SecuriteOff

# La sécurité informatique au service des PME

## par SecuriteOff en partenariat avec Doctor Web

Livre Blanc

juin 2016

# Avant-propos

# SOMMAIRE



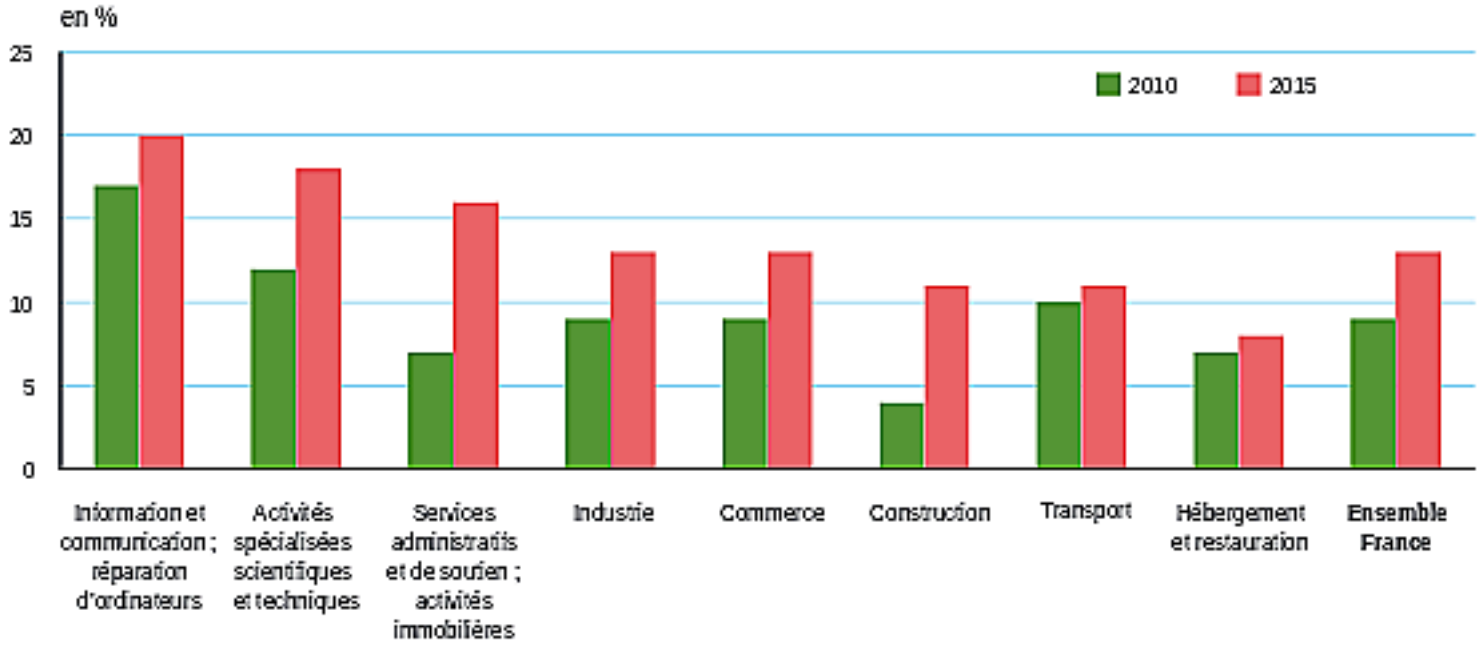
# ANNEXES

# I-INTRODUCTION

## Toutes les entreprises sont concernées

La diffusion sur Internet de codes malveillants, de spams et de campagnes de phishing n'est pas récente. Mais en étant de plus en plus connectées, toutes les PME sont devenues des cibles potentielles.

*« Il ne se passe pas une semaine sans qu'un client ne nous appelle pour nous faire part d'une telle cyberattaque. Les organisations qui les lancent sont désormais passées à un stade industriel, aucune entreprise n'est à l'abri, même pas les plus petites qui pensent souvent ne pas pouvoir être ciblées »*, déclare le responsable d'une filiale d'un cabinet d'expertise-comptable spécialisée dans l'installation et la maintenance de postes de travail et de logiciels.




Champ : sociétés de 10 personnes ou plus, implantées en France, des secteurs principalement marchands hors secteurs agricole, financier et d'assurance.
*Source : Insee, enquêtes TIC 2010 et 2015.*

**13**

C'est le pourcentage, en France, de sociétés de 10 personnes ou plus qui ont subi au moins un incident de sécurité au cours de l'année 2014, portant atteinte à l'intégrité, à la disponibilité ou à la confidentialité des systèmes et données numériques.

**Aucune entreprise n'est à l'abri, quels que soient son secteur d'activité et sa taille.**

Voici quelques exemples d'attaques informatiques ou de piratages récents en France :

- **« Arnaque au président » : 41 personnes licenciées**

En janvier 2016, la justice a prononcé la liquidation de la société BRM (Niort). Spécialisée dans les aménagements de médiathèques et de bibliothèques, elle a été ruinée par une arnaque au « faux président ». Entre le 21 juillet et le 14 août 2015, un escroc avait réussi à usurper le compte email du PDG. Il a mis en place une arnaque et récupéré 1,6 million d'euros.Quelques mois auparavant, l'entreprise avait déjoué une première supercherie à 250.000 €...

- **Un logiciel de racket numérique : des milliers d'euros de rançon**

En avril 2016, une entreprise béarnaise, victime d'un rançongiciel (voir notre chapitre sur « Les principaux risques « techniques »), s'est résolue à payer une « somme à quatre chiffres » aux pirates. Ses 23 salariés ont été au « chômage technique » pendant près d'une semaine. « Plus personne ne pouvait travailler. Tous les fichiers étaient cryptés. Nous n'avions plus accès à aucune donnée », explique la chef d'entreprise.

- **Un virus bloque une cimenterie**

Un automate a été touché par un virus. Son dysfonctionnement a entraîné une série d'alertes en cascade. Bilan : une production arrêtée pendant plusieurs jours pour tout remettre en ordre, nettoyer la cimenterie et éradiquer ce code malveillant.

# 2834 €

C'est le coût moyen par employé d'une cyberattaque classique touchant une PME selon la société Cybelangel.

### ➲ L'avis d'un expert

*« L'expérience montre que, sauf dans le cas d'attaques ciblées, c'est plus la faiblesse de la victime que la force réelle de l'attaquant qui est déterminante »*,

**rappelle Éric Filiol, Directeur du Laboratoire de virologie et de cryptologie opérationnelles (ESIEA Ouest).**

# II-LES MENACES

## A-Les principaux risques « techniques »

Depuis la création, en 1983, d'un des premiers virus, il en existe des dizaines de millions.

Jusqu'à présent, les systèmes d'exploitation sous Windows étaient les principales cibles des développeurs de ces codes malveillants. La situation commence à évoluer avec des attaques virales visant les ordinateurs fonctionnant sous MacOS d'Apple, mais aussi des serveurs sous GNU/Linux ainsi que les environnements Android et iOS.

Il faut d'abord rappeler qu'il existe différentes catégories de codes malveillants. Les trois principales sont les suivantes :

### 1-Les virus

Malgré la diversité des codes malicieux, les virus restent la technique la plus employée pour infecter un poste de travail ou un réseau. Ils sont classifiés selon leurs fonctionnalités. Les deux principaux sont :

Les virus de démarrage (ou virus de boot) : ils visent ou utilisent les organes destinés à amorcer le système d'exploitation comme le BIOS (Basic Input/Output system) et le secteur de démarrage maître (MBR – Master boot record). Principal intérêt de ce programme malicieux : en intervenant avant le lancement du système d'exploitation (comme Windows) et donc de tout logiciel (dont l'antivirus), il est impossible (ou très difficile) d'interrompre son démarrage.

Les macros virus : ils ciblent plus précisément les suites Office de Microsoft, mais aussi les suites bureautiques comme OpenOffice et LibreOffice. Leur principe de fonctionnement est le suivant : lors de l'ouverture d'un document infecté (par défaut, les macros ne sont pas désactivées), le code viral se copie dans certains modèles et notamment le « normal.dot » pour Word.

**LES FAITS**

Das 70% des cas, les réseaux locaux sans connexion Internet sont infectés **via des supports amovibles** (clés USB ou autres).

*Source : Doctor Web, Ltd.*

## 2-Les vers

Un ver (ou worm) est capable de se dupliquer et de se diffuser tout seul par le biais des services de messagerie instantanée ou de courrier électronique. Aujourd'hui, les vers sont très évolués et peuvent passer à travers les mailles des logiciels de sécurité.

## 3-Le Cheval de Troie

Les pirates peuvent aussi employer des techniques de camouflage « classiques », mais toujours efficaces. C'est le cas du Cheval de Troie ou trojan. Ce programme est composé de deux parties : un module serveur (les soldats grecs cachés dans le célèbre animal) et un module client (l'armée grecque entrant dans la ville une fois les portes ouvertes). Rapporté à l'informatique, l'objectif est d'infiltrer un réseau ou un ordinateur sans être repéré par des logiciels de sécurité.

### L'avis d'un expert

*« 99 % des attaques ne sont pas du tout ciblées, car viser une attaque coûte cher aux criminels (c'est le temps et les moyens financiers qui sont en jeu). Attaquer à l'aveugle est beaucoup plus intéressant ».*

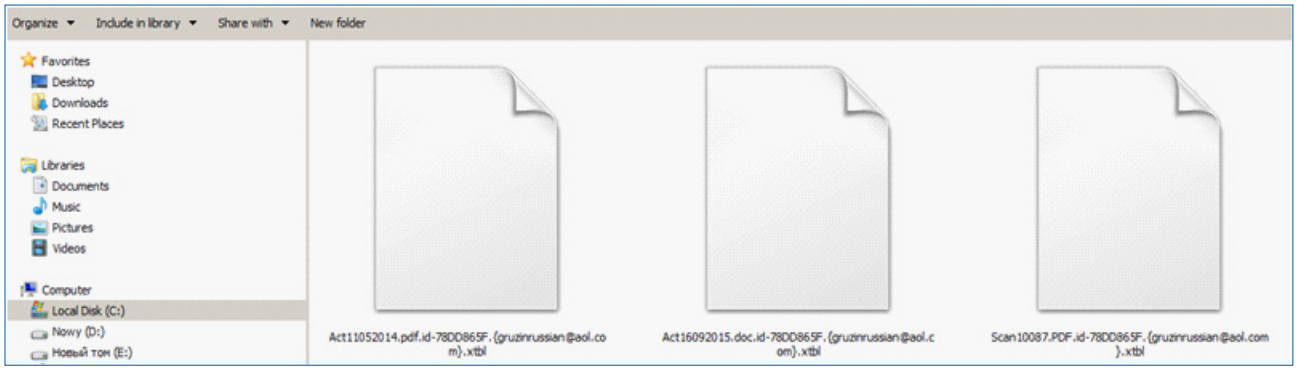
**Boris Sharov, PDG de Doctor Web.**

## FOCUS

### Les rançongiciels ou logiciels de racket

Parmi tous ces codes malicieux, les rançongiciels (ou « ransomware ») sont ceux qui touchent le plus les entreprises en ce moment. Un rançongiciel est un programme malveillant transmis en pièce jointe (aux formats ZIP, RAR, SRC, CAB mais aussi des documents bureautiques) par email ou « caché » dans un PDF par exemple sur un site. Une fois ouvert, il vise à chiffrer (on dit souvent par erreur « crypter ») partiellement ou entièrement les données sur le système cible, en l'occurrence un ordinateur (ou un serveur) dans le cas d'une PME.

L'objectif est de récupérer une rançon en échange de la « libération » des fichiers chiffrés.




*Exemple de fichiers chiffrés sur un PC. (source : Doctor Web, Ltd).*

## Le point de vue d'un responsable informatique

*« Début 2015, nous avons été touchés par un rançongiciel après qu'une collaboratrice ait cliqué un après-midi sur une pièce jointe d'un email en anglais. Le code malveillant a commencé par chiffrer des documents sur son poste de travail puis il est remonté jusqu'à notre serveur. Ce n'est que le lendemain matin, lorsque différentes personnes m'ont contacté, car elles se plaignaient de ne pouvoir accéder à des fichiers. J'ai ensuite découvert un message m'invitant à payer une rançon.*

*À l'époque, nous travaillions avec une société de conseil qui nous avait recommandé de payer. Comme je ne voulais pas entrer dans ce jeu-là, j'ai préféré débrancher tous les ordinateurs, désinfecter avec DrWeb puis restaurer à partir d'une sauvegarde datant de la veille de l'infection. Nous avons perdu une journée et demie de travail.*

*Suite à cet incident, j'en ai profité pour sensibiliser de nouveau tous les collaborateurs qui ont participé à la remise en route des services. Ma crainte principale concerne les emails. Comme nous sommes une mairie, nous en recevons énormément. »*

**Olivier Fleisch, responsable informatique à la mairie de Marsannay-la-Côte.**

Ces rançongiciels se répandent de plus en plus sur le web. Mais des entreprises en sont victimes depuis des années. En 2014, un cabinet d'avocats parisiens a été touché par ce type d'attaque. Le bilan a été catastrophique : trois mois de rupture d'activité et des clients perdus.


*Source : Doctor Web, Ltd.*

**Consultez les « Fiches de SecuriteOff » pour savoir comment réagir en cas d'infection par un rançongiciel.**

# B-Les principaux risques juridiques

## Quand l'entreprise est victime et... responsable

Depuis 1978, la France dispose d'un cadre juridique et législatif dédié à la protection des données personnelles avec les Lois de 1978 et de 2004 et la Directive européenne de 1995. La transposition du dernier « paquet télécom » est intervenue par une ordonnance du 24 août 2011 (n° 2011-1012).

## 1-Le vol de données à caractère personnel ou professionnel

De plus en plus souvent, les pirates récupèrent des informations sensibles : des numéros de carte bancaire, des adresses email, des numéros de téléphone, mais également des factures, des fichiers client...

Le nerf de la guerre économique est l'information. Les chefs d'entreprise l'ont compris ; les escrocs aussi ! Mais le vol de données peut être aussi l'œuvre d'un salarié toujours en poste ou qui ne travaille plus dans la société mais dont les codes d'accès n'ont pas été supprimés dès son départ... Les fuites peuvent être aussi « favorisées » par les négligences en matière de sécurité informatique d'un prestataire auquel vous avez confié le stockage de vos informations sensibles.

Que vous conserviez des données à caractère personnel ou qu'elles soient hébergées en ligne, votre responsabilité et/ou celle de votre prestataire est engagée. L'article 34 bis de la loi « Informatique et Libertés » institue un régime de divulgation obligatoire des atteintes à la sécurité des données personnelles. Ainsi, en *« cas de violation de données à caractère personnel, le fournisseur de services de communications électroniques accessibles au public avertit, sans délai, la Commission nationale de l'informatique et des libertés »*. Le champ d'application de ce texte est limité aux fournisseurs de *« services de communications électroniques accessibles au public »*.

Mais à terme, ces obligations devraient concerner toutes les organisations.Cette réglementation contraint le responsable du traitement à mettre en œuvre « toutes mesures adéquates ». Maître Alain Bensoussan signale toutefois qu'il n'y a *« pas une obligation de résultat, mais une obligation de moyens renforcés ; les entreprises doivent démontrer qu'elles ont pris toutes les mesures utiles et qu'au regard de la pertinence de ces moyens toutes les entreprises placées dans les mêmes conditions auraient subi les mêmes conséquences »*.

### ➲ L'avis d'un expert

*« Il faut rappeler qu'au regard de la Loi "Informatique et Libertés", une entreprise reste la responsable de ses données à caractère personnel même lorsqu'elle les confie à un sous-traitant ».*

**Maître Olivier Iteanu, Avocat spécialisé en droit des nouvelles technologies**

## 2-Les arnaques financières

De plus en plus d'entreprises sont également victimes d'escroqueries financières dont la plus connue est appelée « l'arnaque au président ». Des escrocs se font passer pour le PDG afin que le service comptable effectue « dans l'urgence » un virement sur un compte bancaire à l'étranger.

« Le taux d'élucidation est proche de zéro, car les délinquants se cachent derrière des proxys et utilisent des adresses IP dans des pays lointains. L'enquêteur ou le juge doit passer par des commissions rogatoires internationales. Et parfois, les enquêteurs se heurtent à un mur, car certains pays ne coopèrent pas », constate maître Olivier Iteanu.

## 3-Les données dans le Cloud

Tout contrat d'infogérance ou d'externalisation informatique devrait idéalement, dans l'intérêt du client, faire mention des clauses de réversibilité, c'est-à-dire la capacité pour le client de récupérer en fin de contrat l'ensemble de ses données confiées au prestataire. Or ce dernier peut refuser en évoquant des raisons contractuelles. Autre risque, il vous transfère vos données dans un format d'export qui ne vous convient pas ou qui ne soit pas exploitable.

Pour éviter d'en arriver là, maître Olivier Iteanu rappelle que deux outils juridiques doivent être mis en jeu par leur client. « Il y a premièrement une clause spécifique sur la réversibilité : quand peut-elle être engagée, sous quelle forme, sous quel délai, quel est le coût, quel format... ? La deuxième est la clause d'audit qui permet au client de contrôler la bonne exécution du contrat chez le prestataire et de constater que la réversibilité pourra se faire sans difficulté. Mais elle implique d'avoir accès au prestataire... »

En cas de différend, l'entreprise peut saisir les tribunaux comme l'a fait en novembre 2012 l'UMP. Le parti politique avait décidé de changer de prestataire pour la gestion et l'hébergement de ses données personnelles et donc de récupérer ses données auprès d'Oracle.

« Ce dernieravait fait valoir à l'UMP qu'une fonction d'exportation de son logiciel Oracle CRM On Demand ne fonctionnait pas. En référé, le Président du Tribunal de Nanterre avait dit que ce n'était pas le problème de l'UMP. La juridiction a fait injonction à Oracle, sous astreinte de 5000 € par jour de retard, de se débrouiller pour que la réversibilité soit faite. Cette affaire confirme que la réversibilité est un enjeu qui est compris par les juges », explique Maître Olivier Iteanu.

# III-LES MAILLONS FAIBLES

## A-Les points faibles des postes de travail et du parc informatique

### 1-Les systèmes d'exploitation

Comme c'est le cas notamment avec les rançongiciels, dans la plupart des situations, les environnements Windows sont la cible de ces attaques. Mais d'autres systèmes d'exploitation (MacOS et GNU/Linux) peuvent être victimes d'un mode opératoire similaire.

Si votre parc informatique est principalement sous Windows, il convient d'être très vigilant afin de limiter les risques d'infection.

Mais ne prenez pas des risques inconsidérés : si vous avez des ordinateurs ou des automates fonctionnant sous Windows XP, vous ne devez plus les utiliser. Depuis le 8 avril 2014, Microsoft ne publie plus de correctifs de sécurité visant à corriger des failles repérées (fin du support étendu). Si vous utilisez encore de tels postes de travail, vous risquez d'être infecté.

Il est donc très important de vérifier les dates officielles concernant la durée des supports de Microsoft :

- Windows 7 : fin du support standard (plus de mises à jour fonctionnelles, mais encore des correctifs de sécurité) le 13 janvier 2015.
- Windows 7 : fin du support étendu (publication de correctifs de sécurité) le 14 janvier 2020.
- Windows 8.1 : fin du support standard le 9 janvier 2018.
- Windows 8.1 : fin du support étendu le 10 janvier 2023.
- Windows 10 : fin du support standard le 13 octobre 2020.
- Windows 10 : fin du support étendu le 14 octobre 2025.

### 2-Vos logiciels

Les pirates profitent des failles dans les logiciels et les systèmes d'exploitation pour infiltrer les ordinateurs et les serveurs. Les éditeurs de ces programmes publient des correctifs de sécurité permettant de « colmater » ces brèches.

Dès que vous êtes informés de la diffusion d'un correctif, appliquez-le en ayant au préalable lancé une sauvegarde (à programmer de façon récurrente)... Pour plus de commodité, nous vous conseillons de régler tous vos logiciels et systèmes d'exploitation de façon à ce qu'ils installent automatiquement les mises à jour.

Parfois, des patchs sont publiés à la hâte par certains éditeurs sans avoir été précisément validés et vérifiés. Résultat, ils peuvent provoquer un dysfonctionnement d'un poste de travail. Il est donc très important de réaliser très souvent des sauvegardes de vos fichiers et de créer des « points de restauration » de vos systèmes d'exploitation afin de pouvoir revenir à une date antérieure si la correction d'une vulnérabilité entraine un bug.

## ➲ L'avis d'un expert

*« La meilleure sécurité, c'est celle qui devient un automatisme au quotidien ».*

**Guillaume Desnoes, responsable des marchés européens chez Dashlane, l'un des principaux gestionnaires de mots de passe.**

### 3-Votre antivirus

Contrairement à ce que prétendent certains éditeurs de logiciels de sécurité, aucun antivirus ne peut garantir une protection contre tous les codes malicieux à un instant « t ». Ils sont l'un des éléments de la sécurité informatique. Mais ce ne sont pas des super héros !

Pour simplifier, les antivirus s'appuient sur une base de signatures virales (en quelque sorte l'ADN d'un virus) et des techniques heuristiques pour détecter des codes malicieux et des comportements suspects. Dès qu'un code malveillant est repéré, ils le mettent en quarantaine ou le suppriment, selon la configuration décidée par le responsable informatique de l'entreprise.

**Mais ne prenez pas n'importe quel logiciel !**

En France, en 2009, un concours de hacking - organisé par Éric Filiol avec des experts en sécurité - a permis de constater que les antivirus ne sont pas très bien protégés. Sur les 7 produits testés, 6 ont cédé dans des délais compris entre 2 et 40 minutes.

McAfee a été mis hors d'usage en 1 minute et 56 secondes ! Norton de Symantec n'a tenu que 4 minutes et G Data a cédé au bout de 5 minutes et 14 secondes. AVG a résisté un quart d'heure. NOD32 a craqué à la 33e minute, Kaspersky n'a pas été au-delà de 40 minutes.Un seul, Dr.Web, a survécu à l'heure impartie.

### 4-Vous !

123456 est toujours le mot de passe le plus utilisé. Sans parler de mots de la vie courante (exemple : chat, maison, bureau...) et des incontournables dates de naissance et prénoms !

C'est ce qu'on appelle des mots de passe « faibles ». En clair, ils n'apportent aucune sécurité. Il n'est pas nécessaire de disposer d'un supercalculateur pour les deviner. *« Avec un puissant PC portable, un programme spécialisé dans les "attaques par dictionnaire" (schématiquement, le logiciel scanne pour trouver des mots existants dans un dictionnaire, Ndlr) je peux tester 500 millions de mots de passe à la seconde. Si l'on utilise un ordinateur de bureau, on peut atteindre quelques milliards ! »*, affirme Éric Filiol.

**Vous devez employer des mots de passe « forts » avec au moins une dizaine de caractères.**

**Exemple : Khgr785*!Ed]mP(aq.**

Vous ne devez pas utiliser le même mot de passe pour plusieurs comptes.

Enfin, il est conseillé de les modifier tous les trimestres ou semestres.

## ➲ Le point de vue d'un responsable informatique

*«À Monaco, nous sommes constamment attaqués par email et par téléphone. Nos serveurs sont visés directement. Nous avons beaucoup de tentatives de racket (rançongiciels) et de phishing. Nos collaborateurs, lorsqu'ils sont au téléphone, ne font pas toujours très attention aux pièces jointes qu'ils reçoivent par email. Résultat, un de nos postes de travail a été touché par ce type de virus. Nous avons essayé différentes méthodes pour déchiffrer les données "prises en otage" par le pirate. Comme aucune n'a été efficace, le salarié a perdu ses données.*

*Régulièrement, je diffuse des notes de service pour leur rappeler qu'ils doivent être très vigilants quant aux pièces jointes et qu'ils doivent me prévenir dès qu'ils ont un doute sur un email. J'ai mis en place différentes solutions (antivirus Dr.Web, antispams, listes blanches...). Des pirates arrivent pourtant à nous envoyer des emails en usurpant l'identité de certains de nos contacts qui sont dans la liste blanche. Pour limiter les risques, j'ai mis en place des sauvegardes quotidiennes sur des serveurs distants.*

*Ancien responsable informatique d'une agence bancaire, j'ai été plus sensibilisé que d'autres confrères. Ce n'est pas le cas dans toutes les entreprises pour lesquelles la sécurité informatique reste trop compliquée et onéreuse. Comme ce n'est pas concret, elles ne voient pas l'intérêt de s'intéresser à la protection de leurs données et de payer pour des solutions. Ce n'est que lorsqu'elles sont victimes d'une attaque informatique qu'elles décident de prendre des mesures. Mais c'est souvent trop tard. »*

**Xavier Sobrero, Directeur informatique du groupe Monaco Luxury Group. Créé en 1959, il représente aujourd'hui une dizaine de marques haut de gamme.**

## ➲ L'avis d'un expert

*« L'analyse antivirale actuelle se réfère en grande partie sur des bases de données de signatures de virus. Cela permet de détecter rapidement des virus existants ou certaines variantes, mais il est facile de déjouer cette détection en changeant quelques octets ou encore en créant un nouveau virus qui utilise de nouvelles techniques d'infection ».*

**Paul Irolla, doctorant au Laboratoire de virologie et de cryptologie opérationnelles de l'école d'ingénieurs du numérique ESIEA à Laval.**

# 70 %

C'est le pourcentage de salariés avouant pouvoir accéder aux anciens codes de leurs précédents emplois...

Source : Dashlane

FOCUS

**Comment protéger tous vos mots de passe ?**

Le post-it collé sur les bords de l'écran d'un ordinateur ou sur votre mur, c'est tentant, car... pratique. Cette facilité d'usage est bien sûr à proscrire. Elle n'apporte aucune confidentialité.

Pour sécuriser tous vos mots de passe, vous pouvez n'en apprendre qu'un seul.

Lorsque vous l'avez bien mémorisé, utilisez Gostcrypt (http://www.gostcrypt.org). Ce logiciel gratuit (pour Windows, MacOS et Linux) a été développé par une équipe de chercheurs européens, dont plusieurs Français.

Il permet de mettre à l'abri un fichier Word par exemple sur lequel vous aurez enregistré vos différents mots de passe.

Gostcrypt peut aussi être utilisé comme un coffre-fort sur votre PC ou sur une clé USB pour y stocker des données sensibles.

# 98 %

C'est le pourcentage de clés USB déposées sur des campus et récupérées par des passants. Presque la moitié (45 %)a été insérée et des fichiers ouverts. Étude menée par des chercheurs des Universités de l'Illinois (dans le Michigan) et de Google. Ils avaient réparti 297 clés USB en modifiant leur apparence avec par exemple une étiquette « Confidentiel ».

# IV-LA PRÉVENTION DES RISQUES

## A-La sécurité informatique : un investissement, pas un coût

Face à cette situation délétère, les entreprises ne doivent pas négliger la sécurité de leur réseau informatique et de leurs données confidentielles.

Pourtant, une étude menée par OpinionWay en France (janvier 2016) indique que la cybersécurité ne se place qu'au 5e rang des enjeux prioritaires pour l'entreprise (23 %) derrière la satisfaction des clients (58 %), les résultats financiers (53 %), l'image de l'entreprise (26 %) et la Recherche et Développement (24 %).

Autre raison de s'attaquer dès maintenant à la protection des documents numériques : l'accélération de la dématérialisation. Dès 2020, la facturation électronique sera généralisée. L'article 3 de l'ordonnance n° 2014-697 du 26 juin 2014 relative au développement de la facturation numérique indique notamment que la dématérialisation des factures sera imposée à compter du 1er janvier 2017 aux grandes entreprises et aux fournisseurs publics, puis progressivement généralisée d'ici le 1er janvier 2020 en tenant compte de la taille des entreprises concernées.

**64 %**

Pourcentage de dirigeants déclarant que leur entreprise a subi une défaillance de sécurité. Les causes sont l'attaque externe (49 %), la défaillance humaine interne involontaire (47 %), la défaillance technique interne (44 %) et la défaillance humaine interne volontaire (29 %). La défaillance conduirait à la perte de confidentialité (44 %) ou à la destruction (33 %) d'informations sensibles. Dans un tiers des cas (33 %), aucune mesure spécifique n'a été adoptée suite à une faille de cyber sécurité de cause interne, et dans 25 % des cas suite à des attaques externes.

Les entreprises ne doivent pas considérer la sécurité comme un coût, mais comme un investissement. Sans une politique de sécurité personnalisée et validée par des experts comme ceux de SecuriteOff, il n'y a pas d'activité économique !

## Bon à savoir

**Toutes les entreprises doivent être capables de répondre à ces questions :**

- Que fera-t-on lorsque nous aurons été piratés ?
- A-t-on réellement une visibilité suffisante sur ce qui se passe sur notre réseau ? Et, sinon, qui est en mesure d'observer l'activité et de réagir rapidement ?
- Quelles données doit-on conserver en interne et comment les sauvegarder ?
- Nos contrats nous couvrent-ils réellement ? Que valent nos prestataires qui ont déployé l'infrastructure informatique ou qui hébergent nos informations ?

Devant autant de questions, souvent angoissantes pour les chefs d'entreprise confrontés à de nombreuses problématiques, la politique de l'autruche est couramment appliquée. « On verra ça plus tard ». Mais il sera trop tard lorsqu'un virus aura paralysé des PC ou volé des fichiers confidentiels. La facture, en termes de perte de chiffre d'affaires (et de données commerciales notamment) et d'inactivité de collaborateurs (leurs postes de travail seront infectés), sera élevée.

**Selon des études, le coût d'une attaque informatique peut atteindre l'équivalent de 4 % du chiffre d'affaires d'une entreprise !**

## B-Une politique de sécurité

La protection numérique est une affaire de maturité. Elle implique notamment d'inculquer de bonnes habitudes « d'hygiène » informatique à tous les collaborateurs et en les répétant régulièrement.

Comme pour une alarme dans une maison, s'il n'y a qu'un capteur d'intrusion à la porte d'entrée et à une fenêtre, tous les autres accès sont autant de possibilités pour un cambrioleur.

**Il faut penser à la sécurité informatique de façon globale.**

# 44 %

Pourcentage d'entreprises dans lesquelles les personnes destinées à accéder aux informations sensibles n'ont pas reçu de formation ou d'habilitation particulières (source : étude OpinionWay auprès de 400 dirigeants de sociétés françaises de 50 salariés ou plus. 2016).

# V-CONCLUSION

Pour de nombreux chefs d'entreprise, la sécurité informatique n'est pas une priorité. Trop compliquée à appréhender, trop onéreuse, trop contraignante ; la mise en place d'une politique de sécurité informatique ne représente pas un enjeu majeur.

Et pourtant !

Sans une analyse très fine des failles du réseau informatique (ce qu'on appelle un audit de sécurité) et sans l'application de « bonnes pratiques », la pérennité de l'entreprise peut être mise en péril. Une infection virale dérobant des informations sensibles ou bloquant l'utilisation de plusieurs ordinateurs (attaque par un rançongiciel) peut avoir de graves conséquences sur l'avenir d'une entreprise.

L'image de marque de la société peut être ternie. Les clients peuvent s'inquiéter quant à la confidentialité de leurs données à caractère personnel. Des grands comptes pour lesquels les PME sont des sous-traitants peuvent exiger un renforcement de la sécurité sous peine de changer d'interlocuteur.

Face à une telle situation, les PDG doivent anticiper. Réagir après une infection par un virus peut coûter très cher. Mais il ne faut pas se contenter d'installer un antivirus sur les ordinateurs pour être protégé. *« La sécurité est vue comme une logique de produits développée par les éditeurs alors qu'il s'agit d'un état d'esprit. La sécurité informatique est un process, pas un produit »*, insiste Éric Filiol.

Réaliser un audit de sécurité, sauvegarder toutes les données critiques et former tous les salariés afin qu'ils soient plus sensibilisés ou capables (pour les responsables informatiques notamment) d'analyser par eux même l'infrastructure sont indispensables.

Ce ne sont pas des coûts supplémentaires et inutiles. C'est en quelque sorte « une assurance » complémentaire. C'est la pérennité de votre entreprise qui est en jeu.

## Remerciements

SecuriteOff tient à remercier Cécile Chastanet (Responsable Communication de Doctor Web France), Boris Sharov (PDG de Doctor Web, Ltd), Éric Filiol (Directeur du Laboratoire de virologie et de cryptologie opérationnelles – ESIEA Ouest) et Maître Olivier Iteanu.

# À PROPOS DE SECURITEOFF

**Spécialisée dans la sécurité informatique avec des ingénieurs ayant 20 ans d'expérience, notre société, SecuriteOff, vous aide à renforcer la protection de votre entreprise.**

- ☑ Nous vous proposons différents diagnostics et conseils.
- ☑ Nous vous apportons des solutions adaptées à vos besoins.

# NOS 4 SERVICES POUR LA SÉCURITÉ DE VOTRE ENTREPRISE :

1-Diagnostic d'une journée (ou d'une demi-journée selon le périmètre à analyser) sur le niveau de sécurité informatique d'une entreprise. Analyse faite par un expert ayant 20 ans d'expérience dans la sécurité informatique et la protection des entreprises.

### POURQUOI CETTE MISSION EST-ELLE FAITE POUR VOTRE ENTREPRISE ?

L'identification des principales failles de votre réseau informatique réduit les risques de piratage.

2-Test d'intrusion d'un réseau informatique ou d'un site web par un Laboratoire de sécurité informatique opérationnelle.

### POURQUOI CETTE MISSION EST-ELLE FAITE POUR VOTRE ENTREPRISE ?

En nous mettant à la place des attaquants, nous vérifions que votre réseau informatique ou votre site web ne peut pas être infiltré pour vous voler ou chiffrer vos données.

3-Audit de sécurité conforme à la norme ISO 27001et réalisé par un Laboratoire de sécurité informatique opérationnelle.

### POURQUOI CETTE MISSION EST-ELLE FAITE POUR VOTRE ENTREPRISE ?

L'établissement d'une cartographie détaillée de votre réseau nous permet de repérer les points sensibles qu'il faut absolument protéger. Nous déployons des solutions adaptées à vos besoins. Avec deux objectifs précis : mettre vos informations confidentielles dans un « bunker » et vous permettre de reprendre au plus vite votre activité économique en cas d'attaque informatique, de dégâts des eaux, d'incendie ou de vols de matériels.

4-Formations (tous les niveaux) sur la sécurité informatique, les réseaux sociaux et l'espionnage économique

### POURQUOI CETTE MISSION EST-ELLE FAITE POUR VOTRE ENTREPRISE ?

La sensibilisation de tous vos salariés et l'amélioration des compétences de votre responsable informatique sont indispensables pour appliquer les bonnes pratiques.

## NOS 5 ATOUTS :

- **Des services assurés par des Ingénieurs R&D en cybersécurité ayant 20 ans d'expérience.**
- **Une équipe pluridisciplinaire capable de répondre aux besoins spécifiques de toutes les PME.**
- **Des conseils et des solutions adaptés aux problématiques des PME.**
- **Une équipe à la pointe de la recherche (Laboratoire R&D) en attaques informatiques et en virus.**
- **Une équipe indépendante de tout éditeur de logiciels et de tout prestataire.**

## VOTRE CONTACT :

Philippe Richard – Directeur
13 rue Pierre de Ronsard
37 540 Saint-Cyr-sur-Loire
content@securiteoff.com

☑ Plus d'informations sur www.securiteoff.com

# À PROPOS DE DOCTOR WEB

Doctor Web, Ltd. développe les produits antivirus Dr.Web depuis 1992. Présent en Europe et en Asie, l'éditeur est reconnu pour la qualité technique de ses produits. Doctor Web un des rares fournisseurs de solutions antivirus possédant ses propres technologies de détection et de traitement des programmes malveillants.

Le Laboratoire de recherche en virologie de Doctor Web, fort d'une centaine de collaborateurs, concentre ses efforts sur l'étude et l'analyse des menaces les plus actuelles afin d'anticiper au maximum celles de demain. Doctor Web a développé une expertise particulière sur la sécurité des systèmes mobiles, ainsi que sur les systèmes Mac OS et Linux.

Ses chercheurs ont également développé des outils de lutte contre les ransomwares de type « Cryptolocker ». Doctor Web est présent en France depuis 2007 où il équipe de nombreuses PME et administrations, ainsi que les particuliers.

- ☑ En savoir plus : www.drweb.fr
- ☑ Conseils, explications sur la sécurité avec le projet « Lumières sur la sécurité ».

SecuriteOff

# 6 RÈGLES DE BASE À NE JAMAIS OUBLIER

**Utilisez des mots de passe "forts".** Exemple : kLpù* 875Fr !)jdFR

**N'utilisez le même mot de passe pour tous vos comptes.**

**Mettez à jour en permanence tous vos logiciels et systèmes d'exploitation.**

**N'installez jamais des logiciels piratés** (ils peuvent contenir des virus ou des logiciels espions)

**Effectuez des sauvegardes régulières et délocalisées** (ne pas laisser le disque dur de sauvegarde dans vos locaux ; une sage précaution en cas d'incendie par exemple)

**Protégez vos données et vos emails confidentiels** en utilisant des logiciels de chiffrement comme Gostcrypt (coffre-fort numérique)

SecuriteOff

# 7 RÈGLES À NE JAMAIS OUBLIER PAR UN RESPONSABLE INFORMATIQUE

**Appliquez le principe du moindre privilège :** attribuez aux différents comptes les seuls privilèges qui leur sont strictement nécessaires dans l'exécution de leurs tâches.

**Vérifiez les autorisations d'accès aux ressources partagées.**

**Mettez à jour en permanence tous vos logiciels et systèmes d'exploitation.**

**N'activez pas les macros pour les documents Office.** Même si l'ouverture d'un document vous incite à réactiver celles-ci, ne le faites pas, surtout lorsque l'origine est douteuse.

**Mettez en place une politique de sauvegarde adaptée :** conservez deux ou trois sauvegardes antérieures. La plus récente peut contenir une version chiffrée des données ou un virus.

**Sensibilisez régulièrement tous les collaborateurs** face aux risques associés aux messageries électroniques.

**Testez périodiquement le processus de restauration :** dans le cas où la prestation de sauvegarde/restauration est externalisée, il convient de s'assurer que les points de contact sont clairement identifiés. Des tests réguliers doivent être menés afin de valider l'intégrité des données restaurées.

*Sources : ANSSI, CERT-FR.*

SecuriteOff

# Comment réagir en cas d'infection par un rançongiciel

**Déconnectez immédiatement votre poste de l'Internet** (arrêt du Wi-Fi, câble Ethernet débranché).

**Ne payez pas la rançon :** le paiement ne garantit en rien le « déchiffrement » de vos données et peut compromettre le moyen de paiement utilisé (notamment carte bancaire).

**Faites appel à des experts comme ceux de SecuriteOff** ou contactez DrWeb pour tenter de déchiffrer la clé qui bloque vos fichiers ou éradiquer le code malveillant (Live CD). Attention, ces méthodes ne marchent pas toujours, en particulier si les pirates utilisent une clef unique. Il n'existe aucune technique de décryptement efficace à 100 %.

**En cas d'échec des méthodes précédentes :** faites un formatage du disque dur ou achetez-en un. Toutes les données qui n'auront pas été sauvegardées auparavant auront donc été perdues...

*Source : ANSSI.*

SecuriteOff

# Les rançongiciels (suite). Comment prévenir les risques.

**Effectuez des sauvegardes fréquentes, voire quotidiennes,**des documents les plus sensibles. Ainsi, en cas de chiffrement du disque dur, une restauration des données sera possible.

**N'ouvrez pas les emails dont vous n'êtes pas certain de l'expéditeur :** vérifiez l'adresse d'envoi. Méfiez-vous des courriels imitant les adresses de correspondants que vous connaissez : les attaquants peuvent avoir identifié leurs noms (organigramme d'une entreprise par exemple) pour vous induire en erreur. En cas de doute, ne touchez pas aux pièces jointes.

**Évitez l'ouverture de pièces jointes** de type SCR ou CAB (extensions de compression actuellement utilisées dans la campagne CTB-LOCKER)

**Utilisez un antivirus comme DrWeb et mettez-le à jour :** de même, effectuez toutes les mises à jour logicielles et systèmes.