

Gestion en continu des vulnérabilités

Lorsque des pirates exploitent les faiblesses de l'infrastructure IT d'une entreprise, les conséquences peuvent être dramatiques, aussi bien pour la productivité et la réputation de cette entreprise que pour ses finances. Si vous ne considérez pas la cybersécurité comme un processus permanent, les pirates peuvent repérer votre infrastructure, s'y infiltrer, déployer des virus et vous attaquer plus rapidement que votre équipe ne parvient à appliquer les correctifs de vulnérabilités. Vos systèmes sont sans doute en sécurité aujourd'hui mais, la semaine prochaine, un pirate peut découvrir et exploiter une vulnérabilité critique dans votre environnement.

La gestion en continu des vulnérabilités est décrite par le CIS (Centre de sécurité Internet) comme le fait de « collecter de nouvelles informations en continu, de les évaluer et de prendre des mesures afin d'identifier les vulnérabilités, de les corriger et de limiter les possibilités d'attaque ».

La gestion en continu des vulnérabilités devrait faire partie des pratiques de sécurité dans toutes les entreprises. Cependant, le temps et les opérations manuelles que cela implique, de l'identification initiale d'une vulnérabilité au déploiement d'une mise à jour logicielle sont lourds à porter. Il est recommandé d'entamer le processus en lançant de fréquentes analyses des vulnérabilités pour éviter les zones d'ombre entre les rapports.

Les équipes de sécurité partent des données de vulnérabilité, définissent leur ordre de priorité et les transmettent à votre équipe IT, qui doit traduire ces CVE (Common Vulnerabilities and Exposures) en mises à jour logicielles, puis définir les logiciels dont la mise à jour est prioritaire. Bien qu'il soit facile d'identifier et de

corriger une seule vulnérabilité, qu'en est-il lorsque le système détecte 10 000 CVE, ou même 100 000 ?

Une seule évaluation des vulnérabilités peut détecter les mêmes vulnérabilités sur plusieurs systèmes dans votre environnement. Et une même vulnérabilité peut exister dans un grand nombre de logiciels sur un même système. L'élimination des doublons et l'examen des CVE pour décider des mesures à prendre pour résoudre chaque vulnérabilité peuvent nécessiter 5 à 8 heures chaque fois que l'équipe réalise ce processus. Cela fait une seule journée, ça ne paraît pas énorme. Mais lorsqu'on sait que la majorité des exploits se produisent dans les 14 à 28 jours qui suivent la publication des mises à jour, chaque journée de retard donne du temps aux pirates pour concevoir leurs attaques.

Gain de temps entre vulnérabilité et déploiement du correctif

Les solutions de sécurité Ivanti vous fournissent de meilleures informations et améliorent votre position en matière de sécurité. Vous tenez à jour l'application des correctifs pour l'ensemble des systèmes d'exploitation et des applications tierces, grâce à l'application automatisée des correctifs aux postes clients et aux serveurs. Nos solutions de correctifs s'intègrent aux analyseurs de vulnérabilités, aux outils de gestion des configurations et aux outils de reporting pour optimiser le temps de travail des équipes IT et Sécurité.

Mise en place d'une gestion en continu des vulnérabilités

Nos solutions de sécurité fluidifient le processus d'identification, de classification et de traitement des vulnérabilités afin d'éviter que des pirates exploitent le fossé entre rapports des vulnérabilités de sécurité et correction de ces vulnérabilités. Les équipes IT peuvent facilement importer les résultats des analyses des vulnérabilités réalisées par les équipes Sécurité. Affichez rapidement les CVE identifiées et les correctifs

associés, puis publiez tous les correctifs manquants ou approuvez leur déploiement, ce qui vous fait gagner beaucoup de temps.

Qu'il s'agisse d'appliquer des correctifs aux postes clients avec Ivanti Patch pour SCCM ou Ivanti Patch pour Endpoint Manager, ou d'en appliquer au centre de données avec les solutions de sécurité Ivanti, vous pouvez tirer parti des fonctions « CVE en correctifs » de nos produits.

Vous améliorez ainsi l'expérience et la productivité des équipes IT, qui passaient auparavant de longues heures à manuellement examiner les correctifs, éliminer les doublons et préparer un groupe de mises à jour de correctifs. Vous pouvez facilement importer la liste fournie par un fournisseur de gestion des vulnérabilités, dans le format de votre choix : CSV, XML ou fichier texte. Vous mappez ensuite automatiquement les CVE sur les mises à jour logicielles appropriées pour résoudre des vulnérabilités spécifiques. Vous voyez ainsi rapidement les correctifs qu'il faut appliquer et pouvez créer un groupe de correctifs pour les éléments approuvés dans votre environnement. Vous pouvez même afficher toutes les informations associées à chaque correctif.

De meilleures informations pour une sécurité renforcée

Combien de jours faut-il à votre équipe IT pour rechercher, tester et déployer les correctifs, et comment définissez-vous leur ordre de priorité ? L'examen des problèmes connus signalés par les blogs, la documentation fournisseur ou d'autres sources afin de déterminer la fiabilité des mises à jour de correctif est également une opération qui prend du temps. La définition de l'ordre de priorité des correctifs peut aussi augmenter les risques, si l'entreprise préfère distribuer les correctifs critiques au lieu de distribuer les correctifs correspondant aux vulnérabilités activement exploitées.

Le choix des correctifs prioritaires, leur test et leur déploiement peuvent rendre le processus de gestion des vulnérabilités beaucoup plus lent. Ivanti vous permet de tirer parti de son outil Patch Intelligence, qui

combine les données du catalogue de correctifs tiers Ivanti avec les mesures de fiabilité et de sécurité des correctifs. Optimisez le déploiement des mises à jour importantes, grâce à des informations dont la collecte nécessiterait, sans nos solutions, beaucoup de temps et d'efforts.

- **Améliorez la visibilité** sur les problèmes signalés par le fournisseur pour un correctif ou un groupe de correctifs, ou identifiés par Ivanti dans les informations de bulletin stockées avec les CVE et correctifs associés.
- **Augmentez l'étendue de vos informations** sur les problèmes détectés par l'ensemble des clients d'Ivanti, grâce à des données transmises anonymement par vos homologues, qui vous avertissent quand des clients sont contraints d'annuler (rollback) un correctif.
- **Déterminez la fiabilité** des mises à jour et le niveau de confiance d'un déploiement rapide.
- **Identifiez les correctifs** nécessitant des tests supplémentaires, suivez rapidement les correctifs dont la probabilité de réussite est élevée et facilitez le choix des tests prioritaires et des éléments à déployer immédiatement en fonction de leur score de menace et niveau de fiabilité pour optimiser les cycles de correctifs.

Gardez une longueur d'avance sur les pirates grâce aux solutions Ivanti de gestion en continu des vulnérabilités. Pour en savoir plus, contactez contact@ivanti.fr.

En savoir plus

-  **[ivanti.fr](https://www.ivanti.fr)**
-  **+33 (0)1 49 03 77 80**
-  **contact@ivanti.fr**

Copyright © 2020, Ivanti. Tous droits réservés. IVI-2388 03/20 BB/MK/DH