Livre blanc technique

Respectez les exigences de conformité mises en place en matière de sécurité des données et de votre réseau

Recommandations pour l'application de contrôles de sécurité à l'ensemble de votre parc d'impression

Table des matières

Cliquez ici pour consulter la dernière version de ce document

Le non-respect des règles de conformité peut très sérieusement affecter votre entreprise

Outre les coûts importants liés à un procès ou à des amendes, une faille de sécurité peut également nuire à la réputation et à l'activité d'une entreprise. Lors de la création de votre plan de sécurité, rappelez-vous bien une chose cruciale : la force de la sécurité de votre réseau est définie par l'élément le plus faible de votre organisation. Les appareils d'impression et de numérisation et les ordinateurs présentent à peu de choses près les mêmes points de vulnérabilité en matière de sécurité. Il est donc crucial de mettre en place des appareils et solutions qui vous permettent de respecter les exigences de conformité établies et de protéger vos informations commerciales contre des menaces de sécurité.

Quel est le risque ?

La non-conformité aux dispositions juridiques et réglementaires peut entraîner des coûts importants pour les organisations mondiales (amendes, perte d'activité, réputation ternie et recours collectif).

Des terminaux non ou sous-protégés représentent des opportunités plus nombreuses et exploitables pour les cybercriminels. Les organisations sondées par Ponemon pour une étude récente indiquent qu'elles ont subi en moyenne deux attaques par semaine en 2016, soit une augmentation de 23 % par an, avec une perte moyenne de 9,5 millions de dollars par an pour lutter contre la cybercriminalité.[1] En outre, rien que pour l'année dernière, plus de 4 milliards d'enregistrements de données ont été corrompus dans le monde entier. Soit une augmentation de 400 % par rapport aux deux années précédentes.[2]

Bien que de nombreux départements informatiques appliquent avec rigueur des mesures de sécurité aux ordinateurs et au réseau de leur entreprise, les appareils d'impression et de numérisation restent bien souvent négligés. Mais les imprimantes peuvent représenter un point d'entrée dans votre réseau, et leur sécurité est donc toute aussi importante. Parmi toutes les violations de sécurité importantes signalées par les responsables informatiques, 26 % proviennent des imprimantes[3].

Face à cette menace croissante, les autorités gouvernementales du monde entier mettent en œuvre de nouvelles règles de sécurité strictes en demandant aux organisations de mieux protéger les informations des clients. Par exemple, le Règlement Général sur la Protection des Données (RGPD) ou General Data Protection Regulation (GDPR), entrera en vigueur en 2018. Ce règlement va renforcer les exigences concernant la protection des données des entreprises. C'est pourquoi, il est conseillé de s'assurer que tous les périphériques de votre réseau (ordinateurs, imprimantes ou périphériques mobiles) sont protégés. La nouvelle régulation n'impacte pas uniquement les pays européens. Toutes les entreprises mondiales doivent également s'y conformer si elles collectent et utilisent des données de résidents de pays européens. Les organisations devront contrôler et évaluer chaque périphérique afin de détecter et de signaler les failles de sécurité dans les 72 heures suivant leur connaissance. Si des audits de conformité révèlent que des failles n'ont pas été contrôlées ou signalées, les entreprises risquent de payer des amendes s'élevant à 20 millions d'euros ou 4 % de leur chiffre d'affaires annuel.

Tirez parti de contrôles de sécurité courants afin d'améliorer la conformité

Suivre le rythme des régulations et exigences de conformité d'un secteur peut être difficile. Mais heureusement, le Center for Internet Security (CIS) a élaboré une gamme de contrôles de sécurité courants permettant de simplifier la mise en place de recommandations en matière de cybersécurité. Les CIS Critical Security Controls (Contrôles de sécurité essentiels CIS) se composent de 20 actions spécifiques permettant d'entraver les cyberattaques. (Pour plus de détails, rendez-vous sur https://www.cisecurity.org/critical-controls.cfm.) Les contrôles ont été élaborés en harmonie avec de nombreuses autres régulations du secteur, telles que les normes PCI-DSS et ISO 27001, les recommandations US CERT, et les normes HIPAA, FFIEC, et NIST. Ces contrôles ne visent en aucun cas à remplacer des cadres déjà existants, mais sont utilisés de manière fréquente par les entreprises afin de pleinement tirer parti de ces autres cadres.

Les CIS Critical Security Controls donnent la priorité à un nombre plus réduit d'actions tout en assurant de fort bons résultats. Ils traitent frontalement les motifs d'attaques les plus courants en se basant sur les rapports élaborés sur les menaces principales rencontrées par le passé. Un large groupe d'experts du secteur – incluant certaines des plus grandes entreprises au monde en matière de réponse aux incidents et en recherche criminelle – a participé à leur création. De plus, les contrôles sont également mis à jour de manière constante pour s'adapter à l'évolution des menaces et attaques.

Exploitez les CIS Critical Security Controls afin d'aider à élaborer votre plan d'action en matière de sécurité, et respecter les exigences de conformité mises en place. Ce livre blanc vous présente des suggestions d'actions à effectuer pour chacun des 20 contrôles afin d'aider à sécuriser vos appareils d'impression, données et documents dans le cadre d'un plan de sécurité plus large. Les contrôles 4, 6, 8, 12, 13 et 15 s'appliquent spécifiquement à la protection des données et au contrôle des activités liées aux nouvelles exigences du RGPD.

CIS Critical Security Controls et actions recommandées

CSC 1 : inventaire des appareils autorisés et non autorisés

Contrôle – Gérez de manière active (inventoriez, suivez et corrigez) tous les appareils matériels présents sur votre réseau afin que seuls les appareils autorisés possèdent un droit d'accès, et que les appareils non autorisés ou non gérés soient repérés et qu'aucun droit d'accès ne leur soit accordé.

Recommandation – Assurez-vous que tous les appareils d'impression installés sur le réseau sont bien supervisés et gérés de manière active pour une conformité optimale à votre politique de sécurité. Un outil de gestion de sécurité d'impression efficace peut permettre de découvrir et assurer la visibilité de tous les appareils connectés à votre réseau et à vos ordinateurs.

CSC 2 : inventaire des logiciels autorisés et non autorisés

Contrôle – Gérez de manière active (inventoriez, suivez et corrigez) tous les logiciels installés au sein de votre réseau, afin que seuls les logiciels autorisés soient installés et puissent s'exécuter, et que les logiciels non autorisés ou non gérés puissent être repérés et que leur installation ou exécution soit impossible.

Recommandation – Assurez-vous que toutes les solutions et tous les micrologiciels installés sur vos appareils d'impression et de numérisation sont bien à jour et signés, et que leur authenticité est validée. Choisissez des appareils d'impression possédant une protection de BIOS et de micrologiciel intégrée pour vous assurer que seul un code authentique est chargé. Des mises à jour de micrologiciel proactives peuvent également être mises en place sur l'ensemble de votre parc grâce à des solutions de gestion de parc d'impression. Les logiciels (basés sur serveur et sur client) doivent tous être signés et validés comme authentiques.

CSC 3 : configurations sécurisées pour tous vos appareils et logiciels installés sur vos appareils mobiles, ordinateurs portables, stations de travail et serveurs

Contrôle – Établissez, implémentez et gérez de manière active (suivez, créez des rapports, et corrigez) la configuration de la sécurité de vos ordinateurs portables, serveurs et stations de travail grâce à un processus rigoureux de gestion de la configuration et de contrôle des changements, afin d'empêcher que des personnes mal intentionnées n'exploitent certains de vos services ou paramètres potentiellement vulnérables.

Recommandation – Tout comme d'autres terminaux présents sur votre réseau, vos imprimantes doivent elles aussi être configurées de manière sécurisée. Vous devez créer et mettre en place une politique de sécurité sur l'ensemble de vos appareils d'impression, et apporter de manière active une solution à tout problème de non-respect de cette politique. Des listes de points de sécurité à vérifier (comme NIST) ou des services de conseil en sécurité peuvent également vous aider à créer et mettre en place une politique de sécurité d'impression complète et globale. Un outil efficace de gestion de la sécurité d'impression peut aussi permettre d'automatiser la création de politique, sa mise en place, son évaluation, ainsi que la résolution de problèmes rencontrés vis-à-vis du paramétrage de vos appareils, et ce sur l'ensemble de votre parc. Les imprimantes multifonctions de niveau professionnel possèdent en général plus de 250 paramètres de sécurité, et l'automatisation de ce processus peut donc permettre d'économiser un temps extrêmement précieux.

CSC 4 : évaluation des points de vulnérabilité et résolution des problèmes constantes

Contrôle – Recueillez, analysez et tirez parti des nouvelles informations à votre disposition de manière constante, afin d'identifier vos points de vulnérabilité potentiels, y apporter une solution et minimiser les opportunités d'attaques offertes aux personnes mal intentionnées.

Recommandation – Des solutions d'informations de sécurité et de gestion des événements (SIEM) telles que ArcSight, Splunk ou SIEMonster peuvent contrôler l'activité sur votre réseau en temps réel, et prévenir les administrateurs en cas d'incidents. Contrôler les imprimantes est tout aussi important que contrôler vos ordinateurs : assurez-vous que vos imprimantes peuvent bien transmettre des notifications syslog relatives aux événements à votre outil SIEM.

Choisissez des imprimantes équipées de fonctionnalités permettant de détecter les attaques en temps réel et de résoudre les problèmes de manière automatique, afin d'optimiser le temps de fonctionnement tout en réduisant les interventions du service informatique.

Pour réduire vos points de vulnérabilité potentiels, utilisez un outil de gestion de sécurité de parc qui vous permettra d'identifier les nouvelles imprimantes installées et automatiquement appliquer les règles et paramètres de sécurité que vous avez établis au niveau de l'entreprise dès que vos nouveaux appareils sont connectés à votre réseau. Programmez des évaluations et réparations régulières afin d'assurer la conformité de l'ensemble de votre parc à vos politiques en place.

CSC 5 : utilisation contrôlée des privilèges administrateur

Contrôle – Suivez, contrôlez, évitez et corrigez l'utilisation, l'attribution et la configuration des privilèges administrateur pour vos ordinateurs, réseaux et applications.

Recommandation – Choisissez des imprimantes et des solutions pouvant authentifier les utilisateurs et contrôler l'accès aux différentes fonctionnalités selon le rôle de chaque personne, pour que seule votre équipe informatique ou tout autre personnel autorisé puisse paramétrer et configurer vos appareils. Utilisez des outils de gestion de sécurité de parc pour mettre en place des mots de passe administrateur sur l'ensemble de votre parc.

CSC 6 : maintenance, contrôle et analyse des journaux d'audit

Contrôle – Recueillez, gérez et analysez les journaux d'audit relatifs aux événements rencontrés, qui peuvent vous aider à détecter, comprendre ou tirer des enseignements d'attaques.

Recommandation – Vos imprimantes doivent pouvoir générer des messages syslog relatifs aux incidents, afin que votre équipe en charge de la sécurité puisse analyser de manière régulière les journaux d'audit générés pour découvrir et résoudre les problèmes. Choisissez des imprimantes qui peuvent transmettre ces messages à des solutions de gestion de sécurité de parc et des outils SIEM pour un contrôle en temps réel et une capacité de création de rapports portant sur les audits ou d'autres exigences de conformité.

CSC 7 : protection d'e-mails et de navigateur

Contrôle – Minimisez les possibilités d'attaques et l'échelle potentielle de celles-ci pour les personnes désirant manipuler le comportement des utilisateurs en tirant parti de leur interaction avec des navigateurs web ou des systèmes d'e-mail.

Recommandation – Les imprimantes multifonctions sont souvent connectées à Internet, et peuvent donc par exemple envoyer des fichiers numérisés via e-mail. Assurez-vous que vos fichiers numérisés envoyés par e-mail sont bien cryptés pour protéger toutes vos données sensibles. Mettez en place des appareils et solutions qui permettent d'authentifier les utilisateurs et contrôler l'accès aux ressources intégrées aux appareils (comme les serveurs web ou la fonctionnalité e-mail) selon le rôle de chaque personne. Établissez une liste de « sites de confiance » pour vos multifonctions et gérez celle-ci de manière appropriée afin de vous assurer que seuls les sites auxquels vous faites confiance sont accessibles via l'appareil. Intégrez diverses méthodes d'authentification (telles qu'une identification PIN/PIC, LDAP, ou Kerberos) via Active Directory pour une gestion optimisée et une sécurité renforcée. Les imprimantes connectées à votre réseau doivent posséder une protection intégrée contre les virus et logiciels malveillants, et les micrologiciels de vos imprimantes doivent être mis à jour de manière régulière afin de vous assurer que les toutes dernières mesures de protection sont bel et bien actives.

CSC 8 : défenses contre les logiciels malveillants

Contrôle – Contrôlez l'installation, la propagation et l'exécution de code malveillant à plusieurs niveaux sur l'ensemble de votre entreprise, tout en optimisant l'utilisation de l'automatisation pour permettre une mise à jour rapide de vos moyens de défense, la collecte des données et la mise en place de mesures correctives.

Recommandation – Choisissez des imprimantes qui chargeront uniquement un code ayant été vérifié et signé et qui possèdent des fonctionnalités intégrées de protection contre les logiciels malveillants afin de contrôler de manière active la mémoire de chaque appareil et redémarrer celui-ci en cas d'attaque. Un outil efficace de gestion de la sécurité d'impression peut permettre d'automatiser l'évaluation et la résolution de problèmes rencontrés vis-à-vis du paramétrage de vos appareils, et ce sur l'ensemble de votre parc. Vous devez également vous assurer que toutes vos solutions logicielles d'impression sont bien signées et validées comme authentiques.

CSC 9 : contrôle et limitation de l'accès aux ports, protocoles et services réseau

Contrôle – Gérez (suivez, contrôlez et corrigez) l'utilisation opérationnelle continue des ports, protocoles, et services sur vos appareils en réseau pour minimiser les opportunités et points de vulnérabilité potentiels exploitables par des personnes mal intentionnées.

Recommandation – S'ils ne sont pas déjà désactivés par défaut, désactivez les ports non utilisés et les protocoles non sécurisés (comme FTP ou Telnet) que les criminels peuvent utiliser pour accéder à votre appareil. Économisez un temps précieux pour votre équipe informatique et réduisez les risques en mettant en place un outil de gestion de sécurité d'impression afin d'assurer automatiquement la conformité des paramètres de vos divers appareils sur l'ensemble de votre parc. Utilisez des mots de passe administrateur, une authentification et un contrôle basé sur le rôle des utilisateurs pour limiter l'accès aux fonctionnalités et paramètres de vos appareils.

CSC 10 : capacités de récupération de données

Contrôle – Assurez la bonne sauvegarde de vos informations cruciales grâce à une méthodologie prouvée pour une reprise plus rapide en cas de problèmes.

Recommandation – Ce contrôle n'est actuellement pas applicable aux imprimantes.

CSC 11 : configuration sécurisée de vos appareils en réseau (pare-feu, routeurs et commutateurs)

Contrôle – Établissez, implémentez et gérez de manière active (suivez, créez des rapports, et corrigez) la configuration de la sécurité des appareils constituant votre infrastructure réseau grâce à un processus rigoureux de gestion de la configuration et de contrôle des changements, afin d'empêcher que des personnes mal intentionnées n'exploitent certains de vos services ou paramètres potentiellement vulnérables.

Recommandation – Tout comme d'autres terminaux présents sur votre réseau, vos imprimantes doivent elles aussi être configurées de manière sécurisée. Un outil efficace de gestion de la sécurité d'impression peut permettre d'automatiser la mise en place, l'évaluation, ainsi que la résolution de problèmes rencontrés vis-à-vis du paramétrage de vos appareils, et ce sur l'ensemble de votre parc. Ainsi, votre réseau reste sécurisé, et vous permet de faire gagner un temps précieux à votre équipe informatique.

CSC 12 : défense des limites de votre réseau

Contrôle – Détectez, limitez et corrigez les flux d'informations partagés sur des réseaux, quel que soit leur niveau de confiance, en mettant l'accent sur les données potentiellement sensibles pour la sécurité.

Recommandation – Utilisez un cryptage pour protéger les données en transit (tâches d'impression ou de numérisation transférées vers ou depuis une imprimante) et inactives sur le disque dur de vos appareils. Choisissez des imprimantes et solutions permettant d'authentifier les utilisateurs et contrôler l'accès aux diverses fonctionnalités selon le rôle de chaque personne et permettre ainsi que seuls les utilisateurs autorisés puissent envoyer des fichiers numérisés par e-mail ou vers des destinations cloud. Configurez les sites de confiance que vous avez placés dans votre liste de « sites de confiance » au sein de l'appareil pour éviter l'accès à des sites malveillants. Des solutions d'impression mobile sécurisée peuvent permettre aux utilisateurs de facilement imprimer des documents depuis leurs appareils mobiles, tout en permettant de protéger votre réseau.

CSC 13 : protection des données

Contrôle – Évitez la fuite de données, atténuez les effets liés à celle-ci et assurez la sécurité et l'intégrité de vos informations sensibles.

Recommandation – Utilisez un cryptage pour protéger les données en transit (tâches d'impression ou de numérisation transférées vers ou depuis une imprimante) et inactives sur le disque dur de vos appareils. Déployez des solutions d'impression à la demande pour éviter que des documents sensibles ne restent dans les bacs de sortie de vos appareils. Assurez-vous que les données stockées sur les disques durs de vos appareils sont bien effacées de manière sécurisée avant de renvoyer les appareils loués ou de les recycler à la fin de leur cycle de vie.

CSC 14 : accès contrôlé basé sur le degré d'importance d'accès aux informations

Contrôle – Effectuez un suivi, contrôlez, empêchez, modifiez et sécurisez l'accès aux actifs les plus primordiaux (par exemple, vos informations, ressources, et systèmes) grâce à une détermination officielle des personnes, ordinateurs et applications ayant besoin et le droit d'accéder à ces éléments cruciaux, en vous basant sur un système de classification approuvé.

Recommandation – Choisissez des imprimantes et des solutions pouvant authentifier les utilisateurs et contrôler l'accès aux différentes fonctionnalités selon le rôle de chaque personne. Intégrez diverses méthodes d'authentification (telles qu'une identification PIN/PIC, LDAP, ou Kerberos) via Active Directory pour une gestion optimisée et une sécurité renforcée. Des solutions d'impression à la demande peuvent protéger vos documents sensibles et éviter qu'ils ne tombent entre de mauvaises mains.

CSC 15 : contrôle de l'accès sans fil

Contrôle – Effectuez un suivi, contrôlez, empêchez et modifiez l'utilisation sécurisée de réseaux sans fil locaux (LAN), points d'accès et systèmes sans fil client.

Recommandation – Un outil efficace de gestion de la sécurité d'impression peut automatiser la mise en place et l'évaluation des paramètres de vos appareils – incluant les paramètres sans fil – ainsi que la résolution de problèmes rencontrés vis-à-vis de ceux-ci, et ce sur l'ensemble de votre parc. Utilisez des solutions de contrôle de l'accès utilisateur pour restreindre l'accès aux diverses fonctionnalités de vos appareils, telles que l'envoi de fichiers numérisés par e-mail, en fonction du rôle de chaque utilisateur. Des solutions d'impression mobile sécurisée peuvent permettre aux utilisateurs de facilement imprimer des documents depuis leurs appareils mobiles, tout en permettant de protéger votre réseau. Les appareils compatibles avec l'impression sans fil poste-à-poste, par exemple, donnent aux utilisateurs mobiles la possibilité d'imprimer directement en utilisant le signal sans fil indépendant d'une imprimante, sans devoir se connecter au réseau ou service sans fil de l'entreprise.

CSC 16 : surveillance et contrôle de comptes

Contrôle – Gérez de manière active le cycle de vie de vos comptes système et application – leur création, utilisation, inactivité, ou suppression – de façon à minimiser les opportunités pour les criminels de les exploiter.

Recommandation – Choisissez des appareils d'impression et des solutions pouvant authentifier les utilisateurs et contrôler l'accès aux différentes fonctionnalités selon le rôle de chaque personne. Mettez en place une authentification via Active Directory pour une gestion centralisée et une sécurité renforcée. Évaluez de manière régulière les comptes utilisateur et désactivez tous ceux qui ne sont pas essentiels, et tirez parti de solutions de suivi pour contrôler l'utilisation des comptes existants. Cryptez les noms d'utilisateurs et données d'authentification relatifs aux comptes, que ceux-ci soient en transit ou inactifs sur un espace de stockage intégré à vos appareils. Des conseillers en sécurité peuvent vous aider à élaborer un plan de sécurité d'impression complet et vous aider à réduire les risques potentiels. Et dans certains cas, ils peuvent même vous aider à gérer cette sécurité, ce qui inclut notamment la surveillance et le contrôle des comptes.

CSC 17 : évaluation des compétences de sécurité et formation appropriée afin de combler les lacunes

Contrôle – Identifiez les connaissances, compétences et capacités spécifiques nécessaires pour assurer la protection de l'entreprise. Développez et mettez en place un plan intégré destiné à évaluer, identifier et trouver une solution aux lacunes éventuelles, via l'établissement d'une politique, une planification organisationnelle, une formation et des programmes de sensibilisation pour toutes les personnes assumant un rôle fonctionnel au sein de l'entreprise.

Recommandation – Des conseillers en sécurité d'impression possèdent les connaissances requises pour vous aider à évaluer vos risques de sécurité, développer avec vous un plan et une politique de sécurité, et mettre en place des recommandations de procédés et technologies à adopter. Certains services de sécurité peuvent même gérer la sécurité et la conformité de vos appareils d'impression à votre place.

CSC 18 : sécurité des logiciels et applications

Contrôle – Gérez le cycle de vie et la sécurité de tous vos logiciels ayant été achetés ou développés en interne afin d'éviter, détecter et corriger toute faille potentielle de sécurité.

Recommandation – Respectez les meilleures pratiques recommandées en matière de développement sécurisé pour toutes vos solutions d'impression. Choisissez des solutions logicielles ayant été signées et validées comme authentiques.

CSC 19 : gestion des incidents et réponse

Contrôle – Protégez les informations de l'entreprise, ainsi que sa réputation, en développant et en mettant en place une infrastructure de réponse aux incidents (par ex. des plans, l'établissement de rôles bien définis, une formation, des communications, et l'assignation de responsables de gestion).

Recommandation – Assurez-vous de la prise en charge de votre environnement d'impression dans votre plan de réponse aux incidents.

CSC 20 : tests de pénétration et exercices « Red Team »

Contrôle – Testez la force des défenses de l'entreprise dans leur ensemble (technologie, processus, et personnel) en effectuant une simulation des objectifs et actions d'une personne mettant en place une attaque.

Recommandation – Incluez votre environnement d'impression lorsque vous effectuez ces tests de pénétration. Évaluez de manière régulière votre environnement d'impression à la recherche de vulnérabilités potentielles et mettez à jour votre plan de sécurité en conséquence afin de répondre à ces points d'amélioration.

Passez à l'étape suivante

Mettre en place les recommandations décrites dans ce livre blanc peut vous aider à renforcer votre sécurité d'impression et respecter les exigences de conformité mises en place. Vous avez besoin d'aide ? Des services de conseil et de gestion de la sécurité peuvent vous permettre d'élaborer un plan et mettre en place des procédés et technologies destinés à renforcer la sécurité de vos appareils d'impression, données et documents.

Annexe A : fonctionnalités, solutions et services de sécurité d'impression HP

Les fonctionnalités de sécurité intégrées aux appareils HP, ainsi que leurs solutions logicielles et services de pointe dans le secteur, peuvent vous aider à respecter les exigences de conformité réglementaires et légales en place et à protéger vos informations commerciales de diverses menaces de sécurité.

Les fonctionnalités de sécurité intégrées des imprimantes et multifonctions HP Enterprise aident à protéger les appareils contre les logiciels malveillants et peuvent détecter les attaques et les contrer de manière automatique. La sécurité d'impression HP est la seule à offrir une détection en temps réel, une surveillance automatisée, et une validation intégrée des logiciels afin de bloquer les attaques au moment même où elles surviennent[4]. (Permet de respecter les CSC 2, 4, 6, et 8.) hp.com/go/PrintersThatProtect

Les solutions HP Access Control offrent une large gamme de contrôles d'accès basés sur les rôles et l'authentification des utilisateurs afin d'aider à réduire le nombre de failles potentielles de sécurité, ainsi qu'un suivi et une comptabilité des travaux. (Permettent de respecter les CSC 5, 7, 10, 12, 13, 14, 15, et 16.) hp.com/go/hpac

Le cryptage et **les solutions de flux de travail HP JetAdvantage** protègent les données à la fois quand elles sont stockées sur les appareils HP Enterprise et lorsqu'elles sont en transit vers ou depuis des imprimantes ou le cloud. (Permettent de respecter les CSC 12 et 13.) hp.com/go/upd, hp.com/go/documentmanagement

Les solutions d'impression à la demande HP permettent de protéger les documents confidentiels en stockant les tâches d'impression sur un serveur sécurisé, au sein du cloud, ou directement sur votre PC. Les utilisateurs s'authentifient sur l'imprimante de leur choix puis impriment à la demande les tâches d'impression qu'ils désirent. (Permettent de respecter les CSC 10, 13, et 14.) hp.com/go/hpac, hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Connect offre aux utilisateurs mobiles un accès aisé à l'impression depuis leurs smartphones et tablettes, tout en assurant la sécurité et le contrôle administratif dont vous avez besoin. (Permet de respecter les CSC 12 et 15.) hp.com/go/JetAdvantageConnect

Les données relatives aux événements recueillies par l'imprimante HP peuvent être transmises à des outils SIEM, tels qu'ArcSight, Splunk, ou SIEMonster. Votre équipe en charge de la sécurité peut facilement contrôler les terminaux d'imprimantes dans le cadre d'un écosystème informatique plus large et prendre des mesures correctives. (Permet de respecter les CSC 4 et 6.)

HP JetAdvantage Security Manager est le seul outil de conformité de sécurité d'impression basé sur une politique dans le secteur[5]. Il vous permet de mettre en place une politique de sécurité sur l'ensemble de votre parc, d'automatiser la correction des paramètres de vos appareils, et d'installer et renouveler des certificats uniques tout en tirant parti des rapports dont vous avez besoin pour assurer une conformité optimale. La fonction Instant-On intégrée à la solution configure automatiquement les nouveaux appareils lorsqu'ils sont ajoutés au réseau ou après un redémarrage. (Permet de respecter les CSC 1, 2, 3, 4, 5, 6, 8, 9, 11, et 15.) hp.com/go/securitymanager

La solution HP Secure Managed Print Services assure la protection d'impression la plus poussée et la plus renforcée du secteur[6]. La sécurité d'impression peut être un domaine difficile à appréhender. Laissez HP gérer votre sécurité d'impression, qu'il s'agisse de renforcer les défenses de vos appareils ou proposer des solutions de sécurité avancées qui portent sur votre personnel, vos processus, et les diverses exigences de conformité en place. (Permettent de respecter les CSC 2, 3, 12, 16, 17, 18, et 19.) hp.com/go/SecureMPS

La solution HP Print Security Professional Services vous donne accès à des experts en sécurité qui vous aideront à évaluer votre environnement d'impression, mettre en place de manière proactive des politiques de sécurité, et vous assurer que votre plan de sécurité est constamment actualisé. Il nous est même possible de gérer la conformité de votre sécurité d'impression à votre place. (Permet de respecter les CSC 2, 3, 12, 16, 17, et 19.) hp.com/go/SecureMPS

Notes

[1] Étude Ponemon commandée par HPE, « 2016 Cost of Cyber Crime Study & the Risk of Business Innovation », 2016.

[2] The 2016 Year End Data Breach QuickView report by RiskBased Security, janvier 2017.

[3] 26,2 % des participants à l'enquête ont subi une sérieuse atteinte à la sécurité, ayant nécessité une réparation, et plus de 26,1 % de ces incidents impliquaient l'impression. IDC, « IT and Print Security Survey 2015 » (« Enquête sur la sécurité informatique et relative à l'impression 2015 ») #US40612015, septembre 2015.

[4] Concerne les appareils HP Enterprise depuis 2015 ; basé sur une étude HP 2016 sur les fonctions de sécurité intégrées des imprimantes concurrentes de même catégorie, telles que publiées. HP est le seul à offrir une gamme complète de fonctionnalités de sécurité permettant de contrôler l'intégrité du périphérique, ainsi qu'un BIOS capable de s'auto-réparer. Une mise à jour du service FutureSmart peut s'avérer nécessaire pour activer les fonctionnalités de sécurité. Pour consulter la liste des produits compatibles, rendez-vous sur hp.com/go/PrintersThatProtect. Pour en savoir plus, consultez hp.com/go/printersecurityclaims.

[5] HP JetAdvantage Security Manager est vendu séparément. Pour en savoir plus, veuillez vous rendre sur hp.com/go/securitymanager. Affirmation basée sur des études internes réalisées par HP sur les offres des concurrents (comparaison de la sécurité des périphériques, janvier 2015) et le rapport sur la solution HP JetAdvantage Security Manager 2.1 de Buyers Laboratory LLC, février 2015.

[6] Inclut des fonctionnalités de sécurité pour vos périphériques, documents et données, proposées par des fournisseurs de services d'impression gérée leaders dans le secteur. Sur la base de l'étude réalisée en 2015-2016 par HP sur les informations publiées concernant les services de sécurité, logiciels de gestion et de sécurité, et fonctionnalités de sécurité intégrées pour les imprimantes de la même catégorie proposées par la concurrence. Pour en savoir plus, veuillez consulter hp.com/go/MPSsecurityclaims ou hp.com/go/mps.

Inscrivez-vous pour recevoir les mises à jour
hp.com/go/getupdated

Partager avec des collègues

4AA6-8821FRE, Juin 2017, rév. 1