaus
- Limiter les **pièces jointes autorisées** (rtf, pdf, office) par l'utilisation de **Clamav** et potentiellement des règles **YARA** permettant d'identifier les macros, DDE, javascript, fichier intégré, ... Utiliser également les "clamav-unofficial-sigs"
- Mettre en place des **règles de scoring**
- Mettre en place une politique stricte sur la **réception des courriels** avec vérification de l'expéditeur (comme avec le SPF)
- Mettre en place le **DNS Black Listing**
- Mettre en place la **double authentification pour les accès webmail**

## Sur le serveur de sauvegarde

- Utiliser un référentiel d'identité local (et non pas des **comptes d'accès** de l'AD principal)
- **Exclure** le droit à la suppression des sauvegardes des comptes utilisés dans les agents de sauvegarde
- Choisir un **mot de passe spécifique** qui ne soit pas réutilisé

## Centralisation des journaux d'évènements

- **Centraliser** les logs importants (firewall, proxy, waf, acl, authentification [vpn, webmail, ...], évènements windows ou linux important, ...)
- Utiliser un référentiel d'identité local (et non pas des **comptes d'accès** de l'AD principal) avec un mot de passe spécifique unique
- **Vérifier** que les informations importantes pour la détection et les investigations sont présentes dans les logs collectés (ex : avoir l'adresse IP réelle du client pour l'authentification)

## Références

1. <https://www.dtonias.com/show-hide-extensions-for-known-file-types/>
2. <https://docs.microsoft.com/fr-fr/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview>
3. <http://softwarepolicy.sourceforge.net/>
4. <https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>
5. [https://docs.microsoft.com/fr-fr/archive/blogs/diana\\_tudor/microsoft-project-how-to-control-macro-settings-using-registry-keys](https://docs.microsoft.com/fr-fr/archive/blogs/diana_tudor/microsoft-project-how-to-control-macro-settings-using-registry-keys)
6. <https://blogs.technet.microsoft.com/mmpc/2016/06/14/wheres-the-macro-malware-author-are-now-using-ole-embedding-to-deliver-malicious-files/>
7. <https://social.technet.microsoft.com/Forums/fr-FR/f56b805c-eb55-48ee-9caf-7e9f5e88ab8d/howto-activer-le-mode-quotrestricted-adminquot-pour-les-connexions-bureau-distance-?forum=windowsserver8fr>
8. <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction>
9. <https://feodotracker.abuse.ch/>, <https://github.com/maravento/blackweb>
10. <https://pm.aslpsante.fr>

### Pour en savoir plus,

- <https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-active-directory/>
- [https://www.ssi.gouv.fr/uploads/2017/01/guide\\_hygiene\\_informatique\\_anssi.pdf](https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf)
- <https://www.ssi.gouv.fr/administration/guide/mise-en-oeuvre-des-fonctionnalites-de-securite-de-windows-10-reposant-sur-la-virtualisation/>
- <https://www.ssi.gouv.fr/administration/guide/recommandations-pour-la-mise-en-oeuvre-dune-politique-de-restrictions-logicielles-sous-windows/>
- <https://www.cyberveille-sante.gouv.fr/alertes/1233-cryptovirus-recommandations-pour-protéger-les-sauvegardes-locales-2019-04-03>
- [https://www.fireeye.com/content/dam/fireeye-www/regional/fr\\_FR/current%20threats/pdfs/wp-ransomware-protection-and-containment-strategies.pdf](https://www.fireeye.com/content/dam/fireeye-www/regional/fr_FR/current%20threats/pdfs/wp-ransomware-protection-and-containment-strategies.pdf)
- <https://github.com/securitywithoutborders/hardentools>
- <https://attack.mitre.org/>