La checklist indispensable pour sécuriser vos terminaux d'impression

Une liste pratique pour la sécurisation des terminaux sur votre réseau et la conformité au nouveau règlement européen pour la protection des données (GDPR).

De nouveaux règlements imposent aux entreprises d'accorder une attention croissante à la sécurité informatique, afin de garantir la protection des données du client et de la société. En outre, des directives, telles que le Règlement général sur la protection des données (GDPR) de l'UE, stipulent que les entreprises doivent évaluer et surveiller les failles de sécurité, mais également en faire rapport dans un délai de 72h.

Comme les règlements changent en permanence, les entreprises peuvent éprouver des difficultés à trouver le temps et les ressources nécessaires pour être à jour. Toutefois, si elles ne disposent que d'un simple pare-feu pour se prémunir des attaques, elles peuvent se trouver en infraction et encourir des amendes pouvant s'élever à plusieurs millions. Or, un jour ou l'autre, chaque entreprise connaîtra immanquablement une faille. Il est donc essentiel d'identifier les circonstances de cette faille et de la corriger dès que possible en appliquant les produits, processus et outils appropriés.

La présente liste se veut une ressource pratique pour quiconque cherche à améliorer la sécurité informatique et à protéger la réputation de sa marque, tout en évitant les répercussions financières importantes d'une faille et en assurant la conformité aux nouvelles règles strictes. Cette liste présente tout d'abord les bases, pour terminer par les couches maximales de sécurité. Ainsi, vous pouvez vous assurer que la sécurité de vos terminaux est totalement en accord avec ces nouveaux règlements stricts.

Cette liste pratique aidera aussi votre service informatique à sécuriser ses terminaux d'impression.

Couche basique de sécurité

- N'achetez que des périphériques dotés d'une protection contre les programmes malveillants et de disques durs cryptés.
- Mettez à jour les micrologiciels, en particulier les versions comportant des correctifs critiques de sécurité (comme vous le feriez en mettant à jour les applications de votre téléphone portable).
- Configurez les interfaces de périphérique et verrouillez les protocoles tels que FTP et Telnet dont vos applications n'ont pas besoin.
- Vérifiez les nouveaux périphériques et fermez les ports ou protocoles non utilisés qui pourraient permettre à des intrus d'accéder à vos systèmes.
- Utilisez des mots de passe administrateur uniques pour chaque appareil.
- Verrouillez le panneau de contrôle pour interdire l'accès aux fonctionnalités d'administration.
- Cryptez les données d'entrée-sortie du périphérique.
- Établissez des procédures de suppression des données anciennes sur le disque dur, en particulier pour les imprimantes que vous vendez.

Ensuite, passez à la couche de sécurité suivante.

Couche moyenne de sécurité

- Intégrez le journal d'impression dans votre outil de surveillance des événements d'incidents système (SIEM) afin de mieux surveiller les menaces sur votre réseau. Concernant les nouvelles règles de conformité, la visibilité est un point essentiel pour répondre aux exigences du règlement.
- Mettez en œuvre l'authentification de l'utilisateur au niveau de l'imprimante pour savoir qui copie, scanne et faxe depuis le périphérique. Ces données vous seront précieuses si une enquête doit être menée sur une faille de sécurité.
- Appliquez le pull printing pour éviter que des informations sensibles ne soient oubliées. Cela vous permettra aussi de mieux vous conformer aux normes environnementales en réduisant les quantités de papier d'impression gaspillé.

Enfin, passez à la dernière couche de sécurité.

Couche de sécurité avancée

- Configurez le suivi des tâches d'impressions.
- Envisagez la mise en place et l'application automatique de règles pour déterminer qui peut accéder à quelles imprimantes et dans quels cas, à l'aide d'autorisations par fonction.
- Déployez des certificats numériques uniques pour chaque imprimante, comme pour tout autre périphérique connecté à Internet sur votre réseau.
- Mettez en place une solution de gestion des impressions depuis un appareil mobile pour le chiffrement de données, l'accès aux appareils sur le réseau, l'authentification et le suivi des utilisateurs.

4AA7-1093FRE