Lexmark

Superposition

Comment créer une stratégie de sécurité efficace pour vous assurer que l'impression n'est pas votre maillon faible.

La sécurité d'impression multicouche est plus efficace

Selon le cabinet d'analyse technologique Quocirca, 61% des organisations ont subi une perte de données au cours de la dernière année en raison de pratiques d'impression non sécurisées.[1] La sécurité va au-delà de la fonctionnalité de l'appareil et doit fonctionner à plusieurs niveaux. Une stratégie multicouche qui fonctionne aux niveaux matériels, logiciel et réseau est l'approche la plus efficace et est explorée ci-dessous.

1 **Une approche percutante**

2 **Les logiciels sécurisés sont importants**

3 **Prise en charge de la sécurité du réseau**

4 **La différence Lexmark**

[1]Quocirca Print Security Landscape 2023

Lexmark

À propos de Lexmark

Lexmark offre une sécurité d'impression inégalée, avec nos solutions trouvées dans certains des environnements les plus réglementés et les plus soucieux de la sécurité au monde, y compris les agences fédérales et les services financiers. Qu'il s'agisse d'appareils conçus en toute sécurité, de logiciels de gestion à distance ou de gestion continue des vulnérabilités et de la configuration, les produits, solutions et services Lexmark sont certifiés de manière indépendante selon les normes les plus strictes, notamment les critères communs et les normes FIPS (Federal Information Processing Standards).

Une approche percutante

Impact de la conception et du développement du matériel sur la sécurité de l'impression et ce qu'il faut rechercher dans le cadre d'une approche basée sur les meilleures pratiques.

Trois considérations clés:

Sécurisé par conception

Vos imprimantes et imprimantes multifonctions doivent avoir la sécurité intégrée en tant qu'objectif de conception et d'ingénierie intégrale, et pas seulement en tant que fonctionnalité optionnelle / complémentaire. Cette approche d'ingénierie sécurisée intègre des protections dans l'appareil physique en standard pour améliorer la sécurité des données et aider à empêcher les utilisateurs malveillants d'accéder aux informations confidentielles. Il prend également en charge votre stratégie de sécurité de point de terminaison.

Micrologiciel crypté et signé numériquement

Le micrologiciel de l'appareil contribue directement à la sécurité de l'appareil. Regardez les configurations « prêtes à l'emploi » qui, une fois adoptées, ne peuvent pas être modifiées par des utilisateurs non autorisés. Les protections du micrologiciel, de la mémoire, du stockage et du système d'exploitation sécurisé comprennent le stockage chiffré, l'effacement des fichiers du disque dur, la technologie de démarrage sécurisé, la vérification continue et plus encore. Non seulement ces fonctionnalités offrent une protection optimale, mais elles réduisent les tâches manuelles et allègent la charge pesant sur les ressources informatiques.

Vérifié de manière indépendante selon les normes tierces

Tout le monde peut dire que ses appareils sont sécurisés. Assurez-vous que vos imprimeurs (et plus largement, vos solutions d'impression) sont certifiés conformes aux normes internationales et industrielles pertinentes telles

Les analystes disent : 'Les appareils Lexmark prennent en charge une gamme complète de fonctionnalités intégrées pour le renforcement des périphériques et la protection des points finaux.'

IDC MarketScape : Solutions et services de sécurité mondiaux 2022-2023

que Common Criteria et FIPS. L'intégrité de la chaîne d'approvisionnement a un impact sur la sécurité. La certification ISO 20243 étend cette réglementation à l'ensemble de la chaîne d'approvisionnement pour vous donner l'assurance que vos appareils sont vraiment inviolables et jamais contrefaits.

Lexmark est le premier fournisseur de solutions d'impression à recevoir la certification ISO 20243 pour l'intégrité de la chaîne d'approvisionnement, abordant la sécurité du développement du produit à la fabrication et à la distribution.

Points à retenir

- Les périphériques d'impression doivent être dotés d'une protection de sécurité intégrée.
- Le micrologiciel doit être chiffré et signé numériquement.
- Vérifiez que les normes indépendantes de l'industrie sont entièrement respectées.

Les logiciels sécurisés sont importants

Comment les solutions d'impression logicielles peuvent améliorer la sécurité de l'appareil et de votre environnement d'exploitation.

Trois considérations clés:

Cycle de vie de développement logiciel sécurisé (SSDL)

Le logiciel utilisé pour prendre en charge les imprimantes peut être un point faible pour la sécurité. Recherchez un fournisseur disposant d'un SSDL pour atténuer ce problème et optimiser la protection. Comment ? En abordant de manière exhaustive tous les aspects de la sécurité liés au développement logiciel, de la planification à la conception et à la mise en œuvre. Cela signifie, par exemple, qu'avant d'être expédié, tout code est soumis à des tests multipoints pour vérifier les vulnérabilités et la stabilité du code.

> **'Un SSDL prend en charge tous les aspects de la sécurité d'impression pour offrir des points de contrôle de protection inégalés.'**

Capacité de gestion à distance

Les changements dans les modèles de travail (tels que le travail à domicile et les environnements de travail hybrides) ajoutent à la complexité de la gestion sécurisée d'un parc de périphériques d'impression en réseau, tout en ouvrant la voie à des vulnérabilités. Dans cette nouvelle réalité, un logiciel d'impression robuste pour la gestion à distance est indispensable. Des fonctionnalités telles que la configuration commune, la gestion automatique des certificats et les mises à jour du micrologiciel à durée spécifiée garantissent que la conformité en matière de sécurité est entièrement à jour dans toute votre entreprise. Le personnel non autorisé est également empêché de modifier la configuration de tout appareil.

Applications utilisateur liées à la sécurité

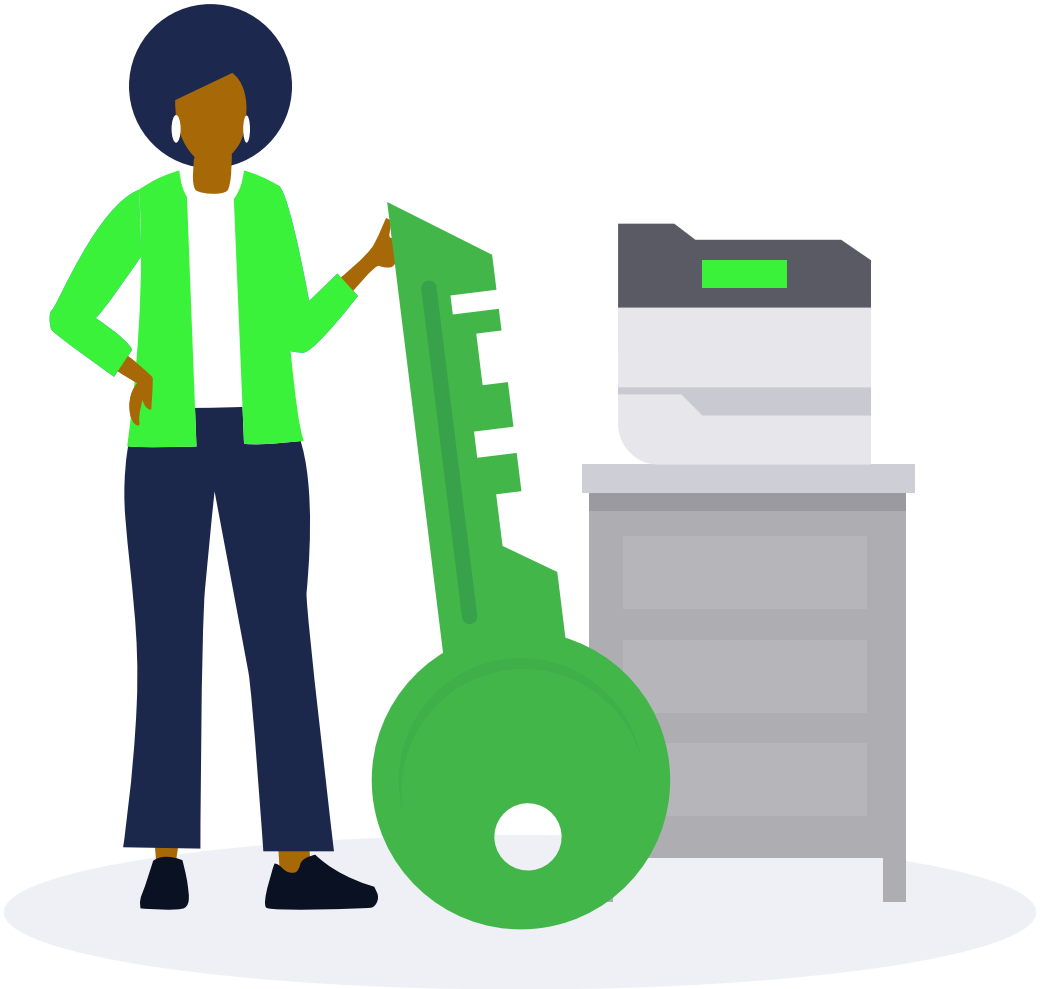
Les fonctionnalités logicielles, telles que la publication sécurisée de l'impression, peuvent améliorer la protection et la confidentialité des données. Ce type d'application restreint l'accès tout en offrant aux utilisateurs la possibilité d'imprimer de n'importe où. Il est exploité via des identifiants utilisateur réseau sécurisés et peut

être via une authentification sans contact ou par carte à puce. Certains secteurs, comme les opérations du gouvernement fédéral, exigent une sécurité accrue des documents. Pour ces secteurs, recherchez des solutions qui prennent en charge les environnements de gestion automatisée des certificats et les solutions d'authentification par carte d'accès commun (CAC) et par vérification de l'identité personnelle (PIV).

Assurez la conformité de la sécurité dans l'ensemble de votre organisation avec Lexmark Markvision Enterprise. Ce logiciel de gestion de l'impression gère à la fois la configuration des périphériques et les politiques de sécurité dans un seul outil facile à utiliser.

Points à retenir

- Un SSDL améliore la sécurité d'impression.
- Un logiciel de gestion à distance est indispensable.
- Recherchez des fonctionnalités d'impression sécurisée basées sur un logiciel.



Prise en charge de la sécurité du réseau

Comment garantir votre infrastructure d'impression en réseau contribue à préserver l'intégrité du réseau au sens large.

Trois considérations clés:

Identifier et gérer les vulnérabilités

Votre environnement réseau et les menaces de sécurité pertinentes sont uniques, ce qui signifie que vous avez besoin d'une solution sur mesure pour sécuriser vos données. L'évaluation des failles de sécurité est essentielle au développement d'une infrastructure d'impression qui sécurise correctement les points de terminaison et les points d'entrée des appareils des utilisateurs finaux. La capacité de modélisation des menaces par votre fournisseur d'impression peut également aider à analyser et à réduire le potentiel d'attaques.

Surveillance continue de la configuration.

Il est essentiel de réduire l'exposition aux vulnérabilités sur l'ensemble du réseau. La surveillance continue des paramètres, du micrologiciel et des vulnérabilités potentielles réduit considérablement le profil de risque de l'impression et simplifie les mises à jour et les ajustements de configuration nécessaires pour maintenir la sécurité.

Analyse des données de performance en temps réel

Les solutions d'impression basées sur le cloud améliorent la sécurité des points de terminaison grâce à la capture et à l'analyse des données, ce qui facilite l'identification des anomalies et l'alerte en cas de modèles d'utilisation suspects et de failles de sécurité potentielles. La visibilité à l'échelle du système améliore le contrôle tout en réduisant vos risques de sécurité, et est particulièrement importante pour les secteurs hautement réglementés tels que les soins de santé, les administrations et les services financiers.

'Lexmark devrait également figurer sur la liste restreinte des fournisseurs lorsqu'il s'agit de prendre en compte des facteurs tels que la sécurité pour relever les défis du travail hybride, la migration de l'infrastructure d'impression vers le cloud, le développement d'une posture de sécurité solide pouvant s'étendre et évoluer au fil du temps, et la nécessité d'une prestation de services mondiale cohérente.'

IDC MarketScape : Évaluation des fournisseurs des solutions et services de sécurité mondiaux 2022-2023

Les services de sécurité Lexmark incluent des évaluations de sécurité, l'optimisation de la configuration et la gestion des vulnérabilités afin de créer un écosystème d'impression sécurisé pour les défis les plus complexes en matière de protection des données.

Points à retenir

- Assurez-vous que vos solutions d'impression prennent en charge la protection des terminaux.
- La configuration doit s'aligner sur la sécurité du réseau.
- L'analyse des données identifie les utilisations suspectes en temps réel.

La différence Lexmark

Secure by Design — protection à tous les niveaux

L'approche Secure by Design unique de Lexmark intègre la sécurité dans tous nos produits, services et solutions afin d'améliorer votre stratégie de protection des terminaux. Secure by Design traite la sécurité comme un objectif de conception et d'ingénierie intégral couvrant la conception des produits, l'intégrité de la chaîne d'approvisionnement, les fonctionnalités de sécurité avancées, la gestion des vulnérabilités et les certifications tierces afin que vous sachiez que les appareils et les données sont protégés à chaque étape du processus.

Sécurité d'impression multicouche

Notre approche systématique de la protection des couches de sécurité d'impression sur les appareils, les données et les informations afin de fournir un écosystème sécurisé pour votre entreprise qui prend en charge une stratégie Zero Trust.

1. Produits - Le matériel et le micrologiciel de pointe améliorent la sécurité de l'imprimante.
2. Solutions - Protégez vos données les plus précieuses, à chaque point du réseau.
3. Services - Simplifiez la gestion de l'impression tout en renforçant la sécurité.
4. Normes - Assurez-vous de vous conformer aux certifications tierces.

Lexmark travaille avec...

7 des 10 plus grandes banques mondiales

7 des 10 principales agences fédérales américaines

> **'La sécurité de base est intégrée à chaque produit Lexmark.'**
>
> Paysage de la sécurité de l'impression Quocirca, 2023

En savoir plus sur Lexmark.com

Lexmark