Un écosystème d'impression sécurisé

Une partie de la série Transformation numérique Brother

Rapport de leadership d'opinion
basé sur la recherche

www.brother.ch

Les obstacles à l'investissement dans la sécurité des impressions

Avec la menace grandissante des atteintes à la confidentialité et des piratages, la plupart des petites et moyennes entreprises (PME) comprennent parfaitement la nécessité de protéger leurs systèmes informatiques.

La gestion de la sécurité du parc informatique est un défi qui doit être abordé en bloc. Imprimantes, scanners et copieurs doivent être tout aussi sécurisés que les autres équipements informatiques. S'ils sont ignorés, ces appareils risquent d'offrir aux hackers une porte d'entrée facile dans l'entreprise. Les PME ont de plus en plus conscience de l'importance de ce problème: 72% des entreprises déclarent qu'il est indispensable que leurs imprimantes, scanners et copieurs soient sécurisés. Ceci est encore plus prégnant dans les entreprises qui manipulent des données sensibles, par exemple dans les services aux entreprises (82%) et la santé (81%).

Cela signifie toutefois qu'il reste encore près d'un tiers des entreprises qui ne considèrent pas cette question comme importante. Et dans le même temps, près de la moitié des personnes interrogées trouvent que leur entreprise n'a pas suffisamment investi dans la sécurité du matériel d'impression.

Si les entreprises reconnaissent la nécessité d'investir dans la sécurité des imprimantes, pourquoi ne le font-elles pas?

Nos recherches font ressortir deux raisons claires:

La responsabilité de la sécurité des imprimantes n'est pas bien déterminée

Les menaces et normes de sécurité sont mal comprises et connues-standards

Dieser Bericht soll Entscheidungsträger in KMU dabei unterstützen, die Wichtigkeit der Drucksicherheit zu verstehen und sichere Drucklösungen zu implementieren. Er ist Teil einer grösseren Serie, mit der wir Entscheidungsträger darüber informieren möchten, wie digitale Technologien in KMU optimal eingesetzt werden.

Die Berichte basieren auf einem umfassenden Forschungsprogramm mit Befragungen von KMU in der EMEA-Region. Zur Serie gehören vier Berichte zu den folgenden Themen:

- Digitale Workflows
- Die richtige Lösung für Ihr Unternehmen
- Sicherheit
- Nachhaltigkeit

Qui est responsable de la sécurité des imprimantes?

Bien trop souvent, la responsabilité des individus quant à la sécurité des imprimantes n'est pas clairement établie. Près de la moitié des PME d'Europe de l'Ouest (44%) indiquent ne pas savoir qui est responsable de la sécurité des imprimantes au sein de l'entreprise. Si les responsabilités ne sont pas clairement établies, il est logique que la prise de décision et la mise en œuvre de la sécurité des imprimantes en souffrent et rendent l'entreprise vulnérable.

La raison de cette lacune est que l'environnement d'impression, à la différence d'autres appareils comme les ordinateurs, n'est pas traditionnellement considéré comme un maillon faible. Même si nos recherches montrent que les décideurs commencent à comprendre que la sécurité des impressions est vitale, les postes au sein des PME ne reflètent pas encore cette prise de conscience.

Les PME sont particulièrement vulnérables à l'absence de responsabilités établies, car c'est généralement un tout petit nombre d'employés qui s'occupent de tout l'équipement matériel et logiciel de l'entreprise. Si les professionnels de l'informatique n'ont pas conscience des risques liés à la sécurité des impressions, celle-ci peut être reléguée au second plan.

Cependant, tous les employés sont plus ou moins responsables de s'assurer que les informations sensibles sont en sécurité.

Si les spécialistes informatique et technologies sont responsable de la sécurité des appareils mêmes, il incombe aux employés de s'assurer que les données sont en sécurité. La sécurité des données est sans doute le domaine le plus risqué pour les informations commerciales sensibles.

La sécurité des données inclut diverses menaces, notamment:

- l'accès non autorisé aux documents imprimés
- l'absence de déconnexion après l'impression de documents confidentiels
- le manque de traçabilité (qui a accédé à quels documents sur l'imprimante

Près de 9 entreprises sur 10 ont connu un incident relatif à la sécurité des impressions...

… et sept sur dix (72%) affirment que la sécurité des données les inquiète plus que la sécurité des appareils. Pourtant, actuellement, moins d'une entreprise sur trois se déclare certaine que son infrastructure d'impression est suffisamment sécurisée, contre 53% des entreprises qui pensent que leur matériel est correctement sécurisé.

La majorité des PME (64%) affirme également que la sécurité de leurs données est une priorité. Elle est perçue comme un défi crucial et peut véritablement entraver les performances.

Actuellement, près de la moitié des PME (48%) déclarent n'avoir que peu ou pas de procédures permettant de savoir qui imprime ou récupère des documents. Sans surprise, près de neuf entreprises sur dix (86%) rapportent avoir connu un incident de sécurité lié à l'impression. Ces incidents de sécurité concernent le plus souvent des documents confidentiels laissés sans surveillance dans l'imprimante, des impressions non récupérées ou des employés qui récupèrent des documents confidentiels qui ne leur sont pas destinés.

Résultat, la majorité des PME (64%) commence à mettre en place des mesures pour régler les problèmes de sécurité des impressions en limitant l'accès à certaines imprimantes ou en forçant les employés à utiliser une carte d'ID ou un code PIN pour récupérer leurs impressions.

C'est un pas dans la bonne direction. Dans les années à venir, il sera important pour toutes les entreprises d'adopter des procédures plus sécurisées et, pour celles qui ont déjà commencé, de poursuivre leurs efforts et d'améliorer leurs pistes de responsabilité et d'audit.

La véritable sécurité des informations passe par la sécurisation des appareils et des données.

Elle poursuit trois objectifs:

Confidentialité

Protéger les données confidentielles de l'entreprise pour s'assurer qu'elles ne parviennent qu'aux destinataires voulus. Pour cela, l'authentification et les autorisations sont la clé pour demander aux utilisateurs de confirmer leur identité et leurs droits avant de les laisser accéder à une impression.

Intégrité

S'assurer que le micrologiciel de l'appareil est sécurisé et résiste au piratage et aux autres menaces extérieures.

Disponibilité

S'assurer que l'appareil fonctionne et est accessible aux utilisateurs autorisés pour les tâches essentielles.

Le manque de connaissances favorise les mauvaises pratiques de sécurité

Moins d'un tiers (32%) des responsables informatiques dans les PME déclarent avoir des connaissances avancées de la sécurité des technologies et des menaces potentielles. Si les responsables informatiques ne connaissent pas suffisamment bien les menaces, les entreprises continueront à batailler pour mettre en place les mesures appropriées pour se protéger. Dans les PME, le poste de responsable informatique couvre généralement beaucoup de technologies différentes. Il est compréhensible qu'il ne soit pas un expert de la sécurité des impressions.

Souvent, le jargon est en cause. Plus de la moitié (51%) des PME trouvent qu'il y a trop de jargon utilisé dans la sécurité des impressions, surtout en France et en Italie.

Et près de 60% des PME déclarent bien comprendre les normes de sécurité applicables.

De ce fait, il y a peu de chances que les responsables sachent véritablement quel fournisseur de technologie d'impression répond le mieux à leurs besoins en matière de sécurité. Il n'est donc pas surprenant que les entreprises se tournent vers les marques qu'elles «connaissent» pour acquérir des imprimantes sécurisées, sans vraiment comprendre les mesures de sécurité qu'elles ont ou n'ont pas en place actuellement.

Les partenaires d'impression doivent se donner plus de mal pour vous aider à décrypter les normes de sécurité applicables et à choisir la meilleure solution pour votre entreprise.

Les conseils de Brother

Vu la complexité du marché de la sécurité des impressions, Brother a formulé sept recommandations essentielles pour aider les PME à se prémunir contre les graves conséquences financières, juridiques et réputationnelles d'une perte de données.

Obtenez l'adhésion de la direction

Étant donné l'ampleur des dégâts causés par les cyberattaques et les fuites de données et les exigences du règlement général européen sur la protection des données (RGPD), la sécurité des impressions est un sujet qui doit interpeller au-delà du service informatique. Elle doit être discutée au niveau de la direction, notamment avec le directeur de l'information (CIO) et le directeur de la sécurité des informations (CISO).

Menez un audit approfondi

Il est crucial pour les entreprises d'identifier toutes les failles potentielles dans la sécurité des impressions en incluant l'environnement d'impression à des audits de sécurité réguliers. Ceci est particulièrement important si votre entreprise combine d'anciens appareils et des nouveaux.
La plupart des fournisseurs de gestion déléguée des impressions (MPS) proposent des évaluations complètes et assurent la surveillance continue des appareils une fois le parc optimisé et sécurisé

Changez les mots de passe d'administration par défaut

Les mots de passe d'administration par défaut sont un point faible des imprimantes, mais la bonne nouvelle est qu'il est facile d'y remédier. Une fois l'appareil installé, changez les mots de passe pour une version plus forte et sécurisée.

Mettez à jour votre micrologiciel et ses correctifs

Vous pouvez réduire considérablement les failles de sécurité potentielles des imprimantes en mettant à jour le micrologiciel et en optant pour les mises à jour automatiques. Pour toute question à ce sujet, contactez le fabricant de votre imprimante.

Protégez les travaux d'impression

Ce ne sont pas seulement les imprimantes qui doivent être protégées, mais aussi les documents imprimés. Le chiffrement de bout en bout du trafic réseau permet d'envoyer des travaux d'impression aux imprimantes en toute sécurité. Comme la plupart des imprimantes conservent les travaux d'impression temporairement, assurez-vous que les données sont chiffrées.

Surveillez les appareils

Connaître le statut actuel de vos imprimantes vous donne une vue d'ensemble de votre environnement d'impression. Les entreprises devraient envisager d'utiliser des outils logiciels pour surveiller les appareils et résoudre les problèmes dès qu'ils surviennent. Les appareils génèrent quantité de données qui permettent souvent d'identifier les potentiels incidents de sécurité et de réagir rapidement aux attaques. Les utilisateurs de MPS peuvent aussi recevoir des rapports de conformité réguliers incluant les atteintes aux données.

Formez les employés

Beaucoup de pertes de données sont involontaires. Il est donc vital pour les entreprises d'éduquer les employés à l'importance de protéger les informations sensibles contre les attaques. Les fournisseurs de MPS apportent souvent une aide pour la formation.

Pour conclure

Par le passé, les systèmes d'impression ont souvent été un angle mort de la sécurité en entreprise, mais les PME prennent de plus en plus conscience de leur importance. Pourtant, il reste des obstacles conséquents à la mise en œuvre de la sécurité des impressions.

Les PME doivent définir clairement les responsabilités en matière de sécurité des impressions afin de protéger correctement leurs appareils contre les menaces. Au-delà des appareils, il faut aussi protéger les données. Et afin de réduire les risques, la coopération des employés est indispensable.

Même quand les responsabilités sont bien définies au sein des PME, il est toujours nécessaire de disposer de connaissances suffisantes pour gérer efficacement la sécurité des impressions. Les technologies d'impression sont de plus en plus complexes et regorgent de jargon. Les entreprises doivent s'appuyer sur des fournisseurs de confiance pour prendre les bonnes décisions.

Un environnement d'impression a besoin de plus que la sécurité pour être efficace. Les autres rapports de la série Transformation numérique abordent plus en détail l'implémentation des flux de travail numériques, l'optimisation de la productivité et la durabilité de la configuration.

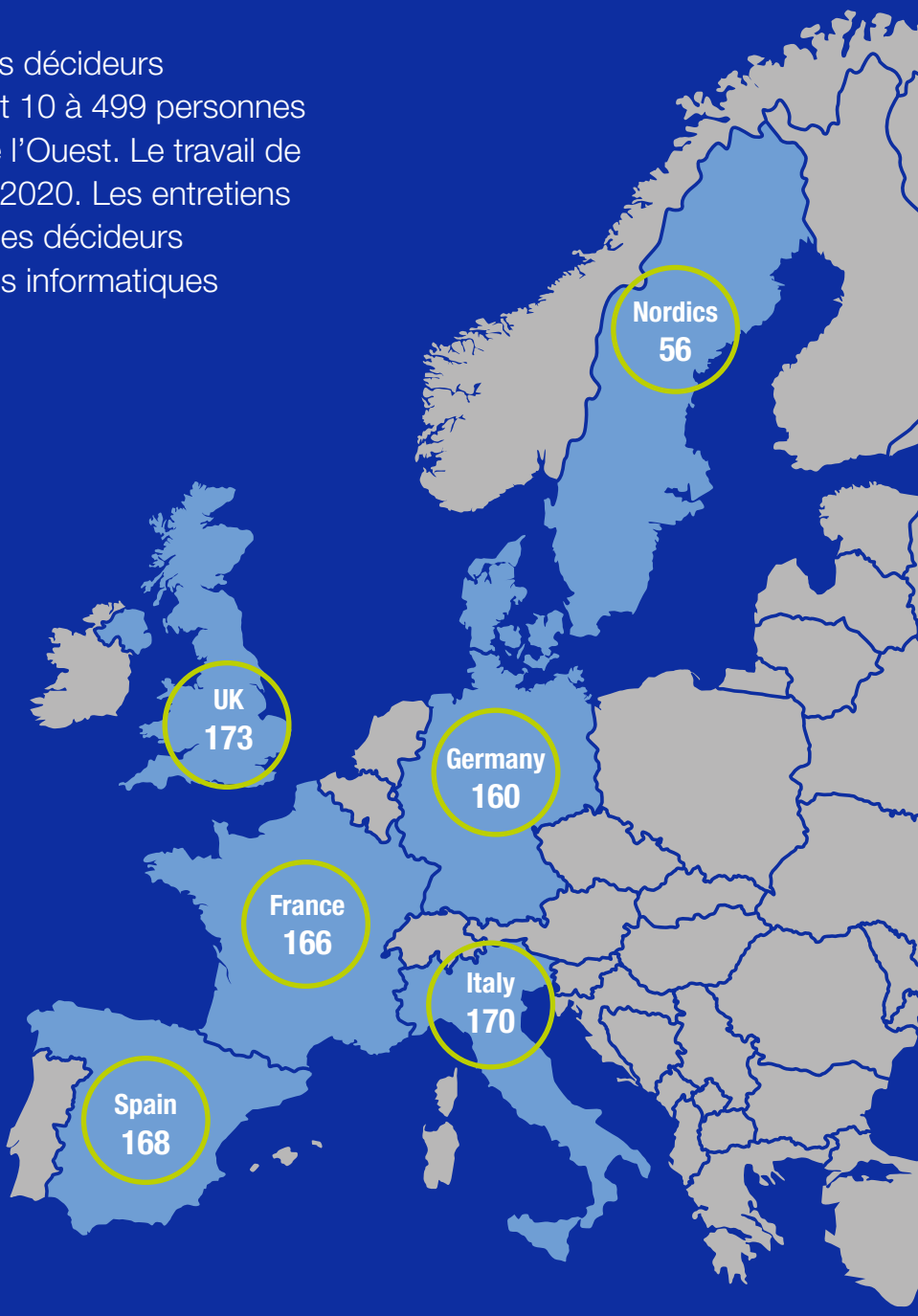
Notre méthodologie

Ce rapport repose sur 893 enquêtes en ligne auprès de responsables informatiques et de décideurs au sein des entreprises.

Les responsables informatiques et les décideurs travaillaient dans des PME employant 10 à 499 personnes dans plusieurs marchés d'Europe de l'Ouest. Le travail de terrain a été mené en 2019 et début 2020. Les entretiens ont été répartis équitablement entre les décideurs stratégiques (448) et les responsables informatiques (445).

Principaux secteurs étudiés:

- Santé - 152
- Commerce - 117
- Logistique - 113
- Hôtellerie - 81
- Transport et stockage - 62
- Services aux entreprises - 65
- Industrie - 54
- Services financiers - 53
- Éducation - 51
- Construction - 39



Les autres secteurs étudiés sont l'énergie, l'industrie pharmaceutique, l'agriculture, la défense, l'immobilier, les sports et loisirs.

Les recherches ont été menées par le cabinet d'étude de marché Savanta.durchgeführt.

Tenez-vous au courant des dernières tendances

avec nos autres rapports de la série Transformation numérique Brother.

À paraître prochainement

brother
at your side

www.brother.ch

Brother (Suisse) SA
Täfernstrasse 30,
CH-5405 Baden
Tel: 0844 484 111
info@brother.ch