ActualTech MEDIA

Hewlett Packard Enterprise

Garder un temps d'avance sur les menaces pour la sécurité

Ed Tittel

SOMMAIRE

DANS CETTE ÉTUDE

Ce rapport technique examine la façon dont HPE et ses partenaires aident les petites et moyennes entreprises à éviter les problèmes de sécurité. Les PME doivent pouvoir identifier les menaces et les vulnérabilités qui posent des risques potentiels, les hiérarchiser en fonction de leur sévérité et établir des plans d'action et de réduction des risques pour y faire face. Pour ce faire, elles doivent consacrer des efforts continus à long terme pour garder un temps d'avance sur un paysage de cybersécurité en constante évolution.

Voici les principales thématiques développées dans ce rapport :

- Aligner la stratégie en matière de sécurité avec les objectifs de l'entreprise
- Établir une culture d'entreprise centrée sur la sécurité
- Surveiller les surfaces exposées aux attaques et régler les problèmes de façon proactive avant qu'un hacker puisse sévir

En matière de cybersécurité, le dicton « mieux vaut prévenir que guérir » est particulièrement pertinent. En effet, les coûts de « guérison » – c'est-à-dire de gestion des conséquences d'un incident de sécurité ou d'un piratage – sont aujourd'hui suffisamment élevés pour mettre en danger la survie même de la plupart des entreprises, en particulier s'il s'agit de PME.

La compréhension et l'anticipation des dangers associés aux menaces pour la sécurité et aux vulnérabilités sont donc extrêmement importantes, voire franchement vitales. Au bout du compte, tout repose sur la gestion des risques, selon les modalités suivantes :

- À mesure que des menaces et des vulnérabilités se font connaître, la première étape consiste à **identifier** celles qui présentent réellement des risques pour l'entreprise, et d'évaluer leurs impacts et conséquences potentiels.
- Pour les éléments qui présentent des risques, il est essentiel de les **hiérarchiser** afin de faire face en premier lieu à ceux qui pourraient entraîner les coûts les plus importants ou les conséquences les plus dramatiques, puis de passer au suivant.
- Pour les éléments qui présentent suffisamment de risques pour justifier une réponse, les entreprises doivent établir des **plans d'action et de réduction des risques** idoines.

En pratique, et en particulier pour les entreprises trop petites pour disposer en interne d'une équipe dédiée à la sécurité, cette approche implique de souscrire à un service d'évaluation et de réduction des menaces. D'ailleurs, HPE et ses partenaires peuvent être d'une grande aide dans ce domaine, en intégrant l'identification, la hiérarchisation et la réduction des risques au sein d'une offre de services de sécurité complète.

Le cloud change tout… y compris la sécurité

À mesure que les entreprises adoptent des abonnements et des services cloud, de nouveaux vecteurs de menaces particulièrement délicats entrent en ligne de compte pour la sécurité de l'entreprise. L'amélioration de la sécurité devient donc absolument cruciale : l'entreprise doit renforcer son approche en la matière et sa résilience face aux cybermenaces. Pour ce faire, l'application des exercices suivants permet à l'entreprise de se préparer :

- **Alignement de votre stratégie en matière de sécurité avec vos objectifs commerciaux :**en comprenant les écarts entre les priorités relevant de l'activité d'un côté et de la cybersécurité de l'autre, les cadres et les parties prenantes peuvent commencer à harmoniser ces deux aspects pour garantir une attention suffisante aux objectifs clés – et des ressources et des budgets en conséquence. Il est de la plus haute importance que les cadres supérieurs atteignent un consensus sur ces priorités et que les profils de risques soient bien compris de tous.
- **Mise en place d'une culture d'entreprise centrée sur la sécurité :** la mise en avant d'une culture d'entreprise centrée sur la sécurité constitue une étape importante en vue de prospérer dans un monde en proie à l'incertitude et aux risques. La protection des actifs essentiels tombe ainsi sous la responsabilité de chacun. Le personnel étant l'une des principales sources de cyberrisques, il est essentiel d'investir pour le sensibiliser : un effort collectif contre les cybermenaces sera toujours plus efficace pour votre entreprise.
- **Connaissance des surfaces exposées aux attaques et correction des vulnérabilités avant que les hackers ne les détectent :** l'analyse des vulnérabilités de cybersécurité, également connue sous les termes de tests de sécurité et de tests de pénétration, est un processus qui consiste à évaluer l'approche de votre entreprise en matière de sécurité (voir la **Figure 1**). Il s'agit d'identifier les vulnérabilités avant qu'un assaillant puisse les exploiter. Ce processus fournit des informations sur les risques encourus par les actifs de l'entreprise, des points de vue interne et externe. Il permet également d'identifier des éventuelles failles de sécurité avant une évaluation ou un audit de conformité officiel. Pour améliorer l'approche de votre entreprise en matière de sécurité, il faut également développer des plans d'action et de correction réalisables. Pour ce faire, la collaboration avec des partenaires d'expérience (comme HPE et ses partenaires) peut combler les lacunes de compétences en cybersécurité que présente votre entreprise et corriger vos vulnérabilités.

Les quatre étapes des tests de pénétration

Figure 1: Les quatre étapes des tests de pénétration

Un point sur la terminologie

Reprise après incident : services et systèmes qui permettent à une entreprise de reprendre son fonctionnement normal, même après un incident majeur ou une interruption totale de l'accès et des services.

Ransomware : type de logiciel malveillant qui empêche l'entreprise d'accéder à ses systèmes et ses données en les cryptant en intégralité afin de bloquer le fonctionnement de l'ensemble. Les pirates prétendent qu'ils rétabliront l'environnement à son état préalable à l'attaque contre le versement d'une rançon, mais le FBI recommande de ne pas céder, car cette promesse n'est pas toujours tenue.

Applications et données virtualisées et conteneurisées : applications et données qui s'exécutent dans des machines virtuelles ou des conteneurs, souvent dans le cloud, généralement dans le cadre d'un modèle informatique à la demande en paiement à l'utilisation.

Edge to Cloud : ressources informatiques et données pouvant être hébergées dans des datacenters ou des salles de serveurs sur site au cœur de l'entreprise, à l'edge du réseau sur des sites distants ou sur le terrain, ou encore sur une ou plusieurs plateformes cloud (Amazon Web Services, Microsoft Azure, Google Cloud Platform...).

Scénarios hybrides et multicloud : un cloud hybride intègre des ressources informatiques locales et basées sur le cloud en un seul et même environnement permettant d'exécuter des tâches de calcul. Le multicloud est basé sur la même approche, à ceci près qu'il implique au moins deux plateformes cloud. La plupart des entreprises modernes utilisent des environnements hybrides multicloud, et cherchent à placer les charges de travail et les données à l'emplacement le plus pertinent du point de vue des coûts, de la sécurité et des performances.

> **Il est de la plus haute importance que les cadres supérieurs atteignent un consensus sur les priorités de l'entreprise et que les profils de risques soient bien compris de tous.**

Comment HPE peut sécuriser l'informatique (avec ses partenaires)

Un rapide examen des solutions de cybersécurité révèle des gammes complètes, innovantes et robustes. Ses fonctionnalités de sécurité démarrent au niveau du matériel et s'étendent à l'ensemble de l'environnement, jusqu'aux utilisateurs et aux systèmes à l'edge du réseau. L'intention globale est de collecter et d'analyser des informations liées à la sécurité afin de garder un temps d'avance sur le paysage de cybersécurité, de sécuriser les systèmes et les services utilisés par l'entreprise et de conseiller (et d'assister) les clients pour la gestion et la réduction des risques de sécurité.

> **Les solutions de cybersécurité HPE sont complètes, innovantes et robustes. Ses fonctionnalités de sécurité démarrent au niveau du matériel et s'étendent à l'ensemble de l'environnement, jusqu'aux utilisateurs et aux systèmes à l'edge du réseau.**

LA SÉCURITÉ HPE DÉBUTE AU NIVEAU DES SERVEURS

HPE est reconnu comme étant le fournisseur des serveurs standard les plus sécurisés du monde. Sa gamme de serveurs ProLiant a remporté de nombreuses récompenses et distinctions, grâce à ces caractéristiques clés :

- **Protection :** ces systèmes évitent toute exposition aux attaques aux niveaux du matériel et du micrologiciel grâce à la Silicon Root of Trust, à des améliorations apportées au TPM (Trusted Platform Module), à plusieurs niveaux d'inviolabilité, et à d'autres innovations HPE telles que le firmware iLO (Integrated Lights Out) pour la mise en œuvre de fonctionnalités centrées sur la sécurité.
- **Détection :** une suite complète d'innovations détecte et repousse les menaces lors de l'exécution, avec notamment des vérifications d'intégrité au démarrage, lors desquelles iLO efface le code de micrologiciel potentiellement (ou effectivement) corrompu et le remplace si possible par une copie valable. Si la réparation s'avère impossible, les systèmes ne peuvent démarrer (on obtient ainsi une protection prédémarrage contre les rootkits et autres attaques insidieuses ciblant le micrologiciel).

- **Récupération :** des fonctionnalités solides de restauration et de récupération rapides et faciles des systèmes à leur dernier état de bon fonctionnement connu s'appuient sur des sauvegardes chiffrées inviolables et des mécanismes de restauration sûrs et sécurisés.

Zerto

En 2021, HPE a finalisé l'acquisition de Zerto, une entreprise spécialisée dans la reprise après incident, la récupération après une attaque de ransomware et les solutions de mobilité multicloud. Faisant désormais partie intégrante de HPE, Zerto propose des solutions de protection des données en continu et de reprise pour les applications et données virtualisées et conteneurisées, de l'edge au cloud. Grâce à Zerto, les entreprises peuvent récupérer en quelques minutes l'état de leurs systèmes quelques secondes avant une attaque, ce qui élimine les interruptions prolongées et les pertes de données coûteuses. Zerto renforce la disponibilité avec une surcharge de travail administratif bien inférieure à celle des solutions de protection des données traditionnelles. En outre, la gestion unifiée, évolutive et automatisée des données mise en œuvre par Zerto facilite considérablement la mobilité des charges de travail et des données entre les clouds. Enfin, Zerto propose des fonctionnalités de protection des données en continu pour les entreprises utilisant une stratégie de cloud hybride, offrant notamment la reprise après incident as-a-service (DRaaS) avec un réseau de plus de 350 prestataires de services gérés. Rendez-vous sur la page HPE/Zerto pour découvrir comment votre entreprise peut réduire les pertes de données et les temps d'arrêt des applications à un niveau aussi proche de zéro que le permet la technologie.

SOLUTIONS DE SÉCURITÉ HPE

Les outils, technologies et solutions HPE utilisent tous trois approches essentielles tout au long de leur cycle de vie (conception, développement, fabrication, maintenance). Il s'agit des principes suivants :

- **Sécurité centrée sur les données :** les mesures de sécurité visent avant tout à protéger les données, surtout celles qui présentent un caractère sensible (informations personnellement identifiables, ou IPI ; comptes et mots de passe ; données financières, de santé ou toute autre information protégée par la loi...). Cette approche conduit directement à la suivante, qui se consacre à décider qui peut accéder aux systèmes et aux données, et dans quel but.

> **La collaboration avec des partenaires d'expérience (comme HPE et ses partenaires) peut combler les lacunes de compétences en cybersécurité que présente votre entreprise et corriger vos vulnérabilités.**

- **Sécurité Zero Trust :** l'Institut national américain des normes et de la technologie (NIST) décrit l'approche zero trust (ZT) par la formule « ne jamais faire confiance, toujours vérifier ». L'approche ZT se concentre sur la protection des données et des services, mais doit également concerner tous les actifs (périphériques, éléments d'infrastructure, applications, et même ressources virtuelles et cloud) et tous les sujets (utilisateurs, applications, services et systèmes). Cette démarche part du principe général que des assaillants sont toujours présents et actifs. Elle n'accorde donc aucune confiance implicite à qui que ce soit, et analyse et évalue systématiquement les risques encourus par les actifs et les fonctions de l'entreprise. La vérification des identités pour toute demande d'accès constitue une stratégie de base, tout comme l'application du « principe de moindre privilège » (PLP), qui consiste à n'accorder aucun privilège au-delà de ceux strictement nécessaires au sujet pour faire son travail.
- **DevSecOps :** pour dire les choses simplement, il s'agit d'une extension de l'idée de DevOps, qui regroupe les développeurs (ainsi que le personnel de soutien comme les testeurs, les assistants de recherche et les formateurs de modèles) et le personnel opérationnel (administrateurs, support technique et techniciens de terrain ou dépanneurs) au sein d'une même organisation avec des buts et des objectifs communs. L'approche DevSecOPs va encore plus loin en intégrant l'équipe de sécurité à l'ensemble du cycle de vie du développement, afin que la sécurité fasse partie intégrante des phases de conception, construction, tests, maintenance et mise au rebut des opérations IT de l'entreprise.

AU-DELÀ DES SOLUTIONS : DES CONSEILS D'EXPERT D'UNE GRANDE AIDE

HPE Pointnext Services peut aider les petites et moyennes entreprises à évaluer, définir et affiner leur stratégie de sécurité. Pointnext propose en effet l'assistance d'experts pour la formulation d'une politique de sécurité ainsi que pour répondre aux exigences de conformité en matière de

confidentialité, de respect de la vie privée et de protection des données. Ces services peuvent également aider les entreprises disposant de ressources ou de connaissances limitées à intégrer des solutions abordables mais efficaces pour la continuité de l'activité et la reprise après incident. Pointnext se spécialise d'ailleurs dans l'assistance aux entreprises pour la préparation de plans de sécurité afin d'ancrer fermement dans la réalité la conception et la mise en œuvre de toute démarche de sécurité (tout en respectant les contraintes budgétaires). Cette branche propose également une aide de bout en bout, des tests aux déploiements de production en passant par les projets pilotes. Au bout du compte, Pointnext peut aider les entreprises à s'assurer que la sécurité est intégrée à tous les niveaux de l'entreprise : personnel en télétravail, edge, sur site, et environnements hybrides multicloud.

Sécuriser la chaîne logistique

Pour proposer aux clients des exigences de sécurité au-delà des normes et des cas d'utilisation sûrs, HPE utilise une chaîne logistique sécurisée (TSC, pour Trusted Supply Chain). Parmi les clients importants inclus dans cette chaîne logistique se trouvent des agences et organismes américains du secteur public et administratif, qui doivent acheter des produits fabriqués aux États-Unis assortis d'une assurance vérifiable. La sécurité est intégrée à la TSC selon deux modes majeurs. Tout d'abord, ces produits comportent des caractéristiques de sécurité renforcées conçues pour les rendre difficiles à corrompre, voire complètement inviolables. Ensuite, HPE supervise l'ensemble de la chaîne logistique et valide tous les composants, surveille l'assemblage et garantit la sécurité et l'intégrité des marchandises emballées jusqu'à leur réception par le client.

Le Projet Aurora fournit une architecture de sécurité complète, comprenant de nouvelles solutions de sécurité intégrées, ancrées dans le silicium. Découvrez comment le Projet Aurora est intégré à la chaîne logistique et crée une chaîne de confiance immuable qui couvre l'infrastructure, le système d'exploitation (SE), la plateforme logicielle et les charges de travail sans nécessiter de signatures, de dégradation des performances ni d'enfermement propriétaire.

Les outils, technologies et solutions HPE utilisent tous trois approches essentielles tout au long de leur cycle de vie (conception, développement, fabrication, maintenance).

HPE et ses partenaires proposent une large gamme de solutions de sécurité soigneusement conçues pour aider les PME à gérer les risques, à protéger leurs systèmes et leurs données, et à faire face au paysage complexe et dangereux de la cybersécurité d'aujourd'hui. Pour plus de détails, rendez-vous sur la page des solutions informatiques HPE pour les petites et moyennes entreprises. N'oubliez pas non plus que HPE et ses partenaires peuvent également vous fournir du coaching, des conseils, une assistance et des services pour aider les petites entreprises à se protéger et à sécuriser leur environnement, grâce à sa branche spécialisée dans les services, Pointnext.