BeyondTrust

2022 Microsoft Vulnerabilities Report

Des progrès contrastés et des vulnérabilités persistantes

BeyondTrust

SOMMAIRE

RÉSUMÉ

Cette neuvième édition annuelle du Microsoft Vulnerabilities Report propose une analyse des différentes catégories de vulnérabilités de l'écosystème Microsoft.

Depuis toujours, ce rapport propose une rétrospective annuelle des vulnérabilités constatées des plateformes et des produits Microsoft et démontre combien il est déterminant de supprimer les droits admins pour réduire les risques.

En novembre 2020, Microsoft a annoncé l'intention de changer le format de reporting des vulnérabilités dans son Microsoft Security Update Guide.

Ainsi, le rapport est désormais au format **CVSS (Common Vulnerability Scoring System)**. Ce format comporte des avantages, comme la création d'une parité et d'une possibilité de comparaison avec les rapports de tiers sur des bugs, mais il crée également des problèmes de visibilité que nous détaillerons.

Comme pour les éditions précédentes, les conclusions de cette année vous aideront à mieux comprendre les risques et savoir comment vous en prémunir dans l'écosystème Microsoft.

Conclusions et faits marquants

Après une forte progression sur 5 ans, le nombre total des vulnérabilités Microsoft signalées a chuté de 5% en 2021.

Cependant, ce n'est pas le nombre des vulnérabilités qui compte mais **leur impact potentiel.**

Est-ce que les vulnérabilités de 2021 exposent à davantage de risques et un plus large impact que les années précédentes ?

1. Pour la seconde année consécutive, **l'élévation de privilèges demeure la catégorie de vulnérabilités n°1** pour le premier éditeur mondial et le 2nd plus grand fournisseur de services cloud.

2. La lecture du rapport CVSS de Microsoft ne permet plus de savoir exactement combien de vulnérabilités auraient pu être évitées par la suppression des droits admin.
Spoiler: le problème des excès de privilèges perdure.

Partant de l'habituelle ventilation des données, nous allons examiner comment ces vulnérabilités tendancielles et l'adoption de solutions de sécurité du cloud devraient influencer notre approche de la cybersécurité et de la gestion des risques en 2022 et au-delà. Ce rapport recense également les failles de sécurité CVE les plus importantes en 2021 (score de sévérité CVSS supérieur à 9.0), il explique comment les cybercriminels s'en saisissent et comment faire pour s'en prémunir ou les réduire. Quelques-uns des plus grands experts mondiaux de la cybersécurité viendront éclairer les conclusions du rapport et partager leur vision de la gestion des risques dans l'actuel contexte de cybermenaces.

Cette édition est unique en son genre et constitue une lecture essentielle pour les professionnels de la sécurité du monde entier.

Données clés

L'élévation de privilèges demeure la catégorie de **vulnérabilités n°1** pour la seconde année consécutive, représentant 49% de toutes les vulnérabilités en 2021.

ENTRE 2015 ET 2020

la suppression des droits admin **aurait pu permettre d'éliminer 75% des vulnérabilités critiques en moyenne.**

En l'absence de données pour 2021 (pour cause de nouveau format de reporting Microsoft), les entreprises ne doivent pas sous-estimer le potentiel de réduction des risques de la suppression des droits admin.

BAISSE DE 47% de vulnérabilités critiques par rapport à l'année précédente, *niveau le plus bas historiquement*

349 vulnérabilités dans IE et Edge, *un record*

40% DE VULNÉRABILITÉS Windows en moins par rapport à 2021

BAISSE DE 50% de vulnérabilités critiques dans Windows Server comparativement à 2021

Adoption par Microsoft du format standard CVSS

Depuis l'e-mail Trustworthy Computing adressé en 2002 par Bill Gates à l'ensemble des salariés à plein temps de Microsoft, Microsoft n'a cessé d'œuvrer pour plus de sécurité et de confidentialité. En effet, dans les années qui ont suivi l'engagement Trustworthy Computing (TWC), Microsoft s'est efforcé de ne proposer que des produits et services intrinsèquement sécurisés et fiables avec des contrôles de sécurité et de la vie privée.

Il y a eu des loupés, il faut le reconnaître (oui, Windows 10, c'est de toi que l'on parle). Depuis le lancement de Patch Tuesday en octobre 2003, Microsoft fournit des patchs ou correctifs de sécurité pour la mise à jour de ses logiciels.

Jusqu'en novembre 2020, Microsoft partageait ses mises à jour de sécurité CVE via le portail Security Update Guide. L'ancien format de reporting proposait un résumé pour chaque vulnérabilité signalée.

Les professionnels de sécurité pouvaient en déduire si une vulnérabilité donnée (surtout les critiques) allait pouvoir être atténuée par la suppression des droits admins de l'utilisateur.

Parfois, Microsoft indiquait :

- *Les clients/utilisateurs dont les comptes sont configurés avec peu de droits sur les systèmes pourraient être moins impactés que les utilisateurs détenteurs de droits admins*
- *Si l'utilisateur se connecte avec des droits admins, le risque existe qu'un agresseur prenne le contrôle d'un système affecté*

Maintenant que Microsoft est passé au format Common Vulnerability Scoring System (CVSS), il est plus facile de recouper les vulnérabilités signalées avec les bugs de tiers.

L'analyse s'en trouve simplifiée.

D'un autre côté, on perd la possibilité de déterminer l'impact des droits admins sur les vulnérabilités critiques.

Or, non seulement les risques d'accès excessivement privilégiés demeurent, mais les vecteurs d'attaque usant de privilèges augmentent avec l'expansion du cloud.

Ce n'est donc pas parce que les statistiques sur les droits admins sont absentes de l'édition de cette année, du fait du seul changement de format, que les entreprises doivent négliger la suppression des droits admins, bien au contraire. La suppression des droits admins est un élément clé de toute stratégie fondée sur le moindre privilège ainsi que d'une politique zero trust.

Qu'est-ce que CVSS ?

VULNÉRABILITÉ COURANTE SYSTÈME D'ÉVALUATION

Le format CVSS (Common Vulnerability Scoring System) capture les principales caractéristiques d'une vulnérabilité et produit un score compris entre 0 et 10 de la sévérité d'une vulnérabilité.

Ce système de notation a beau être standard, il ne permet pas aux chercheurs en sécurité ni aux clients de savoir précisément quelles vulnérabilités auraient pu être atténuées par la suppression des droits admins des utilisateurs.

Il est important de considérer que, lors de la notation des vulnérabilités, il ne faut pas se fier exclusivement au score de base CVSS des fournisseurs pour hiérarchiser les risques et les mesures correctives.

Chaque organisation doit appliquer des métriques propres à son environnement pour exprimer le niveau de risque la concernant. Voir les consignes à ce sujet sur le site web NIST.

FAIBLE	MOYENNE	IMPORTANTE	CRITIQUE
0.1 - 3.9	4.0 - 6.9	7.0 - 8.9	9.0 - 10.0

Rétrospective sur six ans

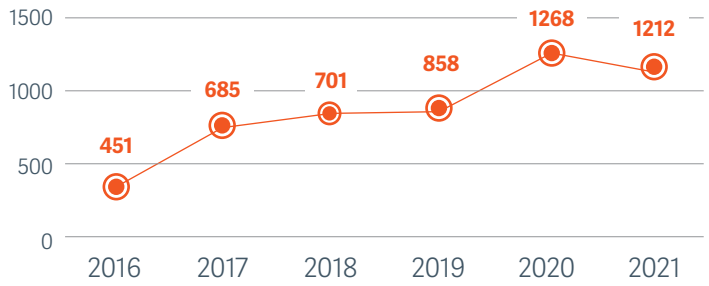
Avant que nous analysions davantage les vulnérabilités Microsoft pour l'année 2021, faisons un point sur les tendances constatées ces dernières années.

2016 - 2020

Entre 2016 et 2020, les vulnérabilités Microsoft ont plus que doublé.

Cependant en 2021, pour la première fois depuis la première publication du rapport, les vulnérabilités Microsoft ont diminué (-5%), passant de 1268 en 2020 à 1212 en 2021.

Nombre total de vulnérabilités Microsoft (2016 - 2021)



2019 - 2020

C'est entre 2019 et 2020 que l'augmentation des vulnérabilités Microsoft a été la plus forte (+48%).

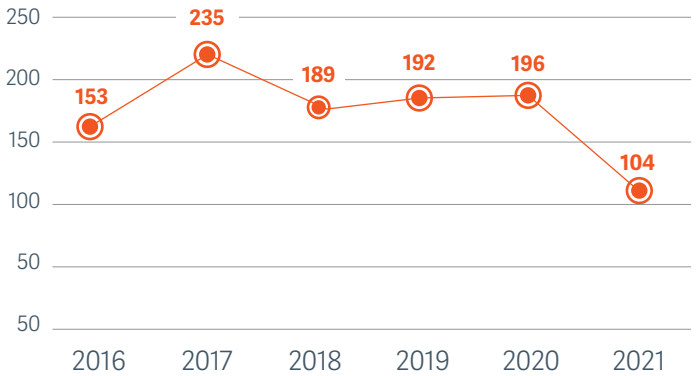
Le contexte de la pandémie a offert davantage d'occasions aux cybercriminels. L'adoption massive du télétravail et la forte accélération des initiatives de transformation digitale ont créé un nombre inédit de failles de sécurité différentes que les agresseurs ne se sont pas faits prier pour exploiter.

2020 - 2021

La vague de vulnérabilités a atteint un sommet en 2020, puis a légèrement reculé en 2021.

La différence la plus frappante que nous avons pu observer entre 2020 et 2021 est la forte diminution des vulnérabilités critiques, passant de 196 en 2020 à 104 en 2021. Cette baisse de 47% des vulnérabilités critiques depuis 2020 correspond au nombre le plus bas jamais relevé.

Vulnérabilités critiques de Microsoft (2016 - 2021)



Catégories de vulnérabilités

Chaque Bulletin de sécurité Microsoft se compose d'une ou de plusieurs vulnérabilités, concernant un ou plusieurs produits Microsoft.

Microsoft regroupe généralement les vulnérabilités dans les catégories suivantes : Exécution de code à distance, Élévation de privilèges, Contournement de sécurité, Falsification, Divulgation d'information, Déni de service et Usurpation.

Depuis la première édition du rapport en 2013 jusqu'en 2019, l'Exécution de code à distance est la catégorie comptant le plus de vulnérabilités.

Cependant en 2020, la donne a changé brutalement avec une explosion des vulnérabilités de la catégorie Élévation de privilèges, loin devant les autres catégories. De même, en 2021, les vulnérabilités de la catégorie Élévation de privilèges ont dominé les autres catégories.

Catégories de vulnérabilités Microsoft (2016 - 2021)

	2021	2020	2019	2018	2017	2016
Exécution de code à distance	326	345	323	292	301	269
Élévation de privilèges	588	559	198	145	90	114
Divulgation d'information	129	179	177	153	193	102
Déni de service	55	46	52	29	43	0
Usurpation	66	104	63	20	16	12
Falsification	3	7	8	8	1	0
Contournement de sécurité	44	30	38	20	41	26

Les vulnérabilités de la catégorie Élévation de privilèges prennent la tête

Cette explosion du nombre des vulnérabilités de type Élévation de privilèges peut s'expliquer par deux raisons :

1. À présent que les entreprises observent les bonnes pratiques de sécurité et suppriment les droits admins des utilisateurs, les acteurs malveillants cherchent à acquérir des privilèges autrement. Faute d'accès aisé à des utilisateurs ayant des droits admins locaux, ils ont cherché à obtenir des privilèges plus élevés utilisables pour compromettre des systèmes, voler des identifiants et progresser latéralement.
2. La surface d'attaque de plus en plus grande, du fait des systèmes et applications cloud, fait que les privilèges élevés séduisent n'importe quel acteur malveillant. Les mesures de sécurité pour gérer ces privilèges dynamiques, et parfois éphémères, au sein des environnements cloud, hybrides et multicloud sont généralement insuffisamment matures.

On constate le recul de plusieurs catégories de vulnérabilités mais cela ne fait que masquer les failles.

Le nombre des vulnérabilités d'autres catégories, comme celles de corruption de mémoire, de débordement et d'attaque sur les éléments dynamiques ou XSS (cross-site scripting), a chuté pour tous les produits Microsoft de 2020 à 2021, avec 215 vulnérabilités en moins au total.

C'est une excellente nouvelle pour la plupart des environnements IT. Toutefois, on ne sait pas expliquer le pourquoi de cette baisse du nombre de vulnérabilités. La diminution s'explique-t-elle par : A. des meilleures pratiques de sécurité et de codage, B. la fin de vie de produits comme Windows 7, ou C. la migration de services dans le cloud ? C'est un peu des trois.

Les anciens logiciels (comme XP et Windows 7) ne sont pas aussi sécurisés et surveillés que les produits et services plus récents. Les efforts de test et de formation sur ces anciennes plateformes ont été abandonnés. Microsoft a effectivement développé des solutions avec moins de failles et veillé à identifier et corriger proactivement les vulnérabilités dans les services cloud sans qu'il faille les faire remonter. Ces efforts promettent de réduire grandement le nombre des vulnérabilités signalées.

À retenir

- Assurez-vous de ne pas conserver de logiciels obsolètes dans votre environnement.
- Le cloud peut être très efficace pour réduire les risques en déchargeant votre équipe de sécurité informatique des correctifs.

Vulnérabilités Exécution de code à distance – Résultats contrastés

Le nombre des vulnérabilités Exécution de code à distance a légèrement baissé en 2021, pour retrouver le niveau de 2019.

Sur les 326 vulnérabilités d'exécution de code à distance signalées en 2021, 35 avaient un score CVSS d'au moins 9.0, selon CVEDetails.com.

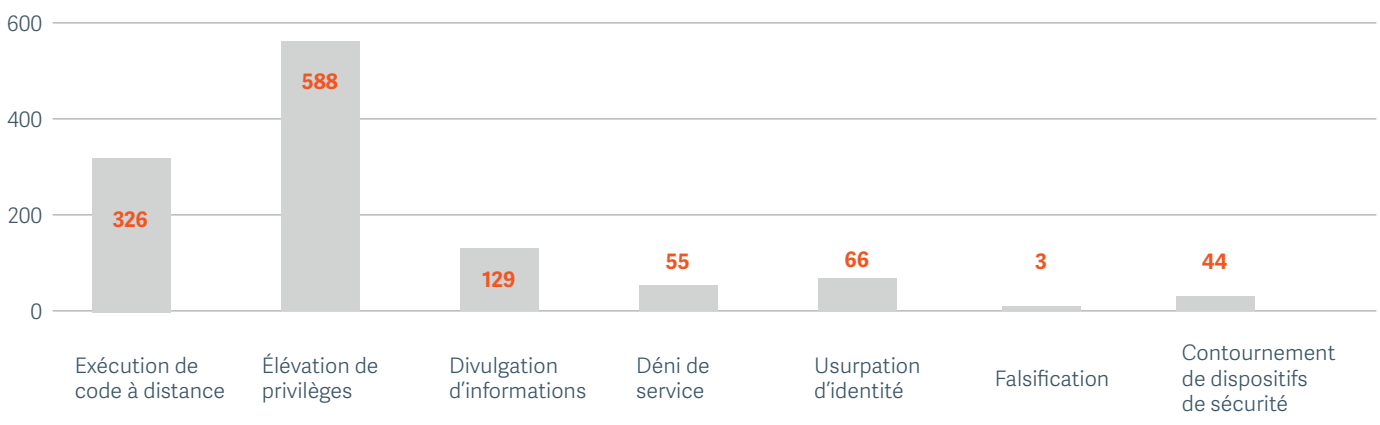
Certaines concernaient l'espace utilisateur, d'autres les applications et le système d'exploitation directement, mais toutes pouvaient être exploitées sans intervention.

Si vous envisagez le concept de moindre privilège pour les utilisateurs et les applications (y compris les comptes de service), un acteur exploitant ces vulnérabilités ne pourra pas aller au-delà des privilèges accordés à l'utilisateur ou à l'application.

Sans les informations des résumés comme pour les années précédentes, savoir si l'élévation des privilèges est seulement possible tient de la spéculation et nécessitera des tests de pénétration.

Avec ce type de risque, il ne s'agit plus de savoir si un exploit existe mais plutôt quand il sera rendu public. Autant dire que toutes les vulnérabilités ou presque avec un score CVSS de 10.0 (9 sur 308) se retrouveront dans les scripts et outils d'évaluation des tests de pénétration. Face à ce type de risque, la meilleure prévention consiste à instaurer le moindre privilège à l'échelle de l'environnement.

Catégories de vulnérabilités Microsoft (2021)



Vulnérabilités par produit

Internet Explorer & Edge
Windows
Microsoft Office
Windows Server
Azure & Dynamics 365

Vulnérabilités d'Internet Explorer et Edge

Depuis janvier 2020, le navigateur Microsoft Edge utilise un moteur Chromium, si bien que Google Chrome et Edge pourraient désormais avoir les mêmes failles.

Ainsi, il ne reste aucun navigateur mainstream « sûr » pour combler les failles de Edge.

Comme Microsoft Edge s'appuie sur la technologie Google Chromium, les vulnérabilités identifiées dans le navigateur Chrome de Google pourraient se retrouver dans Microsoft Edge et devoir être corrigées.

En 2021, Google Chrome comptait 308 vulnérabilités, selon CVEDetails.com. La bonne nouvelle est que 4 vulnérabilités seulement de Google Chrome étaient considérées critiques. Cependant le total n'indique pas que Microsoft ait hérité de failles de Google.

Internet Explorer versions 9 and 11

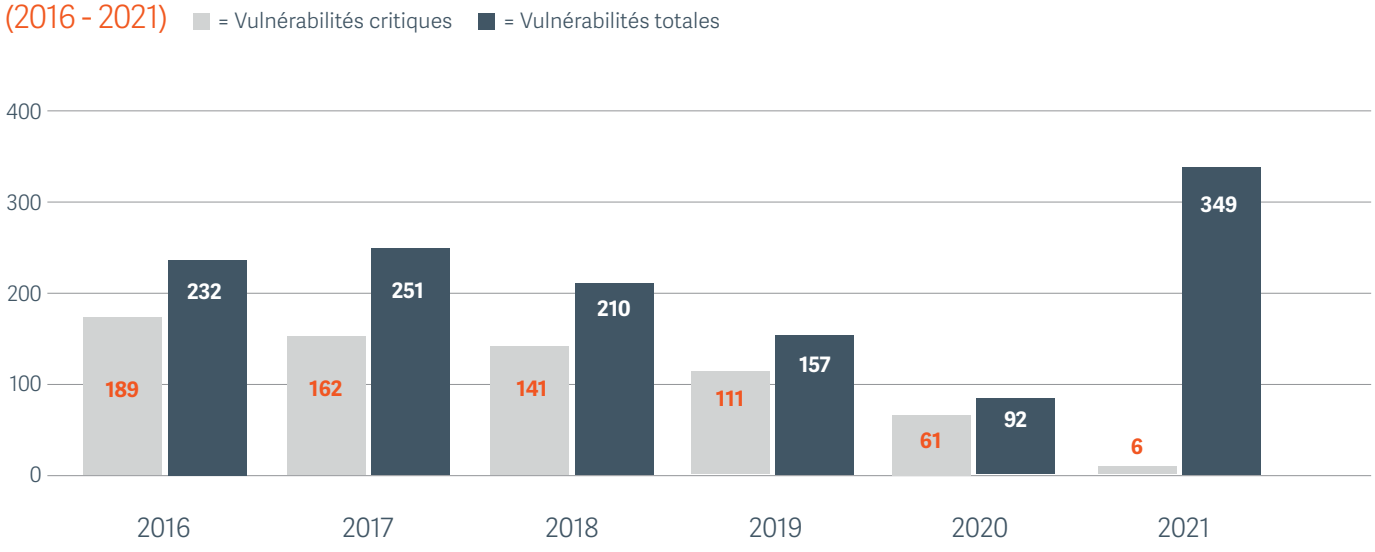
Nous pensons que **trois facteurs clés** sont essentiellement responsables de la brusque augmentation des vulnérabilités de Edge.

1. **Consolidation du marché des navigateurs, maintenant que Edge passe sur une base Chromium partagée.** Avec le déclassement des navigateurs Internet Explorer, les cybercriminels se focalisent sur Edge et Chrome. La dépréciation de plug-ins souvent exploités, comme Adobe Flash, accélère encore cette tendance. Plutôt que de viser les plug-ins dépréciés, ce sont les navigateurs qui sont ciblés.

2. **Google a accru la transparence en matière de signalement des vulnérabilités et propose désormais des incitations financières plus attrayantes pour les signaler.** En 2021, Google a versé près de 3,1 millions de dollars de récompenses pour les bugs signalés dans les rapports de vulnérabilités Chrome.

3. **Le nombre des vulnérabilités critiques Microsoft a diminué là où le nombre total des vulnérabilités a augmenté fortement.** Ceci s'explique par les améliorations de l'architecture de sécurité du navigateur. En effet, les cybercriminels doivent enchaîner plusieurs exploits pour tromper le navigateur et pouvoir exécuter le code sur le système sous-jacent. Auparavant, un seul exploit pouvait suffire pour compromettre un système. Désormais, il faut trouver plusieurs vulnérabilités non critiques dans l'espoir de pouvoir les enchaîner pour perpétrer une attaque.

Vulnérabilités d'Internet Explorer et Edge (2016 - 2021)



Vulnérabilités Windows

En 2020, nous avons constaté 907 vulnérabilités, un record, dans l'ensemble des systèmes d'exploitation Windows 7, Windows RT, Windows 8/8.1 et Windows 10. En 2021, le nombre des vulnérabilités des OS Windows a chuté à 507.

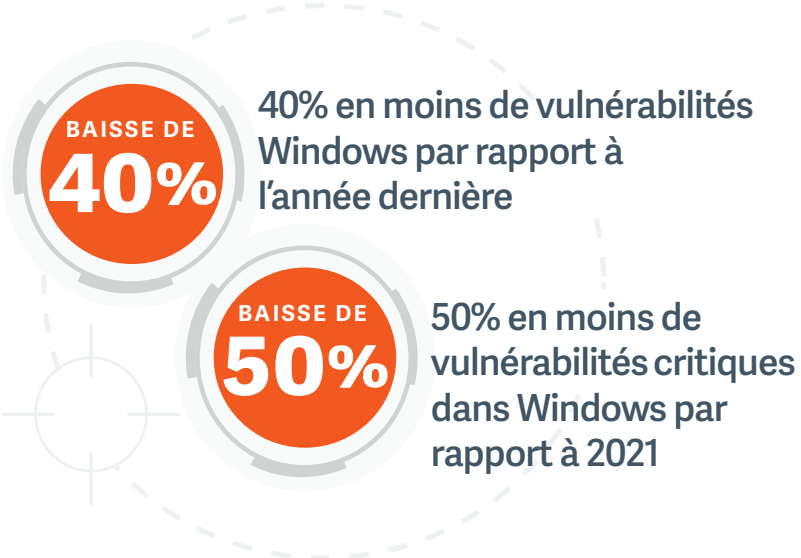
À sa sortie, Windows 10 était prétendument l'OS Windows le plus sûr. Pourtant, on a encore recensé 60 vulnérabilités critiques de Windows 10 l'an dernier. Ceci dit, le nombre des vulnérabilités critiques Windows n'a cessé de diminuer. Le nombre total des vulnérabilités Windows est descendu légèrement en-dessous des niveaux d'avant la pandémie.

Microsoft continue de renforcer son architecture de sécurité avec Windows 11 et d'améliorer ses procédures de mise à jour, aussi pouvons-nous espérer une diminution du nombre des vulnérabilités et des fenêtres de temps où elles risquent d'être exploitées.

Cependant avec tous les systèmes d'exploitation en fin de vie qui sont toujours utilisés en production (ce qui nous amène à Windows XP), on peut s'interroger sur la capacité réelle à faire baisser encore les vulnérabilités Windows. La réponse est oui, mais cette diminution se fera dans des conditions indésirables.

En effet, à l'avenir, il est possible que Microsoft ne recense plus les failles et ne propose plus de patchs pour les produits en fin de vie. Or, il est possible que de nouvelles vulnérabilités perdurent sur ces systèmes d'exploitation en fin de vie. Les utilisateurs ne sauront pas qu'elles existent, sauf contrôles en ce sens, ce qui crée un nouvel angle mort.

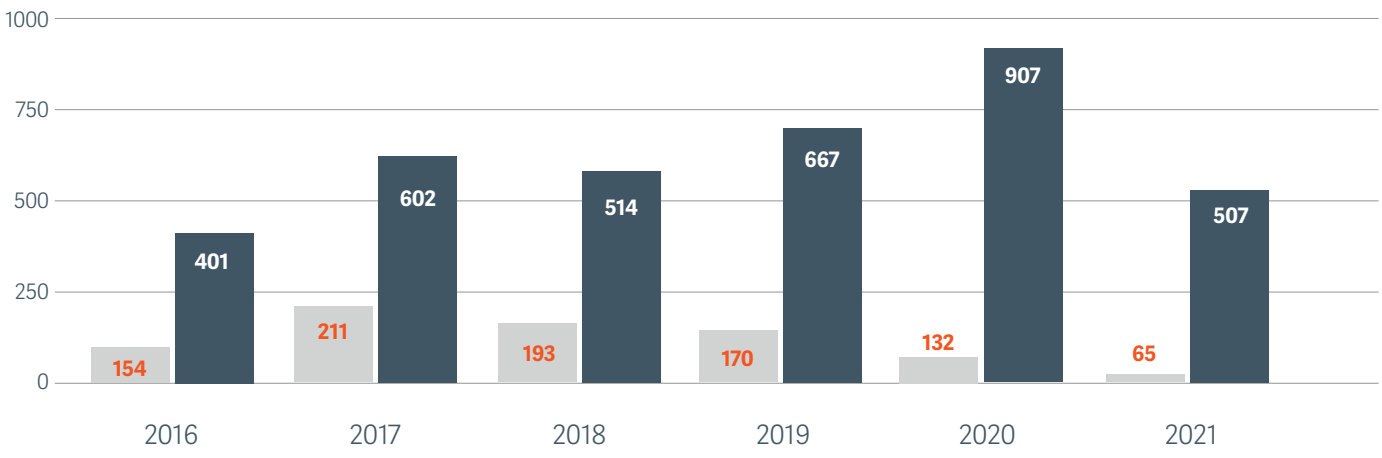
Microsoft continuera de documenter les vulnérabilités des solutions prises en charge. Il est possible que de meilleures pratiques de programmation et de nouveaux contrôles de sécurité se traduisent par une diminution des vulnérabilités. A l'inverse, des solutions en fin de vie mais toujours prises en charge pourraient voir fleurir de très grands nombres de nouvelles vulnérabilités.



Cette baisse de moitié des vulnérabilités critiques Windows sur les 5 dernières années montre combien les investissements dans la sécurité payent pour Microsoft et les utilisateurs de Windows.

L'intensification des efforts de Microsoft pour mettre à jour Windows se traduit également par une réduction des fenêtres de temps pendant lesquelles les systèmes sont exposés. Cette conjugaison de la diminution des vulnérabilités avec l'accélération des correctifs rendus disponibles est une excellente nouvelle après les pressions subies en 2020.

Vulnérabilités Windows (2016 - 2021)



Vulnérabilités Microsoft Office

On enregistre une baisse continue des vulnérabilités critiques dans Microsoft Office (versions 2010, 2013, 2016, 2019) depuis cinq ans.

66 vulnérabilités Microsoft Office au total en 2021

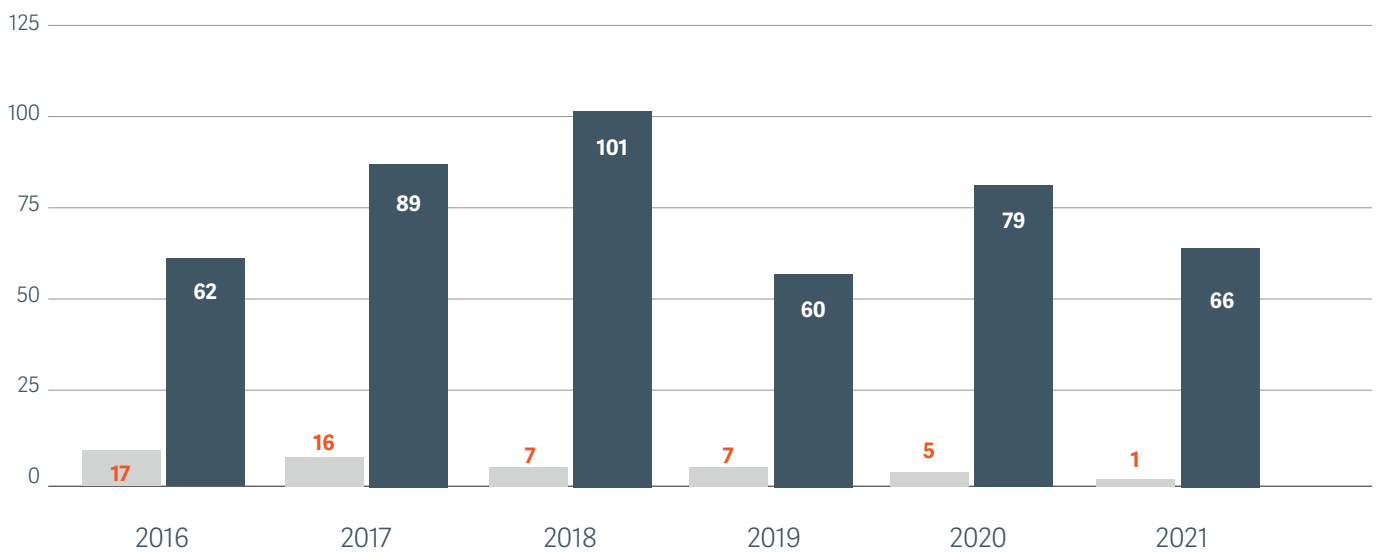
1 seule vulnérabilité critique

En 2021, 66 vulnérabilités ont été identifiées dans les produits Office, mais 1 seule critique.

Cette réduction du nombre total de vulnérabilités et la quasi-élimination des vulnérabilités critiques sont de bonnes nouvelles pour l'application phare de Microsoft. Cependant, les cybercriminels continuent d'exploiter activement des vulnérabilités connues de longue date. La vulnérabilité CVE-2017-11882 (également connue comme bug Equation Editor) a été exploitée de nombreuses fois en 2021, alors même qu'un correctif est disponible depuis novembre 2017. Ce bug permet d'exécuter du code, généralement pour installer un outil RAT (Remote Access Tool) d'accès à distance.

Les applications Office sont une cible courante des campagnes de phishing. Malheureusement, certaines entreprises ne déploient pas les correctifs d'applications aussi souvent que les patchs des systèmes d'exploitation. De nombreux kits de malwares contiennent des exploits Office cumulés en 10 ans, dans l'objectif de trouver un système vulnérable. Ces kits et stratégies s'avèrent très souvent payants !

Vulnérabilités Microsoft Office (2016 - 2021)



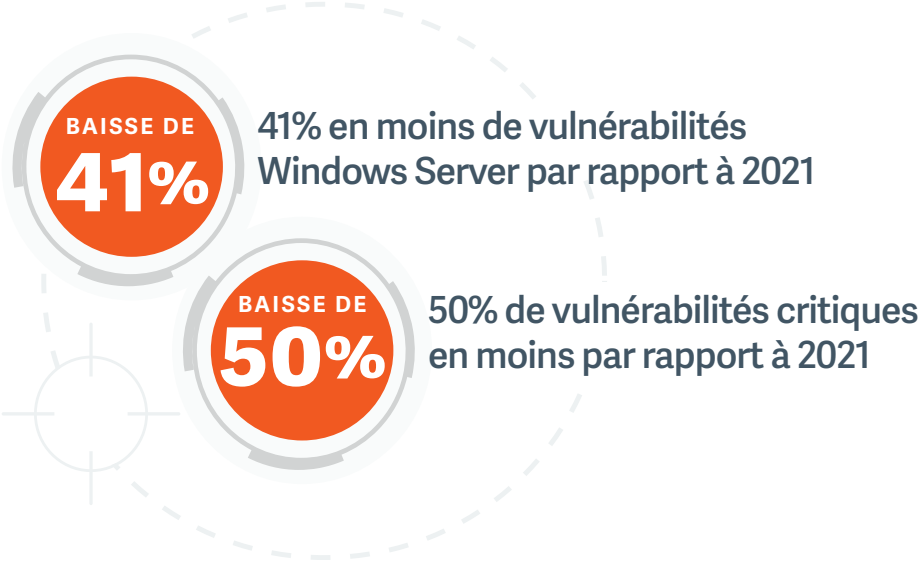
Vulnérabilités Windows Server

Microsoft a parcouru un long chemin depuis que le CTO de BeyondTrust, Marc Maiffret, a identifié le malware Code Red Worm en 2001 et a depuis fortement incité Microsoft à améliorer ses pratiques de sécurité et sa gestion opportune des vulnérabilités.

Jusque-là, la sécurité était largement négligée. Les choses ont commencé à bouger quand les effets des attaques se sont fait sentir sur les chiffres, la continuité des opérations ou les parts de marché.

Il a fallu à Microsoft plusieurs générations de Windows Server pour parvenir à une version intrinsèquement sûre. Les dernières versions de Windows Server éliminent des menaces identifiées jusqu'à 20 ans auparavant. Elles comportent moins de vulnérabilités que jamais même s'il s'agit des bases de code les plus importantes d'un système d'exploitation.

Les vulnérabilités de Windows Server ont atteint leur plus bas niveau depuis 2018, de 902 en 2020 à 531 en 2021, soit une diminution de 41%. Les vulnérabilités critiques de Windows Server ont également diminué de 50% l'an dernier, atteignant leur plus bas niveau depuis 2015.



Vulnérabilités Azure et Dynamics 365

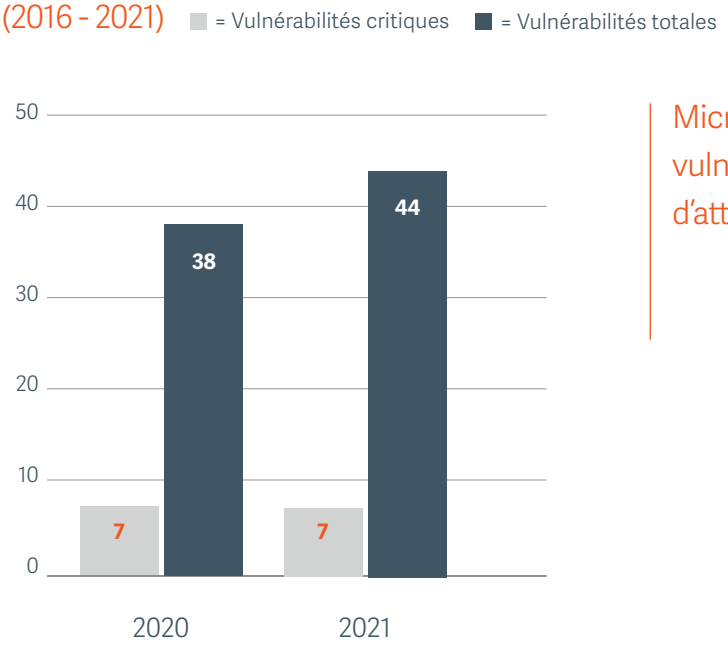
En 2014, dans son premier e-mail aux employés en qualité de nouveau CEO de Microsoft, Sattya Nadella a exposé sa vision d'un monde mobile-first et cloud-first, avant de la rendre publique.

La qualité et la sécurité du code dans le cloud est une priorité de longue date pour Microsoft.

Au vu de la diversité des mises en œuvre d'Azure et de Dynamics 365, même des erreurs de configuration basiques pourraient créer une vulnérabilité ou une faiblesse. Microsoft prend des mesures pour que les vulnérabilités ne soient pas le principal vecteur d'attaque de ces solutions cloud.

Les vulnérabilités dans Azure et Dynamics 365 demeurent peu nombreuses depuis quelques années. En 2021, 30 vulnérabilités Azure ont été détectées et 5 critiques. En 2020, Dynamics 365 comptait 6 vulnérabilités critiques mais ce chiffre est tombé à 2 l'an dernier.

Vulnérabilités Azure et Dynamics 365 (2016 - 2021)



Microsoft prend des mesures pour que les vulnérabilités ne soient pas le principal vecteur d'attaque de Azure et Dynamics 365.

Les vulnérabilités Microsoft diminuent, mais il convient de rester prudents

C'est la première fois en neuf ans de publication de ce rapport que le nombre total de vulnérabilités rapportées dans les produits et les plateformes Microsoft diminue (-5%).

Depuis 2016, la tendance à l'augmentation des vulnérabilités Microsoft était constante. Leur nombre a atteint un record en 2020 dans le contexte de la pandémie.

Le nombre de vulnérabilités Microsoft a connu la plus forte augmentation en pourcentage jamais enregistrée entre 2019 et 2020. En 2021, le nombre total des vulnérabilités a légèrement reculé mais le paysage des vulnérabilités demeure contrasté.

Pour la deuxième fois et la deuxième année consécutive, c'est la catégorie Élévation de privilèges qui enregistre le plus de vulnérabilités. De 2013 à 2019, les vulnérabilités de la catégorie Exécution de code à distance étaient majoritaires chaque année.

L'augmentation brutale et persistante des vulnérabilités Élévation de privilèges sur deux ans s'explique par plusieurs facteurs.

Le nouveau format CVSS ne permet pas de savoir précisément en quoi la suppression des droits admin aurait pu réduire les vulnérabilités critiques de 2021 faute de résumés que Microsoft proposait jusqu'en 2020.

D'après les tendances à ce jour et ce que l'on sait de Microsoft, nous estimons que la suppression des droits admin et la mise en place du moindre privilège demeurent essentielles pour continuer de diminuer le nombre des vulnérabilités et de réduire la surface d'attaque.

Le déploiement de patchs n'est pas toujours correctement effectué, ni même recommandé selon l'environnement, aussi la suppression des droits admins est-elle la meilleure pratique pour instaurer une base de sécurité solide et réduire la surface d'attaque. Outre les initiatives de mise en conformité, la suppression des droits admins, souvent exigée par les cyber assureurs, s'inscrit dans les principes zero trust.

2015 - 2020 : la suppression des droits admins aurait pu permettre d'éliminer 75% des vulnérabilités critiques

7- IDSA study: 2021 Trends in Securing Digital Identities, IDSA, June 2021

Vulnérabilités à fort impact

L'examen des plus hauts risques d'exécution de code à distance en 2021 révèle des différences intéressantes par rapport aux années précédentes.

Voyons comment les vulnérabilités ci-dessous, toutes avec un score supérieur à 9.0, ont affecté de très nombreuses entreprises :

CVE-2021-28480 et CVE-2021-28481

Vulnérabilité Microsoft Exchange Server - Exécution de code à distance

Ces deux CVE sont des vulnérabilités de Microsoft Exchange Server en amont de l'authentification. L'acteur malveillant n'a pas besoin de s'authentifier auprès de Microsoft Exchange Server pour exploiter la vulnérabilité. Ceci est bien documenté par Tenable.

Pour exploiter ces vulnérabilités, le cybercriminel procède à une reconnaissance des cibles et adresse au serveur des requêtes spécifiquement pensées pour l'exploiter. Soit l'agresseur dispose d'un accès sur site, soit le serveur est hébergé sur le web. Les entreprises conscientes de ces vulnérabilités ont accéléré leur migration d'Exchange sur site pour Microsoft 365 dans le cloud.

CVE-2021-34473, CVE-2021-26894, CVE-2021-26895 et CVE-2021-26897

Vulnérabilité Windows DNS Server - Exécution de code à distance

Ces quatre vulnérabilités sont exploitables sur les serveurs Microsoft Windows qui fournissent des services DNS. Aucune authentification n'est nécessaire avant de pouvoir compromettre l'hôte.

Pour qu'un serveur DNS soit éligible, il faut que les mises à jour dynamiques soient activées. Toute entreprise fournissant des services DNS à son infrastructure peut être exposée. La dangerosité de ces vulnérabilités est telle que les entreprises ont intérêt à déployer des patchs au plus vite.

8- 2021 Trends in Securing Digital Identities. IDSA. June 2021.

CVE-2021-42311 et CVE-2021-42313

Vulnérabilité Microsoft Defender - Exécution de code à distance IoT

Ces vulnérabilités visent la solution de sécurité de Microsoft pour l'IoT (Internet des objets), mais l'exploitation de cette solution de sécurité peut se faire sur site ou dans le cloud.

Les deux vulnérabilités se basent sur de l'injection SQL. Elles permettent à un acteur malveillant distant d'exécuter arbitrairement du code sans authentification préalable.

Comme le montrent SentinelOne et SecurityWeek, il est possible d'exécuter du code avec des privilèges root, si le script est bien conçu. Cette faille prouve l'existence d'attaques d'élévation de privilèges, même si celles-ci ne sont plus rapportées par Microsoft d'une façon lisible et quantifiable.

La plupart des vulnérabilités à fort impact précitées font prendre conscience des risques pour la technologie sur site et suggèrent de migrer dans le cloud pour plus de sécurité.

Cet article de CSO Online contient de précieuses informations et offre des perspectives supplémentaires sur les vulnérabilités Microsoft de 2021.

Qu'en disent les experts ?

Sami Laiho
Senior Technical Fellow, MVP

Russell Smith
Editorial Director, Petri IT Knowledgebase

Paula Januszkiewicz
Security Expert & Penetration Tester

James Maude
Lead Cyber Security Researcher, BeyondTrust

Morey Haber
Chief Security Officer, BeyondTrust

Senior Technical Fellow, MVP
samilaiho.com
@samilaiho Twitter

Sami Laiho

Il semble que nous ayons atteint un plateau en ce qui concerne le nombre de vulnérabilités rapportées chaque année. En 2020 et 2021, nous sommes autour de 100 vulnérabilités Microsoft par mois. Même si nous enregistrons pour la première fois une diminution du nombre de vulnérabilités, elle n'est que de 5%. Avec le passage de Microsoft au format CVSS (Common Vulnerability Scoring System), il n'est pas aussi simple de savoir quelles vulnérabilités auraient pu être évitées par la suppression des droits admin. Nous constatons par contre qu'une vulnérabilité sur deux concerne l'élévation de privilèges. C'est donc là que nous devons intervenir pour contrer l'ennemi.

J'ai mené des centaines de projets en ce sens et pour avoir supprimé plus d'1 million de droits admin locaux, les résultats parlent d'eux-mêmes. Beaucoup y voient une mesure de sécurité contraignante qui leur complique la vie au travail. La meilleure stratégie consiste à les sensibiliser aux bienfaits de la suppression des droits admins, surtout en termes de productivité. Certains de mes clients ont constaté une baisse de 75% de leurs tickets auprès du service support après la suppression des droits admin. Les ordinateurs fonctionnent mieux quand ils ne sont pas exposés à l'abus de privilèges.

> « Les avantages du moindre privilège sont tels que cela fait 20 ans que je ne me connecte plus à mes propres ordinateurs comme admin. »

Après avoir supprimé les droits admins, un client américain confirme un recul de 65% des réinstallations d'ordinateurs. Un développeur peu convaincu au départ a finalement reconnu que sans droits admin, son SSD avait une durée de vie plus longue. Les avantages du moindre privilège sont tels que cela fait 20 ans que je ne me connecte plus à mes propres ordinateurs comme admin. Pour rien au monde, je ne reviendrai en arrière. Il en va de même pour mes proches et mes clients.

Editorial Director,
Petri IT Knowledgebase

Russell Smith

Microsoft a fait les frais de l'insistance des professionnels de la sécurité quant aux vulnérabilités, surtout dans les produits Windows et Office. Il s'avère que Microsoft parvient effectivement à réduire le nombre des vulnérabilités critiques de ses principaux logiciels et avec une forte marge.

Ce n'est pas une mince affaire sachant que Microsoft continue de proposer le support d'anciennes fonctionnalités aux entreprises, si bien que sa base de code est de loin la plus importante tous systèmes d'exploitation confondus. Sachant que Windows est installé sur plus d'un milliard d'appareils, cela en fait une cible privilégiée.

En effet, contrairement aux serveurs Linux, ce milliard d'utilisateurs augmente la probabilité que des hackers compromettent l'OS au moyen des tactiques d'ingénierie sociale et de phishing.

Ces dernières années ont également marqué un tournant, puisque Microsoft s'est mis à proposer des solutions de sécurité pour ses propres produits. Le chiffre d'affaires de Microsoft dans la sécurité est passé de 10 milliards de dollars à 15 milliards de dollars en un an, entre 2021 et 2022. Parmi les investissements de Microsoft dans la sécurité, citons Microsoft 365 Defender, Azure Sentinel et les améliorations apportées à Windows et Office.

L'adoption généralisée du télétravail a aussi modifié la façon dont les entreprises gèrent Windows. Beaucoup ont investi dans Microsoft Intune, Endpoint Manager et Windows Autopilot. Ces services permettent aux entreprises de déployer des appareils à distance et mieux les gérer.

Récemment, de nouveaux services, comme Windows Autopatch pour les clients Enterprise E3, permettront aux entreprises de confier à Microsoft la gestion de fonctions de sécurité au moyen de technologies avancées comme le machine learning.

Malgré les efforts de Microsoft pour renforcer la sécurité, Windows restera une cible facile du fait de son omniprésence dans l'entreprise. Pour faire face aux nombreuses vulnérabilités, Microsoft aide pour la première fois les entreprises à gérer l'utilisation des privilèges admin dans Windows.

« Mais il s'avère que Microsoft parvient effectivement à réduire le nombre des vulnérabilités critiques de ses principaux logiciels et avec une forte marge. »

C'est une décision bienvenue et attendue de longue date. Selon les règles d'élévation, les appareils devront être gérés par Intune, la plateforme Mobile Device Management (MDM) de Microsoft. Les options de contrôle de l'utilisation des privilèges admin seront limitées par rapport aux solutions de tiers.

Comme indiqué préalablement dans ce rapport, les entreprises devront continuer à gérer l'utilisation des privilèges admin pour se protéger contre les vulnérabilités des logiciels Microsoft. J'ai toujours été en faveur des restrictions d'accès aux droits admin. Cependant, malgré l'importance de fonctionner avec des privilèges utilisateur standard pour protéger les systèmes et les données, il n'est toujours pas possible de gérer en natif dans Windows. Les entreprises doivent gérer l'accès privilégié sur les endpoints de façon suffisamment sûre et flexible pour réduire les risques tout en permettant aux employés d'effectuer leur travail.

La solution BeyondTrust demeure la meilleure pour équilibrer sécurité et utilisation pratique dans Windows.

Security Expert &
Penetration Tester
@PaulaCqure Twitter

Paula Januszkiewicz

Le 8 avril 2014, Microsoft a officiellement annoncé la fin du support du système d'exploitation Windows XP. Le 14 janvier 2020, ce fut au tour de Windows 7. Or, dans la réalité, ces deux OS tournent toujours.

Il n'est pas rare, loin de là, que des systèmes d'exploitation en fin de support soient toujours utilisés dans des infrastructures critiques et dans le secteur de la santé. D'après une étude menée par Kaspersky en 2021, près d'un quart (24%) des utilisateurs de PC continuent de faire tourner un OS Windows sans support officiel.

C'est un gros problème, surtout avec la technologie opérationnelle, dont la durée de vie est bien plus longue que celle des systèmes IT. Les systèmes OT comportent bien souvent des composants ayant 20 ou 30 ans si ce n'est plus. Et bien souvent, on omet de déployer des patchs de sécurité sur les systèmes OT. Ceci s'explique par le fait que ces systèmes doivent tourner en permanence, quasiment sans interruptions. Les mises à jour et les correctifs risqueraient de perturber la continuité des opérations.

Il y a quelques années, ne pas déployer de correctifs sur les systèmes OT posait moins de problèmes car de nombreux systèmes de contrôle industriels (et les interfaces homme-machine correspondantes) étaient conçus pour des environnements isolés. Plus récemment, surtout depuis l'instauration des mesures sanitaires, la connectivité entre les réseaux OT et IT s'est rapidement intensifiée. Les systèmes OT sont donc davantage exposés à Internet.

> « Les vulnérabilités nouvelles et connues risquent d'exposer les infrastructures critiques surtout maintenant que la distinction entre systèmes IT et OT est de plus en plus floue. »

Les infrastructures critiques ne sont donc plus protégées et utiliser d'anciens systèmes d'exploitation sans support les expose davantage. Les hackeurs peuvent déployer très rapidement des exploits publiquement disponibles. Les vulnérabilités nouvelles et connues risquent d'exposer les infrastructures critiques, surtout maintenant que la distinction entre systèmes IT et OT est de plus en plus floue.

Je suis heureuse de constater que les vulnérabilités Microsoft ont chuté de 5% en 2021. Cependant, il ne faut pas pour autant baisser la garde, les hackers guettent et la négligence pourrait bien se payer au prix fort.

Chief Security Officer,
BeyondTrust

Morey J. Haber

En tant que Chief Security Officer chez un leader de la cybersécurité comme BeyondTrust, je confirme que nous achetons des licences de solutions de sécurité comme n'importe quelle autre entreprise. Nos employés sont les premiers clients des solutions que nous développons mais aucun fournisseur de sécurité ne crée l'ensemble des solutions permettant de constituer une pile de sécurité complète. Il arrive toujours un moment où n'importe quelle entreprise doit acheter la licence d'une technologie auprès d'un tiers.

Une évaluation des risques est préconisée afin de documenter les menaces pour l'entreprise. Il suffit ensuite de classer les risques par priorité, selon qu'il faille intervenir pour apporter une modification ou une correction. Les vulnérabilités critiques sont traitées en priorité, quant à celles qui supposent l'exploitation de privilèges, la stratégie à adopter consiste à mettre en place le moindre privilège.

Nous sommes clients de nos propres solutions. Rien ne vaut la suppression des droits admins des utilisateurs et des endpoints à nos yeux. Ce faisant, vous réduisez la surface d'exposition aux risques des vulnérabilités fortes et critiques, à l'exception des attaques dont le vecteur d'attaque procède de l'élévation de privilèges. Les exploits nécessitant des privilèges ne peuvent plus s'exécuter.

Moi-même et les CSO que je côtoie, nous cherchons tous le moyen le plus efficace de réduire les risques. Parfois, nous changeons les processus, nous développons des règles, nous modifions des configurations ou nous achetons la licence d'une technologie pour faire face à la menace.

> « En supprimant les privilèges admin, vous réduisez la surface d'exposition aux risques des vulnérabilités fortes et critiques. »

Comme chaque année de nouvelles vulnérabilités critiques menacent les entreprises, nous avons pris l'habitude de déployer des patchs pour gérer le problème. Cependant, l'efficacité ne tient pas seulement à une fine gestion des vulnérabilités et des patchs. Il faut aussi anticiper et commencer à réduire les risques par la mise en place du moindre privilège dans toute l'entreprise.

Toute mesure qu'une entreprise prendra pour sortir de l'approche « scan and patch » aidera à se protéger contre les vulnérabilités d'année en année. Nous sommes convaincus que la suppression des privilèges admin est la meilleure décision qu'une entreprise puisse prendre.

Lead Cyber Security Researcher, BeyondTrust

James Maude

Cela fait 20 ans que Bill Gates a fait connaître sa vision Trustworthy Computing selon laquelle la sécurité devait être prioritaire sur l'ajout de nouvelles fonctionnalités. L'intention était de mettre la sécurité et la confiance des clients au premier plan dans l'esprit des employés et de reconstruire la réputation de l'entreprise.

« Nos logiciels devraient être intrinsèquement sûrs de sorte que nos clients n'aient jamais à s'en inquiéter »
- Bill Gates, Trustworthy Computing Memo, 2002

Cela nous fait un point commun. Un an avant, Marc Maiffret, alors jeune chercheur et désormais CTO de BeyondTrust, a découvert le malware Code Red, qui exploitait une vulnérabilité des serveurs web Microsoft IIS. Cette annonce et la révélation d'autres vulnérabilités ont ébranlé la confiance des clients et amené à des réflexions chez Microsoft qui ont conduit à adopter des pratiques de codage plus sûres et à la fameuse vision de Bill Gates.

Est ensuite venu le processus consolidé des mises à jour de sécurité, puis l'année suivante, le Patch Tuesday. C'est ainsi que nos clients ont pu gagner en visibilité et en considération et que nous compilons depuis 9 ans les données de ce rapport.

Un esprit cynique pourrait dire que les choses n'ont pas beaucoup changé puisqu'il existe encore de nouvelles vulnérabilités, mais ce rapport montre au contraire combien nous avons progressé.

Commençons par le format de reporting. Le nouveau format CVSS (Common Vulnerability Scoring System) du Guide des mises à jour de sécurité atteste de la volonté de Microsoft de se conformer aux standards de l'industrie. Les vulnérabilités de Microsoft peuvent ainsi être capturées et notées selon une procédure standard. Les entreprises apprécient cette plus grande transparence et il devient plus facile d'évaluer leur gestion des vulnérabilités et d'établir des priorités.

> « Les cybercriminels ne peuvent plus considérer qu'un utilisateur puisse avoir des droits admins locaux ou qu'un process tourne avec des privilèges. Ceci renforce la nécessité d'instaurer le moindre privilège et de déployer des patchs de sécurité. »

Cette année encore, nous constatons la diminution du nombre de vulnérabilités critiques. Et cela tient plus des investissements de Microsoft dans la sécurité que de la chance. Il est désormais bien plus difficile pour un hackeur de profiter d'une vulnérabilité dans un navigateur pour prendre le contrôle total d'un système. Il devra même enchaîner plusieurs vulnérabilités, d'où l'augmentation globale des vulnérabilités mais un moindre degré de dangerosité.

Et l'augmentation des attaques de type Élévation de privilèges peut laisser entendre que les cybercriminels n'ont plus autant accès aux privilèges. Les cybercriminels ne peuvent plus considérer qu'un utilisateur puisse avoir des droits admins locaux ou qu'un process tourne avec des privilèges. Ceci renforce la nécessité d'instaurer le moindre privilège et de déployer des patchs de sécurité.

Espérons que nos produits seront « intrinsèquement sûrs de sorte que nos clients n'aient jamais à s'en inquiéter » pour les 20 prochaines années !

Comment réduire les risques liés aux vulnérabilités Microsoft ?

Dans un monde où les vols d'identité, le phishing de mots de passe et les deepfakes sont monnaie courante, nul ne peut plus simplement faire confiance aux utilisateurs et aux systèmes.

BeyondTrust protège les identités privilégiées, dimensionne les privilèges et sécurise et audite les accès privilégiés dans toute l'entreprise.

Notre solution Endpoint Privilege Management est la meilleure et la plus efficace pour réduire les risques associés aux droits admins et aux vulnérabilités critiques de Microsoft.

Avec Endpoint Privilege Management, vous pouvez :

1. **Supprimer les privilèges excessifs des utilisateurs sur les postes** Windows, Mac, Unix, Linux et en réseau.

2. **Mettre en place rapidement le moindre privilège** en éliminant les droits admins locaux sur tous les endpoints et réduire rapidement les risques grâce à des règles Quick Start.

3. **Vous protéger des attaques de phishing, de ransomwares et de malwares** et réduire les surfaces d'attaque en attribuant des privilèges juste à temps (JIT) aux seuls scripts, applications, tâches et commandes autorisés.

4. **Assurer la conformité en supprimant** les privilèges excessifs, avec des listes d'autorisations d'applications et une piste d'audit de l'activité des utilisateurs

5. **Souscrire à des polices de cyber assurance** en remplissant les critères de suppression des droits admin, mise en place du moindre privilège, contrôle des applications et d'autres solutions de sécurité, tels qu'exigés par les cyber assureurs.

La plateforme BeyondTrust

Les solutions **Privileged Password Management** permettent d'automatiser la découverte et l'intégration de tous les comptes privilégiés, la sécurisation des accès aux identifiants privilégiés et aux secrets, ainsi que l'audit de toutes les activités privilégiées.

Les solutions **Endpoint Privilege Management** combinent gestion des privilèges et contrôle des applications pour gérer efficacement les droits admin sur les postes Windows, Mac, Unix, Linux et en réseau , sans ralentir la productivité

Les solutions **Secure Remote Access** aident les entreprises à appliquer le moindre privilège et des contrôles d'audit robustes de tous les accès des employés, fournisseurs et services d'assistance.

Les solutions **Cloud Security Management** aident les entreprises à identifier et réduire les risques liés aux autorisations et droits d'accès au cloud en environnements multicloud.

	SUR SITE	CLOUD	HYBRIDE
Beyondinsight	Identifiez | Reporting | Analyse des menaces | Connecteurs | Politique et gestion centrales		

Conclusion

Les réglementations, les standards de conformité, les meilleures pratiques de sécurité et, de plus en plus, les cyber assureurs nous incitent à identifier les dernières menaces et à les prévenir correctement. Analyser chaque année le paysage des menaces peut être utile pour mieux anticiper. Toutefois, la mise en œuvre d'un processus efficace pour faire face aux menaces et éliminer ou atténuer les vulnérabilités en temps voulu est un problème totalement différent.

Recommandations pour tenir ses objectifs de cybersécurité

Soutien de la direction

La direction doit soutenir totalement la mise en place d'un processus de réduction des risques. Il lui revient de trouver le juste équilibre entre coût du programme et les risques potentiels, tant financier que sur la réputation.

À elle également de défendre les avantages secondaires du programme, en termes d'adoption en toute confiance de technologies et d'initiatives de transformation digitale.

Procédures et règles

Il convient d'élaborer un processus de gestion des risques avec des consignes et des accords de niveau de service (SLA), comprenant des responsabilités clairement établies. Ce workflow doit être documenté et revu régulièrement, avec un suivi des activités de correction et de réduction des risques.

Mesures et conséquences

L'une des failles d'un processus d'atténuation des risques réside dans le laisser-aller et l'absence de responsabilité. Outre les procédures et règles, il convient de définir clairement les responsabilités, les métriques utilisées dans l'entreprise et les conséquences si celles-ci ne sont pas tenues.

Mesures de sécurité basiques

En posant bien les bases, telles que l'évaluation des vulnérabilités, la gestion des correctifs, la sécurisation des systèmes et la gestion des accès privilégiés, non seulement vous aurez une posture de sécurité de référence, mais vous identifierez plus rapidement les failles que vous pourrez traiter plus efficacement.

Enfin, selon les risques auxquels votre entreprise est confrontée, envisagez des fonctionnalités PAM, comprenant la mise en place du moindre privilège et la sécurisation des accès à distance, pour soutenir vos efforts d'atténuation des menaces et de réduction de la surface d'attaque. La plupart des exploits, malwares, ransomwares, menaces persistances avancées, ont besoin de privilèges administratifs pour s'exécuter. Le fait d'éliminer des droits admins non nécessaires peut contribuer à éviter qu'une situation s'aggrave.

À la lecture des tendances exposées dans ce rapport et compte tenu des menaces actuelles, n'oubliez pas l'importance d'une posture de sécurité préventive et proactive, , en sus des stratégies de défense, de type gestion des vulnérabilités et des correctifs.

Méthodologie

Publié annuellement, le rapport BeyondTrust sur les vulnérabilités Microsoft analyse les données des bulletins de sécurité émis par Microsoft au cours de l'année écoulée. Ce rapport établit une synthèse de ces mises à jour de sécurité, il dégage des tendances des vulnérabilités constatées et recommande des mesures pour les atténuer.

En novembre 2020, Microsoft a opté pour le format CVSS (Common Vulnerability Scoring System). Ce nouveau format de reporting ne propose plus les habituels résumés de chaque vulnérabilité Microsoft comme c'était le cas auparavant. Sans les informations de ces résumés, il n'est plus possible de déterminer précisément le nombre des vulnérabilités Microsoft qui auraient pu être éliminées ou réduites par la suppression des droits admins. Le nouveau format n'empêche pas cependant de rendre compte du nombre de vulnérabilités par produit et plateforme.

Classification des vulnérabilités par Microsoft

Chaque vulnérabilité peut concerner un ou plusieurs produits Microsoft. Une matrice le précise sur chaque page décrivant une vulnérabilité. Chaque vulnérabilité appartient à une des 7 catégories suivantes : Exécution de code à distance, Élévation de privilèges, Divulgation d'information, Déni de service, Contournement de mesure de sécurité, Usurpation et Falsification, qui peuvent varier selon le type de logiciel ou la combinaison de logiciels. Une vulnérabilité de chaque catégorie concerne souvent plusieurs versions différentes d'un ou de plusieurs produits, parfois toutes les versions des clients Windows. Il arrive qu'une vulnérabilité ne concerne qu'une combinaison de produits, Internet Explorer 11 sur Windows 7.

A chaque vulnérabilité correspond un degré de dangerosité attribué par Microsoft : Critique, Importante, Modérée, qui peut varier selon le type de logiciel ou la combinaison de logiciels. Certaines vulnérabilités se sont produites plusieurs fois en 2021, concernant différents logiciels. Dans ce cas, la vulnérabilité n'est comptée qu'une seule fois pour tous les types de logiciels concernés.

Exactitude des données
Principes généraux appliqués :

1. Chaque vulnérabilité est classée selon le degré de dangerosité le plus élevé de toutes les instances constatées, le cas échéant
2. Chaque vulnérabilité est classée dans la catégorie prédominante de toutes les instances constatées
3. Les versions de produits ne sont pas prises en compte
4. Les combinaisons de produits ne sont pas prises en compte
5. Les vulnérabilités sont comptées pour le logiciel et la version (par exemple, une vulnérabilité concernant Internet Explorer 11 sur Windows 10 compte 1 fois pour Internet Explorer 11 et 1 fois pour Windows 10)

Ressources complémentaires

NOUVEAU ! Privileged Access Discovery Application
Cet outil est le plus puissant actuellement disponible gratuitement pour évaluer le risque lié aux accès privilégiés. Analysez votre environnement à la recherche des comptes excessivement privilégiés, des comptes de service, comptes non utilisés, identifiants privilégiés, outils d'accès à distance, etc.

LIVRE BLANC Cybersecurity Survival Guide

LIVRE BLANC Malware Threat Report 2021

LIVRE BLANC The 7 Perils of Privilege

BeyondTrust

BeyondTrust est le leader mondial de la gestion intelligente des identités et de la sécurité des accès, permettant aux organisations de protéger les identités, de stopper les menaces et de fournir un accès dynamique afin d'autonomiser et de sécuriser le travail à tout moment. Nos produits et notre plateforme intégrés offrent la solution de gestion des accès privilégiés (PAM) la plus avancée du marché, permettant aux organisations de réduire rapidement leur surface d'attaque dans les environnements traditionnels, cloud et hybrides.

BeyondTrust protège toutes les identités privilégiées, les accès et les endpoints dans un environnement informatique contre les menaces de sécurité, tout en créant une expérience utilisateur supérieure et des efficacités opérationnelles. Avec un héritage d'innovation et un engagement ferme envers les clients, les solutions BeyondTrust sont simples à déployer, à gérer et à adapter à l'évolution des entreprises. 20 000 clients, dont 75 des 100 premières entreprises du classement Fortune et un réseau mondial de partenaires nous font confiance. Pour en savoir plus : www.beyondtrust.com/fr.

beyondtrust.com