IDC
Analyze the Future

I D C M A R K E T S P O T L I G H T :

Pour toute transformation numérique, la sécurisation de l'infrastructure d'impression est essentielle

Décembre 2016

Par Robert Palmer, responsable IDC Research pour les solutions d'imagerie, impression et documents

Sponsorisé par HP Inc.

Le plan de sécurité qui protège l'environnement IT d'une entreprise doit avoir une priorité élevée pour garantir une protection et une réponse appropriées aux menaces et aux attaques potentielles. La sécurité de l'impression doit faire partie de ce plan, surtout avec l'émergence de la 3e plate-forme IT (mobilité, cloud, big data, réseaux sociaux). Autrement dit, un plan global visant à sécuriser l'environnement d'impression de l'entreprise doit prévoir des solutions et des services capables de garantir la sécurité des équipements et des données d'impression. Cet article examine l'importance de la sécurisation de l'infrastructure associée à l'impression et à la gestion documentaire et le rôle que les services d'impression gérés (MPS) peuvent jouer dans la réalisation de cet objectif.

Introduction

Depuis plus de dix ans, les questions liées à la sécurité des données et à la protection de la vie privée arrivent régulièrement en tête des préoccupations des DSI et des managers IT. Les recherches effectuées par IDC indiquent également que la sécurité est désormais une priorité de très haut niveau pour la plupart des entreprises, arrivant très rapidement derrière une autre initiative clé : la transformation numérique. Même si ces deux aspects sont généralement considérés comme des différenciateurs essentiels de l'entreprise, il est important de comprendre comment la transformation numérique et la sécurité sont intimement liées.

Les entreprises qui décident de sécuriser leur infrastructure IT font face à des menaces nombreuses et variées. Les entreprises les plus avancées technologiquement ont fait de la sécurité une de leurs priorités en se posant les bonnes questions sur la protection du réseau contre les attaques extérieures, la sécurisation des équipements réseau, la supervision des accès aux équipements connectés et la lutte contre la divulgation des données confidentielles.

Il est clair que toutes ces préoccupations sous-tendent la nécessité de protéger les ressources les plus précieuses de l'entreprise : les données et les informations des clients. Les entreprises dépensent des milliards de dollars dans des logiciels de gestion documentaire et de gestion des contenus (ECM), et elles font des investissements considérables dans des systèmes spécialisés dans le contrôle des contenus stratégiques pour leurs activités. D'autres défis s'ajoutent à cette situation avec l'émergence de la mobilité et des solutions cloud. Les nouveaux « travailleurs de la connaissance » ont besoin d'un accès 24x7 à l'information, ce qui implique que les contenus doivent se déplacer à travers le pare-feu de l'entreprise.

Autre point à prendre en compte : l'infrastructure d'impression et de gestion de contenus d'une entreprise se situe exactement à l'intersection de la transformation numérique et de la sécurité IT. Néanmoins, la plupart des entreprises sont incapables d'identifier les vulnérabilités de sécurité associées à leur environnement d'impression et de gestion documentaire. En examinant cette question, on constate l'importance des imprimantes multifonction (MFP), qui sont désormais un véritable centre intelligent d'accès à l'information – information stockée dans la MFP elle-même, dans le réseau de l'entreprise, sur papier, ou dans le cloud.

Une menace invisible et non administrée...

Une MFP connectée est un risque potentiel de sécurité comme tout autre équipement connecté et non administré. Toutefois, une MFP peut également être utilisée comme équipement de premier plan pour accéder au réseau, superviser la sécurité des données et protéger l'accès à l'information.

Selon l'étude IDC *User Perspectives on Print Security, 2015*, plus de 30 % des entreprises n'ont pas encore mis en place de politiques de sécurité pour la supervision des accès et le contrôle des droits d'usage des imprimantes et des MFP connectées à leur réseau. En parallèle, plus de la moitié des personnes interrogées indiquent un haut niveau de préoccupation quant aux utilisations non autorisées de leurs photocopieuses ou de leurs MFP.

On peut constater des incohérences similaires lorsque les entreprises examinent leurs pratiques de sécurité IT. Dans l'enquête IDC *MaturityScape Benchmark:* Print Security in the United States, 2016, plus de 70 % des répondants ont déclaré que la sécurité de l'impression était un critère prépondérant au moment d'acheter ou des louer des imprimantes ou des MFP. Et pourtant, le nombre de répondants indiquant que la sécurité de l'impression sécurité était « très importante » était seulement de 26 %, soit moins que ceux qui étaient préoccupés par la sécurité globale de leur environnement IT.

Trop souvent, les managers IT et les responsables de la sécurité ont tendance à penser que les systèmes mis en place pour protéger le réseau lui-même seront suffisants pour protéger les équipements connectés à ce réseau. En réalité, la sécurité périmétrique du réseau est généralement insuffisante, et tous les équipements connectés au réseau présentent désormais un risque de sécurité, y compris les imprimantes et les MFP.

La menace est réelle, avec les risques associés à des attaques malveillantes à travers une imprimante ou une MFP en réseau comme point d'entrée ou à une utilisation négligente (généralement involontaire) des équipements par les employés. L'environnement d'impression est unique dans la mesure où il traite des données, des documents et des informations dans les deux formats principaux (numérique et papier) ; autrement dit, des contenus stratégiques sont facilement exposés et présentent de nombreuses vulnérabilités. L'entreprise qui ne se préoccupe pas d'intégrer son environnement d'impression dans une stratégie globale de sécurité IT est aussi vulnérable que si elle ne prenait aucune mesure de sécurité IT !

Les conséquences d'une atteinte à la sécurité de l'infrastructure d'impression et de gestion documentaire sont les mêmes que les conséquences de tout autre type d'atteinte à la sécurité : des coûts élevés en raison des interruptions de service nécessaires pour identifier et corriger l'atteinte à la sécurité, les amendes résultant du non-respect de la gouvernance d'entreprise et de la conformité à la réglementation, des clients perdus et autres dommages nuisibles à la réputation de l'entreprise.

Vers des services d'impression sécurisés

Les défis associés à la sécurité des impressions et des documents sont faciles à identifier, mais élaborer une stratégie d'impression sécurisée efficace peut être difficile pour certaines entreprises. L'un des aspects du problème concerne les différents acteurs de l'entreprise. En général, la sécurité des équipements est associée à la fonction IT et elle comprend le département IT, le responsable sécurité, le service d'assistance (help desk), la sécurité des terminaux et la sécurité des réseaux. En outre, toute discussion portant sur la sécurité des imprimantes et des MFP déborde immanquablement sur la gestion des installations.

De son côté, la sécurité des contenus est souvent considérée en rapport avec les exigences de conformité à la réglementation et les acteurs sont généralement en charge des questions de gouvernance et de gestion des risques. D'autres acteurs peuvent être impliqués, dont les responsables des applications ERP ou des bases de données et de la gestion des contenus et les managers d'autres départements. Dans bien des cas, la sécurité des imprimantes et des contenus est gérée séparément, ce qui conduit à un manque d'intégration et à la multiplication des failles et des vulnérabilités. Par ailleurs, les entreprises sont souvent peu informées des solutions d'impression sécurisées et des services spécialisés qui sont disponibles sur le marché.

Autrement dit, il s'agit d'un domaine où les services d'impression gérés (MPS) pourraient jouer un rôle important dans la promotion de la sécurité de l'impression et des documents. Un grand nombre d'entreprises ont signé un contrat avec un prestataire MPS pour optimiser leur infrastructure d'impression, améliorer l'efficacité globale et réduire les coûts, mais la sécurité des impressions et des contenus est généralement négligée dans la plupart des contrats de services d'impression. Dès aujourd'hui, certains prestataires MPS disposent des capacités, des outils et des ressources nécessaires pour aider les entreprises à identifier et prioriser leurs menaces de sécurité actuelles. Leur intervention peut commencer par une évaluation initiale de la sécurité – une opération vitale pour identifier les lacunes de l'infrastructure actuelle d'équipements et de contenus. L'entreprise peut ensuite travailler en partenariat avec le prestataire MPS pour développer et déployer des services d'impression gérés capables de surmonter les vulnérabilités actuelles, de durcir l'infrastructure de documents et d'anticiper les risques futurs.

Le prestataire MPS peut également réunir les différents acteurs de l'entreprise et organiser la livraison des services d'impression aux différents départements, une démarche essentielle pour le déploiement d'une approche holistique de la sécurité des équipements et des contenus. Par ailleurs, cette approche facilite l'élaboration d'un plan de sécurité qui prend en compte la stratégie de transformation numérique de l'entreprise. Les services d'impression sécurisés peuvent aller d'un niveau de base qui se contente de protéger les équipements et les données à des mesures plus avancées qui sont beaucoup plus complexes à implémenter mais qui offrent un niveau plus élevé de sécurité des équipements et de protection des contenus.

Conclusion : Du réactif au proactif

Le résultat est que l'infrastructure d'impression et de documents n'a pas reçu le niveau d'attention accordé aux autres menaces à la sécurité des réseaux internes et d'Internet. Les atteintes à la sécurité font apparaître des peurs et des incertitudes et leur impact sur les coûts opérationnels, les performances des employés et la réputation de l'entreprise peut être extrêmement grave.

Les entreprises doivent prendre des mesures proactives en réponse aux préoccupations de sécurité suscitées par leur infrastructure d'impression et de documents, et les prestataires MPS doivent être considérés comme des partenaires essentiels de cette démarche. Dans votre recherche de prestataires de services d'impression, identifiez ceux qui démontrent des compétences solides dans l'évaluation du niveau des menaces et des capacités de correction en conséquence

En outre, efforcez-vous de retenir des partenaires qui proposent un matériel et des solutions reposant sur un écosystème de sécurité et prêts à répondre aux vulnérabilités suivantes de l'infrastructure de documents :

- Authentification et autorisation des utilisateurs
- Gestion des équipements
- Protection des équipements contre les malwares
- Mises à jour des firmwares et gestion des mots de passe
- Sécurité et confidentialité des contenus, intégrité des données
- Capacité à tenir compte des éléments humains impliqués dans l'installation, la configuration et l'utilisation des équipements

La solution MPS retenue doit également être conçue pour s'intégrer dans les systèmes tiers de gestion de documents et ECM, afin d'assurer une meilleure protection et de faciliter les exigences de gouvernance et de conformité réglementaire.

En adoptant une approche holistique, les entreprises peuvent commencer à éliminer leurs vulnérabilités et à durcir la protection de leur environnement d'impression et de documents – clairement le maillon faible de leur sécurité.

Siège social international : 5 Speen Street Framingham, MA 01701 (États-Unis) – Tél. (+1-508) 872-82-00 – Fax (+1-508) 935-40-15 – www.idc.com