

Les défis de la gestion des correctifs

Résultats d'enquête et d'informations, alors que les entreprises passent à l'Everywhere Workplace

Introduction

L'environnement de travail actuel ne se limite plus à un espace confiné où des PC contrôlés par le département IT constituent le centre de productivité. Les entreprises sont aujourd'hui mieux réparties géographiquement que jamais, ce qui élargit leur surface d'attaque. Dans l'Everywhere Workplace, les collaborateurs se connectent sur différents périphériques pour accéder aux réseaux, données et services de l'entreprise, car ils travaillent et interagissent depuis des endroits nouveaux, inhabituels. C'est pourquoi l'application des correctifs devient plus complexe.

En parallèle, les équipes IT et Sécurité se battent pour garder le contrôle d'un environnement de télétravail qui ne cesse de s'étendre. Il est nécessaire de protéger le nouvel espace de travail en ligne et de le tenir à jour à l'aide des correctifs de sécurité les plus récents, mais cela devient de plus en plus difficile.

Défis

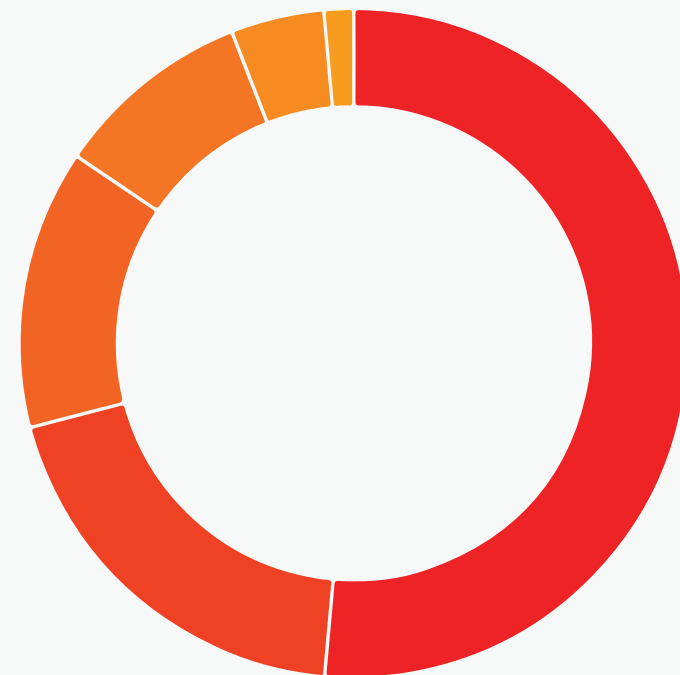
Une nouvelle étude Ivanti montre que 71 % des professionnels de l'IT et de la sécurité trouvent l'application des correctifs trop complexe et trop longue. Les pirates amènent leurs tactiques à maturité et font des vulnérabilités des armes, surtout celles liées à l'exécution de code à distance. C'est pourquoi les entreprises ont du mal à gérer leur surface d'attaque, et cherchent à accélérer la mise en application des correctifs et les actions correctives.

Les professionnels de l'IT et de la sécurité n'arrivent tout simplement pas à réagir assez vite : 53 % disent que l'organisation et la priorisation des vulnérabilités critiques leur prennent presque tout leur temps. C'est inquiétant, parce que plus une vulnérabilité reste longtemps sans correctif, plus l'entreprise est exposée aux risques d'attaque ou de ransomware. Cependant, aucune entreprise ne peut combler toutes ses vulnérabilités, et il faut rapidement définir un ordre de priorité sur la base des risques pour anticiper les attaques automatisées des pirates. Aujourd'hui, les vulnérabilités sans correctif restent l'un des principaux points d'infiltration des attaques par ransomware, qui sont devenues plus fréquentes et impactent des entreprises de toutes tailles.

Les équipes IT et Sécurité passent aussi énormément de temps à résoudre les problèmes d'échec de l'application d'un correctif (19 %), à tester les correctifs (15 %) et à se coordonner avec les autres départements (10 %). La multitude de difficultés que les équipes IT et sécurité doivent résoudre concernant l'application des correctifs explique peut-être pourquoi 49 % des personnes interrogées pensent que les protocoles actuels de gestion des correctifs dans leur entreprise ne limitent pas efficacement les risques.

D'après les professionnels de l'IT et de la sécurité, voici ce qui prend le plus de temps chaque mois:

- 53% - Organisation et priorisation des vulnérabilités
- 19% - Résolution des problèmes d'échec de l'application d'un correctif
- 15% - Test des correctifs
- 10% - Coordination avec les autres départements
- 3% - Mise en conformité
- 1% - Tenue des registres



Causes

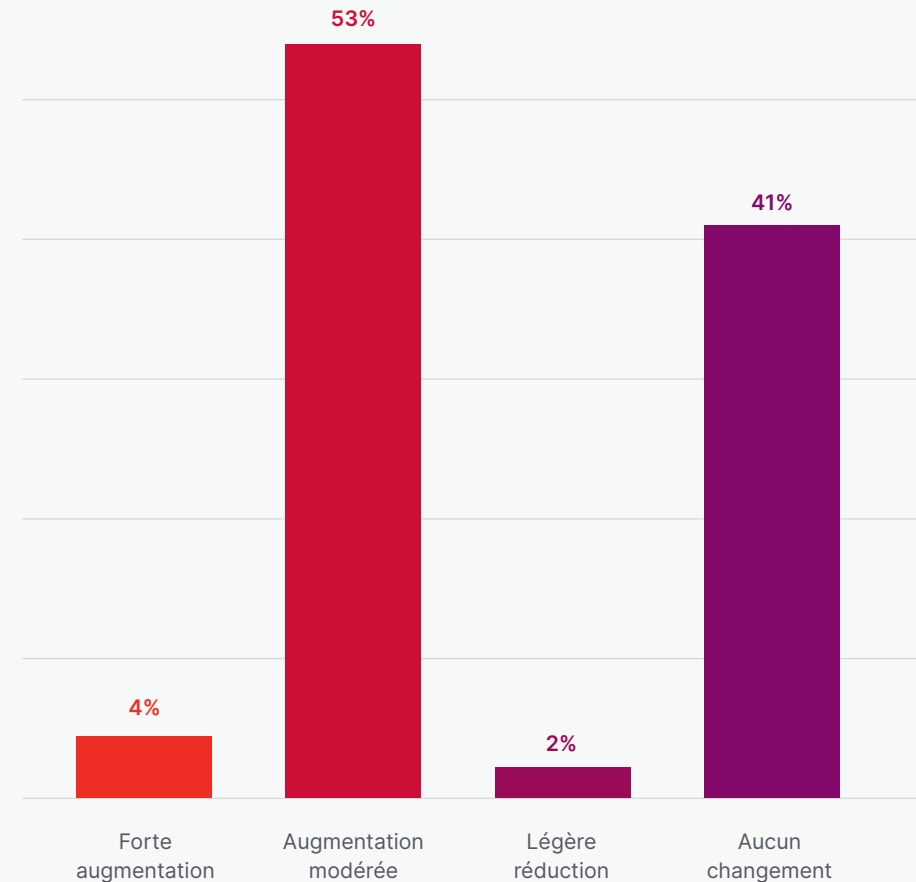
La majorité (57 %) des personnes interrogées pense que le passage mondial à un espace de travail décentralisé a rendu la gestion des correctifs plus complexe. Le champ d'action de la gestion des correctifs a également augmenté, avec la multiplication des différents postes client disponibles pour les utilisateurs, et des systèmes métiers indispensables qui les prennent en charge, de Windows à macOS, en passant par Linux et Windows Servers, entre autres.

Enfin, il est difficile d'appliquer des correctifs à certains systèmes IT parce qu'ils provoquent des coupures. 61 % des professionnels de l'IT et de la sécurité (et c'est énorme) expliquent que les responsables métiers leur demandent une seule fois par trimestre de retarder la fenêtre de maintenance. Et 28 % de plus disent qu'ils reçoivent cette demande tous les mois.

Dans le même temps, la vitesse à laquelle les vulnérabilités deviennent des armes continue d'augmenter, surtout pour les vulnérabilités RCE (celles qui permettent d'exécuter du code à distance). Ces points provoquent une situation qui mène à un manque de visibilité causé par le passage récent au fait de travailler depuis partout, et des pirates toujours plus nombreux qui sont prompts à repérer les vulnérabilités exploitables et à en profiter.

En outre, de nombreuses entreprises n'ont pas l'expertise de la sécurité ou le temps nécessaire pour que leurs ressources puissent collecter des informations sur les menaces et comparer les menaces actives avec les vulnérabilités de l'entreprise pour créer un contexte de gestion des menaces sur la base des risques. Pour de nombreuses entreprises, le manque de personnel IT limite la capacité à résoudre rapidement les problèmes de sécurité. Et dans ce type d'entreprise, les cyberattaques, surtout par ransomware, se sont montrées particulièrement dévastatrices.

Dans quelle mesure le télétravail a-t-il augmenté la complexité et le champ d'action de la gestion des correctifs dans votre entreprise?



L'environnement des menaces

Alors que les équipes IT luttent pour gérer l'augmentation de la surface d'attaque, les pirates amènent leurs tactiques à maturité et surveillent les aspects des entreprises où les vulnérabilités sont les plus nombreuses. Ils ont trouvé un équilibre : ils allient persistance acharnée et patience avec une utilisation sophistiquée des exploitations, des outils et des technologies émergentes. Leur principal objectif est de perturber, de voler et d'obtenir un gain financier en exploitant les activités de l'entreprise.

Une autre enquête d'Ivanti montre qu'une très large portion (63 %) des personnes interrogées disent que leur entreprise a subi une attaque par ransomware au cours de l'année écoulée. Et 89 % disent que les ordinateurs portables, les ordinateurs de bureau et les périphériques mobiles sont les équipements les plus souvent ciblés.

Les pirates sont toujours à l'affût de vulnérabilités, et les équipes IT et Sécurité ont du mal à définir la priorité de leurs efforts de gestion des correctifs pour supprimer rapidement toute exposition des vulnérabilités.

Le ransomware WannaCry, dont on estime qu'il a crypté 200 000 ordinateurs dans 150 pays, reste (même quatre ans plus tard) l'exemple suprême des graves répercussions que peut avoir un retard dans l'application des correctifs. Le correctif de la vulnérabilité concernée existait déjà depuis plusieurs mois quand l'attaque initiale s'est produite. Pour autant, de nombreuses entreprises ne l'avaient pas appliqué. Et même aujourd'hui, les deux tiers des entreprises n'ont toujours pas appliqué de correctifs à leurs systèmes.

Pourtant, des entreprises sont toujours visées par des attaques au ransomware WannaCry partout dans le monde; on a constaté une augmentation de 53% du nombre d'entreprises infectées par WannaCry entre janvier et mars 2021.

Création d'un contexte de confiance pour la gestion de la sécurité et des risques

L'expansion du paysage de travail et la transformation numérique vont continuer. Cependant, il faut trouver un moyen d'étendre le contexte de confiance pour la gestion de la sécurité et des risques.

L'implémentation d'une structure Zero Trust est absolument indispensable pour sécuriser les données d'entreprise sensibles de tout accès non autorisé et pour protéger les failles de cybersécurité contre les attaques. Dans sa version la plus simple, le Zero Trust permet aux entreprises d'évaluer en continu les périphériques de collaborateurs, les postes clients, les biens et les réseaux sur lesquels elles reposent.

En mai 2021, le Président Biden a signé une injonction officielle stipulant que les agences fédérales doivent prendre des mesures pour implémenter une stratégie de sécurité Zero Trust. La sécurité Zero Trust est aussi l'une des principales priorités des professionnels de l'IT et de la cybersécurité: d'après une récente étude menée par Ivanti, 98 % des professionnels de l'IT et de la sécurité en Amérique du Nord disent que leurs pratiques de sécurité vont davantage s'aligner sur une stratégie Zero Trust dans l'année à venir.

Un contexte de confiance examine le niveau de risque des périphériques, postes clients et biens utilisés dans l'Everywhere Workplace. Il faut comprendre le niveau de vulnérabilité acceptable et connaître les correctifs dont l'application est requise pour répondre aux besoins de confiance définis par l'entreprise. La gestion des correctifs sur la base des risques va donc s'avérer encore plus précieuse.

Les principaux chefs d'entreprise, professionnels et cabinets d'analyse recommandent une approche basée sur les risques, qui identifie et priorise les vulnérabilités, puis accélère leur correction et la rend plus efficace. La Maison-Blanche a récemment publié un décret afin d'encourager les entreprises à adopter une stratégie d'évaluation basée sur les risques pour leur gestion des correctifs et renforcer la cybersécurité face aux attaques par ransomware. De plus, Gartner cite la gestion des vulnérabilités sur la base des risques comme un projet de sécurité prioritaire, sur lequel les professionnels de la sécurité et de la gestion des risques doivent se concentrer en 2021 afin de générer de la valeur commerciale et limiter les risques.



Conclusion

Bien que l'Everywhere Workplace ait boosté la productivité, il a aussi provoqué une augmentation en flèche du nombre de menaces. Dans cet écosystème disséminé géographiquement, les collaborateurs utilisent plusieurs périphériques pour accéder aux données, réseaux et applications de l'entreprise pour travailler partout et à tout moment. Cette décentralisation des postes de travail les rend plus sensibles aux menaces des pirates, qui exploitent ce soudain basculement vers un espace de travail hors périmètre et s'en servent pour infiltrer les entreprises.

L'Everywhere Workplace exige une approche de la sécurité et de la gestion des risques qui comprend une évaluation constante du contexte actuel pour définir son niveau de confiance, avec une analyse active basée sur les risques. Ivanti a accès aux meilleures informations sur les vulnérabilités et les correctifs, y compris la liste des exploitations de vulnérabilités actives en environnement réel, des vulnérabilités liées au ransomware et du ressenti des utilisateurs sur la fiabilité des correctifs. Ivanti peut ainsi compléter les outils que les équipes IT et Sécurité peuvent déployer en toute transparence, et améliorer l'efficacité de la gestion de la sécurité et des risques dans les entreprises.

Pour en savoir plus, [consultez notre blog](#) et [inscrivez-vous à la série de webinars Ivanti Patch Tuesday](#).

Écoutez aussi le podcast Ivanti Insights intitulé « The Next Evolution of Patch Management: Don't Try to Patch Everything! » (L'étape suivante dans la gestion des correctifs : n'essayez pas d'appliquer des correctifs partout!)

The Ivanti logo consists of the word "ivanti" in a bold, lowercase, sans-serif font. The letter "i" is red, while the remaining letters "vanti" are black. A small registered trademark symbol (®) is located at the top right of the letter "i".A vertical bar on the right side of the page, transitioning from red at the top to orange at the bottom.

[ivanti.com](https://www.ivanti.com)

1 800 982 2130

sales@ivanti.com