Hewlett Packard Enterprise

Solutions de sécurité de l’infrastructure serveur conformes à la norme RGPD

RGPD, NIST 800-53, ISO 27001, et IT

Contenu

Livre blanc technique

Clause de non-responsabilité

L'objectif de ce document est d'aider les entreprises à comprendre comment les solutions HPE peuvent être utilisées pour répondre à certaines exigences de conformité dans le cadre législatif général de l'UE en matière de protection des données (RGPD). L'information contenue dans ce document n'est pas censée être, et ne doit pas être prise pour un conseil juridique relatif au contenu, à l'interprétation ou à l'applicabilité des lois, des règlementations et des directives réglementaires.

Introduction

Les tendances récentes qui tendent à augmenter les règlementations sur la sécurité peuvent s'expliquer en partie par la hausse du nombre d'infractions sur les données et des incidents relatifs à la cyber-sécurité. Le RGPD est une nouvelle loi de l'Union Européenne qui impose des nouvelles exigences plus rigoureuses pour les entreprises qui recueillent et utilisent des données personnelles, et qui prévoit d'importantes sanctions en cas de non-respect de ces exigences.

Dispositions clés relatives au RGPD

Le RGPD contient 99 articles et 173 raisons qui regroupent les processus et les aspects opérationnels de la protection des données, dont des exigences qui auront un impact direct sur la façon dont les entreprises implémentent la sécurité informatique.

Les entreprises devront démontrer comment les données sont recueillies, gérées, stockées et traitées en fin de vie.

Certains de ces éléments-clés sont :

- La protection en amont : La protection des données devra être prévue par défaut dès le début des processus de conception de systèmes. Sauvegarder et traiter uniquement ces données, ce qui est absolument nécessaire.
- Consentement : Si une entreprise nécessite le consentement, ceci doit être clairement indiqué. Il ne sera plus possible de dépendre du consentement implicite des personnes et de l'option de s'en dégager.
- Notifications relatives aux infractions : Les notifications obligatoires vis à vis des législateurs sont désormais requises en ce qui concerne une infraction, dans un délai de 72 heures, à partir de la date où celle-ci aura été observée. Les personnes doivent également être notifiées s'il existe un haut niveau de risque que les droits et les libertés des personnes puissent être compromises.
- Le droit à l'oubli : Une nouvelle législation qui renforce les droits individuels actuels permettant d'exiger qu'un organisme supprime ses propres données personnelles.

Dans les cas où un organisme ne respecte pas la règlementation GDPE, une amende maximale de 20 millions d'euros ou à hauteur de 4 % du chiffre mondial annuel peut être infligée à l'organisme concerné. Des actions en dommages et intérêts peuvent être engagées individuellement par des personnes ou par le biais d'associations de consommateurs.

Qui doit se conformer au RGPD

Le RGPD a une couverture éditoriale large, il s'applique à tous les organismes de l'UE, que les données soient traitées à l'intérieur ou à l'extérieur de l'UE. Les entreprises domiciliées en dehors de l'UE qui offrent leurs produits et services aux particuliers sont également concernés.

Toute société qui gère des données personnelles européennes doit commencer à se préparer dès à présent, si ce n'est déjà fait. Cela s'adresse également aux entreprises multinationales actives dans les états de l'UE qui devront pour la plupart nommer un délégué à la protection des données (DPD) chargé de gérer la conformité RGPD et les systèmes informatiques.

Le RGPD et la technologie

Le RGPD n'est pas spécifique en ce qui concerne les technologies à déployer. Il appartient aux organismes de déterminer quelle technologie utiliser pour assurer la conformité RGPD du traitement des données personnelles. Dans le cas de la sécurité, l'article 32 impose aux organismes de « mettre en œuvre les mesures techniques et organisationnelles

appropriées afin de garantir un niveau de sécurité adapté au risque. » Il propose les exemples suivants pour s'adapter aux risques : « la pseudonymisation et le chiffrement des données ; des moyens de garantir la confidentialité, l'intégrité, la disponibilité et la résilience du traitement ; des moyens permettant de rétablir la disponibilité des données en cas d'incident et une procédure visant à tester, à analyser et à évaluer l'efficacité de la sécurité. »

Le RGPD introduit le signalement obligatoire des atteintes à la sécurité des données entrainant toute destruction accidentelle ou illicite, toute perte accidentelle ou toute altération ou accès aux données personnelles. Les DPD au niveau national doivent être notifiés de ces atteintes. Selon la nature et la sévérité de l'atteinte à la sécurité, dont l'efficacité de mesures de contrôle utilisées pour protéger les données, il peut être nécessaire d'en notifier les particuliers concernés.

Délai pour évaluer les risques de l'infrastructure

Pour de nombreuses entreprises, l'augmentation des risques de conformité que le RGPD présente servira de catalyseur pour évaluer la robustesse des processus de la protection des données et de la sécurité de l'infrastructure serveur.

Les cyberattaques sont de plus en plus sophistiquées. Les périmètres habituels de prévention et de réaction face aux menaces ne sont plus réalistes. Les adversaires ont des niveaux d'expertise sophistiqués et des ressources importantes pour atteindre leurs objectifs en utilisant des vecteurs d'attaques multiples (cyber, physique, supercherie). Les objectifs consistent habituellement à s'établir et à développer une implantation dans l'infrastructure informatique afin d'exfiltrer, d'affaiblir les activités commerciales ou de se positionner pour effectuer ces objectifs en temps voulu.

De nos jours, les cybercriminels ont généralement accès aux données, non pas en pénétrant dans des périmètres impénétrables, mais plutôt par le biais de l'erreur humaine ou de l'ingénierie sociale. Par exemple, nous sommes intrigués par une clé USB trouvée dans un parking ou un courriel d'apparence authentique auquel on donne sans le savoir les identifiants du réseau, etc. En 2016, une étude sur la cybersécurité publiée dans la revue américaineHarvard Business Review a révélé que les employés ou contractuels étaient la cause de 60 % des intrusions à la sécurité dans un datacenter. Parmi ces infractions internes, 75 % étaient motivées par des intentions malveillantes ou criminelles et 25 % par simple négligence. Pour un pirate doté de faibles valeurs éthiques, ce moyen est le plus sûr pour obtenir l'accès à des données sensibles : une personne sera toujours égale à elle-même. Personne ne peut être vigilant en permanence et les pirates attendent d'en tirer un avantage.

Etant donné le monde dans lequel nous vivons, où aucun serveur n'est fiable et toutes les données exploitables, les systèmes informatiques devraient migrer d'une simple « protection » à un système de « protection, détection et récupération. » Admettons que le logiciel malveillant s'infiltre dans un datacenter, à quelle vitesse un organisme pourra-t-il détecter les menaces ? De plus, l'organisme est-il en mesure de supprimer la menace et récupérer des effets des dégâts ?

Bien heureusement, les outils et les normes existent bien pour donner un cadre adaptable aux exigences règlementaires particulières des entreprises. Cet article examine les contrôles de sécurité que le National Institute of Standards and Technology (NIST - l'Institut National des Normes et de la Technologie) aux USA et l'International Organization for Standardization (ISO - l'Organisation Internationale de Normalisation) ont détaillés.

Le National Institute of Standards and Technology

Le NIST est devenu plus connu à l'extérieur de l'Amérique du Nord grâce aux initiatives coopératives telles que celles de l'Institut pour la protection et la sécurité du citoyen (IPSC) du Centre commun de recherche de l'UE (JRC), lesquelles œuvrent sur des méthodologies de test et d'évaluation en sécurité informatique pour les infrastructures physiques.

Le NIST est affilié au U.S. Department of Commerce (la chambre de commerce américaine), il représente l'un des plus anciens laboratoires scientifiques aux USA et développe des technologies, des évaluations et des normes sur un éventail large de produits et services.

Une partie de leur raison d'être consiste à implémenter une cybersécurité et une confidentialité grâce à la diffusion et l'application effective de normes et de meilleures pratiques, conçues principalement pour les agences fédérales et qui seront adaptées aux exigences RGPD.

La publication NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations préconise des contrôles de sécurité pour les systèmes d'information d'organismes fédéraux et d'entreprises privées. C'est un catalogue de contrôles de sécurité qui apporte une approche holistique à la gestion de la sécurité et des risques. De plus, elle renforce les systèmes d'information et les environnements dans lesquels ces systèmes fonctionnent, et contribue ainsi à des systèmes plus résilients face aux cyberattaques et autres menaces.

Le catalogue des contrôles de sécurité dans la publication NIST 800-53 peut être utilisé efficacement pour protéger l'information et les systèmes d'information des menaces persistantes significatives et traditionnelles, dans un ensemble de scénarios opérationnels, environnementaux et techniques. Les contrôles peuvent s'utiliser pour faire état de la conformité à un ensemble varié d'exigences gouvernementales, organisationnelles ou institutionnelles.

La norme ISO/IEC 27001

La norme ISO/IEC 27001 concerne le système de gestion de la sécurité de l'information (ISMS) qui représente un ensemble d'activités applicables à la gestion des risques liés à la sécurité de l'information. L'ISMS est un cadre de gestion global par lequel l'organisme s'identifie, analyse et aborde les risques liés à la sécurité de l'information. L'ISMS veille à ce que les dispositions relatives à la sécurité soient adaptées aux évolutions des menaces pour la sécurité, de vulnérabilité et d'impact sur les entreprises.

La norme s'applique à tout type d'organismes (tels que les entreprises commerciales, les agences gouvernementales, les associations et bien d'autres), de toutes tailles (de la micro-entreprise aux grandes multinationales) et toutes les industries ou marchés (par exemple le commerce au détail, les banques, la défense, la santé, l'éducation et le gouvernement). Les organismes qui adoptent la norme ISO/IEC 27001 sont libres de choisir les contrôles de la sécurité de l'information qui s'appliquent aux risques spécifiques à leur propre système d'information, en s'appuyant sur ceux précisés dans le menu et en les enrichissant potentiellement d'autres options (connues parfois sous le nom de « control sets » ou réglages de contrôle).

La structure des contrôles de sécurité dans la norme NIST 800-53 est très similaire à celle de la norme ISO 27001. Ses 256 contrôles sont organisés en 18 familles (contre les 114 contrôles organisés en 14 catégories dans la norme ISO 27001), chacun des contrôles contenus sont liés au thème général de la famille, par exemple ISO 27001. Les contrôles dans chaque famille peuvent couvrir des aspects différents, sur les politiques, la surveillance, la supervision, les processus manuels et les actions engendrées par les particuliers, ou les mécanismes automatisés, selon leurs applications (par exemple, gestion, opérations, techniques). De plus, la norme NIST 800-53 fournit une famille de 16 contrôles aux 256 contrôles de sécurité, qui gère les programmes de sécurité de l'information et 14 contrôles regroupés en trois familles, pour la protection de la vie privée.

L'intégralité des contrôles de la norme NIST 800-53 s'applique à la certification ISO 27001/2. La NIST est enrichie de matrices de contrôle qui donnent des indications générales aux organismes sur la couverture des contrôles de sécurité.

Solutions de sécurité d'infrastructures HPE et NIST 800-53

Hewlett Packard Enterprise a pris les mesures nécessaires pour fournir à leurs clients les bases de sécurité de l'infrastructure serveur avec le concours d'une société externe pour appliquer les contrôles de sécurité de la norme NIST 800-53 aux solutions HPE de l'ensemble de ses solutions de serveurs, de réseautage et de stockage. Ce processus rigoureux comprend l'intégration, le développement des contrôles de sécurité, la documentation, l'évaluation des risques, et les tests de vulnérabilité et de pénétration d'une offre complète de technologies HPE et de ses partenaires, répondant aux normes NIST et aux contrôles de sécurité.

Cette information permettra aux organismes de renforcer les solutions d'assistance aux exigences RGPD. De plus, cela permet d'obtenir un package de certification d'autorisation de fonctionnement (ATO) toute faite, constitué de plus d'une douzaine de documents et de centaines de pages. Cela permettra vraisemblablement d'écourter le cycle de certification à plus de 50 % et donner l'assurance que les systèmes résisteront aux rigueurs de leur agence de certification et au programme CDM « en continu » de diagnostic et d'atténuation.

La solution comprend le stockage HPE 3PAR, HPE ProLiant, et les Serveurs HPE Apollo inclus dans le système HPE monté sur rack. Elle est composée d'un lot complet de solutions de réseau pour le cloud tels que Arista EOS et CloudVision, DoubleTake, Red Hat® KVM Hypervisor, Red Hat CloudForms, Red Hat OpenShift, Red Hat Ansible, Red Hat Ceph, AlienVault USM, Cloud Cruiser, et Aruba ClearPass.

La rigueur et l'acceptation générale des normes NIST et du Cadre de Gestion des Risques (RMF) offrent une applicabilité large pour les contrôles sur l'organisation verticale des entreprises, dont la santé (HIPAA), l'énergie (NERC CIP), le commerce en détail (PCI), les services financiers (GLBA) et les données personnelles de l'EU EU (RGPD/ISO 27001).

En somme, tous les contrôles dans le cadre NIST peuvent contribuer directement à obtenir la certification ISO 27001. Pendant que les entreprises se préparent à la mise en vigueur du RGPD, les contrôles NIST que Hewlett Packard Enterprise proposent aideront également les organismes à établir une base solide de sécurité des infrastructures de serveurs.

Solutions de sécurité des serveurs HPE Gen10

Les plans de sécurité d'un organisme ont avantage à inclure le verrouillage du centre de traitement des données, des équipements de périphérie, du périmètre, ainsi que les infrastructures qui domicilient, traitent et manipulent les données. Ces données, qu'elles soient au repos, en cours d'utilisation ou à la volée, doivent disposer des niveaux les plus élevés de protection. Une protection absolue débute par une confiance absolue. Et une confiance absolue doit être ancrée dans le silicium qui protège contre les niveaux d'attaques les plus bas.
Dans les serveurs HPE Gen10 est incluse une racine de confiance qui assure leur protection aussitôt que le serveur est sous tension.

Le code de démarrage HPE iLO comprend un algorithme cryptographique (hachage) brûlé de manière permanente dans le silicium. Le silicium valide le code de microprogramme HPE iLO 5 avant sa saisie et son exécution. Si un logiciel malveillant ou un code compromis a été inséré dans le microprogramme, le silicium le détectera parce qu'un code de microprogramme infecté sera altéré et donc sans correspondance avec le hachage brûlé dans le silicium. A partir de là, le code de microprogramme HPE iLO 5 valide le reste du microprogramme du serveur, c'est-à-dire l'interface HP UEFI (Unified Extensible Firmware Interface), le dispositif de circuits logiques programmables (SPLD), l'ingénierie système pour l'innovation et l'ingénierie système de management (ME). Le UEFI valide alors la connexion au système d'exploitation par l'entremise d'un démarrage sécurisé, complétant ainsi la racine ou chaîne qui est ancrée dans le silicium. Plus d'un million de lignes de code de microprogramme sont exécutées avant le démarrage du système d'exploitation ; cela fait en sorte qu'il est essentiel de confirmer que l'ensemble du microprogramme essentiel du serveur est exempt de logiciels malveillants ou de codes compromis.

Pendant que le serveur fonctionne, une nouvelle technologie HPE mène une vérification du microprogramme en cours de fonctionnement pour vérifier le microprogramme présent sur le serveur. Durant le fonctionnement, l'insertion d'un code compromis ou d'un logiciel malveillant dans l'un des microprogrammes critiques déclenche une alerte de journalisation d'audit
HPE iLO, afin de prévenir le client qu'un compromis a été fait. Cela est possible par le stockage des microprogrammes iLO 5 et UEFI, dans une mémoire flash non volatile qui est attentivement scannée à intervalles réguliers, tels que définis par l'utilisateur et stockée dans un emplacement LockBox à l'intérieur du serveur. Le contenu du microprogramme stocké en mémoire doit être exactement le même jusqu'au plus petit bit individuel ou il sera signalé comme compromis. La récupération se lancera sur une version précédente du microprogramme reconnu pour son authenticité et sa valeur.

HPE Storage

La conformité RGPD repose sur une stratégie de protection des données qui soit gérable, évolutive, simple et fiable qui gère à la fois les données et le stockage en tant qu'entité cohérente. Notre portfolio des systèmes de stockage HPE 3PAR StoreServ, HPE Nimble Storage, and HPE StoreOnce est en capacité de créer une fondation solide à une stratégie de protection des données complète. Un stockage HPE Nimble Storage acquis récemment est une solution idéale pour des services de données optimisés pour le flash, dont les services de support all-flash, hybrid-flash, et multi-cloud renforcés par les services d'analyse prescriptive optimisés par le machine learning.

Les grappes de stockage HPE 3PAR StoreServ centralisent et consolident les données de production. Optimisées pour le flash et d'une grande disponibilité, proposant les meilleures technologies de snapshot et de réplication sur le marché, les grappes de stockage veillent à ce que les applications de production et les données soient disponibles et protégées. Les dispositifs de sauvegarde HPE StoreOnce sont complémentaires aux grappes de stockage HPE 3PAR StoreServ en fournissant la disponibilité, l'évolutivité et la flexibilité dont les organismes ont besoin pour la conservation et la protection des données à court terme et long terme. Le logiciel HPE Recovery Manager Central (RMC) intègre les baies 100 % flash HPE 3PAR StoreServ avec les systèmes HPE StoreOnce pour que la gestion et la circulation des données fonctionnent ensemble de manière harmonieuse, par la gestion centralisée des fonctions du produit et la circulation des données entre chaque produit. Il ajoute des méthodes de sauvegarde traditionnelles en combinant la performance des instantanés avec la protection des sauvegardes.

HPE 3PAR StoreServ Data-at-Rest Encryption protège les données contre les atteintes à la sécurité internes et externes. HPE 3PAR StoreServ peut être configuré avec des lecteurs à chiffrement automatique (SED), avec une option de gestion

des clés de sécurité d'entreprise. La solution HPE 3PAR StoreServ Data-at-Rest Encryption supporte les normes FIPS 140-2 de sécurité de niveau 2 (Federal Information Processing Standard). La norme FIPS 140-2 pour les SED veille à ce qu'un produit utilise des pratiques de sécurité saines, telles que les algorithmes de chiffrement performants approuvés et autres méthodes similaires.

La fonction de chiffrement de données inactives de la solution HPE 3PAR StoreServ Data-at-Rest permet une protection des données pour s'assurer qu'elle ne soit pas accessible sur des disques usurpés, abandonnés ou remplacés. Elle offre une solution de chiffrement de données basé sur logiciel, qui les crypte à mesure qu'elles sont écrites sur les disques, pour les solutions HPE StoreOnce Catalyst, NAS, et VTL. Le chiffrement de données inactives de HPE 3PAR StoreServ assure la conformité aux normes industrielles avec l'algorithme de chiffrement AES-256 et répond à la norme FIPS 140-2 de niveau 1.

Les solutions HPE StoreOnce proposent une gestion des clés locale et externe, mais nous recommandons vivement que la solution de gestion des clés externe soit utilisée pour l'authentification.

Toutefois, dès que le cryptage est utilisé pour protéger les données inactives, un robuste système de gestion des clés est essentiel pour le contrôle et la préservation des clés cryptographiques sous-jacentes sur l'ensemble du cycle de vie des données. Si les clés sont compromises, les données le sont aussi. Si les clés sont perdues, les données le sont aussi et les opérations commerciales en souffrent. Réduisez les coûts et la complexité de la gestion des clés de cryptage sur une infrastructure distribuée avec des contrôles de sécurité cohérents, des services de clés automatisés et un point de gestion unique. Les solutions de stockage HPE 3PAR StoreServ et HPE StoreOnce prennent en charge les dispositifs de gestion des clés aux normes de l'industrie et la norme du protocole d'interopérabilité OASIS Key Management (KMIP).

Le protocole de sécurité internet IPSec est une suite de protocoles de réseaux qui réalisent l'authentification et le déchiffrement des données expédiées par les réseaux. En utilisant IPSec, le chiffrement de données « en mouvement » permet le transfert sécurisé de données sur les réseaux LAN/WAN entre les dispositifs HPE StoreOnce, qu'ils soient physiques ou virtuels.

La solution HPE StoreOnce Secure Erase (destruction de données) offre un service de sécurité à la pointe de l'industrie conforme aux normes NIST SP 800-88. Elle fournit une protection contre la récupération de données supprimées en permettant d'effacer de manière sécurisée les informations confidentielles. Cette fonction est très importante quand vous utilisez des machines virtuelles et que vous avez besoin de convertir votre matériel ou de régler VMS à une valeur spin-down. La solution Secure Erase vous donne l'option d'effacer en toute sécurité toutes les données du dispositif ou seulement supprimer le stockage individuel (datastore) qui nécessite de disparaitre.

La communauté HPE Cloud28+

Développée il y a environ trois ans par Hewlett Packard Enterprise, HPE Cloud28+ a débuté en Europe pour accélérer l'adoption du cloud par les entreprises dans le monde, tout en respectant les exigences légales locales et régionales. Aujourd'hui, HPE Cloud28+ est une communauté grandissante d'environ 600 partenaires utilisateurs de la technologie HPE, qui ont créé un catalogue groupé de services cloud pour les clients à l'échelle mondiale. Avec 360 centres de données dans le réseau de la communauté HPE Cloud28+ et les partenaires certifiés HPE dans plus de 50 pays, les clients peuvent facilement trouver le partenaire qu'ils recherchent et les solutions qui correspondent aux exigences uniques de souveraineté de leurs données, de sécurité et de charge de travail.

Pour avoir favorisé le provisionnement de service local ainsi que la comparaison simplifiée d'un choix plus large d'entreprises de confiance, le catalogue mondial est actuellement enrichi de plus de 20.000 services. La solution HPE Cloud28+ permet aux clients d'optimiser leurs achats de services informatiques, tout en les aidant à identifier et à s'engager auprès des partenaires les mieux positionnés pour les accompagner.

L'optimisation de la plateforme digitale HPE Cloud28+ (cloud28plus.com/emea) permet aux clients de lire des articles sur le sujet du RGPD pour savoir comment améliorer le RGPD pour faire évoluer les meilleurs pratiques informatiques. Rejoindre la communauté est gratuit et aucun frais de commission ne sera facturé pour contacter un membre partenaire.

Résumé

Pour les entreprises, il n'y a pas meilleure affaire que le RGPD : il fortifie leur cybersécurité et leurs portefeuilles de gestion des risques. Le besoin de respecter les normes RGPD plus exigeantes sur la protection des données donneront aux entreprises l'opportunité d'uniformiser les services informatiques, de développer la sécurité de l'infrastructure serveur, et d'améliorer la gestion des données.

Lorsque les entreprises prennent les mesures nécessaires pour respecter les nouvelles règlementations, elles pourraient avoir l'obligation de faire un « nettoyage printanier » de leurs données, ce qui pourrait à son tour optimiser l'efficacité opérationnelle. Uniformiser l'information améliore les pratiques d'analytique des données des entreprises et peut même engendrer d'autres sources de revenus. En même temps, mettre de l'ordre dans les données pour répondre aux normes RGPD peut impliquer le remplacement de systèmes existants moins sécurisés et l'adoption de systèmes informatiques hybrides pour une meilleure agilité.

Pour les entreprises qui ont des axes commerciaux multiples, oublier un client n'est pas tâche facile. Si un client demande à être supprimé de la base de données, cela implique des fichiers, des formats et des emplacements qui comprennent des informations inutiles et obsolètes. Imaginez combien la complexité potentielle de ce domaine de conformité pourrait devenir positive pour l'entreprise en réduisant la taille de ses données pour les rendre plus accessibles, réduire les frais de stockage, ainsi que les frais de développement d'infrastructures de stockage et les dépenses liées à la sauvegarde.

Cela va bien au-delà de la réduction des coûts. Les entreprises qui ont une vision holistique de la sécurité informatique, de la sécurité des données et de la gestion de l'information peuvent accélérer leur activité digitale avec davantage de confiance, pour mieux protéger leur marque et leur réputation. Une meilleure protection de l'activité digitale est un avantage concurrentiel et un moyen pour les entreprises de construire de meilleures relations de confiance avec leurs clients, ce qui favorise la loyauté, la fidélisation et des revenus.

La sécurité des données personnelles est devenue encore plus au centre de la croissance économique et de la société en général. Ainsi, les coûts opérationnels que les pertes et les mauvais usages engendrent peuvent devenir dévastateurs du point de vue de la réputation et des perspectives financières.

Hewlett Packard Enterprise se focalise sur tout un monde de nouvelles menaces et les meilleurs moyens de s'en protéger. Les solutionsde sécurité de l'infrastructure serveur HPE peuvent accompagner les démarches de conformité à la norme RGPD.

Sécurité intégrée

Les serveurs HPE Gen10 sont dotés d'une sécurité intégrée avec une racine de confiance mise en œuvre en amont du processus de production.

Chiffrement pour protéger les données

Hewlett Packard Enterprise a une stratégie complète de chiffrement, à l'échelle, avec les solutions de chiffrement HPE Smart Array, les lecteurs à chiffrement automatique HPE 3PAR, et une compatibilité avec Atalla ESKM.

La résilience pour la récupération des données

Les fonctions HPE de récupération des données commencent le processus en récupérant le microprogramme du serveur.

Notification rapide d'une brèche de sécurité

Hewlett Packard Enterprise est le seul fabricant de serveur à surveiller le microprogramme du serveur toutes les 24 heures pour renforcer la sensibilisation à la brèche de sécurité et ainsi promouvoir la bonne notification aux autorités concernées.[1]

Pour plus de détails

hpe.com/security

[1] Sur la base d'un test de pénétration de la cybersécurité réalisé par une entreprise externe sur une gamme de produits serveur de plusieurs fabricants, mai 2017

Abonnez-vous :

a00029111FRE, octobre 2017