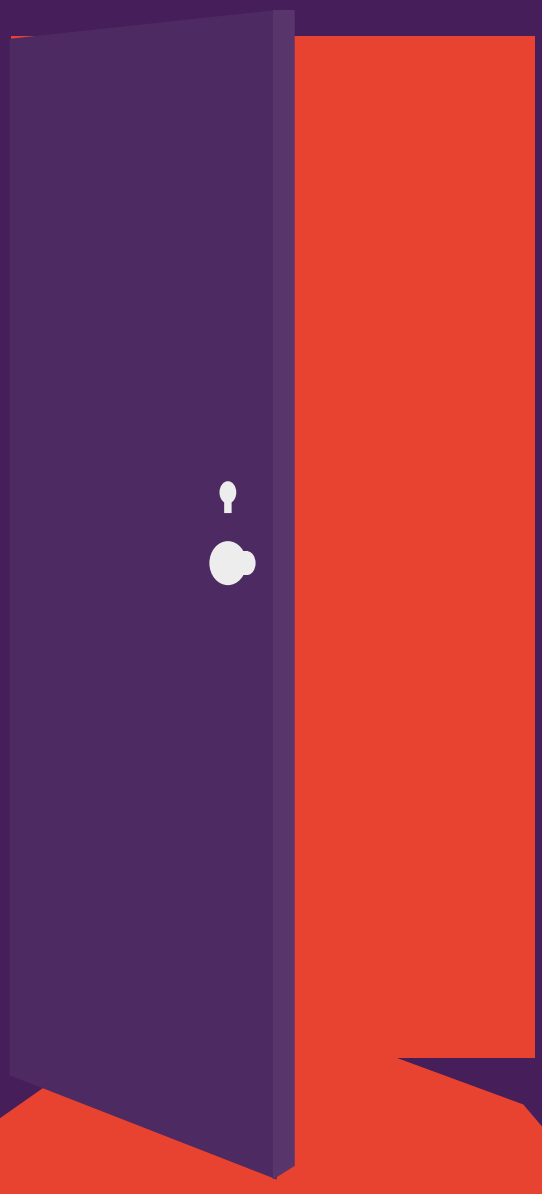
LIVRE BLANC

ACCÈS NON VERROUILLÉS

LA RECHERCHE DÉMONTRE QUE LES IMPRIMANTES SONT VULNÉRABLES AUX CYBERATTAQUES

Alors que les équipes informatiques se concentrent sur d'autres points de terminaison, la sécurité des imprimantes d'entreprise est à la traîne



Lesimprimantessontdesciblesfaciles:tropd'imprimantes connectéesauréseausontdépourvuesderestrictionsetne sont pas verrouillées en toute sécurité.

Mais la menace est réelle, et ne doit pas être ignorée. Les imprimantes de classe professionnelle ont évolué pour devenir de puissants périphériques en réseau souffrant des mêmes vulnérabilités que n'importe quel autre point d'accès de votre réseau. Ces points d'entrée généralement non sécurisés offrent de réelles possibilités de cyberattaques ; ils peuvent même donner accès aux données financières et privées de la société, avec des conséquences commerciales catastrophiques.

Malgré cela, une enquête récente de Spiceworks sur plus de 300 décideurs informatiques d'entreprise a démontré que seulement 16 % des participants estiment que les imprimantes représentent un risque élevé de menace ou faille de sécurité, sensiblement moins que les ordinateurs portables/ordinateurs de bureau et périphériques mobiles.[1] Ce sentiment a déformé la façon dont les personnels informatiques perçoivent la sécurité du réseau. Même si près de trois organisations sur cinq ont des procédures de sécurité en place pour leurs imprimantes, cette proportion est nettement inférieure à celle des autres points de terminaison, ce qui rend les imprimantes vulnérables, alors que des solutions simples existent pour protéger ces points d'accès.

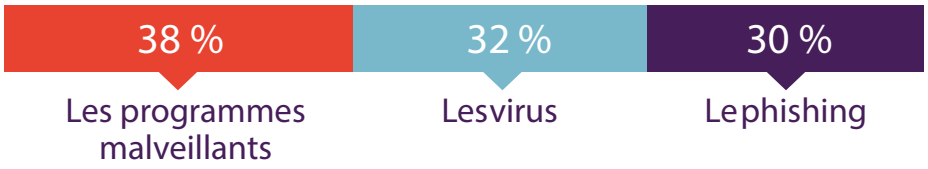
Le présent livre blanc présente des informations sur la sécurité des imprimantes sur la base de l'enquête de Spiceworks, l'impact des failles de sécurité, et certaines des fonctionnalités modernes de sécurité intégrées aux imprimantes pour les protéger contre les cyberattaques.

SEULEMENT 16 % DES PARTICIPANTS PENSENT QUE LES IMPRIMANTES REPRÉSENTENT UN RISQUE ÉLEVÉ DE MENACE OU FAILLE DE SÉCURITÉ.[1]

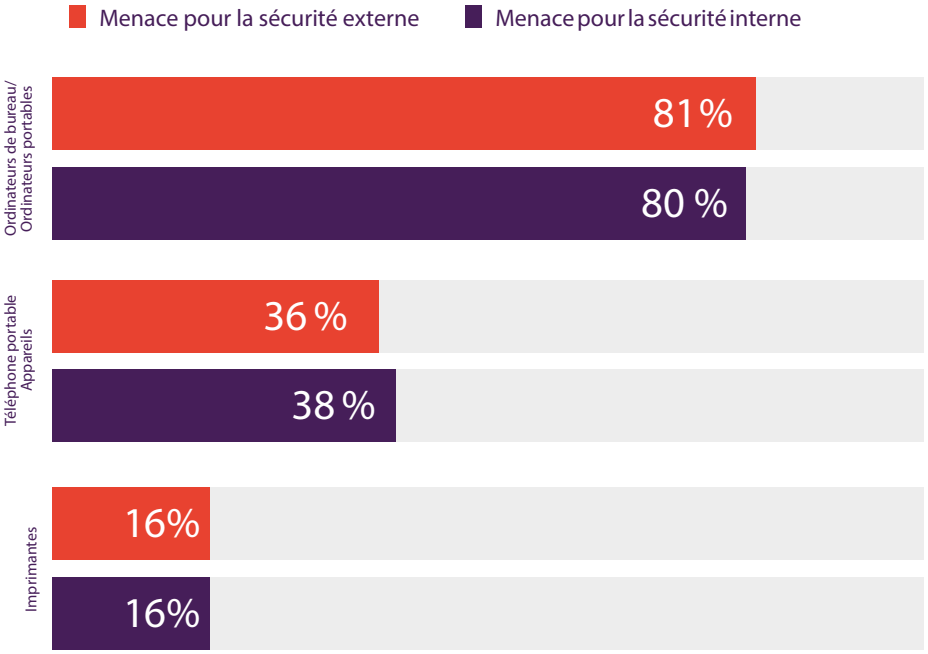
PORTES D'ENTRÉE POUR LES ATTAQUES

L'enquête de Spiceworks indique que l'organisation de 74 % des personnes interrogées a subi au moins une menace ou faille de sécurité informatique externe au cours de l'année passée. Et 70 % ont subi une menace ou faille de sécurité interne, généralement à cause d'une erreur utilisateur, de l'utilisation d'appareils personnels ou d'employés utilisant un réseau personnel ou public pour des raisons professionnelles.[1]

PRINCIPALES MENACES POUR LA SÉCURITÉ INFORMATIQUE INTERNE RENCONTRÉES



Les principales menaces se sont principalement faufilées à travers des ordinateurs de bureau et des ordinateurs portables, et d'autres à travers des appareils mobiles et des imprimantes.[1] (Les 16 % à travers les imprimantes représentent une forte hausse par rapport aux 4 % trouvés dans une enquête similaire de Spiceworks en 2014.) Il est également possible que le nombre d'attaques à travers des imprimantes soit sous-estimé, car les imprimantes sont moins surveillées que les ordinateurs de bureau et les appareils mobiles.

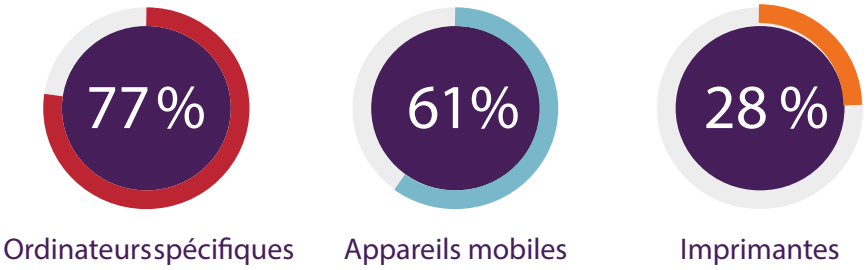


NOUS NÉGLIGEONS NOS IMPRIMANTES

Quel que soit le cas, l'enquête de Spiceworks prouve que la sécurité des imprimantes est souvent négligée.

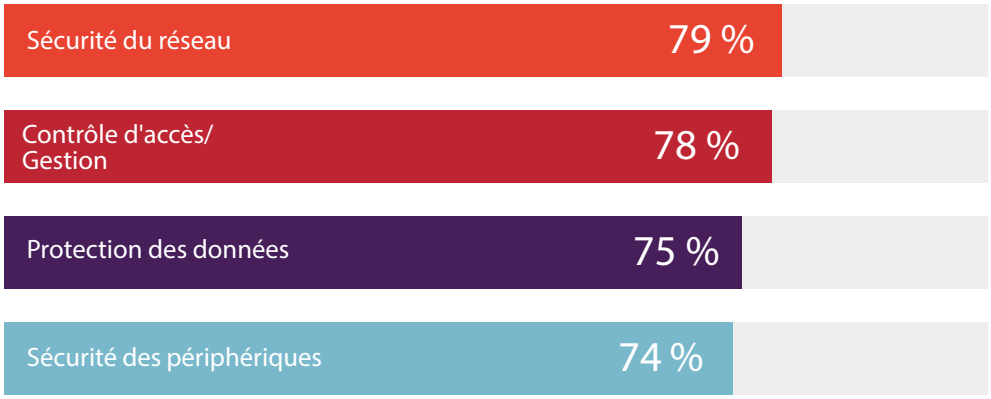
Les organisations sont très conscientes de l'importance de la sécurité des données et des points d'accès. En fait, plus de trois quarts des personnes interrogées utilisent soit une sécurité réseau, une gestion/un contrôle des accès, une protection des données, une sécurité des points d'accès, soit une combinaison de ceux-ci.[1]

Mais ces solutions sont déployées bien moins souvent sur les imprimantes. Tandis que 83 % des participants utilisent la sécurité du réseau sur leurs ordinateurs de bureau/portables et 55 % sur les appareils mobiles, seulement 41 % l'utilisent sur les imprimantes.[1]



L'écart est encore plus important pour la sécurité des points d'accès : En outre, moins d'un tiers (28 %) des participants déploient des certificats de sécurité pour leurs imprimantes, à comparer aux 79 % qui le font pour les ordinateurs de bureau et 54 % pour les appareils mobiles.[1]

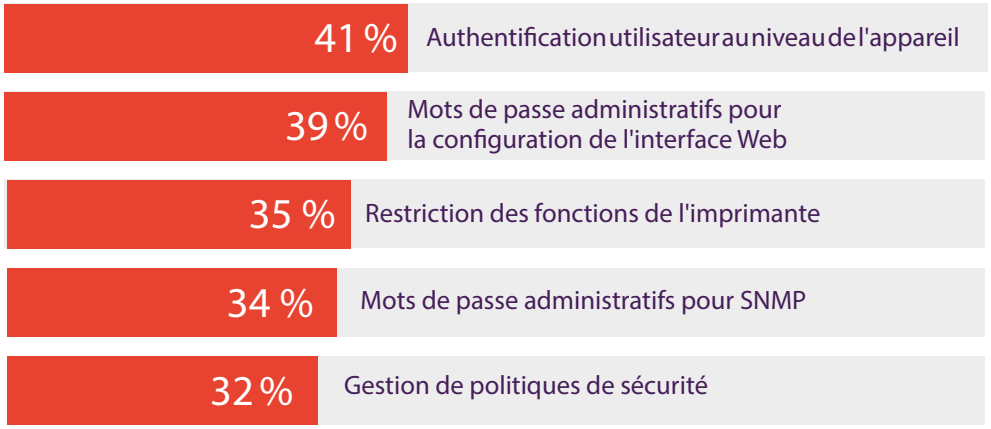
PRINCIPALES PRATIQUES DE SÉCURITÉ AUX POINTS D'ACCÈS



Parmi les protections utilisées sur les périphériques de terminaison généraux, les mesures de sécurité les plus communément utilisées pour les imprimantes étaient la sécurité des documents, la sécurité du réseau et le contrôle d'accès, mais moins de la moitié des personnes interrogées ont indiqué que leur organisation utilisait l'une ou l'autre de ces mesures.[1]

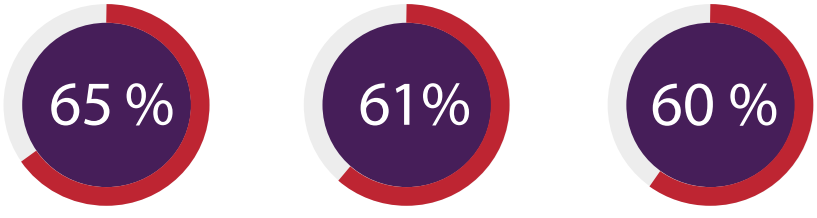
Certaines sociétés ont des pratiques de sécurité spécifiques aux imprimantes, mais même là, ces pratiques sont très hétérogènes. À peine plus de 40 % des organisations ont déployé l'authentification utilisateur, et moins de 40 % utilisent des mots de passe d'administrateur pour l'interface de configuration Web.[1] Pour une défense renforcée, chaque organisation devrait utiliser une combinaison de toutes ces approches—voire plus.

PRINCIPALES PRATIQUES DE SÉCURITÉ SPÉCIFIQUES AUX IMPRIMANTES



En matière de conformité des points d'accès et de pratiques d'audit, les contrôles de la sécurité des imprimantes sont loin derrière presque tous les autres points de terminaison. Près de 90 % des organisations ont déployé une stratégie de sécurité des informations, mais celle-ci ne s'étend généralement pas aux imprimantes. Par exemple, alors que 57 % des participants indiquent qu'une protection contre les logiciels malveillants est déployée sur leurs ordinateurs de bureau, seulement 17 % en ont déployé une sur leurs imprimantes.[1]

PRÈS DE 90 % DES PROFESSIONNELS DE L'INFORMATIQUE DISENT QUE LEUR ORGANISATION DISPOSE D'UNE POLITIQUE DE SÉCURITÉ DES INFORMATIONS POUR LES RAISONS SUIVANTES :



Il est clair que les organisations ne prennent pas au sérieux la sécurité de leurs imprimantes, mais c'est une erreur.

« Beaucoup d'imprimantes ont encore leur mot de passe par défaut, ou pas de mot de passe du tout, ou dix utilisent le même mot de passe », selon Michael Howard, consultant en sécurité pour HP, dans des propos recueillis par Computerworld en juin dernier. « Une imprimante sans protection par mot de passe est une mine d'or pour un pirate. L'une des intrusions que nous voyons souvent est l'attaque de l'homme du milieu, dans laquelle le pirate prend le contrôle d'une imprimante et détourne [les documents entrants] vers un ordinateur portable avant qu'ils soient imprimés. Le pirate peut voir tout ce que le PDG imprime ».[2]

L'IMPACT POTENTIEL DES INTRUSIONS PAR LES IMPRIMANTES

Selon Bogdan Botezatu, analyste chevronné des menaces informatiques chez Bitdefender, les imprimantes représentent une faille potentielle de sécurité considérable. « Nous recueillons beaucoup de télémétrie dans nos laboratoires d'évaluation de la vulnérabilité. Le routeur n'est plus le pire périphérique sur internet. C'est désormais l'imprimante ».[3]

Cette vulnérabilité peut avoir des répercussions profondes sur une entreprise. Une seule imprimante non sécurisée peut rendre l'intégralité de votre réseau d'appareils connectés vulnérable à une attaque, en laissant les pirates espionner vos appareils connectés—et en compromettant ainsi la sécurité de l'ensemble du réseau.

1. Augmentation du temps de soutien et d'appel au service d'assistance

2. Réduction de la productivité et de l'efficacité

3. Augmentation de l'indisponibilité du système

4. Augmentation de la durée des appels de soutien

5. Application renforcée des stratégies liées à l'utilisateur final

Nous avons tous vu les effets des failles de sécurité. Dans l'enquête de Spiceworks, les participants indiquent que les cinq principales conséquences des intrusions sont :[1]

Mais une intrusion sur une imprimante peut être encore plus grave que cela, et tout particulièrement si vous utilisez une imprimante multifonction capable de stocker électroniquement des données imprimées. Les tâches d'impression stockées dans l'antémémoire

de l'imprimante permettent aux pirates d'accéder à des informations d'entreprise ou personnelles sensibles.

Encore plus préoccupant, les pirates peuvent accéder au réseau principal de l'entreprise à travers une imprimante non sécurisée, et voler ainsi des informations telles que des numéros d'assurance sociale, des informations financières ou des notes de service internes et autres documents.
Ces informations volées peuvent non seulement avoir une incidence sur les employés eux-mêmes, mais aussi être utilisées par la concurrence ou entacher gravement la réputation de l'entreprise.

LA SOLUTION FACILE : FONCTIONS DE SÉCURITÉ INTÉGRÉES

Il est clair que les sociétés doivent prendre en charge la sécurité, même au niveau de leurs imprimantes. Certaines imprimantes modernes professionnelles disposent de fonctionnalités intégrées faciles à utiliser pour combattre les menaces contre la sécurité. À savoir :

- Détection automatique des attaques, protection et guérison
- Suivi de l'utilisation pour éviter toute utilisation non autorisée
- Options d'identification simples telles que les codes PIN ou les cartes à puces
- Un lecteur de cartes de proximité qui permet à l'utilisateur de s'authentifier rapidement et d'imprimer en toute sécurité à partir du panneau de l'imprimante avec son badge d'identification
- Impression cryptée sécurisée pour les documents sensibles

Lorsque vous envisagez d'acheter une nouvelle imprimante, qu'elle soit simple ou multifonction, renseignez-vous sur les fonctionnalités de sécurité intégrées, et pensez à les activer. Grâce à ces fonctionnalités simples spécifiques aux imprimantes, il n'y a plus aucune raison de rester vulnérable à travers vos imprimantes : après tout, avec l'Internet des objets, il y a tellement d'autres points d'accès dont il faut se préoccuper, que vos imprimantes n'ont pas à en faire partie.

VOUS CHERCHEZ DES IMPRIMANTES MIEUX SÉCURISÉES ?

POUR EN SAVOIR PLUS ›

Sources :

[1] Enquête de Spiceworks concernant 309 professionnels de l'informatique en Amérique du Nord, zones EMEA et Asie-Pacifique, réalisée pour le compte de HP, novembre 2016

[2] « Printer Security: Is your company's data really safe? » Computerworld, 1er juin 2016. http://www.computerworld.com/article/3074902/security/printer-security-is-your-companys-data-really-safe.html

[3] « Printers Now the Least-secure Things on the Internet, » The Register, 8 septembre 2016. http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/