IDC
Analyze the Future

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

L'angle mort du GDPR – Les équipements d'impression, un point faible pour votre conformité

Juillet 2017

Par Duncan Brown

Sponsorisé par HP

Ce document IDC Market Spotlight met en lumière la vulnérabilité des équipements d'impression présents au sein des réseaux d'entreprise. Il décrit l'impact de cette vulnérabilité sur les programmes de conformité liés au Règlement général sur la protection des données (GDPR) et à d'autres règlementations à venir. Par ailleurs, ce document propose des mesures à mettre en place, visant à réduire les risques liés aux équipements d'impression dont la sécurité est aujourd'hui insuffisante.

Introduction

L'attention accordée à la sécurité de l'Internet des objets (IoT) s'est largement intensifiée suite à une série d'attaques par déni de service distribué (DDoS). Ces attaques ont concentré un volume important de trafic malveillant provenant de plusieurs milliers d'équipements connectés (caméras de vidéosurveillance, magnétoscopes numériques, etc.). Ces équipements ont été piratés pour empêcher le fonctionnement de certains sites Web très connus. Quels seront alors les prochains équipements ciblés ?

Alors que nous étions à la recherche d'équipements IoT présentant les mêmes caractéristiques que ceux cité précédemment, notre attention a été attirée sur les équipements d'impression des particuliers, des PME/TPE et des grandes sociétés. Les mises à jour logicielles et le contrôle des accès, qui sont des priorités sur le matériel informatique traditionnel, sont souvent négligés sur les équipements d'impression. De ce fait, les équipements d'impression pourraient être le prochain vecteur d'une attaque IoT de grande ampleur. Ils pourraient représenter de nouveaux risques pour l'activité des entreprises dans la mesure où ils se trouvent à l'intérieur même du réseau de l'entreprise. Sans parler du potentiel de vol de données et de DDoS sur la partie interne des réseaux. Avec l'entrée en vigueur du GDPR (et d'autres contraintes annoncées) et l'impact qu'il peut avoir sur les entreprises en termes de piratage des données personnelles, les équipements d'impression en réseau apparaissent comme des points de terminaison négligés, exigeant une attention extrême.

Les équipements d'impression sont également des points de terminaison

Imaginez le scénario suivant : un équipement inconnu se connecte à un réseau d'entreprise derrière des défenses telles que les pare-feu, les systèmes de prévention des intrusions et autres infrastructures informatiques. Cet équipement dispose alors d'un accès illimité à l'ensemble des ressources de ce réseau. Pour utiliser toute la puissance des fonctionnalités de cet équipement, un serveur Web est intégré dans celui-ci. Tous ses ports sont « ouverts » par défaut et disposent d'une connectivité Ethernet jusqu'à 1 gigabit de connectivité pour faciliter l'accès à cet équipement. Toujours dans l'optique de maximiser l'accès à ses fonctionnalités, l'équipement dispose d'un OS tel que Linux. Cet équipement n'est pas examiné régulièrement par le scanner de vulnérabilité de l'entreprise dans la mesure où son serveur Web intégré risque de faire apparaître des faux positifs

sur les systèmes de gestion de la sécurité (SIEM). Le scanner de vulnérabilité est donc configuré en excluant cet équipement. Logiquement, selon la marque et le modèle, cet équipement ne bénéficiera d'AUCUNE opération de mise à jour, de maintenance ou de patching pendant sa durée de vie de 5 à 10 ans. La protection de l'équipement se limitera à un mot de passe par défaut et sa maintenance sera assurée par des parties tierces non contrôlées. Ce type d'équipement étant essentiel à la productivité de l'entreprise, nous comptons en moyenne un équipement d'impression pour 10 employés. Ces employés utiliseront non seulement cet équipement pour imprimer et récupérer leurs documents. Ils l'utiliseront également pour envoyer des données personnelles sensibles qui seront stockées sur le disque dur de cet équipement. Pire encore, ces données stockées pourront très facilement être imprimées par des utilisateurs occasionnels qui n'auront pas à s'authentifier ni à être soumis au contrôle des accès.

Certains pourraient appeler cela un cauchemar – d'autres pourraient appeler cela... une imprimante !

Un point très important doit être clarifié. La « sécurité des impressions » est une pratique de sécurité mature, régie par le besoin de garantir la sécurité des données. Les normes de conformité jouent un rôle important dans la mise en place d'une politique de sécurité efficace des impressions. Dans la région EMEA (Europe Middle East & Africa), la réglementation en vigueur est le GDPR. Toutefois, il convient également de tenir compte de la directive sur la sécurité des réseaux et des systèmes d'information (SNI), de la mise à jour de la directive ePrivacy ainsi que de la directive révisée sur les services de paiement (PSD2). Ces différentes normes et réglementations doivent servir de base pour des *objectifs* de sécurité. Toutefois aucune précision n'est mentionnée en ce qui concerne les détails techniques de conformité.

L'essentiel du GDPR

Le GDPR met à jour les lois européennes en matière de protection des données. Il remplace la législation actuelle datant de 1995 (boom dot-com, émergence de Twitter, Facebook, du cloud...). La mise à jour proposée par le GDPR prend compte de ce nouveau paysage de développement et de création de données personnelles.
Un autre avantage du GDPR est qu'il s'applique à tous les états membres de l'Union européenne (UE).

Le GDPR a été adopté en avril 2016 et prendra effet le 25 mai 2018. Les entreprises ont donc moins d'un an pour s'assurer de la mise en conformité de leurs activités. Les pénalités en cas de non-conformité peuvent atteindre 20 millions € ou 4 % du chiffre d'affaires global annuel de la société (la valeur la plus élevée étant celle retenue). Par ailleurs, le GDPR introduit l'obligation de notification pour toute atteinte te violations aux données. Les conséquences de cette obligation doivent alerter les dirigeants sur les répercussions qu'elle peut avoir sur la réputation de leur entreprise.

Il est à noter que la sortie du Royaume-Uni de l'UE (Brexit) n'aura aucune incidence sur l'application du GDPR :

- Les entreprises du Royaume-Uni qui traitent des données à caractère personnel liées à l'UE devront se conformer au GDPR. En effet, ce dernier s'applique aux données personnelles de tout individu résidant dans l'UE, quel que soit le pays où a lieu le traitement des données
- Le Royaume-Uni va par ailleurs probablement implémenter des lois locales ou des directives semblables à celles du GDPR afin de faciliter les transferts de données avec l'UE (par application des « règles d'adéquation »).

Le GDPR ne se limite donc pas à des enjeux de sécurité. Il intègre une multitude de nouvelles mesures relatives à : la portabilité des données, au consentement, la révocation du consentement, la vérification de l'âge des utilisateurs et au droit à l'oubli. Cependant, il convient de souligner que la conformité s'appuie en grande partie sur la qualité de la sécurité. Que dit le GDPR à cet égard ?

Le GDPR n'émet aucune prescription quant à la définition des mesures de sécurité à mettre en œuvre. Sur ses 99 articles, seul l'Article 32 parle spécifiquement de la sécurité en invitant les entreprises à : « implémenter les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques ». En d'autres termes, il appartient à chaque entreprise d'évaluer les risques associés à ses données personnelles et de mettre en place les contrôles de sécurité qu'elle juge nécessaires et suffisants.

Un aspect de cette considération est ce que le GDPR qualifie d' « état de l'art ». Les entreprises ne sont pas dans l'obligation de mettre en place des technologies d' « état de l'art". Toutefois, elles doivent savoir de quoi il s'agit et défendre leur position. Une situation à éviter est d'avoir à justifier le fait de ne pas avoir mis en œuvre un contrôle ou une technique de sécurité particulière, surtout lorsque cela a facilité l'atteinte aux données.

L'un des principaux tests susceptibles d'être appliqués par les régulateurs du GDPR est ce que IDC appelle « Avez-vous vraiment tout essayé ? / How hard did you try? ». Ne pas détecter une vulnérabilité est une mauvaise chose. Néanmoins être conscient de cette vulnérabilité et ne rien faire est bien pire. Le fait de négliger intentionnellement une vulnérabilité dans un parc d'équipements d'impression entraînera l'échec du test pour l'entreprise. Par extension cela peut représenter une infraction à plusieurs principes du GDPR dont : la « limitation des finalités », la « réduction des données personnelles au minimum nécessaire », la « limitation de la durée du stockage » et les notions « d'intégrité et confidentialité » (cf. Article 5 du GDPR).

Il est important de souligner que la portée matérielle du GDPR concerne « le traitement des données personnelles, en totalité ou en partie, par des moyens automatisés ainsi que le traitement par des moyens non automatisés de données personnelles présentes dans un système de classement ou devant être intégrées dans un système de classement ». En d'autres termes, cette portée matérielle ne se limite pas aux données personnelles sous forme électronique. Les données sur papier sont également concernées par le GDPR.

Directive sur la sécurité des réseaux et des systèmes d'information (NIS)

L'UE a réalisé que, face à la multiplication des cyber-attaques, les services les plus importants des entreprises devaient être protégés, en particulier ceux étant considérés comme essentiels au fonctionnement économique ou sociétal de ces entreprises. Pour garantir la cohérence en matière de protection contre les cyber-attaques au sein des 27 états, l'UE a adopté la directive NIS (NISD).

Tout comme le GDPR, la directive NIS reste superficielle sur les conditions de sécurité. L'accent est mis sur la protection des infrastructures, incluant les ressources matérielles et la résilience (gestion des incidents, continuité des activités, etc.). La directive NIS inclut une clause obligatoire de notification d'infraction (Cf. Article 16), mais aucune amende n'est stipulée en cas de non-conformité.

Comme NIS est une directive, elle doit être transposée en loi par chaque État membre et ratifiée par son corps législatif. La directive NIS est entrée en vigueur en août 2016. Les États membres ont jusqu'au 10 mai 2018 pour transposer la directive dans leurs législations nationales et six mois supplémentaires, pour identifier les opérateurs des services essentiels.

Avantages d'une sécurité efficace pour les équipements d'impression

La « sécurité des équipements d'impression », contrairement à la « sécurité d'impression », se concentre uniquement sur les équipements physiques associés à l'impression (il s'agit d'un aspect de la sécurité du réseau). La sécurité des équipements d'impression considère chaque équipement d'impression comme un « point de terminaison ». Cette politique de sécurité les traite avec la même attention que tout autre point de terminaison (systèmes de bureau, ordinateurs portables, serveurs ou terminaux mobiles). Bien que les appellations soient proches et que ces deux types de sécurité

partagent les mêmes préoccupations, la sécurité d'impression et la sécurité des équipements d'impression sont des pratiques bien distinctes.

Quelle est la véritable vulnérabilité des imprimantes en réseau ?

Les imprimantes reçoivent des volumes considérables de données. Ces données sont soit personnelles ou confidentielles.
Peu d'utilisateurs, de professionnels de la conformité ou d'administrateurs informatiques se préoccupent de la sécurité des données transmises aux équipements d'impression ou stockées sur celles-ci. Les données stockées sur les équipements d'impression restent soumises aux exigences de conformité. Un principe fondamental du GDPR (cf. Article 5 f) stipule le fait suivant :« la sécurité des données personnelles concerne la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) ». Toutefois la plupart des entreprises n'accordent pas autant d'importance à la sécurité des données résidant sur les équipements d'impression.

De plus, il est courant de voir des documents abandonnés dans les bacs de sortie des imprimantes. Dans le contexte du GDPR, il est possible que les solutions d'impression à la demande (pull printing), obligeant les utilisateurs à se déplacer pour s'authentifier et collecter le document, deviennent une exigence concrète pour les entreprises qui autorisent l'impression de données personnelles.

Les équipements d'impression sont une cible privilégiée pour les cyber-malfrats. En effet, ces équipements sont exclus de l'environnement informatique et requièrent peu d'attention de la part du personnel de sécurité. Les équipements d'impression sont souvent considérés comme faisant partie des infrastructures (bâtiments, bureaux, data center...). Quand les équipements d'impression ont commencé à se connecter au réseau, tant qu'ils étaient situés derrière un pare-feu, ces derniers étaient considérés comme « à faible risque ».Quant à la vulnérabilité des points de terminaison de type impression, elle était largement sous-estimée.

Les équipements d'impression de type multifonction combinant une imprimante, un scanner et un fax sont de plus en plus développés. Ils intègrent de véritables ordinateurs polyvalents permettant de contrôler toute action. Les équipements d'impression les plus puissants intègrent souvent un système d'exploitation Windows ou Linux. Ces ordinateurs-contrôleurs sont généralement ignorés lors des opérations de durcissement et de patching, les rendant ainsi plus vulnérables. En outre, un certain nombre de fonctionnalités des équipements d'impression exigent une connectivité réseau et par conséquent l'ouverture d'une multitude de ports.

La combinaison du manque de considération et d'une forte puissance de traitement couplée à nombreuses options de connexion démontre que les attaques et menaces peuvent se manifester de plusieurs manières. Par exemple à travers un modem, un point d'accès sans fil, ou par un saut de puce à partir de postes de travail infectés par des logiciels malveillants. Après avoir réussi à s'introduire dans le réseau, les cyber-malfrats peuvent utiliser cette puissance pour frapper d'autres équipements ou participer à une attaque de type DDoS (déni de service distribué). La plupart des équipements d'impression disposent d'un accès illimité au réseau interne. Un cyber-malfrat ayant réussi à s'introduire dans le réseau via un équipement d'impression pourra ensuite examiner l'ensemble du réseau et rechercher les systèmes exploitables.

Comme tout autre point de terminaison exigeant une protection, les équipements d'impression ne sont pas seulement une passerelle vers le réseau. Ils sont aussi une cible à part entière pour les cyber-malfrats. Certains équipements d'impression stockent des documents sensibles dans leur file d'attente. Ces équipements intègrent souvent un scanner et les utilisateurs ne se doutent pas que leurs documents peuvent être stockés dans l'archive des numérisations pendant très longtemps.

Considérations générales

Si la sécurité des équipements d'impression n'a pas encore été élevée au rang de priorité dans votre entreprise, IDC vous propose quelques recommandations.

Commencer par la visibilité

Pour tout point de terminaison à sécuriser, il est conseillé de procéder par étapes. La première étape est toujours la visibilité : effectuer un inventaire complet des équipements d'impression existants (marque, modèle, fonctionnalités et configurations). Cet inventaire peut être plus problématique. Cela est particulièrement le cas, lorsque certains utilisateurs placent certains équipements d'impression dans des emplacements qui échappent au département IT (« shadow IT »). Par exemple, les laboratoires, les bureaux de la direction ou les bureaux de service clientèle ont tendance à connecter une imprimante au réseau (ou à un PC déjà connecté au réseau) par convenances personnelles, sans prendre en considération les impacts pour la sécurité globale.

La solution idéale pour un inventaire de points de terminaison (incluant les équipements d'impression) consiste à utiliser les informations d'un contrôleur d'accès réseau NAC ou d'un outil de gestion des ressources comprenant une fonctionnalité de découverte comme fonctionnalité principale. En l'absence de NAC, la visibilité complète des équipements d'impression est extrêmement difficile, même si certains modèles d'imprimante génèrent des informations d'auto-découverte lorsqu'elles sont connectées au réseau. Si votre environnement réseau ne propose pas de base installée homogène des équipements d'impression connectés, un contrôleur NAC fera parfaitement l'affaire.

Renforcer les points de terminaison des équipements d'impression

Les imprimantes connectées au réseau de l'entreprise doivent être gérées comme tout autre point de terminaison. Il est conseillé de désactiver les services superflus de l'imprimante (par exemple : FTP, Telnet). La plupart des entreprises n'ont pas besoin d'accéder à leurs imprimantes en mode FTP. Ce type de service peut souvent causer plus de mal que de bien. Avec certaines imprimantes, un cyber-malfrat pourrait émettre des requêtes FTP et voler des fichiers dans la file d'attente de l'imprimante tout en restant anonyme. En outre, certains services FTP disponibles sur les imprimantes les plus récentes peuvent subir des attaques FTP bounce. Avec un outil tel que Nmap (Network Mapper), un cyber-malfrat peut masquer la source qu'elle utilise pour examiner les ports et demander à un serveur FTP (lui- même parfaitement conforme) d'autoriser les connexions FTP par proxy. Bien que ces examens FTP bounce soient des techniques anciennes, les serveurs d'impression de dernière génération en sont fréquemment victimes.

L'activité la plus importante pour la sécurisation des points de terminaison de type imprimante est la gestion des mots de passe.
L'erreur la plus flagrante des entreprises est de ne pas changer les mots de passe par défaut. Selon le rapport Verizon *2016 Data Breach Investigations Report*, 63% des attaques portant atteinte aux données, impliquaient des mots de passe faibles, par défaut ou volés. Si les imprimantes sont gérées par les responsables des installations ou par des fournisseurs tiers, la commodité est alors primordiale (pour eux). Lorsqu'un équipement doit aller en maintenance, trouver le mot de passe peut être un problème. Dans une entreprise de 10.000 employés, tout en considérant qu'il y a en moyenne une imprimante pour 10 employés, le service Maintenance est alors confronté à plus de 1000 mots de passe ! Autrement dit, la sécurité cède le pas sur la commodité. La mauvaise gestion des mots de passe n'est pas seulement le fait du personnel non technique. En effet, la deuxième erreur la plus flagrante provient des utilisateurs. Ces derniers incluent leur nom d'utilisateur et leur mot de passe dans du texte non crypté, qui pourra facilement être consulté par toute personne disposant d'une simple connexion http://.

Maintenance et patching

La plupart des attaques portant atteinte aux données se produisent en raison d'un « manque d'hygiène ». Selon le rapport Verizon's *2016 Data Breach Investigations Report*, les 10 vulnérabilités les plus exploitées en 2015 avaient permis 85 % du trafic de piratage réussi. Les vulnérabilités les plus exploitées sont connues et décrites publiquement. Les cyber-malfrats privilégieront les solutions qui fonctionnent le plus, dans le but de maximiser l'investissement qu'ils ont réalisé en outils de logiciels malveillants.

La maintenance et le patching réguliers des points de terminaison de type imprimante renforcent la sécurité. Ils poussent les cyber-malfrats à se tourner vers les entreprises qui n'ont pas assuré la maintenance de leurs systèmes.

En matière de patching, toutes les imprimantes ne sont pas logées à la même enseigne. Certains fabricants proposent des outils qui permettent de superviser, administrer et patcher certaines marques ou certains modèles d'imprimante. Ces outils dédiés sont extrêmement utiles car le scanner de vulnérabilité de l'entreprise peut rencontrer des problèmes d'interprétation (faux positifs). Ces derniers impliquent certaines imprimantes en raison du serveur Web intégré dans celles-ci. En l'absence d'outils de ce type, il sera nécessaire de patcher manuellement chaque imprimante (développer une solution automatisée en interne est généralement difficile).

En outre, pour empêcher l'importation du « bruit » dans les outils de gestion de sécurité SIEM, les entreprises configurent souvent leurs scanners de vulnérabilité de manière à ignorer les équipements d'impression. Il peut être compliqué de configurer de tels outils pour accepter seulement certains messages en provenance des équipements d'impression. A court terme, cette configuration aidera à protéger le réseau contre les infections transmises par ces équipements.

Sécuriser les connexions

Renforcez les protocoles d'administration utilisés avec chaque imprimante. La plupart des imprimantes récentes disposent d'une solution d'administration via http et/ou https et quelques-unes supportent Telnet ou Secure Shell (SSH). Choisissez un protocole d'administration qui assure le cryptage des données (par exemple https ou SSH) et désactivez les cryptages faibles ou inefficaces tels que SSL v3.

Assurez-vous également que vos imprimantes n'autorisent pas un accès trop facile au reste de votre réseau interne. La segmentation des réseaux d'entreprise est une bonne pratique de sécurité réseau et les imprimantes doivent être incluses dans cette opération. Il est possible d'utiliser des certificats pour segmenter de manière logique les accès aux ressources réseau et pour le cryptage du trafic. Notez toutefois que ces mesures de sécurité supplémentaires peuvent nuire à certaines fonctionnalités de l'imprimante. Par exemple la restriction des accès aux services d'annuaire tels que Active Directory ou les services d'administration et de supervision en cloud. L'équilibre entre la sécurisation des imprimantes et la préservation de leurs fonctionnalités est toujours une question de bon sens et d'évaluation des risques.

Conclusion

Les équipements d'impression n'ont pas bénéficié de la même attention que les autres vecteurs de menace à la cyber-sécurité. Les vulnérabilités et les menaces correspondantes sont très réelles. Les entreprises de toutes tailles doivent prendre des mesures nécessaires et y remédier rapidement. Notez par ailleurs que les cyber-malfrats sont des imitateurs voraces : dès qu'un vecteur de menace a été exploité par un acteur malveillant, d'autres suivront rapidement.

Négliger la sécurité des équipements d'impressions aura sans aucun doute des conséquences financières et des conséquences sur la réputation de l'entreprise, encore plus avec l'arrivée du GDPR. Il serait malheureux de voir une entreprise conforme et ayant effectué de gros efforts sur les processus et les technologies de gouvernance de l'information, être trahie par « l'angle mort » que représente un équipement d'impression mal sécurisé.
