STORMSHIELD

Comment choisir une solution d'Endpoint Protection

Entre EDR et HIPS : quelle approche pour bloquer efficacement les cyberattaques sophistiquées ?

LIVRE BLANC

Alors que la thématique de la cybersécurité n'en finit plus d'être régulièrement sur le devant de la scène, les cyber-criminels cherchent quant à eux à passer sous le radar. Un objectif qui les pousse à constamment faire évoluer leurs techniques d'attaques. Et parce qu'ils en connaissent bien les rouages, ils cherchent à développer des outils malveillants pour tromper les solutions de cybersécurité présentes sur les postes de travail des collaborateurs.

Les antivirus et autres systèmes de détection classiques, notamment ceux exclusivement basés sur des signatures, semblent aujourd'hui dépassés par des techniques complexes, comme le détournement d'applications légitimes et l'élévation de privilèges, ainsi que par des logiciels malveillants furtifs. C'est pourquoi, les solutions se focalisant sur la détection et la prévention d'attaques connues deviennent insuffisantes pour affronter cette nouvelle génération de cyberattaques sophistiquées et inconnues.

Il est primordial pour les organisations d'implémenter ***des solutions analysant de façon très détaillée les comportements des processus en cours d'exécution pour repérer les menaces potentielles présentes dans la machine****. La solution choisie doit donc être en mesure de les détecter et de les bloquer de façon proactive, automatique et en temps réel pour une continuité de l'activité la plus sereine possible.*

Ce livre blanc décrit les différents mécanismes qu'un système de protection de postes de travail et de serveurs doit posséder pour mener à bien sa mission de détection de la menace et de protection des terminaux.

S'adressant aux Responsables de la Sécurité des Systèmes d'Information, il vous apportera les éléments nécessaires afin de mieux vous accompagner dans votre prise de décision en fonction de vos besoins.

Table des matières

01

Cyberattaques : mode opératoire

Selon l'ANSSI, entre 2019 et 2020, le nombre de victimes de cyberattaques a été multiplié par 4. Comme l'indique un rapport du Sénat français[2], les cyber-criminels en ont bien profité, ce qui a eu pour effet une augmentation des attaques par phishing (ou hameçonnage) de 667% enregistrées entre le 1er et le 23 mars 2020.

Par ailleurs, même si la sensibilisation des utilisateurs s'est progressivement améliorée, aucun système ou infrastructure ne peut être sécurisé à 100%. C'est pourquoi les cyberattaquants trouvent toujours de nouvelles astuces pour pénétrer de façon de plus en plus ciblée dans les systèmes d'information des entreprises de toutes tailles.

91%

des attaques ciblées passent par la méthode de spear phishing

Leur objectif ? Exfiltrer des données sensibles (médicales, bancaires, industrielles, etc.), les chiffrer pour les rançonner ou les publier voire mettre à mal la productivité de l'entreprise ciblée (site marchand, des chaînes de production etc.). Pour ce faire, les cyberattaquants cherchent à outrepasser les systèmes de sécurité mis en place afin de s'y installer en exploitant, par exemple, des vulnérabilités présentes dans les logiciels ou dispositifs installés.

Pour mieux comprendre comment fonctionne une cyberattaque, nous allons nous concentrer sur les trois phases les plus décisives permettant à un attaquant d'atteindre son objectif final. La phase initiale sera la compromission d'une machine utilisateur ou d'un service exposé, lui offrant un premier accès sans privilège au système. En phase deux, le cyberattaquant cherche alors à rentrer en profondeur dans le système d'information en obtenant par exemple l'accès à un compte à privilèges ou encore en infectant d'autres machines. En phase trois, l'attaquant peut procéder au déclenchement de l'action malveillante en tant que telle : chiffrement, exfiltration...

Nous allons aborder avec plus de détails ces trois phases.

[2] http://www.senat.fr/rap/r20-678/r20-678_mono.html

D'abord, les cyber-criminels se renseignent pour identifier des victimes au sein de l'entreprise ciblée. En effet, l'attaquant cherche à mettre en œuvre des vecteurs d'attaque qui peuvent être humains et/ou technologiques.

Au niveau humain, l'attaquant utilise les techniques d'ingénierie sociale (LinkedIn, Facebook, etc.) pour collecter des informations qui serviront à détourner la vigilance de la ou les personnes qu'il a choisies pour lancer la primo-infection.

PHASE 1

DÉCOUVERTE ET PRIMO-INFECTION

Il tente ainsi de duper le destinataire afin qu'il ouvre une pièce jointe ou bien qu'il clique sur un lien web malveillant. Une technique réputée pour son efficacité : 91% des attaques ciblées[2] passent par cette méthode de spear phishing (hameçonnage ciblé).

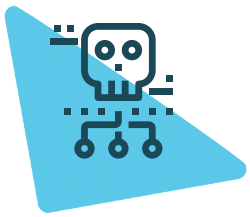
Le détournement de vigilance peut par exemple consister pour le cyberattaquant à usurper l'identité d'un expéditeur (établissement financier, fournisseur etc.) connu de la personne ciblée.

Sur le plan technologique, le cybercriminel cherche à exploiter des failles dans le système de protection. Il profite des systèmes qui ne sont pas correctement protégés, comme des serveurs RDP accessibles depuis Internet. Il peut aussi tenter d'exploiter les faiblesses des applications vulnérables et non mises à jour. À titre d'exemple, l'alerte émise en mars 2021 par le centre canadien pour la cybersécurité[3] qui recommande plusieurs mises à jour contre l'exploitation active de vulnérabilités liées à Microsoft Exchange.

Le but : exécuter du code malveillant pour installer un programme dans la machine ciblée qui permet l'infiltration du cyberattaquant.

[2] http://www.itpronews.fr/3648/2012/12/spear-phishing-plus-de-90-des-attaques-ciblees.html

[3] https://cyber.gc.ca/fr/avis/exploitation-active-des-vulnerabilites-de-microsoft-exchange



PHASE 2

LATÉRALISATION ET EXPANSION

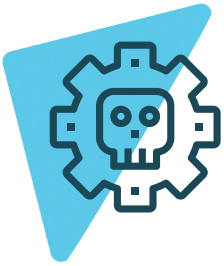
La phase de primo-infection achevée, l'attaquant cherche à scanner le réseau pour mieux le connaître. Dans cette phase de latéralisation, il veut pénétrer plus en profondeur le système d'information pour identifier les machines et les comptes d'utilisateurs ou d'administrateurs qui serviront à atteindre ses objectifs.

Dans un premier temps, il va donc naviguer et pivoter à travers différents systèmes et comptes. Il peut également installer à distance ses propres outils pour tenter d'exploiter des failles dans le système et de récupérer des identifiants de connexion.

Le but : s'implanter en profondeur dans l'infrastructure afin de trouver des machines ciblées sur lesquelles l'attaque aura le plus d'impact.

Ensuite, il cherche à s'introduire en profondeur dans le système ce qui correspond à la phase d'expansion. Il se fait souvent passer pour un utilisateur autorisé, ce qui est très difficile à détecter. Pour y arriver, il peut effectuer une élévation de privilèges pour se faire passer pour un administrateur local ou encore s'approprier un compte utilisateur ayant accès à un logiciel en particulier. Il combine également plusieurs vecteurs d'attaque pour tenter de compromettre d'autres machines vulnérables.

Pour ce faire, les approches courantes consistent à se servir des faiblesses, de mauvaises configurations de l'infrastructure ou encore des vulnérabilités existantes. Par exemple une mauvaise segmentation au sein du réseau de l'entreprise permettant d'accéder aux machines intéressantes pour lui, par exemple, un serveur avec des données sensibles.



PHASE 3

IMPACT

Cette troisième phase constitue l'aboutissement de l'attaque où le cybercriminel effectue des actions en ligne avec l'objectif qu'il s'était fixé. La cyberattaque activée, elle peut permettre **d'exfiltrer / voler des données, modifier des processus opérationnels ou encore arrêter un serveur vital** au bon fonctionnement de la structure.

Dans cette phase, l'attaquant peut également prendre soin de rester furtif pour réexploiter la machine ultérieurement ou lancer une attaque (plus ou moins virulente) comme celle subie par TV5 Monde[4] en 2015.

À noter que dans certains cas, il prendra soin de supprimer les différentes sauvegardes et ses traces d'activité malveillante.

Le but : mettre à mal l'infrastructure pour bloquer un élément nécessaire à la production de l'entreprise. Également, exfiltrer les données pour revente et / ou publication (comme des données de santé dans le dark web) ou pour chiffrement afin d'obtenir une rançon de la structure ciblée.

[4] https://www.lemonde.fr/pixels/article/2017/06/10/le-piratage-de-tv5-monde-vu-de-l-interieur_5142046_4408996.html

02

L'analyse comportementale des solutions

Les cybercriminels se servent notamment des techniques d'attaque pour passer sous le radar et éviter la détection de leur code malveillant par les différentes solutions de sécurité. **La détection des comportements suspects ainsi que la suspension préventive des activités potentiellement dangereuses s'avèrent donc essentielles.**

De ce fait, le système *Host Intrusion Prevention System* (HIPS) permet de protéger les postes de travail et serveurs contre les logiciels malveillants en bloquant les activités suspectes qui peuvent affecter les systèmes de l'infrastructure.

« Certains systèmes de prévention d'intrusion permettent aux utilisateurs d'envoyer des journaux d'activités malveillantes et des fragments de code suspect directement au éditeur pour analyse et une possible identification. »

Stephen J. Bigelow

Senior Technology Editor

Source : Techtarget

Ci-dessous, nous allons aborder les aspects principaux entre les différents types de système HIPS pour mieux répondre aux besoins de chacun.

HIPS **par signature**

Ils se basent sur la **connaissance de vulnérabilités d'une application et des menaces connues** et bloque leur exploitation. Ils fonctionnent avec une base de données qui doit être actualisée régulièrement.

Ils identifient des attaques connues. En revanche, ils **ne savent pas détecter** des attaques inconnues ou encore de type 0-day. Ils sont **peu adaptés aux situations où le poste doit être déconnecté** de son serveur de mise à jour.

Peu d'options présentes dans le logiciel.

HIPS **comportemental**

Blocage **en temps réel des attaques connues et 0-Day** : détection des activités suspectes des applications légitimes et des processus sans recourir à des bases de signatures ni à des anomalies applicatives.

Certains HIPS allient des **méthodes comportementales et heuristiques, protection de la mémoire ou encore du durcissement du système d'exploitation** (OS) assurant une meilleure protection face aux menaces.

Haut niveau de paramétrage de listes ou de règles et filtres s'adaptant aux différentes organisations.

*« Une solution HIPS d'analyse comportementale reconnaît et bloque les **techniques d'attaques** courantes ou sophistiquées telle que l'exploitation des vulnérabilités applicatives afin d'assurer une **protection efficace du poste utilisateur.** »*

Edouard Simpère

Responsable Pôle Sécurité
Stormshield

Omniprésents dans le lexique de ces dernières années du monde de la cybersécurité, les EDR ou Endpoint Detection & Response[5] sont des logiciels permettant de détecter et de bloquer les menaces connues et inconnues sans attendre les correctifs ou mises à jour. Ils se matérialisent généralement par des agents déployés sur les différents points de terminaison d'un réseau, notamment sur les postes de travail, les téléphones portables ou encore les différents serveurs de l'infrastructure.

L'une des caractéristiques générales des EDR consiste à effectuer **une surveillance continue des endpoints**. De plus, certaines solutions intègrent des briques de type EPP pour fournir une protection en temps réel. Celui-ci constitue une première barrière efficace de protection pour la plupart d'attaques connues et certaines menaces inconnues.

Endpoint Detection & Response : l'idéal de la sécurité ?

Comme le souligne l'ANSSI[6], ces solutions gérant une grande quantité de données proposent généralement des capacités de **détection** (des comportements suspects des applications légitimes, des attaques de type *fileless*[7]), d'**investigation** (visualisation complète de l'attaque détectée) et de **remédiation** (restauration de fichiers etc.).

De ce fait, les EDR complètent aujourd'hui les solutions traditionnelles basés essentiellement sur des bases de signatures. Ils proposent une **visibilité globale** et détectent généralement les comportements anormaux des processus légitimes. Suite à cette détection, la solution met en place une réponse pour interrompre l'attaque en mettant fin au processus malveillant. De manière plus ou moins automatisée, elle permet d'avertir l'administrateur. Ensuite soit il applique une réponse, soit l'EDR est capable de la fournir automatiquement et en quasi temps réel (cela va dépendre de la solution utilisée). Par conséquent, les ransomwares et les attaques polymorphes peuvent être détectés et bloqués à l'aide de ces outils.

[5] https://www.ssi.gouv.fr/uploads/2021/06/anssi-france_relance-edr.pdf

[6] https://www.ssi.gouv.fr/uploads/2021/06/anssi-france_relance-edr.pdf

[7] https://www.riskinsight-wavestone.com/2018/10/fileless-attack-le-retour-a-la-terre/

Côté administration, ils peuvent s'intégrer au SIEM de l'organisation afin de remonter les logs nécessaires constituant une aide pour les analystes du SOC afin d'optimiser l'efficacité dans la recherche d'attaques.

Par ailleurs, la plupart des solutions EDR du marché optent aujourd'hui pour une approche de type *cloud-only* ou *cloud-first*[8] pour centraliser la récolte des données et réaliser l'analyse des signaux précurseurs ou de compromission révélant une attaque. En effet, le cloud se prête à cette collecte massive et à l'analyse sur d'importantes quantités de données à traiter.

Néanmoins, dans certains cas d'usage, cette possibilité ne peut pas être envisagée compte tenu de la sensibilité de la donnée à traiter. De ce fait, **le mode *on-premise* peut s'avérer une option efficace dans un environnement sensible** (Défense, ministères, industrie, etc.). De plus, il est important de distinguer le niveau de protection établi soit par le serveur soit par le client installé sur le poste.

Nous allons observer les différences majeures entre les deux approches :

Protection focalisée **sur le serveur**

Dans cette approche, l'agent léger installé sur le poste **remonte toutes les informations au serveur**. Il ne dispose pas de fonctionnalités étendues.

Le serveur, on-premise ou cloud, analyse les logs remontés par l'agent à la recherche des comportements malveillants, des anomalies présentes sur un poste en particulier etc.

L'agent léger a besoin **d'une connexion en permanence pour remonter les informations**. Il peut avoir une certaine latence dans la réponse obtenue.

Protection focalisée **sur l'agent**

L'agent présent sur le poste est **autonome pour prendre des décisions** et protéger le poste sans nécessité d'accéder à son serveur.

Le serveur dispose d'une visibilité moins globale compte tenu des **capacités étendues de l'agent** pour la gestion du poste contre les malwares.

L'agent peut **travailler en indépendance bloquant en temps réel** des comportements malveillants.

Ainsi, pour assurer la meilleure protection à tout moment, **il faut privilégier des solutions capables de détecter des malwares sans avoir recours à une connexion réseau pour garantir une protection en temps réel et fiable du poste de travail.**

[8] https://www.pcpresse.com/wp-content/uploads/2020/10/LINFO-CR01_MD.pdf

04

Les différentes techniques de protection HIPS

Les cybercriminels sont conscients que leurs attaques ne doivent pas attirer l'attention pour passer inaperçus (phase 2 : latéralisation et expansion). Pour ce faire, ils s'efforcent de développer constamment de nouvelles compétences en déployant de nouvelles tactiques et techniques d'attaque afin de contourner les protections traditionnelles.

Nous allons aborder les principales techniques utilisées et comment l'attaquant va s'en servir pour essayer de contrecarrer les différentes protections de sécurité.

255%

Ce chiffre correspond à l'augmentation des signalements par ransomware en 2020, selon une étude de l'ANSSI

Dans le tableau ci-dessous, nous avons observé différentes techniques d'attaque dans les trois phases lors d'une cyberattaque. Pour rappel, dans la troisième phase, l'attaquant a déjà pris le contrôle et il commence la phase d'impact comme par exemple : l'exfiltration ou le vol de données. Il faut savoir que ces extractions sont souvent compliquées à détecter car les attaquants se servent des outils et des identifiants *a priori* légitimes.

Phase	Techniques	Comment l'attaquant s'en sert ?	Impacts
Phase 1 : découverte et primo infection	Buffer overflow. Exemple : - Stack Pivot	L'attaquant utilise un buffer overflow en fournissant des données d'entrée mal formatées dans l'objectif de faire écrire à l'application ciblée des données en mémoire au-delà de la limite normale. Cette opération écrase les bonnes données et permet à l'attaquant de prendre le contrôle du flux d'exécution de l'application.	Le code que l'attaquant a inséré dans l'application ciblée lui permet d'obtenir un accès à distance et/ou de télécharger et exécuter d'autres fichiers malveillants (payload).
Phase 1 : découverte et primo infection	Packed Malware	Cette technique consiste à empêcher l'analyse du fichier malveillant par des solutions de sécurité en chargeant dynamiquement l'ensemble des fonctions.	Les packers complexifient la tâche d'identification du malware pour les équipes de sécurité et augmente le temps d'analyse. De plus, packer un fichier permet d'échapper aux solutions par signature.
Phase 1 : découverte et primo infection	Process Hollowing. Exemples : - RunPE - Doppelgänging	Le principe étant de faire exécuter du code malveillant au système en le camouflant sous l'identité d'un processus légitime. D'un côté, la technique RunPE abuse des faiblesses du système de chargement des codes exécutables. D'un autre côté, la technique Doppelgänging se sert du mécanisme de transaction NTFS.	Le process hollowing permet à l'attaquant de passer sous le radar des solutions de sécurité qui ignorent en général les processus systèmes légitimes pour lesquels il se fait passer.
Phase 2 : latéralisation et expansion	Elévation des privilèges Exemples : - DLL hijacking - Access token manipulation	L'attaquant essaie d'obtenir des accès de niveau supérieur sur un poste ou système pour atteindre ses objectifs. D'une part, pour la technique DLL hijacking, l'attaquant manipule une application disposant des privilèges élevés en lui faisant charger une DLL malveillante. D'autre part, l'access token manipulation. L'attaquant peut voler ou dupliquer des jetons d'accès dans le but de modifier le contexte d'exécution de l'application ciblée lui permettant de s'octroyer des permissions supplémentaires.	Après obtention des droits élevés (droits d'administrateur ou système), l'attaquant devient alors difficile à arrêter car il dispose d'une forte empreinte dans la machine cible. Ces droits élevés facilitent la latérisation de l'attaque. Celle-ci peut être possible dans certains cas sans droits élevés.
Phase 2 : latéralisation et expansion	Pass the hash	L'attaquant effectue le vol d'un hash servant à l'identification d'un compte plus privilégié utilisé potentiellement pour se connecter sur d'autres machines.	Cette technique permet à l'attaquant de s'authentifier sur d'autres postes grâce à cette identité volée. Le but étant d'infecter de nouvelles machines.
Phase 2 : latéralisation et expansion	Découverte du réseau en ligne de commande	L'attaquant utilise des commandes (comme netdiscover) pour détecter les postes d'un même réseau.	L'attaquant peut avoir une vision complète des différents réseaux mis en place.
Phase 3 : impact	Chiffrement de données	L'attaquant chiffre des données stockées sur les machines (postes et serveurs) pour les rendre inaccessibles à la victime. Il se sert en général de techniques cryptographiques légitimes liées aux API Windows.	Cette technique est utilisée dans le cadre des attaques par ransomware dans lesquelles le cybercriminel exige une rançon pour la récupération des données.

4.1
L'approche par règles : une méthode efficace

Il existe un certain nombre de solutions utilisant des règles pour effectuer de la détection sur les postes. Cependant, dans certaines, il n'est pas possible pour les administrateurs d'y accéder. Il est vrai que l'implémentation de ces règles est plutôt simple mais elles ne peuvent pas s'adapter aux différents usages métier avec des cadres de sécurité particuliers.

En revanche, dans d'autres solutions, il est possible de trouver un certain niveau de paramétrage pour s'adapter au mieux aux organisations où la solution est déployée. Ainsi, en plus des règles prévues par l'éditeur de sécurité, l'utilisateur peut également en inclure en fonction du poste, du métier, etc.

D'ailleurs, certains systèmes HIPS vont combiner plusieurs techniques de protection assemblées sous forme de paramètres ou règles qui forment ce que l'on désigne comme « politique de sécurité de la solution ». Celle-ci permet à l'administrateur de l'adapter en fonction du processus métier à protéger. Pour certaines solutions, les différents paramètres ou règles peuvent se personnaliser ce qui offre une meilleure adaptation et protection pour l'organisation.

Le saviez-vous ?

Les règles comportementales appliquées du côté agent proposent une protection immédiate du poste pour limiter les impacts d'une attaque.

La granularité des solutions de protection utilisées

Certaines solutions proposent des listes de règles prédéfinies et extensibles par l'administrateur pour contrer les malwares.

Comme nous le constatons ci-dessus, il faut privilégier des solutions HIPS fournissant **des ensembles de règles configurables et très fines pour contrôler toute action effectuée sur les postes de travail** comme la surveillance de processus en cours, les fichiers et clés de registre, l'élévation des privilèges etc.

Cette granularité permet aux administrateurs de l'organisation une personnalisation très élevée et plus globalement la possibilité de mettre en œuvre une politique de sécurité au plus près des besoins et des exigences de l'organisation.

En règle générale, il faut considérer un poste de travail ou serveur en fonction de son contexte (par exemple : en dehors ou dans le réseau de l'entreprise) et de son niveau d'exposition aux menaces.

4.2 L'approche contextuelle : mieux comprendre l'environnement

Compte tenu que chaque organisation est configurée d'une manière unique ayant des besoins spécifiques, il faut que la solution de protection puisse s'adapter aux différents cas d'usage au sein de l'organisation. De ce fait, la protection des postes de travail et des serveurs choisie doit **s'adapter au contexte d'utilisation de chacun et prendre en compte les différents scénarios de mobilité**. Par exemple, maîtriser les réseaux Wi-Fi autorisés, les désactiver lorsqu'une connexion LAN est active. Ou encore, bloquer toute autre connexion que celle du VPN quand il est actif pour empêcher les attaques par rebond.

Ainsi, la mise en place et l'utilisation d'une solution de protection de postes de travail se doit de disposer d'une politique de sécurité capable d'être dynamique. C'est-à-dire qu'elle doit **savoir où se trouve le poste en question et adapter sa sécurité à l'environnement en particulier**.

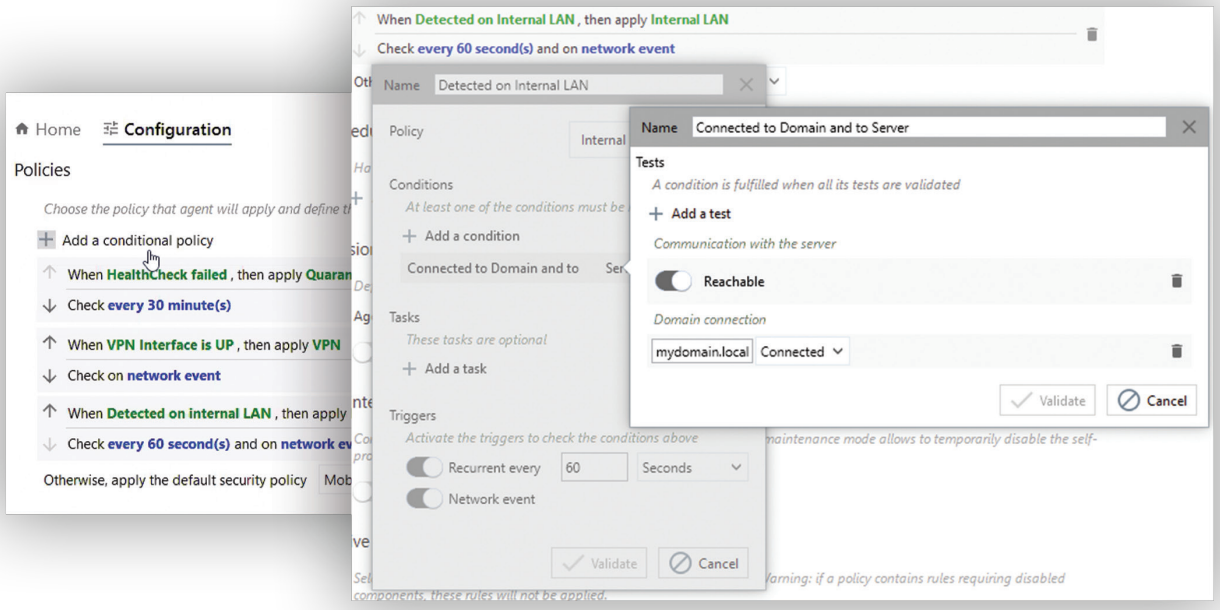


Figure 1

Solution de sécurité endpoint avec différentes politiques de sécurité

4.3
Le « hardening » pour la protection du système lui-même

Les solutions de sécurité constituent une cible d'attaque pour les cybercriminels. Ils cherchent à désactiver la protection ou bien profiter des droits privilégiés de ces solutions en les détournant. D'ailleurs, comme le souligne l'ANSSI[9], les logiciels (et matériels) d'une infrastructure doivent être vérifiés et leur configuration durcie avant leur exploitation.

Par ailleurs, il faut également prendre en compte la surface d'attaque. Les experts s'accordent sur le fait que chaque nouvel élément (matériel et logiciel) rajouté à l'infrastructure augmente le risque qu'il y ait un bug ou une vulnérabilité liée à ce composant, permettant son exploitation par un cyberattaquant.

Pour limiter la surface d'attaque et renforcer la protection des postes, certaines solutions de protection de postes de travail intègrent dans leur développement l'approche *Security by design*[10]. C'est-à-dire des solutions dont la sécurité et les risques associés sont intégrés et étudiés dès la conception du produit.

Cyberattaque à Mitsubishi Electric[11]

Le constructeur japonais a reconnu avoir subi une cyberattaque en juin 2019. Selon une enquête de plusieurs mois, les attaquants auraient eu accès au réseau interne de l'entreprise et auraient volé 200 Mo de fichiers sensibles sur des milliers de collaborateurs et des informations techniques confidentielles.

Comment cela s'est produit ?

Un groupe cybercriminel d'origine chinoise aurait exploité une faille de type 0-Day présente dans l'antivirus de l'organisation pour installer des fichiers malveillants. Selon le constructeur du logiciel piraté, les criminels auraient exploité une vulnérabilité de traversée de répertoire pour extraire des fichiers d'un fichier zip arbitraire vers un dossier spécifique du serveur de l'antivirus. Cela aurait pu provoquer l'exécution du code à distance ou *Remote Code Execution*.

9 https://www.ssi.gouv.fr/uploads/2020/08/anssi-guide-recommandations_architectures_systemes_information_sensibles_ou_diffusion_restreinte-v1.1.pdf

10 https://www.securecontrolsframework.com/security-privacy-design-principles

11 https://www.zdnet.fr/actualites/une-faille-0day-de-l-antivirus-trend-micro-utilisee-dans-le-piratage-de-mitsubishi-electric-39898077.htm

Pour ce faire, l'architecture générale de ce type de solutions doit être développée selon des règles de programmation logicielle défensive autour d'une architecture sécurisée en micro services. C'est justement sur ce point que s'applique le principe de moindre privilège.

Cela permet de découper la solution en **plusieurs services indépendants** garantissant une sécurité maximale où chacun dispose d'un rôle spécifique avec des privilèges limités. Ainsi, par exemple, le module qui gère la connexion au serveur de configuration ne doit pas être celui en charge de l'interprétation de ces données. Ou encore le service gérant les logs s'occupe exclusivement de cette tâche et ne peut pas accéder à la politique de sécurité mise en place.

Figure 2
Solution de sécurité divisée en plusieurs services indépendants

Pour atteindre un niveau de robustesse élevé, les processus de construction du logiciel de sécurité doivent également définir des règles de codage strictes et prévoir l'utilisation des diverses options de compilation et d'exécution. Ces options permettent de limiter les risques d'exploitation en cas de bug et limitent également le nombre d'erreurs en augmentant les contrôles avant et pendant l'exécution.

En synthèse, **les solutions durcies ou robustes se basant sur ces principes garantissent une meilleure protection face aux cyberattaques.**

Stormshield Endpoint Security Evolution : la solution de protection des postes de travail

Stormshield Endpoint Security Evolution **protège les environnements sensibles** en bloquant au plus tôt les attaques, avant qu'elles n'aient d'impact sur vos environnements

Analyse comportementale avancée capable de bloquer les menaces inconnues, les attaques 0-Day et les attaques de type *fileless*.

Solution autonome ne nécessitant aucune connexion réseau pour fonctionner et maintenir le niveau de sécurité des endpoints.

Contrôle avancé des périphériques. Large éventail de contrôle de périphériques : vérification des réseaux Wi-Fi et des clés USB, les accès de volumes disques ou encore les connexions réseau.

91%

des attaques ciblées passent par la méthode de **spear phishing**

40%

des primo infections utilisent la technique du **process hollowing**

255%

Augmentation des signalements par ransomware en 2020 (selon une étude réalisée par l'ANSSI)

QUELQUES EXEMPLES D'ATTAQUE

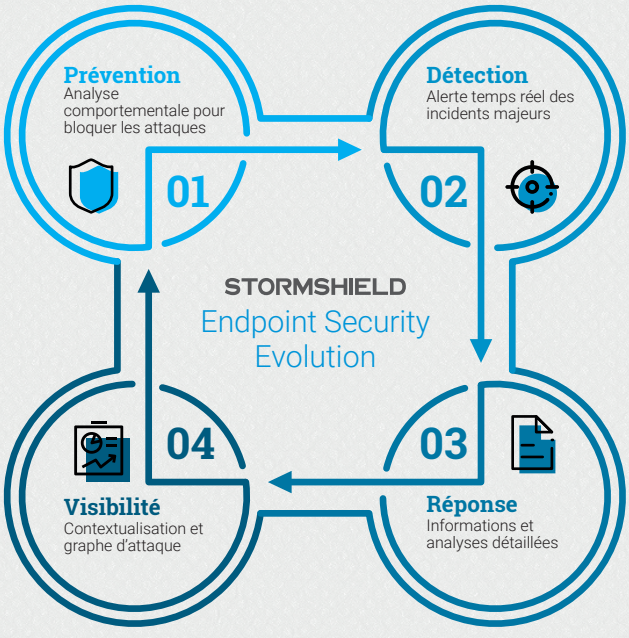
- COMPUTER WORM
- E-MAIL MALWARE
- INFECTED DEVICES
- PASSWORD STEALING
- SCANNING SYSTEM
- FILELESS ATTACK
- PHISHING STEALING
- HACKER
- TROJAN
- DATA LOSS
- SOFTWARE VULNERABILITIES
- ...

QUELQUES CONSEILS INDISPENSABLES

Méfiez-vous des emails suspects avec des pièces jointes ou des sites douteux.

Effectuez **régulièrement des sauvegardes**.

Mettez à jour vos applications, plugins et systèmes d'exploitation.



LE **CHOIX EUROPÉEN** DE LA **CYBERSÉCURITÉ**

www.stormshield.com