- LIVRE BLANC

Bitdefender

Sécurité

Top 5 des problèmes de configuration des endpoints qui génèrent des failles de sécurité

RÉDUIRE LA SURFACE D'ATTAQUE GRÂCE À DES CONTRÔLES EFFICACES ET AU RENFORCEMENT DES SYSTÈMES

www.bitdefender.fr

Sommaire

Auteur :

Filip Truta, Analyste en Sécurité de l'Information, Bitdefender

Introduction

Le terme « cyberattaque » peut évoquer les malwares, l'ingénierie sociale, les vulnérabilités des réseaux ou encore les endpoints non corrigés. Mais comment les cybercriminels parviennent-ils à lancer leur chaîne de frappe (kill chain) en premier lieu ? Quels éléments leur permettent d'exploiter une faille afin de s'introduire dans une infrastructure ? Les erreurs humaines étant à l'origine de la plupart des attaques réussies[1], il pourrait être utile de s'intéresser à celles-ci plutôt qu'aux coupables.

Les mauvaises configurations sont une lacune de cybersécurité courante. Les experts de la sécurité s'accordent à dire[2] que les erreurs de configuration en matière de privilèges, de paramétrage des endpoints, de réglages Internet et d'activation inutile de services risqués ainsi qu'en matière de contrôle des accès sont aujourd'hui les principales causes des incidents de cybersécurité.

Les erreurs de configuration permettent aux cybercriminels de tromper la vigilance des administrateurs IT en quelques jours, en quelques heures, voire en quelques minutes dans certains cas. Si la correction d'une erreur de configuration prend plus d'une journée, les adversaires disposent de l'avantage dont ils besoin pour déployer une véritable attaque et s'introduire dans l'infrastructure ciblée par ce qui semble à première vue n'être qu'une toute petite fenêtre d'opportunité.

Sur la base de données de télémétrie issues de la Threat Intelligence de Bitdefender, ce livre blanc explore 5 catégories courantes d'erreurs de configuration exploitées par les cybercriminels pour s'introduire dans les infrastructures IT. Bitdefender permet aux équipes de sécurité de pallier efficacement ces lacunes, moyennant un minimum d'efforts et sans que les activités de l'entreprise soient impactées d'aucune manière.

Points clés

- Les mauvaises configurations des endpoints représentent 27% des points d'entrée exploités de nos jours par les attaquants
- Les mauvaises configurations liées à des comptes, au stockage de mots de passe et à la gestion de mots de passe représentent les principales erreurs de configuration des endpoints individuels, pour 12,5%
- Les erreurs de configuration liées à WinRM se classent en tête des problèmes de configuration associés aux composants Microsoft et en deuxième position sur la liste des erreurs courantes de configuration des endpoints
- Parmi les domaines les plus couramment touchés par les erreurs de configuration, la catégorie des réglages Internet arrive en tête, avec une part cumulée de 73,1%
- Les mauvaises configurations liées à la signature Authenticode arrivent en tête des problèmes de configuration liés aux réglages Internet, et en troisième position sur la liste des erreurs courantes de configuration des endpoints
- L'analyse des risques associés aux endpoints permet aux administrateurs de réduire la surface d'attaque, en limitant les éventuelles compromissions et en offrant une visibilité sur les risques associés aux mauvaises configurations

Les erreurs de configuration en tant que vecteurs d'attaque

Les cybercriminels utilisent généralement des tactiques d'ingénierie sociale ainsi que des malwares pour lancer leurs attaques. Les solutions de sécurité des endpoints sont bien équipées pour offrir une protection contre la plupart des vecteurs d'attaque, y compris les menaces internes - qu'elles soient dues à une malveillance ou à une négligence - mais sont moins performantes lorsque le service informatique ne parvient pas à configurer correctement la protection. Par exemple, lorsque le personnel informatique ne parvient pas à empêcher les employés de modifier les réglages de sécurité, ou néglige de restreindre le stockage sur support USB ou dans le cloud.

1 Bitdefender BusinessInsights Blog https://businessinsights.bitdefender.com/human-error-identified-as-the-1-reason-behind-most-cyberattacks
2 ESG Video: Closing the Gap with an Expanded Endpoint Protection Platformhttps://www.youtube.com/watch?v=6KLvimsmwe0&feature=youtu.be

Plus d'un quart des entreprises citent[3] la gestion des configurations comme représentant l'un des plus grand défi auxquels elles sont confrontées dans la sécurisation des endpoints. En effet, les mauvaises configurations des endpoints représentent 27% des points d'entrée exploités de nos jours par les attaquants.

La mauvaise configuration des endpoints est courante dans la plupart des entreprises, représentant 27% des points d'entrée des menaces. *– ESG: The Emerging Era of Configuration Risk Analysis*

Les équipes de sécurité sont submergées de tâches réactives et répétitives telles que la gestion des vulnérabilités, le tri des incidents et l'application de correctifs. Par conséquent, les mauvaises configurations de sécurité représentent un vecteur d'attaque lucratif - les cybercriminels ayant conscience que les ingénieurs IT qui manquent d'automatisation sont toujours sur le qui-vive. Les équipes de sécurité doivent disposer des moyens nécessaires à l'évaluation des risques et à la remédiation rapide des problèmes de configuration sans que leurs systèmes informatiques soient perturbés.

"Pourquoi les mauvaises configurations de sécurité sont-elles un vecteur d'attaque courant ? Parce que les cybercriminels savent que les ingénieurs IT ne disposent généralement pas de l'automatisation et sont toujours sur le qui-vive, écopant l'eau d'un bateau qui coule." *- Bogdan Botezatu, Directeur des recherches et des rapports sur les menaces, Bitdefender*

Le piratage retentissant de **Capital One** l'année dernière a été la conséquence de la mauvaise configuration d'un pare-feu d'applications Web. Paige Thompson, autrefois ingénieure chez AWS, a exploité l'erreur pour accéder à un serveur détenu et utilisé par Capital One. Paige Thompson a pu accéder sans autorisation à 140 000 numéros de sécurité sociale, 1 million de numéros d'assurance sociale canadiens, 80 000 numéros de comptes bancaires ainsi qu'à des informations plus personnelles concernant les clients touchés. Paige Thompson a ensuite tenté de partager l'accès aux informations en ligne [4].

Lors de l'incident **Imperva** [5], des pirates ont réussi à dérober une clé API d'administrateur de AWS hébergée dans une instance de calcul laissée exposée à l'Internet public. Et lorsque **CenturyLink** a exposé 2,8 millions de dossiers clients [6], il a été révélé qu'une base de données MongoDB tierce contenant les dossiers avait été laissée sans protection sur Internet.

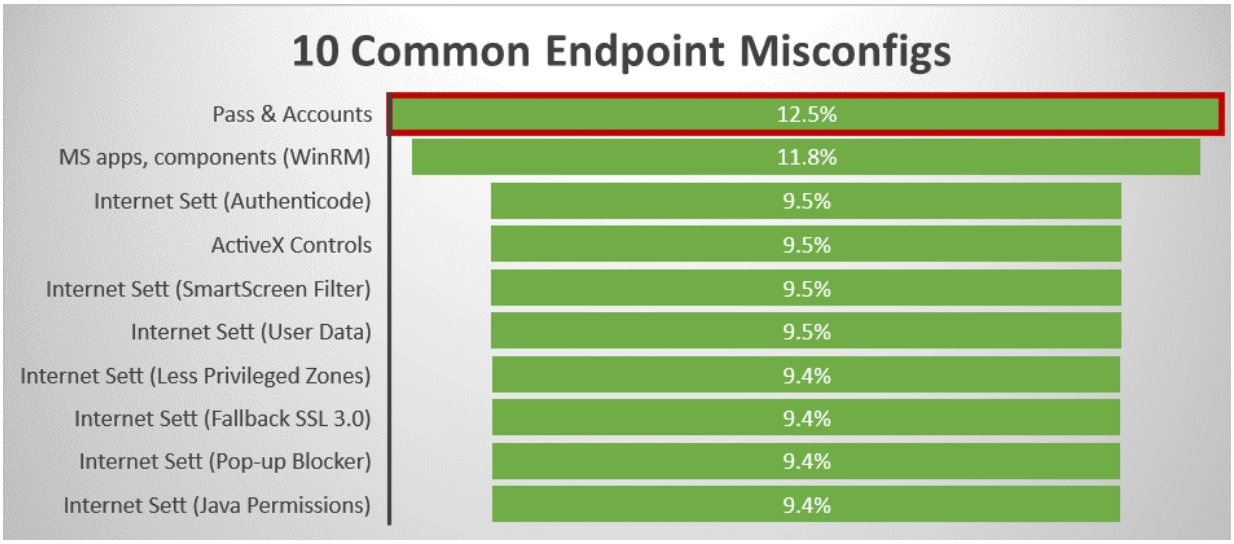
Les mauvaises configurations sont une affaire granulaire, ce qui signifie que les responsables IT sont constamment surmenés. Les exemples ne manquent pas : comptes fortuits par défaut utilisant des identifiants par défaut. Ports ouverts, inutiles. Contrôle du compte de l'utilisateur (UAC) non sécurisé ou désactivé. La protection avancée est désactivée. La connexion automatique est dangereusement activée ou les réglages empêchant l'exécution automatique sont désactivés. La connexion invité non sécurisée est activée et, bien sûr, les privilèges mal configurés abondent.

Mais, en plus de ces sujets de préoccupation immédiats, les équipes de sécurité doivent jongler quotidiennement avec des catégories entières de mauvaises configurations. Par exemple, parmi les négligences informatiques les plus courantes, la plupart, et de loin, se produisent dans le domaine des réglages Internet, comme nous l'évoquerons par la suite. Et les erreurs de configuration liées à la gestion à distance de Windows arrivent en tête de la liste des mauvaises configurations des applications Microsoft. Mais un service IT manquant de personnel et de ressources, à l'instar de ceux que l'on trouve dans les petites et moyennes entreprises, doit s'occuper de milliers d'autres modules et commutateurs. Examinons quelques-uns des 5 principaux domaines dans lesquels les services IT rencontrent le plus de difficulté avec les mauvaises configurations, sur la base de données de télémétrie récentes issues des Bitdefender Labs.

3 ESG: The Emerging Era of Configuration Risk Analysis https://enhancedreports.com/bitdefender/6371/index.html?__hssc=27765283.2.1581574751226&__hstc=27765283.5b81ba1a3a40b54efa99bccbfcefee93.1575920737386.1581551172637.1581574751226.34&__hsfp=3054740584&hsCtaTracking=e1b1b274-49ff-4a9b-8a5b-bda8fabd0e78%7C3ed220b4-5356-4029-ac55-348a61137e6c
4 https://www.cnn.com/2019/07/29/business/capital-one-data-breach/index.html
5 https://threatpost.com/imperva-data-breach-cloud-misconfiguration/149127/
6 https://www.scmagazine.com/home/security-news/data-breach/2-8-million-centurylink-customer-records-exposed-by-unprotected-database/

1.Mauvaise configuration des comptes et de la gestion des mots de passe

Les mauvaises configurations liées à des comptes, au stockage de mots de passe et à la gestion de mots de passe représentent les principales erreurs de configuration des endpoints individuels (autrement dit ne relevant pas d'une catégorie unique), avec une part de 12,5%. L'un des écueils les plus couramment rencontrés est l'incapacité à vérifier si le navigateur de l'utilisateur (Mozilla Firefox, Internet Explorer, Chrome, etc.) stocke des mots de passe sur le disque. Un attaquant qui prend le contrôle du système peut dérober les identifiants qui y sont stockés.



Une alerte [7] publiée conjointement par le Département de la sécurité intérieure des États-Unis (DHS), la Cybersecurity and Infrastructure Security Agence (CISA) des États-Unis et le National Cyber Security Center (NCSC) du Royaume-Uni a révélé comment les auteurs de menaces persistantes avancées (APT) ciblaient activement des organisations impliquées dans les réponses nationale et internationale à la Covid-19. Ces organisations incluent des organismes de santé, des laboratoires pharmaceutiques, des universités, des établissements de recherche médicale et des gouvernements locaux. La CISA et le NCSC enquêtent activement sur les campagnes de type **password spraying** lancées par des groupes APT. Les pirates utilisent ce type d'attaques pour cibler des organismes de santé, principalement au Royaume-Uni et aux États-Unis.

Le “password spraying” est un type d’attaque par force brute fréquemment utilisée par les cybercriminels, qui utilisent des mots de passe couramment utilisés lors de précédentes violations de données. Cette technique permet aux attaquants de passer inaperçus lorsqu’ils déploient leurs attaques. “Ces attaques donnent de bons résultats parce que, dans un ensemble d’utilisateurs donné, il y en aura sûrement quelques-uns qui utiliseront des mots de passe courants.“ -- https://www.us-cert.gov/

Alors que les campagnes de phishing et de compromission d'e-mails professionnels (BEC) prolifèrent, les identifiants compromis restent l'un des vecteurs d'attaque favoris des cybercriminels.

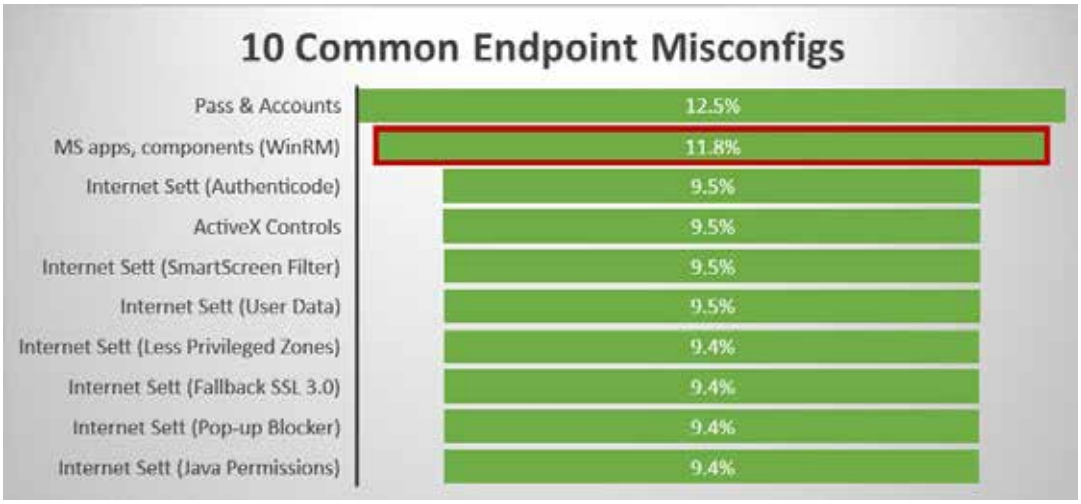
7 https://www.us-cert.gov/ncas/alerts/AA20126A

2. Mauvaises configurations des applications, composants et frameworks Microsoft

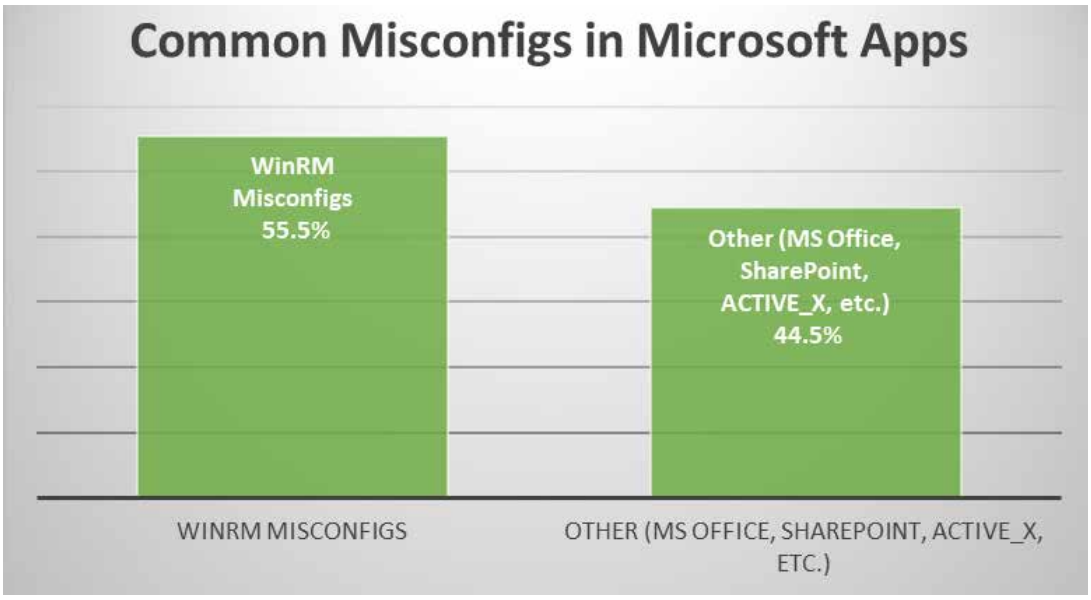
Les données Bitdefender montrent que les administrateurs IT commettent régulièrement des erreurs dans la configuration des applications et des composants liés aux systèmes d'exploitation et, avec Microsoft dominant le paysage des environnements professionnels, il n'est guère surprenant que les erreurs informatiques les plus communes surviennent dans des logiciels tels que Microsoft Office, SharePoint, ACTIVE_X et WinRM (Windows Remote Management).

Le service WinRM (Windows Remote Management) suscite des préoccupations particulières , car il permet à un utilisateur d'interagir avec le système, de lancer un exécutable, de modifier le registre ou de modifier des services, le tout à distance. Elle peut être appelée avec la commande winrm ou par plusieurs programmes, comme PowerShell. Une mauvaise configuration de WinRM peut avoir des conséquences dévastatrices du point de vue de la sécurité.

Les erreurs de configuration liées à WinRM se classent en tête des problèmes de configuration associés aux applications, aux composants et aux frameworks Microsoft et en deuxième position sur la liste des erreurs courantes de configuration des endpoints.



Si l'on s'intéresse exclusivement aux applications et aux composants Microsoft, les erreurs associées à WinRM représentent la majeure partie des problèmes de configuration signalés, pour 55,5 %.



3. Systèmes et applications non corrigés (EternalDarkness)

Le 12 mars 2020, Microsoft a publié un patch important qui corrige une faille critique dans le pilote du noyau du protocole SMB. Accidentellement révélée, puis omise dans le Patch Tuesday de mars 2020, cette faille affecte la version 3.1.1 du client et du serveur SMB (Server Message Block) pour Windows et peut être exploitée en dehors de l'organisation ciblée afin de déclencher une attaque par déni de service et, dans certaines circonstances, l'exécution de code à distance.

Il n'est pas simple de mesurer tous les problèmes de configuration des systèmes ni de leur attribuer un pourcentage sur la liste des erreurs humaines courantes. Un exploit actif qui tire parti de la vulnérabilité CVE-2020-0796[8], aussi appelée "EternalDarkness", peut entraîner des dommages dépassant toutes les prévisions, même celles du plus perspicace des analystes.

La pandémie extraordinaire de ransomwares WannaCry, la large diffusion de l'incident Equifax ainsi que la violation de données qui a touché Marriott ont toutes été possibles parce que des services IT ont omis de corriger à temps des vulnérabilités connues. Les préjudices financiers associés à WannaCry, qui exploitait un bug similaire touchant le protocole SMB dans des instances Windows non corrigées, se comptent en milliards de dollars.

Les vulnérabilités connues non corrigées, telles que CVE-2020-0796, trouvent leur place dans notre liste des 5 principales négligences informatiques, rien que pour les dégâts potentiels qu'elles sont susceptibles d'entraîner si elles venaient à être exploitées par des personnes malveillantes.

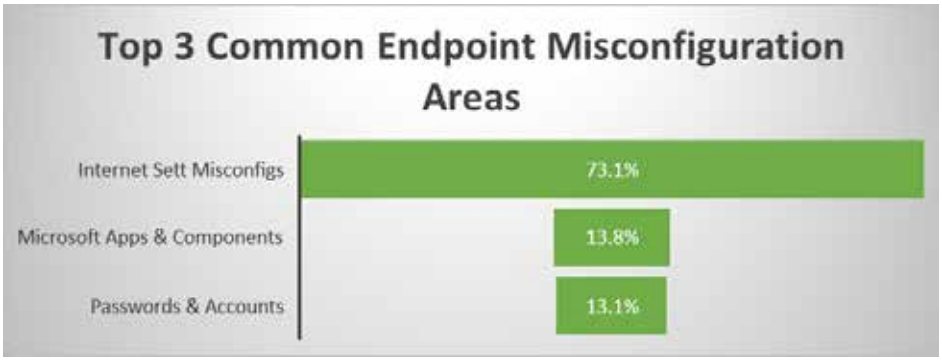
Microsoft a publié le 12 mars une mise à jour de sécurité, “KB4551762”, qui corrige la vulnérabilité. Les clients Bitdefender GravityZone peuvent automatiser le déploiement des mises à jour via le module Patch Management. Si l’application de correctifs est impossible, désactivez la compression SMBv3 sur les serveurs. VEUILLEZ NOTER que **cette action ne résout pas le problème sur les clients vulnérables**. Les utilisateurs peuvent désactiver la compression à l’aide la commande PowerShell suivante : Set-ItemProperty -Path “HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters” DisableCompression -Type DWORD -Value 1 -Force

La Cybersecurity and Infrastructure Security Agency (CISA) aux États-Unis a publié la liste des **10 vulnérabilités les plus fréquemment exploitées**[9] entre 2016 et 2019, dont sept affectent les offres Microsoft telles que MS Office, Windows, SharePoint et .NET Framework. L'alerte comporte des descriptions détaillées de chaque faille, ainsi que des mesures d'atténuation. La CISA, le FBI et, plus largement, le gouvernement des États-Unis, recommandent aux organisations de **s'abstenir d'utiliser tout logiciel en fin de vie**.

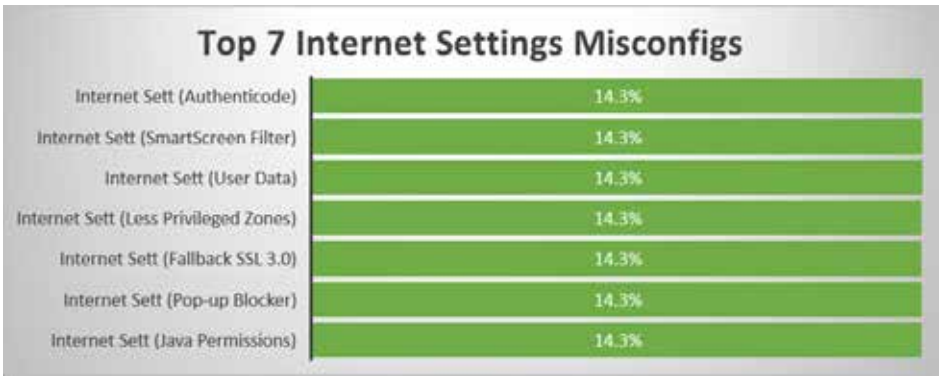
8 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796
9 https://www.us-cert.gov/ncas/alerts/aa20-133a

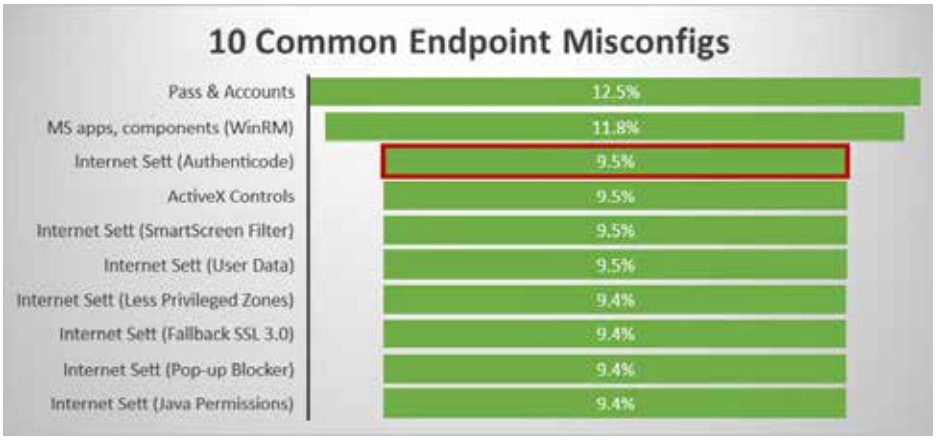
4. Réglages Internet

Parmi les catégories de mauvaises configurations des endpoints les plus couramment signalées par nos moteurs, les réglages Internet constituent de loin la catégorie comportant le plus d'erreurs, avec une part cumulée de 73,1%. Les mots de passe & les comptes arrivent en deuxième position à 13,8% et les applications & les composants Microsoft se classent en troisième position, à 13,1%.



Les mauvaises configurations liées à la signature Authenticode arrivent en tête des problèmes de configuration liés aux réglages Internet, et en troisième position sur la liste des erreurs courantes de configuration des endpoints. Authenticode est une technologie de signature développée par Microsoft qui permet aux éditeurs de logiciels de signer leur code et de prouver qu'il est fiable - autrement dit qu'il ne s'agit pas d'un malware.





Avec l'existence d'un taux relativement élevé (9,5%) de mauvaises configurations, ce réglage de politique revêt une importance particulière pour les ingénieurs IT, dans la mesure où il leur permet de décider si les composants de .NET Framework non signés avec Authenticode peuvent être exécutés ou non depuis Internet Explorer - la seconde option étant évidemment recommandée.

Tout composant du cadre .NET dans Internet Explorer doit être certifié comme étant sécurisé, faute de quoi des cybercriminels peuvent lui injecter une version infectée par un malware.

Un autre erreur fréquente de configuration des réglages Internet qui apparaît dans nos renseignements sur les menaces, avec une part de 9,4%, est celle consistant à **autoriser le retour à une version de SSL antérieure à la version 3.0**. Le bon réglage de politique consiste à bloquer tout retour non sécurisé à SSL 3.0. Négliger de le faire expose l'organisation aux attaques de type "man-in-the-middle" et aux écoutes clandestines.

5. Modifications par les utilisateurs des réglages de sécurité et des réglages du client

Comme indiqué ci-dessus, toutes les erreurs informatiques n'ont pas une incidence immédiatement quantifiable. Mais si vos employés peuvent agir sur les logiciels de sécurité, n'importe quelle autre erreur de configuration du système paraîtra secondaire par rapport à cette négligence. Les négligences telles que laisser des clés USB branchées ou maintenir la connexion au stockage dans le cloud sont également fréquentes dans les organisations de toutes tailles. Et bien que la plupart des plateformes de protection des endpoints soient très fiables, elles ne sont pas inviolables - en particulier si les administrateurs autorisent les utilisateurs à ajouter ou à supprimer des exceptions.

D'après le rapport d'enquête 2019 de Verizon sur les compromissions de données, même si les cas d'un administrateur malveillant est possible, les menaces internes émergent le plus souvent suite à des erreurs.

> Les approches en matière de défense contre les malwares sont différentes selon que le malware est déployé via l'ingénierie sociale, injecté via un téléchargement furtif ou importé par une personne interne via un dispositif USB. De plus, bien que nous soyons confrontés à ce qui semble être une liste interminable d'attaques potentielles, nous limiter à des aperçus entrave notre capacité à trouver des points communs entre ces attaques. De tels points communs, qui peuvent constituer des dépendances clés dans le processus d'un attaquant, représentent pour nous des possibilités de le perturber. Plus nous comprenons la séquence d'évènements qui se produit lors d'une attaque, plus nous pouvons, en tant que communauté, rendre difficile pour nos adversaires de réutiliser le même processus.
> *– Verizon 2019 Data Breach Investigations Report*[10]

Par exemple, la désactivation des sauvegardes, en plus de contrevenir à la loi (autrement dit au RGPD), peut conduire à la perte des données d'une organisation en cas d'attaque de ransomware, compromettant ainsi ses actifs financiers et ses actifs de propriété intellectuelle. À moins d'oublier de les faire, les sauvegardes représentent la ligne de défense unique la plus importante contre les ransomwares. Le montage de ressources réseau supplémentaires devrait lui aussi être prohibé. Les ransomwares sont "entraînés" à détecter tout ce qui ressemble à un volume et se présente comme tel (autrement dit, le disque Z:) et à le chiffrer.

10 https://enterprise.verizon.com/resources/reports/dbir/

Analyse des risques. Intégrée.

Les administrateurs informatiques disposent de multiples ressources pour lutter contre les vulnérabilités et les mauvaises configurations système les plus courantes, dont la liste OWASP Top 10 des 10 principales failles de sécurité,[11], les indicateurs CIS[12] ainsi que des rapports utiles établis par le secteur, qui mettent l'accent sur les principales lacunes à combler. Mais ils ne peuvent pas consacrer tout leur temps à passer au crible les indicateurs et les meilleures pratiques afin de se prémunir contre la cybercriminalité. Après tout, leurs fonctions ne se limitent pas à la gestion des problèmes de cybersécurité.

Toute perturbation touchant les endpoints affecte les activités de l'entreprise. Toutefois, les cyberattaques ciblant les endpoints représentent le point initial de compromission dans 39% des violations.[13] Aujourd'hui, l'une des principales causes de perturbation des systèmes trouve son origine dans les attaques liées à des erreurs de configuration, lors desquelles des cybercriminels tirent parti de systèmes mal configurés pour lancer des attaques basées sur des vulnérabilités de configuration bien connues, en vue de s'introduire dans lesdits systèmes. À l'inverse, les entreprises manquent généralement de processus et de politiques de renforcement formels et systématiques. Pourtant, les équipes de sécurité doivent disposer des moyens nécessaires pour évaluer les risques ainsi que pour trier et remédier rapidement à ces erreurs, y compris les nouveaux bugs dangereux tels que EternalDarkness, sans que les opérations informatiques - et a fortiori celles de l'entreprise - soient perturbées. Des entreprises comme Bitdefender règlent ce problème en intégrant l'analyse des risques de configuration des endpoints au cœur de leurs offres et en donnant aux équipes de sécurité la visibilité et les outils de remédiation automatique dont elles ont besoin pour diluer les risques de cybersécurité.

La plupart des plateformes de protection des endpoints ne peuvent pas évaluer les risques associés aux mauvaises configurations, tandis que les équipes de sécurité sont submergées par des tâches réactives et répétitives, telles que la gestion des vulnérabilités, le tri des incidents et l'application de correctifs. Bitdefender a introduit l'analyse des risques associés aux endpoints au cœur de sa plateforme GravityZone de protection. L'analyse des risques associés aux endpoints permet aux administrateurs de réduire la surface d'attaque, en limitant les éventuelles compromissions et en offrant une visibilité sur les risques associés aux mauvaises configurations. Bitdefender GravityZone fournit une gestion des risques associés aux endpoints et aux humains, des outils de prévention et de protection et un EDR complet, le tout via un seul agent et une seule console. Plus d'informations **ICI**.

11 https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A6-Security_Misconfiguration
12 https://www.cisecurity.org/cis-benchmarks/
13 https://enhancedreports.com/bitdefender/6371/index.html?__hssc=27765283.2.1581574751226&__hstc=27765283.5b81ba1a3a40b54efa99bccbfcefee93.1575920737386.1581551172637.1581574751226.34&__hsfp=3054740584&hsCtaTracking=e1b1b274-49ff-4a9b-8a5b-bda8fabd0e78%7C3ed220b4-5356-4029-ac55-348a61137e6c

Pourquoi Bitdefender

Au service de nos clients

Bitdefender propose des solutions et services pour les petites, moyennes et grandes entreprises, les prestataires et les intégrateurs de technologie. Nous sommes fiers de la confiance que nous portent entre autres **RG System, Groupe SNEF, Yamaha Motors, TUI ou encore** Mentor Graphics.

Leader dans le premier rapport Forrester Wave™ sur la sécurité des charges de travail dans le cloud.

Recommandé dans le NSS Labs AEP Group Test de NSS Labs

Trophée « SC Media Industry Innovator Award » pour Bitdefender Hypervisor Introspection, 2 ans d'affilée

Gartner® Representative Vendor of Cloud-Workload Protection Platforms

Dédiés à plus de 20 000 partenaires du monde entier

Bitdefender a une stratégie commerciale 100% orientée channel et partage sa réussite avec des dizaines de milliers de revendeurs et distributeurs dans le monde entier.

Partenaire 5 étoiles selon CRN, pendant 4 années consécutives. Présent dans la « Security 100 List » de CRN. CRN Cloud Partner, pour la 2e année consécutive

Intégration dans le plus grand nombre de solutions MSP sur le marché

3 programmes partenaires Bitdefender - pour que tous nos partenaires– revendeurs, prestataires de services et hybrides– se concentrent sur la vente les solutions Bitdefender qui correspondent à leur propre spécialisation

Acteur reconnu des autorités

Bitdefender est fier d'être le partenaire technologique de grands noms de la virtualisation et contribue au développement d'écosystèmes sécurisés avec **VMware, Nutanix, Citrix, Linux Foundation, Microsoft, AWS ou encore Pivotal.**

Grâce à son équipe R&D, Bitdefender est également activement engagé dans la lutte contre le cybercrime avec des agences nationales telles que le FBI et Europol, dans des initiatives telles que NoMoreRansom et TechAccord. Depuis 2019, Bitdefender est également fier de faire partie de la CVE Numbering Authority, dans le cadre du partenariat MITRE.

RECONNU PAR LES ANALYSTES ET ORGANISMES DE TESTS INDÉPENDANTS

ALLIANCES TECHNOLOGIQUES

Bitdefender®

Création en 2001, Roumanie
Nombre d'employés : plus de 1800

Siège
Enterprise HQ - Santa Clara, CA, États-Unis
Technology HQ - Bucarest, Roumanie

BUREAUX DANS LE MONDE
USA & Canada : Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europe : Copenhague, DANEMARK | Paris, FRANCE | Munich, ALLEMAGNE | Milan, ITALIE | Bucarest, Iasi, Cluj, Timisoara, ROUMANIE | Barcelone, ESPAGNE | Dubai, UAE | Londres, ROYAUME-UNI | La Haye, PAYS-BAS
Australie : Sydney, Melbourne

SOUS LE SIGNE DU LOUP

La sécurité des données est un domaine où seuls l'ingéniosité, la vision la plus claire, l'esprit le plus vif et la plus grande perspicacité permettent de gagner dans un contexte qui ne tolère aucune erreur. Notre travail consiste à gagner mille fois sur mille, un million de fois sur un million, et à chaque fois que nécessaire.

Et c'est ce que nous faisons. Nous surpassons les standards de l'industrie, non seulement parce que nous avons la vision la plus claire, l'esprit le plus vif et la meilleure perspicacité, mais aussi parce que nous avons une longueur d'avance sur tous les autres acteurs, qu'il s'agisse des cybercriminels ou de nos confrères experts en cybersécurité. Nous puisons dans le **loup-dragon**, symbole des guerriers roumains au temps des Daces, son intuition, sa force, son agilité et sa clairvoyance, pour vous prémunir contre tous les dangers cachés dans les arcanes du monde numérique.

Nous sommes le loup-dragon et nous utilisons son super pouvoir au cœur de tous nos produits et solutions qui changent la donne.

Bitdefender-PR-Whitepaper-TopSSS-creat1469-fr_FR
02/05/21February 5, 2021 5:52 pm02/05/21