ivanti

Le guide ultime pour la gestion des correctifs basée sur les risques

Une référence indispensable pour les équipes IT Ops et Sécurité qui souhaitent moderniser la gestion des correctifs

Avant-propos

Avec plus de 187 000 vulnérabilités de sécurité actuellement répertoriées dans la base NVD (National Vulnerability Database)[1]– auxquelles s'ajoutent chaque jour 61 vulnérabilités supplémentaires[2] – **les entreprises ne peuvent manifestement pas remédier à toutes les menaces qui pèsent sur leurs systèmes.**

Un examen approfondi des données disponibles révèle qu'il existe plus de 236 000 vulnérabilités, le pourcentage réel de menaces étant représenté par environ 12,4 % de vulnérabilités militarisées par des cybercriminels.[3]

Les structures traditionnelles de gestion des correctifs n'offrent pas de visibilité sur le paysage complet des vulnérabilités, ouvrant ainsi des brèches dans le bouclier de cybersécurité.

Pourtant, même en connaissant toutes les vulnérabilités possibles, comment décider des CVE traitées en priorité ? Quand faut-il interrompre le cycle de maintenance pour déployer les correctifs les plus prioritaires ?

La solution : la gestion des correctifs basée sur les risques (RBPM ou Risk-Based Patch Management).

La gestion des correctifs basée sur les risques est l'une des approches les plus efficaces de l'atténuation des risques. Elle va au-delà des scores CVSS (Common Vulnerability Scoring Systems) et scanners habituels, afin d'identifier et de qualifier les vulnérabilités spécifiques les plus dangereuses pour les périphériques, les données et les utilisateurs d'une entreprise.

> "Les entreprises ne peuvent manifestement pas remédier à toutes les menaces qui pèsent sur leurs systèmes."

Cette extension de la gestion des vulnérabilités basée sur les risques permet d'intégrer un contexte de risques réels dans le processus de gestion des correctifs grâce aux mises à jour prenant en compte les vulnérabilités exploitées connues considérées comme cruciales pour la sécurité d'une entreprise.

Avec cette approche qui met les vulnérabilités en contexte, les administrateurs de correctifs sont en mesure de prioriser les activités de remédiation critiques. Quant aux équipes opérationnelles, elles peuvent ainsi comprendre l'urgence de leurs activités à travers le même prisme de risques réels que les équipes de sécurité.

La gestion des correctifs basée sur les risques nécessite des ressources supplémentaires, au-delà de la structure linéaire traditionnelle de priorisation des correctifs, notamment :

- Des sources de données multiples (à la fois externes et internes) dynamiquement mises à jour et rapidement synthétisées afin de produire les informations nécessaires à l'identification des risques spécifiques d'une entreprise, en les comparant aux vulnérabilités et correctifs connus.
- Un schéma de priorisation qui classe les vulnérabilités critiques pour l'entreprise en fonction de la gravité des dommages qu'elles peuvent causer, des activités de ransomware connues, de la facilité de remédiation, etc.
- Des ressources suffisantes (ressources humaines ou fonctions automatisées) pour identifier les vulnérabilités critiques au fur et à mesure qu'elles se produisent, émettre des alertes et exécuter les mesures correctives nécessaires.

Table des matières

L’heure est critique : Trop de vulnérabilités, pas assez de temps

La base NVD (National Vulnerability Database) répertorie plus de 187 000 vulnérabilités, chacune avec des scores de gravité différents qui masquent parfois les risques propres à chaque entreprise.[4]

Les entreprises capables d’étendre leurs capacités de surveillance pour couvrir toutes les sources de données possibles (y compris les bases de données NVD et CISA, les scanners du secteur, les primes aux bugs, les tests d’intrusion et diverses études sur les tendances des menaces) estiment que le nombre réel de vulnérabilités potentielles dépasse les 236 000 en juin 2022.[5]

Parmi ces vulnérabilités, 12,4 % constituent des exploitations possibles pour les ransomwares et les cybercriminels.[6]

À lui seul, cet énorme volume exige une approche proactive et priorisée de la gestion des correctifs pour les entreprises ayant l’intention de maintenir une sécurité constante.

Il existe plus de 236 000 vulnérabilités connues.

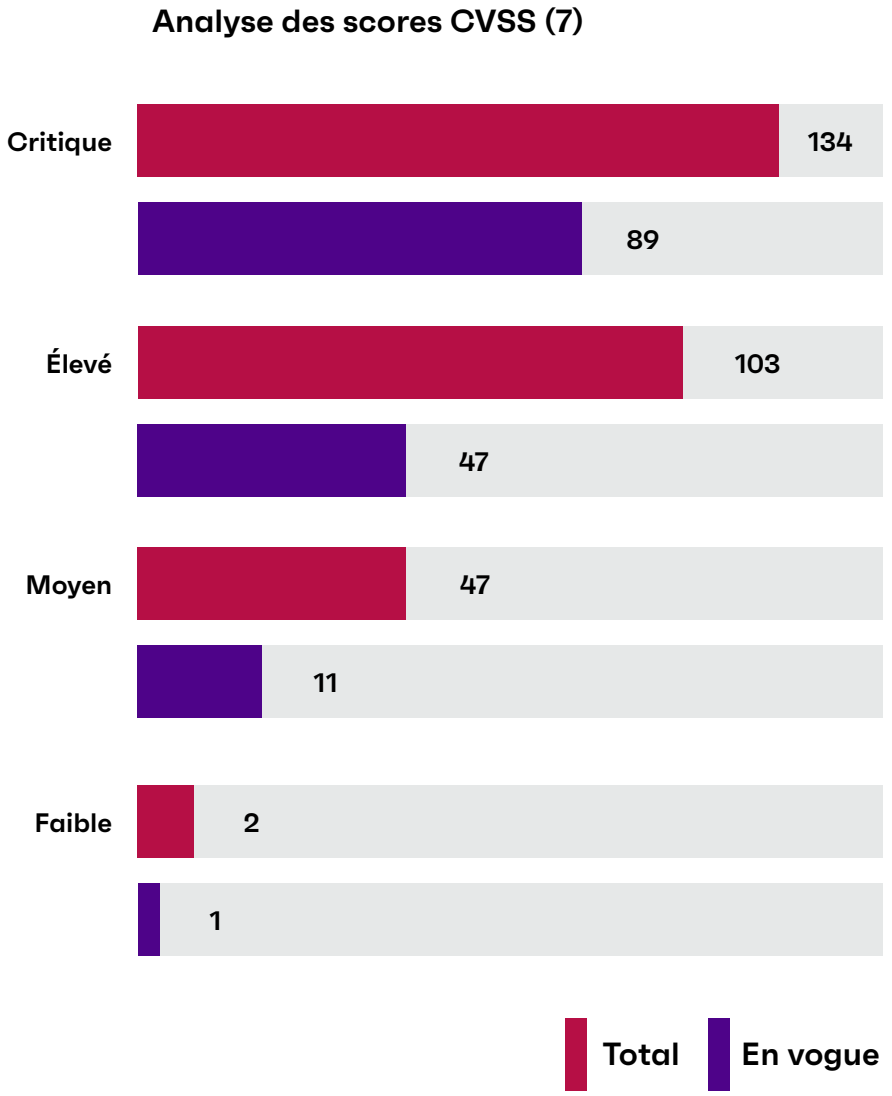
12,4 % de ces vulnérabilités sont activement exploitées ou reliées à des ransomwares.

Malheureusement, les scores de gravité des fournisseurs et les scores CVSS ne fournissent pas assez de contexte pour aider les équipes de sécurité internes à déterminer les vulnérabilités à traiter en premier.

Prenons par exemple le dernier rapport Ivanti sur les ransomwares[8] dont les conclusions sont les suivantes :

- Les entreprises qui appliquent uniquement les correctifs des CVE considérées comme « Critiques » manquent presque 40 % des vulnérabilités en vogue activement exploitées par les gangs de ransomwares et autres cybercriminels.

- 91 % des vulnérabilités actives liées aux ransomwares datent de plus d'un an.



Si aucune correspondance n'est établie entre les vulnérabilités et les menaces réelles de ransomware – sans oublier les exploitations pouvant permettre l'exécution de code à distance (RCE) et l'élévation des privilèges (PE) – les entreprises ont du mal à prioriser efficacement les mesures correctives pour garantir à la fois la sécurité et la productivité.

C'est pourquoi les équipes de sécurité doivent corriger chaque vulnérabilité pertinente pour assurer la sécurité de leur entreprise (périphériques, données et utilisateurs finaux).

Il suffit d'une seule défaillance pour faire la joie des cybercriminels.

Répercussions dans le monde réel :

Microsoft

En 2021, Microsoft[9] a résolu 23 vulnérabilités Zero-Day.

15 d'entre elles étaient seulement classées en tant que priorités de niveau « Critique » (et pas « Critique »).

100 % de toutes les vulnérabilités Zero-Day 2021 de Microsoft ont été activement exploitées par les cybercriminels et les ransomwares.

Le processus traditionnel de gestion des correctifs

Historiquement, la gestion des correctifs a toujours suivi une approche linéaire de type cascade :

1. **Le scanner de vulnérabilités ou la base de données de l'équipe** de sécurité détecte une nouvelle vulnérabilité dans l'environnement, ce qui déclenche une évaluation de criticité CVSS pour les vulnérabilités de score élevé, afin de hiérarchiser les opérations de remédiation.
2. **Pendant ce temps, les administrateurs de correctifs évaluent** l'environnement pour rechercher si des logiciels doivent être mis à jour dans le cadre du cycle de maintenance standard (la gravité fournisseur Critique est évaluée dans le cadre de la priorisation des opérations de remédiation), séparément de l'évaluation effectuée par l'équipe de sécurité.
3. **Les équipes de sécurité et les administrateurs de correctifs** débattent de la priorisation des correctifs pour obtenir une liste conjointe des correctifs critiques à déployer.
   - En général, les recommandations de l'équipe Sécurité deviennent prioritaires sur celles des administrateurs de correctifs et celles de l'équipe IT Ops (lesquelles reposent sur les informations fournies par les fournisseurs).
4. **Les administrateurs de correctifs déterminent les correctifs pertinents** pour remédier aux vulnérabilités prioritaires (s'ils existent) et, dans l'idéal, les testent dans un environnement sandbox avant de les déployer dans toute l'entreprise.
   - Les administrateurs sont face à une réalité : les environnements de tests reflètent rarement toutes les facettes du réseau de l'entreprise.
5. **Le correctif est déployé,** ce qui provoque parfois des arrêts ou des plantages dus à des interférences avec le fonctionnement du système ou l'interconnectivité avec d'autres applications, même s'il a été reconnu comme sain et sans impact lors de la série de tests en sandbox.
6. **Un cycle « rincer, nettoyer, répéter » démarre,** tandis que les administrateurs de correctifs et les équipes de sécurité examinent les résultats du déploiement, et identifient les machines sur lesquelles la mise à jour a échoué ou celles ayant été complètement ignorées au cours du processus.

Les écueils d'une gestion traditionnelle des correctifs

Toute personne qui a déjà géré les correctifs connaît les faiblesses de l'approche linéaire traditionnelle. Par exemple, les gangs de ransomwares peuvent exploiter les vulnérabilités à peine quelques jours après qu'elles aient été identifiées dans les bases de données centrales, ce qui réduit le délai accordé aux administrateurs de correctifs pour identifier la vulnérabilité et y remédier avant toute attaque.

Cette année, plusieurs vulnérabilités majeures (QNAP, Sonic Wall, Kaseya, Apache Log4j, par exemple) ont été exploitées avant même d'apparaître dans la base NVD.[11]

des exploitations se produisent dans les 14-28 jours suivant la publication des correctifs(12) et les cybercriminels n'ont besoin, en moyenne, que de 22 jours pour développer des exploitations fonctionnelles.[13]

Répercussions dans le monde réel : BlueKeep[10]

14 mai 2019
Publication de CVE-2019-0708 avec correctif.

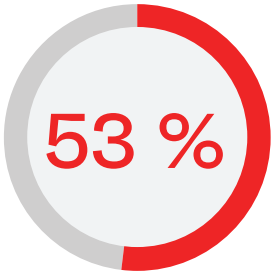
15 mai 2019
Début des recherches PoC (Proof of Concept - Validation de principe).

20 mai 2019
Exploitation BSOD confirmée par les cabinets de recherche.

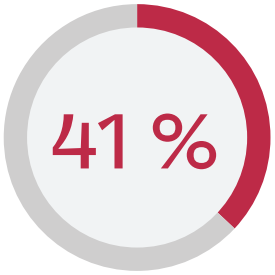
28 mai 2019
6 cabinets de recherche indépendants parviennent à exécuter du code à distance (RCE). Des exploitations supplémentaires sont confirmées par des cybercriminels.

Il se passe seulement 14 jours entre la publication de la vulnérabilité et l'exploitation active par les cybercriminels.

Sans moyens, ressources et effectifs supplémentaires,
les administrateurs de correctifs et les équipes Sécurité ne peuvent s'appuyer que sur les scores de gravité fournisseur et les scores CVSS. Ils se retrouvent sans contexte supplémentaire pour leur environnement de risques spécifique.

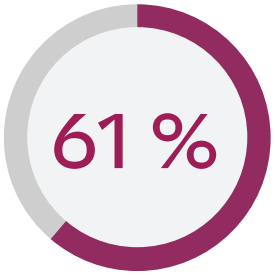


53 % des équipes IT Ops et Sécurité interrogées déclarent passer presque tout leur temps à simplement organiser et prioriser les vulnérabilités, au lieu d'appliquer activement les correctifs !(14)

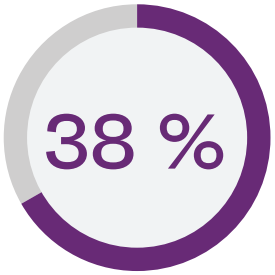


Une enquête internationale récente révèle que 41 % des entreprises interrogées ont perdu du personnel IT en raison des lourdes charges de travail sur un marché de l'emploi de plus en plus compétitif.(15)

Le manque d'alignement entre les objectifs de l'équipe Sécurité et ceux de l'IT Ops provoque
souvent l'échec de l'application des correctifs et une perte de productivité.

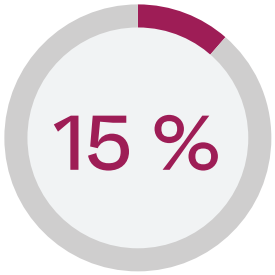


61 % des professionnels de l'IT et de la sécurité interrogés reçoivent des demandes de report de la fenêtre de maintenance une fois par trimestre (et 28 % en reçoivent chaque mois). Les entreprises sont donc vulnérables aux cyberattaques, pour quelques « gains » de productivité.(16)



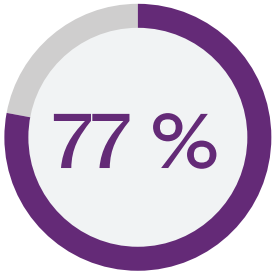
En cas de cyberattaque effective (comme ce fut le cas en 2021 pour 63 % des entreprises interrogées), 38 % des entreprises attaquées perdent une semaine de productivité (à l'échelle de l'entreprise). 24 % ont même perdu un mois entier de travail.(17)

La plupart des départements n'ont pas le temps de tester les mises à jour ou de se coordonner avec les autres départements avant de déployer les correctifs.



15 % seulement des équipes IT Ops et Sécurité disent passer la plupart de leur temps à tester les correctifs, alors que 10 % seulement déclarent passer l'essentiel de leur temps à se coordonner avec les autres départements.[18]

Les scanners et les bases de données ne repèrent et ne publient pas toutes les vulnérabilités exploitables.



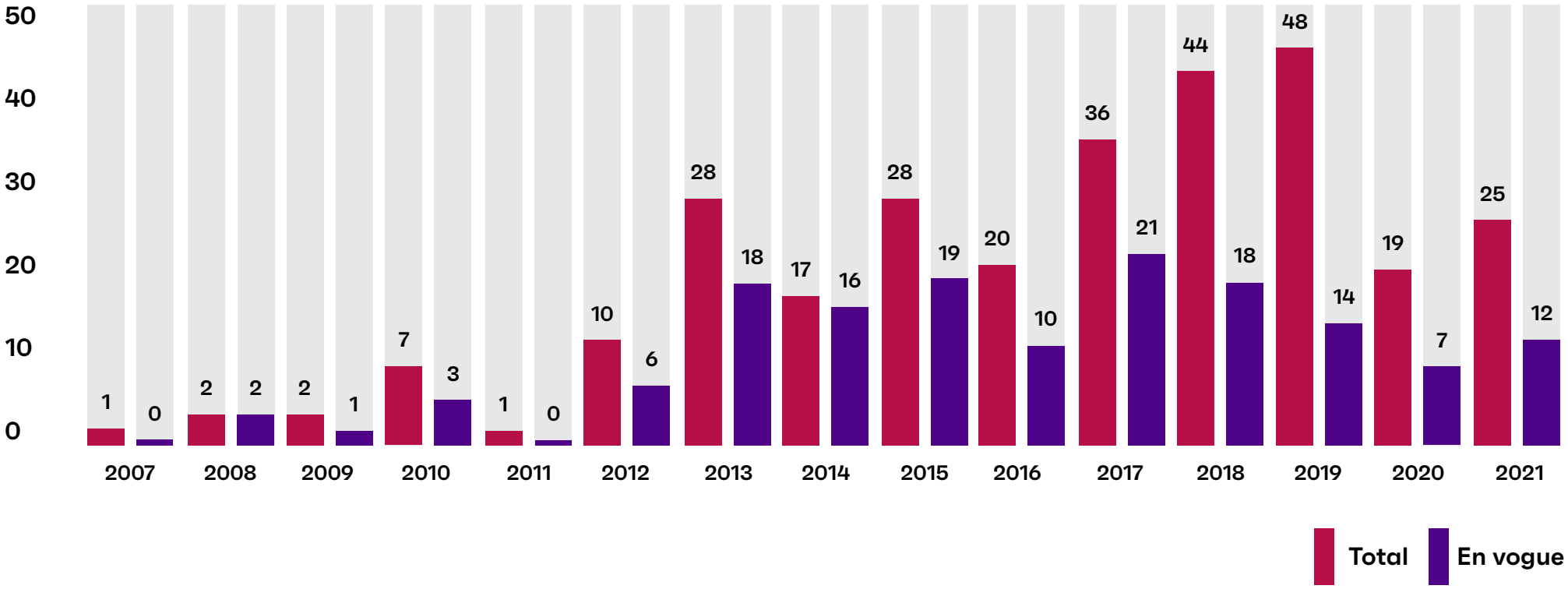
Trois des scanners de vulnérabilités les plus populaires (Nessus, Qualys et Nexpose) n'ont détecté que 77 % de toutes les vulnérabilités exploitables l'an dernier.[19]

ivanti

Les cybercriminels et les gangs de ransomwares peuvent toujours utiliser des vulnérabilités non critiques ou plus anciennes pour leurs attaques.

- Les entreprises qui appliquent uniquement les correctifs des CVE marquées du score CVSS Critique manquent 53 % des vulnérabilités exploitables liées aux ransomwares.[20]
- 92 % des vulnérabilités activement en vogue ont été divulguées publiquement avant 2021. Deux vulnérabilités récemment exploitées ont même été divulguées pour la première fois en 2008 ! [21]
- D'après une étude du Rand Consulting Group, les vulnérabilités sont toujours activement exploitées par les cybercriminels jusqu'à 7 ans après leur publication initiale.[22]

Vulnérabilités liées aux ransomwares et en vogue par année de publication NVD[23]



38 %

des entreprises victimes de cybercrimes perdent une semaine de productivité.

24 %

perdent un mois entier.

Les vulnérabilités sans correctif restent le vecteur d'attaque principal des organisations cybercriminelles par ransomware. L'absence de réponse rapide peut vite compromettre l'environnement de sécurité d'une entreprise, avec un impact significatif sur sa productivité et sa rentabilité.

De plus, comme le coût moyen d'une attaque par ransomware est estimé à 4,62 millions de dollars[24], une stratégie efficace de remédiation des vulnérabilités est essentielle pour que les équipes Sécurité et IT Ops puissent éliminer ces failles et ces vulnérabilités avec des correctifs.

Cependant, les équipes IT Ops ou Sécurité sont dans l'impossibilité de traiter l'ensemble des vulnérabilités, d'autant qu'elles sont souvent débordées ou en sous-effectif.

Les administrateurs de correctifs ont besoin d'un plan d'attaque stratégique qui optimise des ressources souvent limitées (temps, personnel et moyens internes) tout en gardant un temps d'avance sur les cybercriminels et autres pirates.

La solution : le RBPM (la gestion des correctifs basée sur les risques).

Le coût moyen d'une attaque par ransomware est estimé à

4,62 millions de dollars.

La gestion des correctifs basée sur les risques (RBPM) : vue d'ensemble

À la différence de l'approche linéaire traditionnelle qui consiste à traiter le profil de risques d'une entreprise avec une solution « à taille unique », la RBPM (gestion des correctifs basée sur les risques) adopte une approche de niche.

D'abord, les administrateurs collectent des informations auprès de sources externes : scanners de réseau, bases de données telles que NVD et CISA, et vulnérabilités trouvées lors des recherches manuelles et des tests d'intrusion.

Ils collectent également des points de données internes pour cartographier le profil de risque exact que présente l'ensemble du périmètre IT.

Ces données incluent :

- La liste des périphériques utilisés et des OS pris en charge par les équipes IT et Opérations.
- Tous les logiciels et applications actuellement utilisés par les utilisateurs finaux de l'entreprise, qu'il s'agisse de logiciels officiellement installés ou d'applications choisies par l'utilisateur, téléchargées ou hébergées dans le Cloud.
- Une bonne compréhension de la méthode de récupération des données propriétaires ou clients, de leur emplacement de stockage et de leur mode d'utilisation.

Les administrateurs de correctifs vont rapprocher les données sur les menaces et vulnérabilités externes de celles qui concernent l'environnement de sécurité propre à l'entreprise. Ils peuvent ainsi contextualiser les informations sur les menaces et prioriser les correctifs cruciaux, au lieu de se fier à la façon dont une source externe perçoit la menace.

Avec le RBPM, une équipe réduite peut gérer un nombre croissant de vulnérabilités et protéger l'entreprise, ses utilisateurs finaux et ses clients sans surcharger des équipes IT Ops et Sécurité déjà débordées.

4 avantages de l'approche de gestion des correctifs basée sur les risques (RBPM)

- Le RBPM constitue un **juste milieu pragmatique** entre « appliquer tous les correctifs » et l'« à-quoi-bonisme ».

- Le RBPM permet une **priorisation « basée sur la réalité »** des vulnérabilités, personnalisée pour votre entreprise, contextualisée avec des informations sur les attaques dans le monde réel afin de déterminer ce qui est vraiment important.

- Le RBPM peut être **plus rapide** qu'une approche traditionnelle de la gestion des correctifs.

- Le RBPM forme un **pont entre les différents départements** pour la sécurité et les Opérations IT.

ivanti

1. Le RBPM encourage une approche pragmatique (et pas idéalisée) des correctifs.

La méthode de gestion des correctifs basée sur les risques reconnaît et tient compte de la réalité que connaissent tous les administrateurs : il existe tout simplement trop de vulnérabilités et trop peu de ressources pour tout traiter.

En 2021, le nombre de vulnérabilités exploitées par des ransomwares a bondi de 29 % par rapport à l'année précédente.

D'un autre côté, il n'est pas non plus envisageable de ne rien faire : les vulnérabilités sans correctif sont le vecteur d'attaque le plus fréquemment exploité par les groupes de ransomwares et les cybercriminels. L'an dernier, le nombre de vulnérabilités exploitées par des ransomwares a bondi de 29 % par rapport à l'année précédente.[25]

Le juste milieu optimal entre « appliquer tous les correctifs » et l'« à-quoi-bonisme » est le RBPM.

Plus vite l'entreprise comprend qu'appliquer tous les correctifs sans distinction (ou même toutes les CVE portant le score CVSS ou le niveau de gravité fournisseur « Critique ») n'est plus un objectif réaliste, plus vite elle pourra passer à une stratégie de gestion des correctifs nouvelle, proactive, qui protégera mieux ses utilisateurs, ses systèmes et ses actifs.

De plus, d'après les études Gartner, même si une entreprise n'applique pas tous les correctifs, un programme complet de gestion

Un programme RBPM peut réduire de 80 % le nombre d'incidents de fuite de données d'une entreprise.

des vulnérabilités basée sur les risques (ce qui inclut le RBPM) peut réduire les incidents de fuite de données d'une entreprise de jusqu'à 80 %.[26]

Cet ajustement minime dans la stratégie de l'entreprise est source d'améliorations considérables.

2. Le RBPM est un processus de priorisation « basée sur la réalité », qui classe les risques en fonction du contexte de l'entreprise.

En triant les problèmes d'après le comportement des groupes criminels de ransomwares et les vulnérabilités exploitées (entre autres priorités, comme le potentiel RCE et PE des vulnérabilités), les administrateurs de correctifs obtiennent une évaluation plus réaliste de l'éventuel impact d'une vulnérabilité.

Cette évaluation traite les vulnérabilités non pas comme une menace isolée, mais elle s'intéresse aussi aux « chaînes de vulnérabilités » où plusieurs CVE sont exploitées ensemble.

On parle de chaînage des vulnérabilités lorsqu'un ransomware en exploite plusieurs en même temps, souvent d'âges et de niveaux de gravité différents, pour lancer une attaque complète sur une entreprise.

Par exemple, les attaques par ransomware LockFile de 2021[27] chaînent un total de 4 vulnérabilités de Microsoft Exchange et de l'OS Windows :

Les vulnérabilités « ProxyShell »

permettent non seulement aux cybercriminels d'accéder au réseau d'une entreprise et de déclencher du code à distance pour entraîner d'autres exploitations, mais aussi d'installer des portes dérobées pour un accès ultérieur.[28]

La vulnérabilité « PetitPotam »

permet au pirate de s'enfoncer encore plus profondément dans les systèmes de l'entreprise afin d'obtenir un accès plus large à des systèmes plus précieux et plus cruciaux.

Les entreprises qui suivent uniquement le processus linéaire traditionnel de gestion des correctifs n'ont sûrement pas corrigé toutes les vulnérabilités impliquées dans ces attaques ou d'autres similaires.

Parmi les quatre vulnérabilités chaînées dans le ransomware LockFile, une seule était classée Critique. Deux d'entre elles n'avaient qu'une importance « moyenne » – en matière de correctifs.[30]

Vulnérabilités LockFile

Vulnérabilité	Score CVSS	Gravité CVSS	Produit
CVE-2021-31207	7.2	Élevée	Microsoft Exchange Server
CVE-2021-34473	9.8	Critique	Microsoft Exchange Server
CVE-2021-34523	9.8	Moyenne	Microsoft Exchange Server
CVE-2021-36942	5.3	Moyenne	Microsoft Windows Windows Server 2008, 2012, 2016 et 2019

Et, même si les premières attaques par ransomware LockFile se sont produites en 2021, les études montrent qu'il existe encore plus de 34 000 expositions ProxyShell en ligne[29] … qui attendent seulement le prochain groupe de pirates susceptible d'exploiter ces vulnérabilités.

3. Le RBPM réduit le délai d'application des correctifs.

Plus une exposition critique reste longtemps sans correctif, plus l'entreprise est exposée aux fuites de données ou aux attaques par ransomware.

En 2021, le Department of Homeland Security, via la CISA (Cybersecurity and Infrastructure Security Agency), a émis la Directive Binding Operational Directive 22-01.

Ces nouvelles obligations, qui s'imposent aux entreprises du secteur public, réduisent le délai de correction des vulnérabilités critiques à deux semaines et suggèrent des calendriers ajustés supplémentaires en cas de « risque sévère » pour l'infrastructure de l'entreprise.[32]

Sachez par ailleurs que cette liste CISA des vulnérabilités qu'il est obligatoire de corriger contient 20 % de toutes les CVE actuellement identifiées comme activement exploitées par des familles de ransomwares.[33]

Ainsi, même quand les équipes de sécurité tirent parti d'un système de priorisation des vulnérabilités pour déterminer les correctifs les plus importants à appliquer, il lui reste des tonnes de vulnérabilités à corriger et peu de temps pour le faire.

Avec les méthodes traditionnelles de gestion des correctifs, les administrateurs passent parfois des heures à faire des recherches et à déterminer les actions à exécuter chaque fois qu'ils reçoivent un rapport de vulnérabilités.

À l'opposé, certains systèmes modernes de gestion des correctifs rapprochent automatiquement les informations de vulnérabilité avec les données de correctifs et le contexte de l'entreprise. Ces rapprochements améliorent la visibilité des risques propres à l'entreprise, accélèrent le processus global de remédiation et réduisent le nettoyage nécessaire après chaque cycle de maintenance.

La liste CISA des vulnérabilités qu'il est obligatoire de corriger contient seulement 20 % de toutes les vulnérabilités activement exploitées.

De plus, une approche complète de la gestion des correctifs basée sur les risques est la plus susceptible de contrer ou de limiter l'impact des vulnérabilités Zero-Day, car elle permet de :

- Simplement savoir que la vulnérabilité existe, afin que le correctif (lorsqu'il est publié) soit prioritaire pour publication et déploiement dans les systèmes de l'entreprise.
- Développer des stratégies ad hoc pour limiter l'impact des systèmes potentiellement vulnérables sans gêner les opérations quotidiennes.
- Configurer un système d'alerte interne pour être averti à l'instant même où un cybercriminel utilise cette vulnérabilité.

En découvrant et en priorisant les mises à jour de façon à protéger les systèmes les plus vulnérables, les administrateurs de correctifs utilisent aux mieux leurs ressources et protègent leurs systèmes contre les cybercriminels externes et les groupes de ransomwares.

Qu'est-ce qu'une vulnérabilité Zero-Day ?

Une vulnérabilité Zero-Day est :

- Identifiée par le fournisseur, souvent après une attaque qui l'exploite.
- Activement exploitée par des cybercriminels.
- Impossible à corriger (ou pour laquelle il n'existe aucun correctif).

4. Le RBPM réduit les frictions entre les équipes IT Ops et Sécurité.

La gestion des correctifs basée sur les risques crée un climat d'empathie :

L'équipe IT Ops

comprend mieux les priorités de la Sécurité et la logique qui détermine l'importance de tel ou tel correctif pour les vulnérabilités critiques.

L'équipe Sécurité

se rend mieux compte des impacts éventuels d'un correctif incorrect sur l'entreprise, des perturbations des applications critiques et de la vague de tickets utilisateur.

Quand l'équipe IT Ops reconnaît la capacité de l'équipe Sécurité à bien prioriser les correctifs (pour ne pas perdre leur temps ni celui des utilisateurs finaux à traiter toutes les vulnérabilités possibles), elle est plus encline à coopérer et à proactivement dégager du temps pour les risques de sécurité les plus importants.

Plus largement, un processus de gestion des vulnérabilités basé sur les risques permet aussi de sensibiliser les équipes sur ce qu'elles risquent de perdre si une vulnérabilité particulière n'est pas corrigée.(34)

Soudain, le correctif demandé ne résout pas simplement une vulnérabilité parmi d'autres : le risque est contextualisé en termes de résultats pour le service et l'entreprise, d'impact sur l'expérience utilisateur, et de chiffre d'affaires si une fuite n'est pas traitée.

Le coût moyen d'une attaque par ransomware était de 4,62 millions de dollars en 2021.(34)

L'inconvénient immédiat à court terme d'être contraint de trouver quelques heures pour la mise à jour est largement contrebalancé par le risque à long terme de perdre une semaine ou plus de son temps en raison d'une attaque par ransomware.

De même, quand l'équipe Sécurité n'essaie pas de tout corriger d'un seul coup, mais seulement les éléments importants, elle peut se montrer plus souple avec ses partenaires des Opérations IT — repousser l'application de correctifs hors des pics d'activité, condenser le cycle de maintenance et éviter de planter des systèmes lors de mises à jour non planifiées.

Une plateforme RBPM moderne centralise l'analyse des données et la priorisation en un seul emplacement ou tableau de bord accessible, ce qui présente des avantages.

L'équipe IT Ops

n'a pas besoin d'attendre que l'équipe Sécurité lui transmette les rapports de vulnérabilités. Elle voit dans le tableau de bord ce qui est le plus important pour son entreprise et commence immédiatement à tester les mises à jour dans un environnement sain pour améliorer le délai de réponse, y compris pour le mappage des CVE pertinentes dans les environnements internes.

L'équipe Sécurité

voit d'un seul coup d'œil l'état de déploiement des correctifs, les goulets d'étranglement potentiels et les correctifs en retard, qu'il faudra traiter lors d'un prochain sprint ou cycle de maintenance.

Le RBPM donne naissance à un processus de rapprochement mutuel. C'est la fin des interruptions constantes.

Peut-on mettre en œuvre manuellement sa stratégie RBPM ?

La gestion des correctifs basée sur les risques est une bonne alternative pour les équipes dont l'objectif est d'appliquer un maximum de correctifs, mais cette démarche n'est pas simple.

(En effet, si c'était facile, ce guide n'existerait pas.)

Définir les priorités en fonction des risques, suivre les vulnérabilités en temps réel, sans parler de l'exécution des tests adaptés et du déploiement des correctifs… il y a de quoi submerger rapidement les équipes non préparées qui tenteraient d'effectuer le RBPM à la main, sans outils explicites ou processus automatisés.

Prenons l'exemple d'une entreprise qui veut implémenter une stratégie RBPM. Elle veut éviter de se laisser submerger par d'innombrables sources de données et décide donc de se concentrer uniquement sur la base NVD, où 61 nouvelles vulnérabilités en moyenne ont été ajoutées chaque jour l'an dernier.[35]

Dans le cadre de sa stratégie RBPM, qui implique de contextualiser les nouvelles vulnérabilités avec la surface d'attaque possible en interne et non de reprendre telle quelle une évaluation externe de la criticité, l'équipe doit passer manuellement en revue ces 61 nouvelles vulnérabilités NVD tous les jours, pour définir 61 appels de priorisation distincts.

(La file d'attente qui attendra cette équipe chaque lundi sera terrible.)

De plus, notre entreprise hypothétique ne consulte qu'une seule source de données, même si elle est complète.

C'est ignorer l'immense flux d'informations brutes sur les vulnérabilités qui pourrait être disponible dans d'autres bases de données, études et rapports.

Répercussions dans le monde réel :

rapprochement des vulnérabilités et des correctifs

Dans leurs conversations avec les experts Ivanti, les équipes IT Ops et Sécurité du monde entier mentionnent en passant que les rapports traditionnels de rapprochement des vulnérabilités et des correctifs, rédigés manuellement, représentent au moins 8 heures de travail.

Cependant, dans l'intérêt de la discussion, disons que notre entreprise a suffisamment de personnel dans ses équipes IT Ops et Sécurité pour surveiller à intervalle régulier de gros fournisseurs comme Microsoft, Apple, Linux et autres éditeurs d'applis pour détecter les vulnérabilités et leurs exploitations dès qu'elles sont divulguées.

Il existe même des sites Internet, comme PatchMangement.org, Reddit et le webinar Ivanti Patch Tuesday , qui répertorient les vulnérabilités particulièrement pertinentes. Ces sites Web et d'autres sont évidemment d'excellentes ressources pour aider les équipes à explorer cette portion du processus RBPM, gratuitement !

Pourtant, la surveillance est seulement l'une des nombreuses tâches à effectuer avant la fin du cycle de correctifs.

Dans le cadre du processus RBPM, les équipes IT Ops et Sécurité de notre entreprise hypothétique doivent encore :

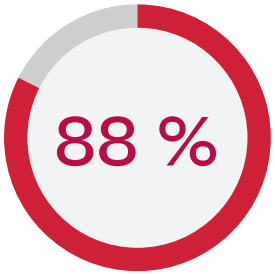
- Identifier tous les appareils et applications internes, approuvés par le service IT et installés par l'utilisateur.
- Déterminer les utilisateurs finaux et cas d'usage auxquels appliquer les correctifs en premier.
- Tester le correctif pour toutes les variations et variantes, ou sur autant de cas de figure que nécessaire pour la vulnérabilité concernée.
- Planifier et exécuter le déploiement du correctif.

Dans les environnements hybrides ou entièrement distants, en particulier, ces procédures peuvent dégénérer en processus interminables qui ne tiennent pas le rythme de la réalité.

Enfin, et surtout, de nombreux systèmes manuels utilisent une documentation et un rapprochement de bases de données de type feuille de calcul.

Cependant, compter sur des feuilles de calcul ouvre tout simplement la porte aux erreurs. Plus les personnes qui modifient fréquemment le même rapport sont nombreuses, plus il y a de risques d'avoir des erreurs qui font boule de neige, et provoquent des corrections et des retards coûteux.

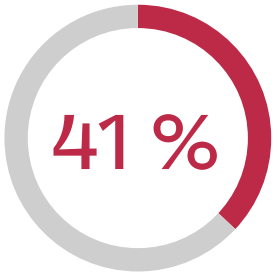
En fait, une étude montre que 88 % des feuilles de calcul contiennent des erreurs « significatives », dont la plupart causées par les personnes mêmes qui les utilisent ![(36)]



des feuilles de calcul contiennent des erreurs « significatives » dues à l'erreur humaine.

Ainsi, même si la mise en œuvre manuelle d'une stratégie de gestion des correctifs basée sur les risques est parfaitement possible, en particulier au tout début pour se familiariser avec cette approche avant d'acheter des outils dédiés, c'est loin d'être la configuration optimale pour les équipes qui souhaitent vraiment adopter l'approche RBPM.

Ajouter davantage d'opérations manuelles alors que 41 % des entreprises interrogées signalent qu'elles ont perdu du personnel IT en raison des trop lourdes charges de travail semble également peu judicieux.[37]



des entreprises interrogées signalent qu'elles ont perdu du personnel IT critique en raison des trop lourdes charges de travail.

Finalement, une approche entièrement manuelle finira par tuer dans l'œuf votre plan RBPM, en raison des interminables opérations d'administration et des retards occasionnés.

5 meilleures pratiques pour une stratégie RBPM réussie

1. On ne peut corriger que ce qu'on connaît.
2. Les équipes IT Ops et Sécurité doivent jouer la même partition.
3. Travailler en parallèle selon un SLA interne.
4. Définir des groupes pilotes.
5. Automatiser !

ivanti

1. Découvrir ce que vous possédez et comment vous l'utilisez.

Vous ne pouvez pas protéger ni corriger quelque chose dont vous ignorez l'existence. Par conséquent, la découverte des actifs (trouver ce que vous avez, avec quels profils utilisateur final) joue un rôle critique dans tout projet de gestion des vulnérabilités.

Gestion des actifs pour le RBPM

Les outils modernes de gestion des actifs aident les entreprises à comprendre et à suivre leur pile technologique actuelle. La première étape consiste à identifier tous les périphériques (ordinateurs portables, ordinateurs de bureau, téléphones, tablettes, serveurs et périphériques réseau) et logiciels utilisés dans l'entreprise.

Comme dans la stratégie évoquée précédemment, les informations sur vos actifs doivent provenir de plusieurs sources, notamment :[38]

- ☐ Microsoft Endpoint Configuration Manager (SCCM) et Microsoft Intune
- ☐ Fichiers CSV ou feuilles de calcul
- ☐ Microsoft Active Directory
- ☐ Workspace One (AirWatch)
- ☐ Ivanti Neurons for Discovery

Une fois tous les actifs répertoriés, vous devez éliminer les doublons et vous assurer de la cohérence des données dans la base de données.

Enfin, et surtout, les gestionnaires d'actifs de l'équipe IT Ops organisent les enregistrements, ce qui permet aux administrateurs de correctifs de trouver les terminaux les plus critiques et les faiblesses potentielles. Autant d'informations qui vous aideront à prioriser vos correctifs.

Cartographie des services pour le RBPM

Extension du processus de découverte, la cartographie des services sert à repérer les systèmes à gérer et à sécuriser, en mettant en évidence les interconnexions entre ces systèmes (et les données qu'ils utilisent) et les modes d'accès.

Une carte des services peut contenir :

- L'inventaire de l'infrastructure et du matériel.
- Les applications, la documentation de configuration et la bibliothèque de logiciels répertoriant la version la plus récente des logiciels utilisés.
- Les paramètres et diagrammes réseau, qui mettent en évidence les flux d'informations et la façon dont les périphériques se connectent dans toute l'entreprise.
- Les utilisateurs finaux, profils d'utilisateur et terminaux à haut risque, ainsi que le niveau d'impact de chacun sur les systèmes critiques de l'entreprise en cas de compromission.

Les équipes de sécurité déterminent ensuite le chemin à suivre pour profiter d'une vulnérabilité et atteindre un système critique via les systèmes utilisateur ou applications connectés.

En même temps, l'équipe IT Ops va mieux appréhender les connexions des nombreux systèmes aux applications critiques : elle obtient ainsi des informations importantes sur comment configurer et implémenter au mieux les tests de correctifs.

2. Garantir que tout le monde a accès aux mêmes informations.

L'efficacité de la gestion des correctifs basée sur les risques dépend de la capacité de vos équipes IT Ops et Sécurité à collaborer pour synchroniser leurs interventions. Pour ce faire, elles auront probablement besoin d'aide pour s'aligner de manière interfonctionnelle afin d'atteindre tous leurs objectifs.

Théoriquement, toutes les équipes doivent viser le même objectif : une entreprise sécurisée qui peut faire son travail sans être interrompue par des cyberattaques.

En pratique, leurs objectifs semblent diamétralement opposés : l'équipe Sécurité cherche à atténuer les risques, tandis que l'équipe IT Ops veut optimiser les performances et l'expérience de l'utilisateur final.

L'équipe Sécurité

avait tendance à tout considérer comme un risque, mais elle manquait souvent de moyens pratiques d'identifier les menaces pertinentes pour l'entreprise et de connaissances sur l'impact des déploiements de correctifs sur le travail quotidien.

L'équipe IT Ops

doit trouver l'équilibre entre les accords de niveau de service (SLA) conclus avec les utilisateurs finaux pour que le travail quotidien se déroule comme prévu et une menace théorique de ransomware potentiel qui semble sans fin.

Un bon système RBPM va chercher à atténuer ce point de friction naturel grâce au partage d'informations et à une analyse des risques comprise par tous.

L'équipe Sécurité

ne priorisera que les vulnérabilités réellement importantes pour la cybersécurité de l'entreprise.

L'équipe IT Ops

verra par elle-même comment les vulnérabilités peuvent affecter ses utilisateurs finaux en temps réel, et sera donc plus disposée à consacrer du temps aux déploiements.

3. Travailler en parallèle pour accélérer l'application des correctifs via un SLA RBPM.

Dans un scénario optimal, la solution de gestion des correctifs basée sur les risques informe toutes les parties concernées des vulnérabilités et de la façon de les contrer en temps réel.

Les équipes IT Ops et Sécurité doivent utiliser et comprendre la même méthodologie de priorisation des risques. Elles peuvent ainsi fonctionner en parallèle et se synchroniser à différents stades du processus de remédiation pour s'assurer de rester d'accord sur les problèmes à résoudre.

Cette approche peut réduire le cycle de maintenance de plusieurs semaines à quelques jours ou quelques heures, selon la gravité des vulnérabilités et la synchronisation de chaque équipe avec ses partenaires des autres départements.

Les équipes IT Ops et Sécurité doivent toutes les deux mettre en place les meilleures pratiques en interne et s'entendre sur des fenêtres de maintenance qui tiennent compte des objectifs de chaque équipe, ainsi que des objectifs globaux de l'entreprise.

À cette fin, envisagez de créer un accord de niveau de service (SLA) pour la gestion des correctifs, entre les équipes IT Ops et Sécurité.

Création de votre SLA

Ce SLA doit définir les attentes en matière de collaboration et de délais pour chaque étape, afin que chacun sache ce qui va se passer, quand et par qui.

Le SLA doit intégrer :

- **Toutes les définitions,** même pour les éléments les plus évidents (par ex. définition de ce qu'on entend par « vulnérabilité »)
- **Les spécifications nécessaires** et les piles technologiques déployées à chaque étape.
- **Les critères de priorisation des vulnérabilités.**
- **La fréquence des communications** au cours du cycle d'application des correctifs.
- **Les exceptions explicites** relatives aux situations impliquant la remédiation des vulnérabilités hors bande et/ou en dehors du cycle de maintenance habituel.

Il faut accorder une attention particulière à la définition d'indicateurs de performance clés (KPI) réalisables et réalistes pour tous les services concernés, avec des KPI partagés chaque fois que c'est possible.

Répercussions dans le monde réel :

SLA de correctifs et de vulnérabilités

Un grand fabricant mondial avec plus de 100 000 appareils a informé Ivanti de la mise en œuvre d'un SLA de vulnérabilités entre ses équipes IT Ops et Sécurité.

Depuis, cette entreprise a atteint un taux de conformité de remédiation des vulnérabilités de 95 %, dans le délai de 2 semaines dicté par le SLA.

4. Définir des groupes pilotes avec les principales parties prenantes pour prioriser et tester les correctifs.

Les groupes pilotes sont des groupes prédéterminés (et préentraînés) de rôles d'utilisateur et de configurations de périphériques représentatifs. Il s'agit de leur faire tester les correctifs de vulnérabilité dans un environnement réel avant le déploiement global.

Après tout, si un correctif doit faire planter un logiciel critique, il est préférable que cela se produise sur quelques machines plutôt que d'arrêter toute l'entreprise.

Les groupes pilotes complètent les environnements de laboratoire de tests contrôlés, pour mieux prédire l'impact des correctifs sur l'activité.

De fait, les systèmes de test déterminent rarement l'impact en aval : il est indispensable de déployer votre correctif à un ou plusieurs groupes pilotes pour réduire les éventuels effets négatifs sur vos opérations.

"Après tout, si un correctif doit faire planter un logiciel critique, il est préférable que cela se produise sur quelques machines plutôt que d'arrêter toute l'entreprise."

Adhésion des groupes pilotes

Cette bonne pratique exige que vos administrateurs de correctifs obtiennent l'adhésion de l'ensemble de l'entreprise (et pas seulement de l'IT Ops). En effet, réunir des groupes pilotes pertinents implique la participation de tous les groupes d'applications ou les départements essentiels où des systèmes critiques sont en place.

À cette fin, **sortez de votre rôle habituel et demandez directement aux groupes d'utilisateurs cibles** comment leurs périphériques et leurs données interagissent, ainsi que l'impact de chaque mise à jour sur leurs processus habituels.

Vous rehausserez votre réputation si vous posez la question avant qu'un correctif n'arrête accidentellement leurs applications pendant les heures ouvrables. De plus, les liens créés serviront à former de futurs groupes pilotes, avec des parties prenantes impliquées qui offriront proactivement leur aide et des informations que vous n'auriez pas autrement.

Création de vos groupes pilotes

Les groupes pilotes doivent :

- **Être organisés comme suit :** au moins un groupe pilote « principal » initial (pour vous assurer que rien de majeur n'est endommagé), puis des groupes pilotes plus larges pour identifier les problèmes plus rares ou propres aux applications.
- **Tenir compte des objectifs** de l'entreprise et des buts spécifiques de tous les départements concernés (IT Ops et Sécurité).
- Remonter leur avis à tout moment.
- **Représenter** tous les appareils utilisés dans l'entreprise pour identifier les problèmes de compatibilité des correctifs.
- **Tenir compte de tous les profils d'utilisateur** (également appelés « persona d'utilisateur ») dans l'environnement de l'entreprise.

Les collaborateurs et les parties prenantes, membres ou non des groupes pilotes, doivent comprendre pourquoi la correction des vulnérabilités est essentielle à la réduction du risque de ransomwares et d'autres cyberattaques.

Le message doit être clair : les tests sont essentiels à la sécurité de l'entreprise et de votre travail. En supportant une légère gêne sur votre périphérique en tant que membre d'un groupe pilote de test, vous sauvez l'ensemble du service d'une panne critique.

Répercussions dans le monde réel :

PrintNightmare[39]

En juin 2021, un chercheur a découvert une vulnérabilité RCE dans le spouleur d'impression Windows.

- Lorsque Windows a publié un correctif de vulnérabilité pour le spouleur d'impression au cours de ce même mois de juin, le chercheur a pensé que cette exploitation spécifique avait été résolue et a publié ses conclusions… pour découvrir finalement que Windows avait corrigé une autre vulnérabilité.
- Les cybercriminels ont très rapidement exploité ces recherches, avec des exploitations actives permettant aux pirates de prendre à distance le contrôle du système visé, avec des permissions de niveau Administrateur.
- La première exploitation PrintNightmare a reçu le 1er juillet 2021 un correctif qui a été suivi d'une nouvelle publication le 16 juillet 2021.
- Depuis, plusieurs autres correctifs du spouleur d'impression ont été publiés… dont 4 nouveaux en mai 2022.

De nombreuses entreprises donnent désormais la priorité à ces correctifs pour la remédiation et les tests en groupe pilote, en raison de l'énorme impact opérationnel.

Juin 2021
Un chercheur découvre une vulnérabilité du spouleur d'impression Windows.

Juillet 2021
Windows publie les premiers correctifs PrintNightmare.

Juin 2021
Windows corrige une vulnérabilité différente ; le chercheur publie ses conclusions.

Mai 2022
4 nouveaux correctifs de spouleur d'impression sont publiés.

5. Automatiser, surtout pour les déploiements.

En matière de gestion des correctifs basée sur les risques, l'automatisation présente de nombreux avantages, notamment pour la collecte, la contextualisation et la priorisation des rapports de vulnérabilité externes.

Comme nous l'avons déjà évoqué, essayer de mettre en place une initiative RBPM manuelle serait très difficile, c'est le moins qu'on puisse dire… sans parler de l'impact sur vos mesures de rétention du personnel.

Cependant, l'automatisation aide également à segmenter le déploiement de correctifs pour en garantir le bon déroulement et l'application à grande échelle.

Meilleures pratiques de déploiement automatisé des correctifs

Les règles d'automatisation et les portes logiques permettent d'appliquer les meilleures pratiques sur les systèmes de test, les groupes pilotes, puis des groupes de production de plus en plus larges, afin de créer une expérience de gestion des correctifs qui accélère l'exécution tout en minimisant l'impact sur l'entreprise.

Envisagez de commencer votre déploiement automatisé des correctifs avec un premier groupe de test. Étendez ensuite votre champ d'action à :

1. **Un groupe pilote initial dans votre environnement actif.**
2. **De premiers** utilisateurs ayant adopté le système, à raison d'environ 10 % de votre environnement.
3. **Le reste (majorité)** des utilisateurs finaux de l'entreprise.

Pour ce cas d'usage, les administrateurs de correctifs peuvent définir des critères et attribuer à chaque utilisateur final un rôle spécifique dans chaque groupe distinct, dans le cadre d'un déploiement de correctifs complet. L'automatisation détermine ensuite qui doit obtenir le correctif et quand.

Les administrateurs de correctifs peuvent programmer le processus automatisé pour qu'il fonctionne avec des règles et des critères d'acceptation complexes, par exemple en exigeant un taux de réussite spécifique ou une remontée d'informations directe de la part des utilisateurs pour déclencher une nouvelle étape de déploiement.

Avantages de la maintenance automatisée

L'automatisation peut gérer la maintenance régulière, laissant au personnel plus de temps pour améliorer la collaboration, prendre en charge un processus de rapprochement cohérent et traiter les menaces exceptionnelles lorsqu'elles arrivent.

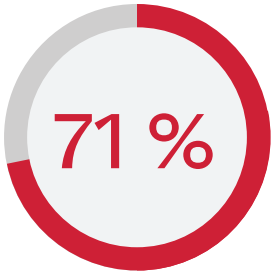
Les équipes IT Ops et Sécurité peuvent même codévelopper et configurer des contrôles de sécurité automatisés : l'équipe Sécurité peut alors exécuter et superviser des activités de confinement plus réduites, activées par des déclencheurs prédéterminés, sans dépendre de l'équipe IT Ops pour chaque tâche.

Comment choisir un fournisseur de solution RBPM

71 % des professionnels de l'IT et de la sécurité trouvent l'application des correctifs trop complexe et chronophage[40], principalement parce qu'ils manquent d'outils adéquats pour soutenir leur stratégie de gestion des correctifs.

Avant d'implémenter une approche basée sur les risques, évaluez vos processus actuels de gestion des vulnérabilités et des correctifs. Les équipes IT Ops et Sécurité doivent aligner leurs objectifs et s'entendre sur les mesures à utiliser.

Plus précisément, les deux équipes doivent accepter d'utiliser la même approche basée sur les risques et le même système de classement - pour prioriser les mises à jour, ce dernier doit prendre en compte plus de critères que les scores de gravité fournisseur et les scores CVSS.



71 % des professionnels de l'IT et de la sécurité interrogés trouvent l'application des correctifs complexe et trop longue.[41]

Votre prochaine plateforme de gestion des correctifs basée sur les risques doit inclure les critères suivants :

- ☐ **Données** provenant de scanners de réseau, de postes client, de bases de données, de constatations, de périphériques IoT et d'autres sources indépendantes pour fournir un haut niveau d'insights.
- ☐ **Prise en charge hétérogène** qui couvre tous les systèmes d'exploitation supportés en interne.
- ☐ **Des insights sur les menaces** (vulnérabilités liées aux ransomwares ou pouvant être exploitées pour RCE ou PE), provenant à la fois du renseignement humain et d'autres sources de Threat Intelligence.
- ☐ **Un système clair d'évaluation des risques** (automatique ou personnalisable lors de la configuration), qui tient compte des attributs intrinsèques de chaque vulnérabilité et du contexte des menaces dans le monde réel, pour un maximum d'exactitude et de pertinence.
- ☐ **Prise en compte de facteurs de risque uniques,** en fonction des actifs de votre entreprise, de plusieurs sources de Threat Intelligence et de l'accessibilité externe.
- ☐ **Capacités d'automatisation** (ou intégration avec des réseaux d'automatisation) pour la remédiation et la surveillance des risques.
- ☐ Alertes et notifications transférables à des profils d'utilisateur spécifiques en fonction des besoins et de l'urgence de chaque utilisateur.
- ☐ **Des tableaux de bord prêts à l'emploi et/ou personnalisables** pour partager rapidement les informations pertinentes avec la partie prenante appropriée, sans attendre un transfert d'e-mail ou des rappels en chaîne.
- ☐ **Filtres personnalisables basés sur les menaces,** montrant comment les vulnérabilités exploitées se manifestent dans l'environnement particulier d'une entreprise.

Sources citées

1. The National Vulnerability Database, données de mai 2022
2. « The Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management »
3. « 48,285+ Vulnerabilities Beyond the NVD » : Une enquête Ivanti
4. The National Vulnerability Database, données de mai 2022
5. « 48,285+ Vulnerabilities Beyond the NVD » : Une enquête Ivanti
6. « 48,285+ Vulnerabilities Beyond the NVD » : Une enquête Ivanti
7. « The Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management »
8. The Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
9. « The Problem With Patching Only Critical Vulnerabilities » : Étude de cas Microsoft sur les vulnérabilités Zero-Day
10. « Everything You Need to Know About Bluekeep »
11. « The Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management »
12. « 2016 Data Breach Investigations Report »
13. Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits
14. « Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits »(2021)
15. « Top IT Trends for the Everywhere Workplace »(2021)
16. Les défis de la gestion des correctifs : Résultats d'enquête et informations, alors que les entreprises passent à l'Everywhere Workplace(2021)
17. 7 tendances des ransomwares que vous devez connaître (2021)
18. Les défis de la gestion des correctifs : Résultats d'enquête et informations, alors que les entreprises passent à l'Everywhere Workplace(2021)
19. « The Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management »
20. « The Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management »
21. « The Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management »
22. « Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits »
23. « The Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management »
24. IBM Security : « Cost of a Data Breach Report 2021 »
25. « The Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management »
26. « Implement a Risk-Based Approach to Vulnerability Management »
27. « The Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management »
28. « Microsoft Exchange ProxyShell and Windows PetitPotam vulnerabilities chained in New Attack »
29. « The Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management »
30. « The Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management »
31. « The Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management »
32. Directive opérationnelle contraignante (BOD) 22-01, « Reducing the Significant Risk of Known Exploited Vulnerabilities » (Réduction des risques sévères liés aux vulnérabilités dont l'exploitation est connue)
33. Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
34. https://www.ibm.com/downloads/cas/OJDVQGRY
35. « The Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management »
36. Pank, Raymond R. « What We Know About Spreadsheet Errors. » Journal of Organizational and End User Computing (JOEUC) 10, numéro 2 : 15-21. http://doi.org/10.4018/joeuc.1998040102
37. « Top IT Trends for the Everywhere Workplace » (2021)
38. « Why IT Asset Management is Like Building a Jigsaw Puzzle »
39. Patch Tuesday de mai 2022
40. Les défis de la gestion des correctifs : Résultats d'enquête et informations, alors que les entreprises passent à l'Everywhere Workplace
41. Les défis de la gestion des correctifs : Résultats d'enquête et informations, alors que les entreprises passent à l'Everywhere Workplace

À propos d'Ivanti

Ivanti rend possible l'Everywhere Workplace. Dans l'Everywhere Workplace, les collaborateurs utilisent une multitude de périphériques pour accéder aux réseaux, aux données et aux applications du département IT, afin de rester productifs en travaillant de partout. La plateforme d'automatisation Ivanti connecte les solutions Ivanti de gestion unifiée des terminaux (UEM), de sécurité Zero Trust et de gestion des services d'entreprise (ESM), leaders du marché, afin d'offrir aux entreprises une vitrine unique permettant l'autoréparation et l'autosécurisation des périphériques, et le self-service aux utilisateurs. Plus de 40 000 clients, dont 96 des entreprises Fortune 100, ont choisi Ivanti pour découvrir, gérer, sécuriser et servir leurs actifs IT du Cloud à la périphérique, ainsi que pour fournir une expérience utilisateur final d'excellence aux collaborateurs, où qu'ils se trouvent et quelle que soit la façon dont ils travaillent. Pour en savoir plus, visitez le sitet ivanti.com

À propos d'Ivanti Neurons for Patch Management

Ivanti Neurons for Patch Management est une solution native de gestion des correctifs dans le Cloud, qui fournit des informations utiles sur l'exposition active aux risques, la fiabilité des correctifs et la conformité des périphériques, l'état de santé et les risques. Elle aide les entreprises à mieux se protéger contre les menaces, y compris les ransomwares.

ivanti.fr
+33 (0)1 76 40 26 20
contact@ivanti.fr