HP WOLF SECURITY

5 FAÇONS DE SÉCURISER L'ENVIRONNEMENT DE TRAVAIL HYBRIDE

GÉNÉRALEMENT, LES MODES D'ORGANISATION DU TRAVAIL METTENT DU TEMPS À CHANGER

Il a fallu tout un siècle pour que le bureau s'impose comme lieu de travail. Une lenteur qui a permis aux entreprises de s'adapter, de mettre en place des mesures de sécurité et de modifier progressivement leur culture. La pandémie, cependant, a complètement changé la donne.

Un mouvement sans précédent s'est opéré en faveur du travail à distance, sans qu'aucun pays soit épargné. Même si, dans la plupart des organisations, des politiques de sécurité encadraient déjà le travail au bureau et à distance, ces entreprises n'étaient pas préparées à la prise d'ampleur du phénomène. Malheureusement, les cyberattaquants l'étaient : dans les premiers temps de la crise de COVID-19, les attaques de hameçonnage ont augmenté de plus de 600 %.[1]

Maintenant, nous devons relever le nouveau défi que présente le travail hybride. Des personnes qui travaillent au bureau, d'autres qui télétravaillent, avec toutes les variations que l'on peut trouver entre les deux : telle est la nouvelle norme. Une fois de plus, la question se pose : sommes-nous bien préparés à faire face à cette nouvelle réalité en termes de protection de la sécurité ? Le plus gros risque provient probablement des terminaux. Installés dans les foyers du monde entier, ils ont maintenant franchi la ligne de protection fournie par les pare-feux. Ces terminaux incluent les PC, les ordinateurs portables, les smartphones, les environnements virtuels, les serveurs et, à la surprise de nombre d'entre nous, les imprimantes. Plus on a de terminaux, plus on est vulnérable. Et cette vulnérabilité accrue s'est avérée une tentation impossible à ignorer pour les pirates.

Les personnes qui télétravaillent doivent être conscientes de la façon dont les cybercriminels peuvent pénétrer dans leurs systèmes domestiques et les attaquer, notamment par le biais de logiciels malveillants, d'attaques DoS (Denial of Service, ou attaque par déni de service), de hameçonnage et d'attaques sur les mots de passe. En effet, la lutte va être constante : les attaquants connaissent nos vulnérabilités, qui incluent entre autres les comportements humains. Si une seule donnée statistique doit guider nos actions, c'est la suivante : 90 % des violations de données sont causées par une erreur humaine.[2]

Pour vous défendre au mieux, vous devez imaginer le pire. Vous devez vous assurer que vos appareils à domicile bénéficient du même niveau de sécurité que les systèmes d'entreprise de votre bureau. Pour cela, vous allez devoir vous doter d'un ensemble solide de matériel, de logiciels et de services pour vous aider à détecter les attaques, vous protéger contre elles et récupérer.

DANS CETTE PERSPECTIVE, VOICI 5 FAÇONS DE SÉCURISER L'ENVIRONNEMENT DE TRAVAIL HYBRIDE.

1

UTILISEZ DES APPAREILS AVEC UNE SÉCURITÉ INTÉGRÉE DE NIVEAU PROFESSIONNEL

Votre chaîne de sécurité n'est pas plus solide que son maillon le plus faible. Si les membres de votre équipe utilisent un matériel destiné aux particuliers, il est probable que la sécurité dont ils bénéficient soit du même niveau. Cela pourrait se traduire, par exemple, par l'oubli d'un document d'entreprise sensible dans une imprimante personnelle parce qu'il n'y a pas de protection par code PIN. Autre exemple : en plein multitâche, l'un de vos employés pourraient cliquer sur un e-mail par manque d'attention et déclencher le téléchargement d'un logiciel malveillant. Ou encore, quelqu'un pourrait brièvement voir des informations confidentielles de votre entreprise sur l'écran de l'ordinateur portable d'un collègue dans un aéroport ou un café.

Pour saisir toute l'étendue des risques de sécurité, pensez à la rapidité avec laquelle la définition d'une imprimante est passée d'un « appareil qui imprime des documents » à « un appareil mis en réseau qui imprime/scanne, avec système d'exploitation, capacité de stockage local et dans le Cloud, et accès mobile ». Aujourd'hui, le nombre de risques de sécurité est en augmentation constante, ce qui exige d'adopter une démarche de sécurisation des appareils, des documents et des données plus intelligente et de niveau professionnel. Une sécurité de niveau professionnel est tout simplement plus efficace pour gérer un plus grand nombre de terminaux. Elle vous permet d'assurer cette gestion à distance, depuis une plate-forme centrale, et de configurer la protection selon les appareils qui en ont besoin.

2

COMPTEZ VOS TERMINAUX POUR COMPRENDRE À QUELLES MENACES VOUS ÊTES EXPOSÉ

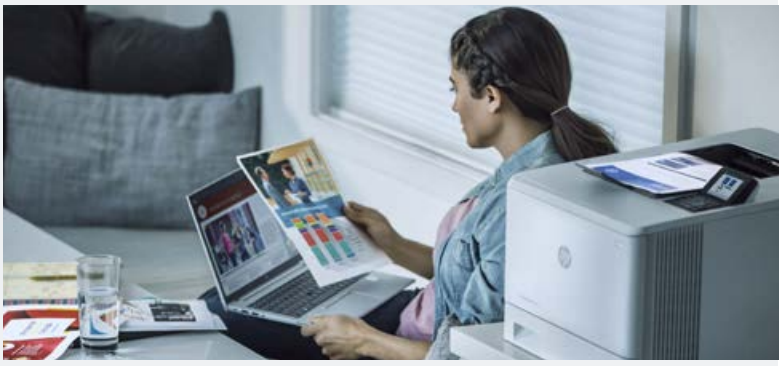
Savez-vous combien d'appareils ont accès à vos données ? Avez-vous réfléchi à ce qu'implique le fait que toutes vos imprimantes soient connectées au réseau ? Lorsque vous prenez en compte les risques cachés du travail hors du bureau, tels que les assistants numériques à commande vocale, les montres, les capteurs connectés au réseau de votre voiture et le nombre incalculable d'autres appareils auxquels on ne pense pas, la démarche a de quoi vous ouvrir les yeux.

Identifier vos terminaux, une tâche que compliquent les conditions de télétravail et les politiques de BYOD, constitue une étape cruciale pour sécuriser l'environnement de travail hybride. Vous assurer que ces terminaux sont sécurisés constitue votre meilleure défense contre le nombre croissant de menaces auquel votre entreprise est confrontée.

Que vous traitiez directement avec HP ou avec l'un de nos partenaires, nous proposons des outils d'évaluation qui vous permettent d'identifier tous vos terminaux. L'étape suivante consiste à choisir les plus sécurisés.

45 %

DES RESPONSABLES IT DÉCLARENT QUE LEUR ENTREPRISE N'EST PAS ENTIÈREMENT OPÉRATIONNELLE POUR FONCTIONNER EN TÉLÉTRAVAIL ; ILS COMBLENT CES LACUNES EN RENFORÇANT LA SÉCURITÉ DE LEUR SYSTÈME ET EN OFFRANT UNE ASSISTANCE SUPPLÉMENTAIRE AUX UTILISATEURS QUI TRAVAILLENT CHEZ EUX.[3]



3

OPTIMISEZ LA SÉCURITÉ POUR TOUS VOS TERMINAUX

Les télétravailleurs veulent rester productifs et travailler où qu'ils se trouvent, ce qui implique par exemple de pouvoir imprimer des documents sensibles chez eux et de bénéficier d'une sécurité optimisée dans les environnements publics. Politiques et consignes de sécurité sont utiles, mais leur portée reste limitée. Si vous souhaitez vraiment renforcer la sécurité de votre système, assurez-vous d'utiliser les PC[4] et les imprimantes[5] les plus sûrs qui existent et qui vous offrent la meilleure implémentation possible.

Les PC HP Elite intègrent des fonctions de sécurité matérielles ainsi que des niveaux de protection en amont et en aval du système d'exploitation, mais aussi intégrés à ce dernier, afin d'anticiper les menaces et de permettre au système de se rétablir rapidement après une faille. Côté bureau, les imprimantes HP Enterprise sont capables de détecter les logiciels malveillants et de s'auto-réparer. De plus, comme elles sont dotées du seul microprogramme évolutif de l'industrie, elles peuvent accueillir de nouvelles fonctionnalités de sécurité au fil du temps.

SÉCURISEZ VOTRE PC :

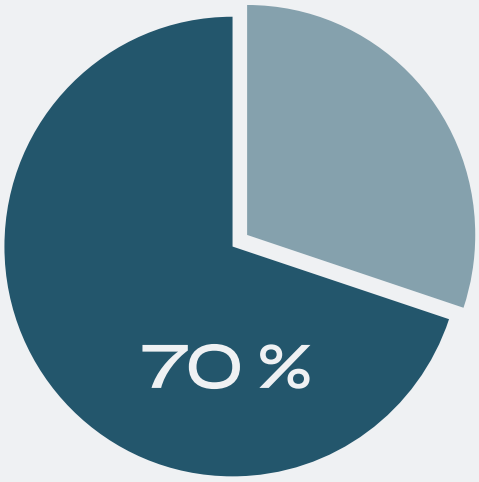
- Vérifiez que votre microprogramme est valide et à jour afin de garantir qu'il n'y ait pas de bugs et que les fonctions les plus récentes soient disponibles.
- Protégez votre BIOS contre les attaques de logiciels malveillants en automatisant sa protection (avec HP Sure Start, par exemple).
- Protégez votre PC en capturant les logiciels malveillants téléchargés ou en pièce jointe (HP Sure Click).
- Protégez ce qui s'affiche sur votre écran en réduisant significativement la visibilité des gens qui vous entourent grâce à HP Sure View.

SÉCURISEZ VOTRE IMPRIMANTE :

- Faites évaluer votre environnement par des experts en cybersécurité HP certifiés.
- Vérifiez que votre microprogramme est valide et à jour, et qu'il offre les fonctions de sécurité les plus récentes.
- Étendez votre politique de sécurité pour les imprimantes à l'ensemble de votre parc avec HP Security Manager.[6]
- Protégez votre imprimante contre les menaces en ligne grâce à des fonctions de surveillance et de correction intégrées garantissant sa sécurité.

4

OUBLIEZ L'IDÉE QUE VOTRE ENTREPRISE EST UNE FORTERESSE



DES MOYENNES ET GRANDES ENTREPRISES SONT D'ACCORD POUR DIRE QU'AVOIR UN PERSONNEL DISPERSÉ POSE DES PROBLÈMES DE SÉCURITÉ.[3]

L'entreprise était auparavant une forteresse délimitée par quatre murs physiques, avec un seul pare-feu puissant pour protéger son réseau. Les choses ne sont plus aussi simples. Avec le modèle de travail hybride, les entreprises doivent mettre en place de nouvelles défenses numériques capables de protéger leurs travailleurs où qu'ils se trouvent.

Cela peut impliquer, par exemple, de passer à un flux de travail numérique où les documents imprimés sont numérisés de façon sécurisée et où les niveaux de sécurité attribués sont déterminés par apprentissage automatique. Il peut s'agir de stocker les données dans un Cloud public sécurisé, qui prendra probablement la forme d'un stockage multicloud, afin de garantir la continuité des opérations et la récupération des données.

Enfin, cela peut nécessiter un renforcement de la sécurité de vos terminaux à distance et le déploiement d'un nouveau matériel, spécialement conçu pour le travailleur hybride. Ce qui est certain, c'est que vous allez devoir envisager d'adopter un système d'authentification multifacteur contextuel et adaptable pour garantir la protection de vos bureaux à domicile à un niveau granulaire.

5

ADOPTEZ UNE POLITIQUE DE CONFIANCE ZÉRO

Une fois passées les quatre premières étapes, la dernière consiste à adopter une politique de confiance zéro (aussi appelée Zero Trust). Dans l'environnement de travail actuel, les menaces sont partout, aussi bien au-delà des limites de votre réseau qu'au cœur de ce dernier. Alors, comme le disent les professionnels de la sécurité, il faut « ne jamais faire confiance, toujours vérifier ». Dans le cadre d'une politique de confiance zéro, vous contrôlez l'accès des utilisateurs.

Le principe de confiance zéro implique de fonctionner comme si la violation des données était inévitable ou qu'elle s'était déjà produite. Toute action est soumise à une vérification stricte et, chaque fois qu'un accès est demandé, il est par principe limité au maximum.

Un utilisateur essaie d'accéder à des ressources en utilisant des identifiants valides, mais depuis un appareil non autorisé ? L'accès lui est refusé. Au moindre soupçon de menace détecté, l'accès aux applications est coupé.

Pour qu'une stratégie de confiance zéro puisse fonctionner, tous les utilisateurs et tous les appareils doivent être authentifiés. Ensuite, le niveau de confiance qui leur est accordé ne s'étend qu'à une seule application spécifique, afin d'éviter au maximum d'exposer les zones sensibles du réseau.

39 %

PRÈS DE DEUX EMPLOYÉS SUR CINQ ACCÈDENT AUX DONNÉES DE L'ENTREPRISE DEPUIS DES APPAREILS PERSONNELS.[7]

Résumé

Quelles sont les menaces qui existent et les actions à mettre en place pour les contrer ? Pour répondre en une seule phrase : les organisations doivent prendre immédiatement les mesures nécessaires pour affronter les risques de sécurité inhérents à la transition vers un environnement de travail qui se trouve non seulement à distance, mais aussi n'importe où.

HP offre à la fois les PC[4] et imprimantes[5] les plus sécurisés au monde, mais aussi une stratégie de défense multiniveau en profondeur pour vous aider à détecter les attaques, vous protéger contre elles et récupérer. Gardez toujours une longueur d'avance sur les menaces qui pèsent sur votre réseau et vos flux de travail numériques, et restez toujours en conformité.

UNE SÉCURITÉ NOUVELLE GÉNÉRATION POUR LES TERMINAUX[8]

Contactez un représentant HP ou consultez hp.com/wolf pour en savoir plus

HP WOLF SECURITY

1. #COVID19 Drives Phishing Emails Up 667% in Under a Month (Le COVID-19 a entraîné une augmentation de 667 % du hameçonnage par e-mail en moins d'un mois) https://www.infosecurity-magazine.com/news/covid19-drive-phishing-emails-667/, mars 2020
2. 90 percent of data breaches are caused by human error (90 % des violations de données sont dues à une erreur humaine), https://www.techradar.com/news/90-percent-of-data-breaches-are-caused-by-human-error, mai 2019
3. Remote work changing landscape: IT Leader View, (Le paysage changeant du télétravail : Le point de vue d'un DSI), HP, mai 2020
4. Sur la base des capacités de sécurité uniques et complètes HP proposées sans frais supplémentaires par les différents fournisseurs sur les PC HP Elite équipés de Windows et de processeurs Intel® de 8e génération et supérieurs ou de processeurs AMD Ryzen™ 4000 et supérieurs, les ordinateurs HP ProDesk 600 G6 avec processeurs Intel® de 10e génération et supérieurs et les PC portables HP ProBook 600 avec processeurs AMD Ryzen™ 4000 ou Intel® 11e génération et supérieurs.
5. Les fonctions de sécurité intégrées HP les plus avancées sont disponibles sur les appareils HP Enterprise et HP Managed avec micrologiciel HP FutureSmart 4.5 ou supérieur. Basé sur l'étude réalisée par HP sur les informations relatives aux fonctionnalités publiées en 2021 pour les imprimantes de la même catégorie proposées par la concurrence. Seul HP propose un ensemble de fonctions de sécurité permettant de détecter et d'arrêter automatiquement les attaques, mais aussi de restaurer les terminaux avec un redémarrage d'autoréparation, conformément aux directives NIST SP 800-193 pour la cyberésilience des périphériques. Pour consulter la liste des produits compatibles, rendez-vous sur hp.com/go/PrintersThatProtect. Pour en savoir plus, consultez hp.com/go/PrinterSecurityClaims.
6. Proposé avec certains modèles de produit et versions de micrologiciel.
7. Head in the Clouds: How remote working behaviors are exposing organizations to risk (La tête dans les nuages : de quelles façons les comportements professionnels exposent les entreprises aux risques), Trend Micro https://resources.trendmicro.com/rs/945-CXD-062/images/HeadintheCloudReport.pdf, juillet 2020
8. HP Security devient HP Wolf Security. Les fonctions de sécurité varient selon les plateformes. Veuillez vous référer à la fiche technique du produit pour plus d'informations.

4AA8-0097FRE, Mai 2021