EBOOK

KONICA MINOLTA

La gestion de la sécurité des environnements de travail

Gérer et piloter
son activité

* La passion de l'innovation

Giving Shape to Ideas*

Introduction
Sécuriser l'environnement de travail face aux nouveaux risques

A l'ère de la transformation digitale, la sécurité est la préoccupation numéro un de tout dirigeant de PME. Car qui dit adoption de nouvelles technologies, dit exposition à de nouveaux risques, qui sont aussi variés et sophistiqués que les nouvelles pratiques digitales qu'ils adoptent. Travailler depuis un **environnement de travail simplifié et collaboratif** est l'une d'entre elles. Cet environnement, qui **centralise des services applicatifs et des communications unifiées - et géré par une plateforme unique de services informatiques** - doit pouvoir garantir aux collaborateurs de générer, recevoir et échanger des données en toute sécurité. C'est-à-dire que **tous les points d'entrées sur le réseau de l'entreprise doivent être protégés des cyber attaques**.

80 %

des entreprises
ont subi
AU MOINS UNE TENTATIVE
de fraude en 2016 (1)

80 %

des cibles visées en priorité
par les pirates
SONT DES PME (2)

Pourtant, de nombreuses PME ne se préoccupent de la sécurité de leurs données qu'à l'occasion d'une confrontation douloureuse ou coûteuse avec une attaque malveillante. Il en va alors de leur performance et de leur image de marque. Aussi doivent-elles se familiariser dès aujourd'hui avec ces menaces et avec la meilleure manière de sécuriser leur environnement de travail.

Quelle est la nature de ces cyber attaques ? Où se trouvent les potentielles failles de sécurité liées aux outils de travail et de communication ? Et comment s'en prémunir ? Voici les questions que tout dirigeant de PME doit se poser avant de faire l'acquisition d'une solution d'environnement de travail collaboratif, et auxquelles cet ebook répond.

1 - Etude Euler Hermes / DFCG 2017
2 - Enquête 2016 : Les entreprises françaises face aux cyber-attaques, Deanjean Associés et Gan Assurances

1/ Les menaces, leurs objectifs, et les dommages causés

Quelles sont les principales menaces ?

Le type d'attaques les plus subies par les PME sont :

- Les demandes de rançon (80%)
- Les attaques par déni de service (40%)
- Les attaques virales (36%)
- Les fraudes externes (29%). (*)

Les techniques utilisées sont multiples : logiciels malveillant, logiciel espion, virus, vers, malware, cheval de troie, porte dérobée, botnets, ou encore rançongiciels. Ces derniers se propagent extrêmement rapidement via les réseaux d'entreprise, ou via internet.

Pour quoi faire ?

Principalement pour soutirer de l'argent et pour entraver ou interrompre les activités des entreprises. L'Agence Nationale pour la Sécurité des Systèmes d'Information (ANSSI) les a répertoriées en 4 catégories :

- La cyber criminalité, pour extorquer de l'argent
- La déstabilisation, pour porter atteinte et à décrédibiliser l'image d'une entreprise
- L'espionnage, pour gagner en compétitivité au dépend de tiers, en leur dérobant des informations confidentielles
- Le sabotage, pour nuire au bon déroulement des activités des entreprises

Quels sont les dommages ?

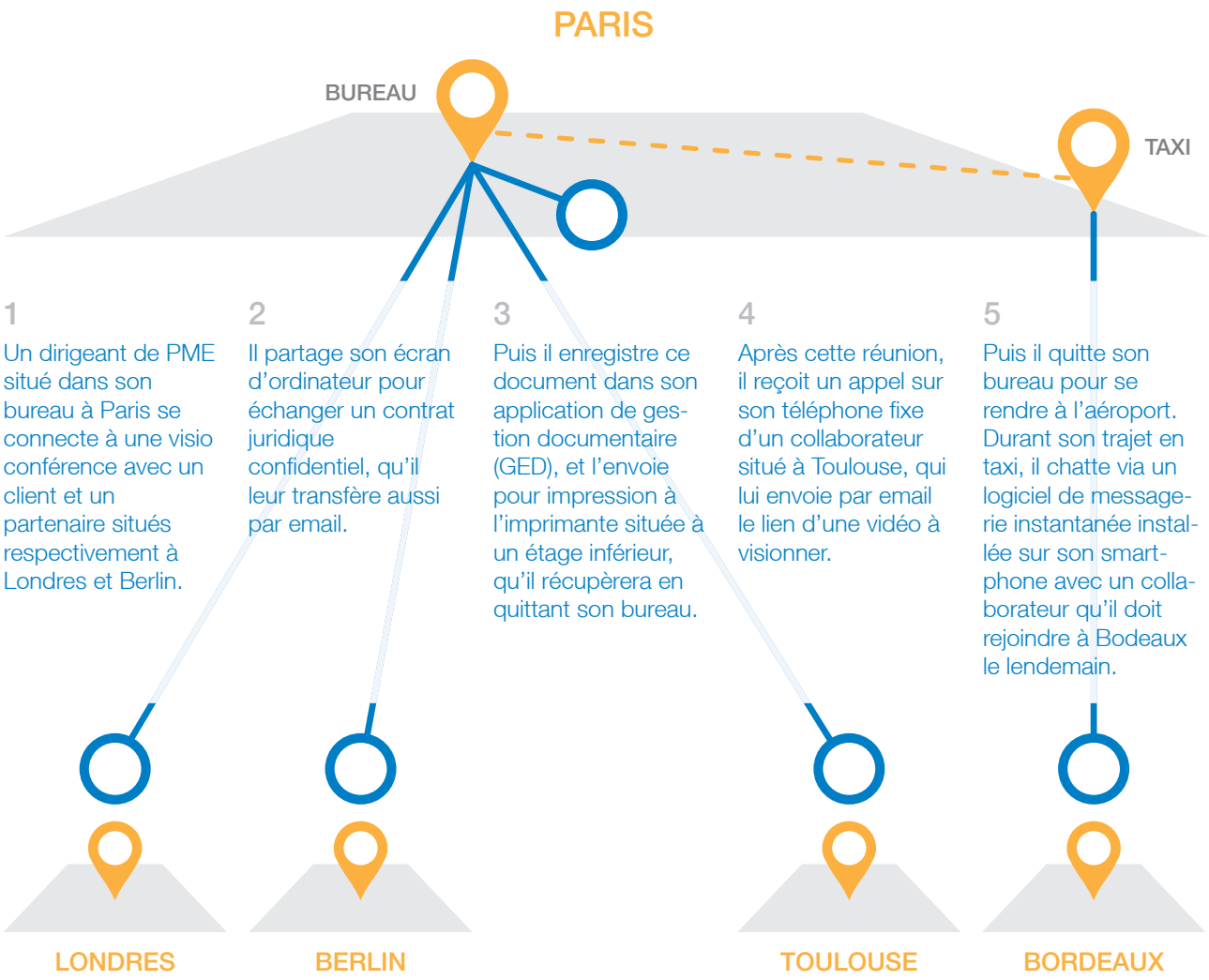
- Des pertes financières liées:
  - aux actions d'urgence pour contenir la diffusion des attaques
  - aux actions pour protéger en priorité les clients, puis les systèmes de l'entreprise
  - aux relations publiques pour assurer l'image de marque
  - aux frais d'avocat et de justice
  - aux frais de récupération des données sauvegardées et reprise d'activité
- Des pertes de productivité, liées à l'interruption de tout ou partie des activités touchées par les attaques, les pertes de données, les collaborateurs mis au chômage technique, ceux mobilisés pour maitriser la crise, ou encore les commandes clients perdues.
- La non-conformité règlementaire : notamment au texte de loi européen RGPD (Règlement Général sur la Protection des Données), qui vise à renforcer et unifier le contrôle des données à caractère personnel et concerne toute entreprise collectant les données personnelles de citoyens européens, c'est-à-dire toutes les entreprises.

2/ Où se trouvent les vulnérabilités de l'environnement de travail ?

L'environnement de travail est composé d'applications métier et de communications unifiées. Elles permettent aux collaborateurs d'émettre, de réceptionner et d'échanger des données avec des tiers internes ou externes. Et ce avec tout type de terminal (smartphone, tablette, ordinateur portable ou fixe), en temps réel, depuis n'importe où et à tout moment. Chaque appareil, imprimante, serveur, connexion web fixe ou mobile constitue alors un point d'entrée sur le réseau de l'entreprise qui doit être sécurisé.

Un exemple d'usage :

Grâce à son environnement de travail, ce dirigeant peut échanger en temps réel et en mobilité des données texte, voix et vidéo. Ces informations transitent depuis le serveur de l'entreprise, via son réseau interne et via internet. Chacun de ces points d'entrée : serveur, réseaux, application, et équipement, constituent des vulnérabilités via lesquelles une intrusion malveillante est possible à tout moment.



3/ Comment sécuriser les environnements de travail ?

En adoptant une solution innovante, tout en un, et sécurisée de bout en bout. C'est dans cette optique que l'expert en services informatique **Konica Minolta a développé le Workplace hub©**. Cet environnement de travail centralise, via un guichet unique, les services applicatifs de travail, de communications unifiées, et les services informatiques qui les sous-tendent. Toutes les données qui y transitent et les systèmes sont **protégés d'attaques malveillantes**, grâce à **la solution de gestion unifiée des menaces de l'éditeur Sophos**. Elle permet de :

Fiabiliser

- Les réseaux, grâce:
  - Aux pare-feux
  - Aux protocoles de communications adaptés
- Les données stockées sur les serveurs et circulant sur les réseaux, grâce :
  - Aux systèmes d'authentification des accès - aux applications de travail et de communication, et aux imprimantes - via des mots de passe, de badges, ou la reconnaissance par empreinte digitale
  - Aux techniques de chiffrement des données
- Les systèmes matériels (ordinateurs, tablettes, smartphones, imprimantes) et logiciels (applications de travail et de communications), grâce aux :
  - Mises à jour logicielles régulières
  - Antivirus

Administrer

Administrer les processus de sécurisation grâce à un tableau de bord qui centralise tous les paramètres de sécurité et en donne un aperçu complet. Cette vision exhaustive permet de détecter, de protéger et de prévoir les menaces, pour tous les points d'entrées du réseau. Il s'agit en effet d'identifier les sources d'intrusion, et de limiter ou d'interdire les accès aux actifs informatiques impactés le temps d'isoler et de résoudre le problème.

Analyser

Analyser le comportement et le développement des menaces afin de pouvoir mieux les appréhender et les identifier.

Conclusion

Une maison dont la porte d'entrée est blindée n'est pas protégée si une fenêtre y est ouverte. Il en va de même pour tout environnement de travail composé d'applications métiers, de communications unifiées, et d'équipements. Chacun de ces composants doit bénéficier d'une protection maximale, afin de prémunir les PME contre les cyber attaques qui les menacent chaque jour. Les technologies de l'Internet des Objets et de l'Intelligence Artificielle étant les prochaines étapes du développement des environnements de travail, il est plus que temps pour les PME de se doter d'une solution de sécurité fiable, simple, et capable d'intégrer ces nouvelles technologies.

KONICA MINOLTA

Konica Minolta
Business Solutions France

365–367 route de Saint–Germain
78424 Carrières–sur–Seine Cedex
www.konicaminolta.fr

S.A.S au capital de 29 365 200 Euros
RCS Versailles B302 695 614

Retrouvez toutes nos solutions sur **www.digital-solutions.konicaminolta.fr**