TeamViewer
Remote Management

LIVRE BLANC

Ne ratez plus aucun correctif :

réduisez les risques liés
à la sécurité et protégez votre
infrastructure informatique
avec une gestion des correctifs

Table des **matières**

Introduction :
Qu’est-ce qu’une solution de gestion des correctifs ?

Pour entretenir les performances et la sécurité de votre infrastructure informatique, une maintenance régulière et des mises à jour en temps utile sont nécessaires pour tous les ordinateurs et appareils. Négliger de mettre à jour vos ordinateurs et vos appareils peut entraîner d’importantes failles de sécurité dues à des logiciels obsolètes.

Les sociétés informatiques sont confrontées à de nouveaux défis pour s’assurer que les appareils sont toujours à jour ou corrigés en raison du nombre croissant d’appareils de service, d’applications et de failles virtuelles.

En langage informatique, un « correctif » ou « patch » est une liste de modifications apportées à un programme d’ordinateur spécialement conçue pour le mettre à jour, l’optimiser ou le réparer. Les correctifs sont utilisés pour combler les failles des logiciels et d’autres bogues, et sont mis à la disposition des utilisateurs par le biais de mises à jour logicielles. Surveiller la disponibilité des correctifs et installer les correctifs manquants nécessitent une solution de gestion automatisée des correctifs.

Avec une solution de gestion des correctifs, vous pouvez détecter et corriger les logiciels obsolètes et vulnérables.

Par conséquent, les correctifs constituent une part essentielle de votre sécurité informatique. Sans eux, les failles de sécurité ne sont jamais réparées, offrant le champ libre aux pirates et autres cybercriminels pour voler des données de l’entreprise. Selon une étude de NIST, 90 % des attaques réalisées contre des entreprises sont imputables à des failles connues et auraient pu être évités avec les bons correctifs installés à temps.[1]

De l'importance d'une gestion des correctifs pour les entreprises

Les cyberattaques à base de malware peuvent sérieusement nuire aux entreprises. La perte de données, les préjudices causés à l'image ou les arrêts de production peuvent coûter des millions aux entreprises. Le nombre de variantes de malwares augmente quasi-quotidiennement. En d'autres termes, votre infrastructure informatique nécessite une gestion efficace de la sécurité.

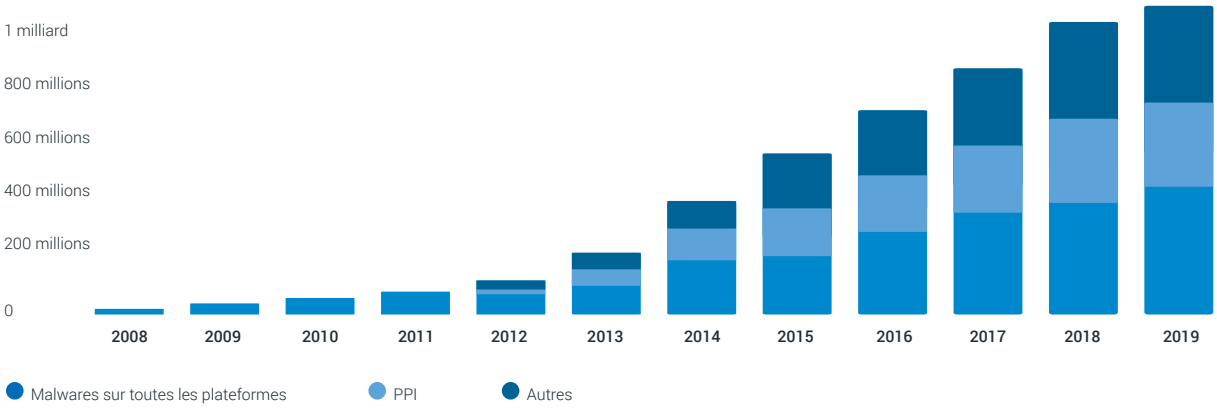

Figure 1 : total des variantes de malware connues *PPI (programme potentiellement indésirable)[2]

Les cyberattaques, comme celle de WannaCry en 2017, ont montré une fois de plus combien il est important de protéger votre matériel et vos logiciels contre les attaques. Aujourd'hui, la plupart des systèmes et applications des grandes entreprises est accessible par Internet, ce qui facilite l'accès des criminels. Un logiciel antivirus ne suffit pas, à lui seul, pour protéger intégralement les infrastructures informatiques. En raison de la grande complexité des logiciels, davantage d'erreurs sont commises lors du développement, ce qui rend les logiciels vulnérables.

L'Office fédéral allemand pour la sécurité de l'information (BSI) a annoncé que « les attaques réussies étaient souvent dues à des attaques via des vulnérabilités inconnues et à un manque de gestion des correctifs. »[3] En effet, le nombre de failles critiques dans les produits informatiques standard a fortement augmenté ces dernières années.

Rien qu'en 2017, il y avait plus de 450 failles connues parmi les 10 applications les plus connues. Selon le BSI, rien n'indique que la situation va évoluer dans les prochaines années. 12 174 failles ont déjà été vérifiées en 2019, dans le top 50 des logiciels les plus fréquemment utilisés.4

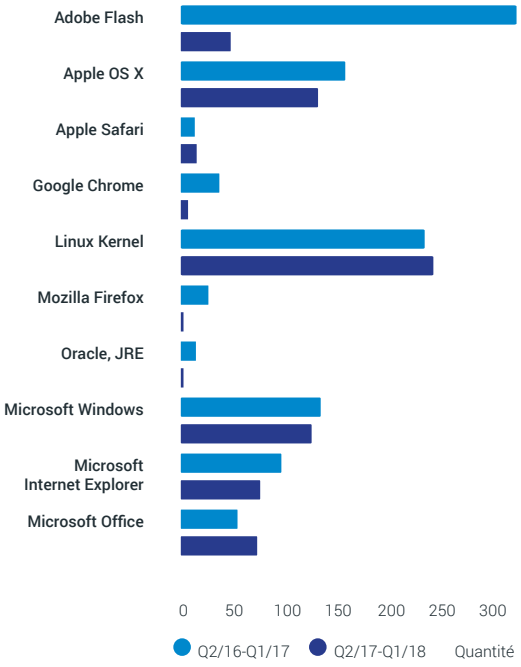

Figure 2 : entrées CVE critiques au 31 mars 20185

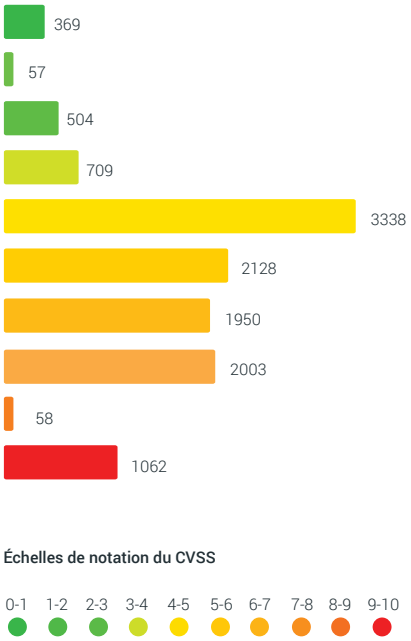

Figure 3 : répartition des failles en 2019 au 30 octobre 2019. De non critique (vert) à critique (rouge) du top 504

90 % des failles logicielles exploitées se produisent dans les 40 à 60 jours suivant leur publication. Les administrateurs informatiques étant tenus responsables, ils doivent agir rapidement. Les correctifs doivent être déployés, testés et mis en place. Pour les administrateurs informatiques, cela prend non seulement énormément de temps, mais représente aussi un facteur de coût important.

Avec l'augmentation du volume des failles, la correction manuelle est devenue plus fastidieuse et moins pratique à effectuer régulièrement avec l'assurance que tous les appareils ont effectivement été corrigés avec succès. Les processus de correctifs manuels nécessitent également des processus de suivi manuels, ce qui augmente la pression sur le temps et les ressources des administrateurs informatiques.

En ce qui concerne les processus de correction manuelle, selon la complexité du système, il peut être nécessaire de s'en remettre aux utilisateurs finaux pour mettre en œuvre les correctifs. Cela a généralement un impact sur la réussite de la mise en œuvre des correctifs.

Il est relativement facile de corriger le côté serveur car le service informatique en a le contrôle total, mais c'est du côté client que se trouve la plupart des failles (environ 95 %) et il est difficile de tenir les clients à jour. Les problèmes logistiques font obstacle tout comme le facteur humain ; les utilisateurs retardent les correctifs parce qu'ils ne veulent pas interrompre leur travail. Pour ces raisons, la correction est souvent négligée : bien que les correctifs soient souvent disponibles pendant longtemps, ils ne sont jamais mis en œuvre pour des raisons de temps et de coût. Toutefois, si le correctif n'est pas appliqué correctement, les cybercriminels peuvent exploiter ces failles de manière systématique.

Ces failles logicielles peuvent entraîner de graves failles de sécurité dans une application ou un réseau informatique. C'est pourquoi les entreprises doivent aujourd'hui relever le grand défi qui consiste à mieux organiser et gérer leur infrastructure informatique. La gestion des correctifs est la solution optimale pour soulager les administrateurs informatiques et augmenter la performance, l'efficacité et l'efficience de l'infrastructure informatique. Une solution efficace de gestion des correctifs vérifie quels correctifs sont les mieux adaptés aux systèmes, automatise la distribution et le déploiement des correctifs, et les classe par ordre d'urgence. Par conséquent, la gestion des correctifs non seulement améliore le déploiement des correctifs, mais réduit aussi les

Risques induits par une mauvaise gestion des correctifs

Temps d'arrêt coûteux du système

Crédibilité entachée auprès des clients

Longue durée de réparation

Intégrité douteuse des données

Influence négative sur les relations publiques

Environnement informatique non sécurisé

Avantages de la gestion des correctifs

Le déploiement régulier et automatisé de correctifs augmente considérablement la sécurité des systèmes informatiques et l'intégrité des réseaux. Tel est l'avantage indéniable de la gestion des correctifs. Toutefois, une solution de gestion automatisée des correctifs apporte d'autres avantages importants aux entreprises.

Hausse de la productivité informatique et baisse des temps d'arrêt imprévus

La gestion manuelle des correctifs prend beaucoup de temps pour les administrateurs informatiques. Identifier les failles, déterminer les points de terminaison qui nécessitent des correctifs, puis déployer ces derniers et s'assurer qu'ils ont été correctement appliqués aux ordinateurs et portables concernés demande beaucoup de temps et de ressources.

De plus, cela entraîne des temps d'arrêt imprévus pour les employés qui ont besoin d'accéder à leurs appareils. Une solution de gestion automatisée des correctifs aide donc non seulement le personnel informatique à accroître son efficacité, mais aussi à réduire les temps d'arrêt imprévus pour les employés.

Sécurité et conformité des données garanties pour atténuer les risques

Les directives de conformité en matière de sécurité dans les services informatiques sont essentielles et ne doivent pas être négligées. La conformité informatique protège les entreprises contre les pénalités ou les préjudices potentiels à leur marque. Par exemple, les failles de logiciels sont des risques de sécurité majeurs qui peuvent entraîner de graves atteintes aux données.

Si les données sensibles des employés ou des clients sont divulguées, les entreprises peuvent encourir des sanctions pour avoir enfreint la réglementation sur la protection des données. Cela pourrait entraîner une perte de clientèle ou une publicité négative. Une solution efficace de gestion des correctifs détecte les vulnérabilités de sécurité et peut contribuer à

Avantages **clés**

Gain de temps grâce aux mises à jour rapides et complètes du système informatique

Déploiement automatique de correctifs pour corriger les failles logicielles

Gestion centralisée des ordinateurs

Stimulation de la productivité des employés

Gain d'informations fournies par les rapports détaillés des réseaux

Compréhension de l'infrastructure grâce à des aperçus de l'état des systèmes

Réduction des temps d'arrêt imprévus des appareils

Atténuation des risques liés à la sécurité et à la conformité

Caractéristiques **clés**

Identification des failles

Obtenez une visibilité totale sur votre réseau en détectant automatiquement les failles dues à des logiciels obsolètes.

Lancement rapide intégré avec TeamViewer

Déployez Patch Management à tout votre réseau en quelques clics.

Déploiement automatique de correctifs

Détectez et déployez automatiquement des correctifs basés sur des stratégies pour les logiciels, les systèmes d'exploitation et les applications tierces obsolètes et vulnérables, afin de maintenir votre infrastructure informatique sécurisée et à jour.

La solution TeamViewer
Patch Management

Le déploiement de correctifs sur les terminaux peut protéger l'ensemble de votre réseau contre les cyberattaques. Saviez-vous cependant qu'un seul appareil non corrigé pouvait mettre en péril votre infrastructure informatique complète ?

Protégez votre réseau informatique avec Patch Management

Restez au courant des correctifs critiques grâce à la gestion automatisée des correctifs. Découvrez instantanément si des mises à jour sont disponibles et déployez-les en masse à partir d'une plateforme centralisée.

Gérez et déployez les mises à jour Windows à partir d'un tableau de bord centralisé, en vous assurant que tous vos appareils Windows sont à jour.

Réduisez les risques, surveillez et déployez automatiquement des correctifs pour les applications tierces et les mises à jour des systèmes d'exploitation.

Consultez les statuts de correction de vos appareils et tous les correctifs disponibles depuis un seul tableau de bord.

Définissez des stratégies individuelles pour différents services ou clients afin de personnaliser et d'automatiser les tâches de correctifs.

Classez les correctifs par ordre de priorité, voyez quels correctifs sont critiques, urgents ou peuvent être reportés en les classant par ordre de priorité.

Gérez et vérifiez vos correctifs à distance, où que vous soyez. L'intégration transparente entre TeamViewer Remote Management et TeamViewer Remote Access vous permet d'accéder aux appareils selon vos besoins en quelques clics seulement.

Conclusion

Les sociétés informatiques savent qu'elles doivent continuellement protéger leurs entreprises contre les cybercriminels et qu'une solution de gestion automatisée des correctifs est essentielle pour améliorer la sécurité des terminaux. Si la gestion des correctifs est essentielle, elle n'a pas besoin d'être compliquée.

Grâce à des fonctionnalités faciles à utiliser, la gestion des correctifs par TeamViewer vous permet de protéger de manière proactive votre infrastructure informatique et d'éliminer les tâches de correctifs manuelles fastidieuses, tout en augmentant la sécurité, la stabilité et l'intégrité de votre réseau.

Ressources

Demandez une démonstration gratuite de TeamViewer Remote Management (y compris Patch Management)

Découvrez-en plus sur teamviewer.com/patchmanagement

Démarrez un essai gratuit de Patch Management

Références

1. National Institute of Standards and Technology (novembre 2019) : Automation Support for Security Control Assessments: Software Vulnerability Management, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8011-4-draft.pdf
2. Bundesamt für Sicherheit in der Informationstechnik (2018) : Die Lage der IT-Sicherheit in Deutschland 2018, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-2018.pdf
3. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2015.pdf;jsessionid=F64FE0EE50A281C976D952B395DCD531.2_cid369?__blob=publicationFile&v=5 S.11
4. CVE Details (2019) : Current CVSS Score Distribution for all Vulnerabilities, https://www.cvedetails.com/cvss-score-distribution.php
5. Bundesamt für Sicherheit in der Informationstechnik (2018) : Die Lage der IT-Sicherheit in Deutschland 2018. URL : https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-2018.pdf?__blob=publicationFile&v=3 page. 43
6. CVE Details (2019) : Vulnerabilities by Date, https://www.cvedetails.com/browse-by-date.php

À propos de TeamViewer

En tant que plateforme de connectivité à distance parmi les leaders mondiaux, TeamViewer garantit la connexion de tous les utilisateurs, sur tous types d'appareils, partout et à tout moment. TeamViewer offre un accès, une assistance et un contrôle à distance, ainsi que des possibilités de collaboration pour les points de terminaison en ligne de toute sorte et aide les entreprises de toute taille à exploiter pleinement leur potentiel numérique. TeamViewer est activé sur environ 2 milliards d'appareils. Près de 45 millions d'appareils sont en ligne simultanément. Fondée en 2005 à Göppingen, en Allemagne, TeamViewer est une société publique cotée à la Bourse de Francfort et qui emploie près de 800 personnes dans des bureaux répartis en Europe, aux États-Unis et en Asie-Pacifique.

www.teamviewer.com