L'ANTIVIRUS NE FAIT PAS PARTIE DES MEUBLES

LIVRE BLANC

F-Secure®

SOMMAIRE

PARTIE 1

CHALLENGER LA SOLUTION ACTUELLE

1 Les méthodes de détection *(p4)*
2 Les nouveaux usages *(p2)*
3 Le format *(p7)*
4 Le support *(p8)*
5 Le prix *(p9)*
6 Performances *(p10)*
7 Diversité *(p11)*

PARTIE 2

DEBLOQUER LE CHANGEMENT

1 Faire sauter les freins *(p13)*
2 Evoluer au même rythme que les menaces *(p14)*
3 Avoir conscience du danger *(p15)*

Conclusion - sources et références *(p16)*

A priori, un antivirus, c'est un peu comme les pneus d'une voiture. On n'en change pas si facilement à moins d'avoir une bonne raison de le faire. La seule différence c'est qu'il existe plus de bonnes raisons de changer d'antivirus qu'il n'y paraît. Et la première étant bien évidemment de vous garantir la meilleure protection pour vos données sur le long terme. Mais ça, vous le saviez déjà probablement. Dans ce livre blanc, vous découvrirez pourquoi vous devriez être bien protégé et ne pas considérer votre antivirus et son éditeur comme faisant partie du patrimoine de votre entreprise.
Alors ? Etes-vous réellement sûr d'être bien protégé ?

CHALLENGER LA SOLUTION ACTUELLE

L'achat de votre actuel antivirus a probablement dû donner lieu à un benchmark acharné pour savoir quelle solution était la plus adaptée à vos exigences. Mais êtes-vous sûr qu'aujourd'hui elle le soit toujours autant ? Votre solution vous apporte-t-elle le niveau de satisfaction que vous êtes en droit de réclamer ? Vous en êtes-vous préoccupé depuis que vous l'avez achetée ?

Voici les critères essentiels qu'une solution efficace doit couvrir.

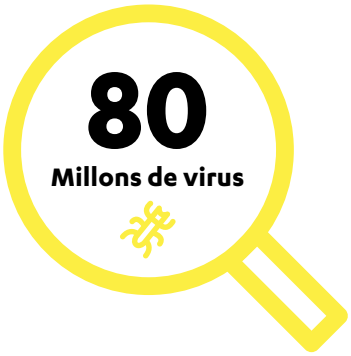
PARTIE 1

PARTIE 1

1 LES METHODES DE DETECTION

Les antivirus aussi bénéficient des avancées technologiques. Aujourd'hui, il ne suffit plus d'installer le premier antivirus venu, basé sur des signatures ou des registres, sur un poste de travail et décréter qu'il est sécurisé, pour qu'il le soit vraiment.

D'après l'institut indépendant AV-Test, il existe aujourd'hui 80 millions de virus. Enfin, plus pour très longtemps puisque l'on dénombre 2 292 nouveaux malwares par heure. Ce qui fait 38 par minute et plus d'un toutes les deux secondes. C'est-à-dire qu'au moment où vous lisez ces lignes, plusieurs nouvelles menaces sont apparues.



L'ANTIVIRUS SUR BASE DE SIGNATURE EST (PRESQUE) MORT

C'est pourquoi les antivirus basés sur les signatures ne suffisent plus : par définition, ils ont un train de retard sur les cybercriminels puisque chaque menace doit être analysée pour pouvoir être intégrée dans une base de signature et repoussée en cas d'attaque. Et assigner une signature à un virus peut parfois prendre plusieurs semaines voire des mois si un virus se révèle être suffisamment rare. Entre temps, le malware a eu le temps de causer des dégâts. C'est donc une défense rétroactive, une fois que le mal est fait.

Et ce modèle de protection montre aussi ses limites quand il s'agit de prévenir les vulnérabilités « Zéro Day ». C'est-à-dire les vulnérabilités de solutions logicielles que l'éditeur ne connaît pas et qui ne peuvent donc pas être corrigées... ni protégées par conséquent. C'est généralement le cybercriminel qui trouve cette faille le premier et qui l'exploite à sa guise le temps que tout le monde comprenne ce qui se passe et que l'antivirus sur base de registre ou de signature reste à la traîne.

ANALYSER LE COMPORTEMENT ET LA REPUTATION POUR ANTICIPER LES ATTAQUES

Une réponse face à ces enjeux de réactivité et de prévention des risques sont les antivirus à analyse heuristique. C'est-à-dire un antivirus capable d'identifier et de reconnaître le comportement d'un programme pour déterminer si ce dernier est malveillant ou non. Il garantit donc une protection proactive contre les virus et toutes leurs variantes puisqu'il prend en compte la signature des virus mais aussi leur mode opératoire. Plus besoin d'attendre que le virus ait une signature pour le repousser.

Les antivirus à analyse heuristique se sont montrés (et se montrent toujours) particulièrement pratiques contre Cryptolocker et ses clones ransomware par exemple. Chaque jour, des milliers de variantes de ce virus voient le jour. Les antivirus traditionnels sont incapables de les détecter parce que les signatures ne sont pas les mêmes d'un ransomware à l'autre. Alors que leur fonctionnement est totalement similaire.

D'une manière générale, les cybercriminels auront toujours un temps d'avance, que ce soit sur le développement de

nouveaux virus dont le mode opératoire est différent, ou d'exploitations de failles. Tout l'enjeu de la sécurité informatique réside donc dans la capacité des cibles des cybercriminels (c'est-à-dire vous) à réduire au maximum ce temps d'avance. Ce que permettent aujourd'hui l'heuristique et l'analyse de réputation réalisées par les antivirus de dernière génération.

Votre antivirus actuel est-il de cet acabit ?
Etes-vous sûr de vouloir rester exposé plusieurs semaines avant que votre antivirus ne reconnaisse une menace ?

« **38 malwares par minute**

⊕ de 1 toutes les 2 minutes »

PARTIE 1

2 LES NOUVEAUX USAGES

Introduire de nouveaux équipements dans le système d'information d'une entreprise est généralement synonyme de nouvelles brèches. C'est notamment le cas des smartphones ou des tablettes tactiles. La politique de sécurité doit donc accompagner ces nouveaux usages (en tous cas c'est ce que nous préconisons), et ne pas oublier qu'il faut re-paramétrer l'antivirus en conséquence... si celui-ci peut l'être.

LES ENTREPRISES SONT MOBILES

Aujourd'hui, 80% des PME disposent de terminaux mobiles[1]. La détection des virus sur les postes de travail n'est que la partie émergée de l'iceberg et ne représente qu'une petite partie des enjeux de la sécurité informatique de manière générale. En soi, l'antivirus n'est qu'un outil de sécurité parmi toutes les solutions existantes pour protéger le système d'information dans sa globalité. De même, les postes de travail ne sont qu'un équipement parmi tant d'autres (téléphones, tablettes, serveurs, ordinateurs fixes et mobiles), qui eux-mêmes peuvent être très hétérogènes (Windows, iOS, Android, Windows Phone, iPhone, Linux Serveur, etc.).

Les nouveaux usages doivent donc être accompagnés par la politique de sécurité de l'entreprise pour ne pas créer de nouvelles brèches dans un système d'information préalablement protégé. Votre antivirus doit donc être en mesure de prendre en charge les nouveaux usages quand ceux-ci se développent.

80%
des
PME

disposent de terminaux mobiles

ET DEMAIN ?

Aujourd'hui il est surtout question de mobilité et de sécurisation des terminaux mobiles (smartphone, tablettes, ordinateurs portables). Mais demain, les usages et les enjeux seront probablement différents et viendront enrichir la palette des équipements et environnements à prendre en compte pour une sécurisation globale et totale du système d'information. C'est l'alerte qu'avait tenté de lancer le chercheur en sécurité informatique Chris Roberts. Il prétendait avoir pu détourner un avion en reliant son ordinateur par câble Ethernet sur un boîtier situé sous son siège. Bien que son histoire ait été remise en question par des spécialistes de l'aéronautique, son intervention a eu le mérite de questionner sur les dangers de l'informatisation de notre quotidien.

Et si la prochaine menace venait des objets connectés ? Ces objets pratiques mais très gourmands en informations qui ont envahi le quotidien de chacun et donc, celui des entreprises. Les montres, les Smart TV, les thermostats et même les outils de production d'une entreprise constituent des cibles idéales. Vous saviez qu'il était possible de prendre en main à distance, et très facilement, les commandes d'un crématorium ou d'une station d'épuration ? Que se passerait-t-il si la même chose arrivait à vos outils de production ?

Le choix d'une solution de protection doit donc être lié à la capacité de l'éditeur à répondre aux enjeux actuels des entreprises, mais aussi à la confiance qui lui est accordée pour anticiper les enjeux futurs et les usages de demain.

Etes-vous en mesure d'accompagner ces nouveaux usages ?

PARTIE 1

3 LE FORMAT

Le format SaaS (Software as a Service) ou « On Premise » pour un antivirus est un choix qui va au-delà du simple dilemme : héberger la solution chez soi ou dans le cloud ? Le format SaaS intègre de nouvelles possibilités pouvant impacter positivement le confort utilisateur et la productivité des travailleurs nomades.

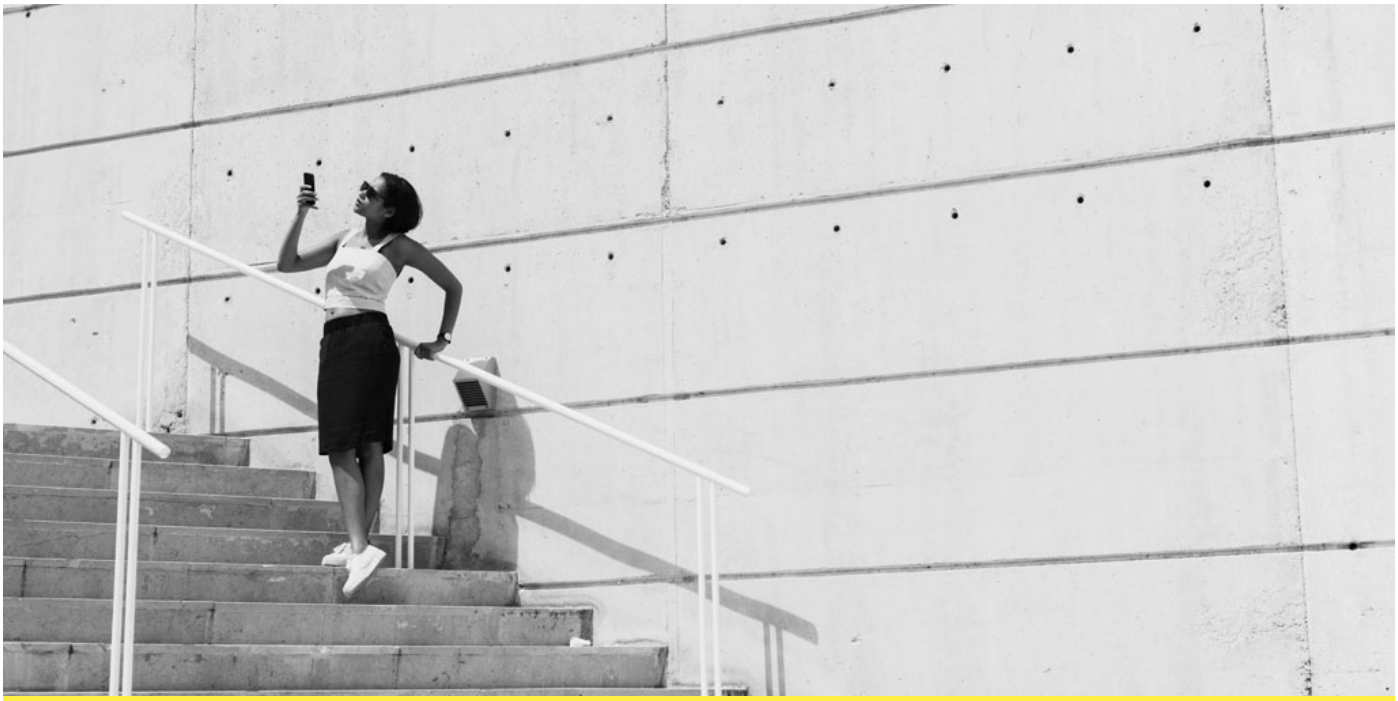
Le modèle SaaS facilite le déploiement et l'installation de la solution sur les postes utilisateurs. Surtout quand une entreprise possède plusieurs sites distants. Au lieu d'avoir une console par site ou d'adapter son réseau pour avoir une console centralisée, le format SaaS permet de piloter le déploiement et l'administration de l'antivirus, sans avoir à apporter de modifications aux installations existantes.

CONFORT ET PRODUCTIVITE

C'est un format qui permet aussi de faire oublier l'antivirus à l'utilisateur la plupart du temps. Le mode SaaS garantit des mises à jour régulières et automatiques de l'antivirus, parfaitement transparentes pour l'utilisateur.

Concernant les travailleurs les plus mobiles, ce format présente aussi des avantages. Sur un modèle « On Premise », les utilisateurs doivent impérativement se connecter sur le réseau de leur entreprise pour bénéficier des mises à jour de la solution et d'une protection maximale.

Pas forcément pratique pour ces utilisateurs et avec un impact certain sur leur productivité si ces derniers deviennent réticents à utiliser leurs appareils parce qu'ils ne sont plus parfaitement protégés. C'est aussi problématique pour la politique de sécurité en tant que telle. A contrario, le modèle SaaS permet d'accompagner ces utilisateurs nomades et d'effectuer les mises à jour de l'antivirus, peu importe la localisation de l'utilisateur (pour peu qu'il ait une connexion Internet).



Le format de votre solution actuelle vous convent-il ?
Et si non, votre éditeur vous laisse-t-il vraiment le choix ?

PARTIE 1

4 LE SUPPORT

Etre protégé c'est bien, mais être protégé avec un support adapté c'est mieux.

CHOISIR LE BON SUPPORT...

Un bon support est un support qui, avant tout, est adapté à votre niveau d'exigence. Il n'existe donc pas de réponse empirique pour déterminer si un support est bon ou pas. Juste quelques bonnes questions à vous poser ainsi qu'à votre éditeur :

Le support de votre logiciel antivirus est-il dans votre langue ?

Est-il disponible sur vos heures de travail ?

Etes-vous obligé d'attendre plusieurs jours/semaines/mois avant d'y accéder ?

Devez-vous payer le prix fort pour y avoir accès ?

Si vous portez votre attention sur ces problématiques, vous devez vous assurer que votre support répond à vos enjeux.

...C'EST AUSSI CHOISIR LE BON REVENDEUR

Globalement, les revendeurs ont accès à des niveaux de support plus élevés que les utilisateurs finaux. Les contacts fournis par les éditeurs à leurs clients sont généralement ceux du support de niveau 1. Alors qu'un revendeur peut directement accéder au niveau 2 ou au niveau 3 en fonction de son niveau de partenariat avec la marque.

Les éditeurs d'antivirus qui ont une stratégie commerciale centrée sur les partenaires revendeurs offrent en général de meilleures prestations de support. Pour bénéficier du meilleur support il faut donc également veiller au sérieux et à la réputation du revendeur, ainsi qu'à la capacité des éditeurs d'antivirus de s'entourer des bons partenaires.

Votre actuel support vous offre-t-il les garanties que vous êtes en droit de demander ?

5 LE PRIX

Quand vous l'avez choisie, votre solution antivirale devait probablement être la plus compétitive. Ou en tous cas, c'était sûrement celle qui vous apportait le plus de satisfaction en termes de qualité/prix (du moins on l'espère). Mais est-ce toujours le cas ?

LE PARADOXE FRANÇAIS

En moyenne en France, le budget consacré à la sécurité informatique est de 50 euros par an et par employé dans plus d'une PME sur deux[1]. Parallèlement, les attaques informatiques coûtent en moyenne 4,8 millions d'euros aux entreprises françaises[2]. Certes, le prix est un facteur très important pour les entreprises surtout quand le contexte économique est morose. Mais en matière de sécurité informatique, un choix effectué uniquement basé sur des raisons budgétaires peut s'avérer être un mauvais calcul en cas d'attaque.

Budget sécurité pour les PME

4,8

La comparaison prix/fonctionnalités devrait donc se faire, dans l'idéal, au profit des fonctionnalités qui vous paraissent être les plus essentielles, le prix étant un élément à regarder dans un second temps : « De quoi ai-je réellement besoin ? Et combien suis-je prêt à mettre pour l'obtenir ? » au lieu de « Quel est mon budget ? Sur quels aspects de sécurité suis-je prêt à faire des concessions ? ». Si nous reprenons l'exemple de Cryptolocker, dans quel sens préféreriez-vous payer :

- Pour récupérer vos données sans garantie de succès ?
- Ou pour ne jamais être atteint par aucun ransomware ?

DES OFFRES ENRICHIES

C'est la raison pour laquelle aujourd'hui, certains éditeurs intègrent par défaut des fonctionnalités supplémentaires à leurs offres. C'est le cas par exemple du **Patch Management**. Il s'agit d'un module qui se charge d'apporter les correctifs nécessaires aux logiciels présentant des vulnérabilités reconnues, en toute transparence pour l'utilisateur. Ce simple module permet, à lui seul, de prévenir 80% des menaces auxquelles les entreprises sont quotidiennement exposées. Et ce n'est qu'un exemple parmi d'autres.

PATCH MANAGEMENT

Prévient **80%** des menaces

Votre éditeur vous demande-t-il encore de payer le prix fort pour disposer d'un niveau de protection basique ?

PARTIE 1

6 PERFORMANCES

En 2013, les utilisateurs de PC ont perdu en moyenne 120 heures de travail à cause d'applications, de fichiers ou d'ordinateurs lents. C'est-à-dire 5 jours complets. Un antivirus mal adapté peut impacter fortement votre productivité... alors qu'il devrait simplement vous protéger.

En cas de ralentissements sur le réseau, l'antivirus représente toujours le coupable idéal. C'est vrai dans la majeure partie des cas mais ces ralentissements ne sont pas une fatalité et peuvent être supprimés avec une protection adaptée.

LES SIGNATURES ET LE PARAMETRAGE

Au moment d'enregistrer un document par exemple, un antivirus cherche à déterminer si celui-ci est dangereux. Les antivirus sur base de signatures vont donc comparer ce fichier avec **toutes les signatures présentes dans la base**. Le temps qu'il compare le documents aux millions de signatures répertoriées, cela peut prendre du temps. Alors quand il s'agit de plusieurs dizaines voire centaines de documents en même temps, cela peut créer quelques complications. Un cas de figure qui ne se présente pas pour les antivirus heuristiques basés sur l'analyse des comportements.

De même, le paramétrage de l'antivirus peut être la cause des ralentissements. Vous pouvez avoir la solution la plus performante et la plus rapide du monde, si celle-ci est mal paramétrée elle représentera un poids mort pour votre informatique. Par exemple, les mises à jour de l'antivirus peuvent créer un goulet d'étranglement sur le réseau si chaque client installé sur chaque poste de travail est indépendant et que l'antivirus est programmé pour faire ses mises à jour le même jour à la même heure.

Antivirus et productivité ne font pas bon ménage chez vous ?
Ces ralentissements vous mènent la vie dure ?

PARTIE 1

7 DIVERSITE

La volonté de ne « pas mettre tous ses œufs dans le même panier » en matière de sécurité informatique était assez répandue il y a quelques années, conduisant la plupart des grandes entreprises à adopter une solution de protection pour les serveurs, une autre pour les postes de travail, une différente encore pour la messagerie, etc...

Pour les entreprises moins dimensionnées, la diversité est apparue avec les nouveaux usages : comme certains éditeurs n'évoluaient pas assez vite, les nouvelles failles du système d'information étaient comblées avec une solution de protection dédiée. Si, sur le papier, ces solutions sont compatibles entre elles, elles peuvent néanmoins avoir des effets pervers pour les entreprises.

DES CONSEQUENCES SUR LA PRODUCTIVITE

La diversité des solutions de protection est avant tout très chronophage puisqu'elles nécessitent d'être administrées indépendamment les unes des autres. Ce qui implique de bien connaître chaque solution et donc une perte de temps pour les équipes dédiées à l'administration des outils informatiques.

L'autre aspect concerne surtout le support. En cas de problème, les éditeurs auront tendance à se renvoyer la balle, accusant l'autre d'être à l'origine des problèmes rencontrés. Le temps de démêler le vrai du faux, un problème, aussi simple soit-il, peut avoir des conséquences financières catastrophiques pour une entreprise. Alors que de tout regrouper chez un seul éditeur permet d'éviter ces situations.

Tous ces environnements différents vous pèsent au quotidien ?
Vous n'avez peut-être pas encore trouvé le bon panier pour y mettre tous vos œufs ?

DEBLOQUER LE CHANGEMENT

Changer d'antivirus peut paraître compliqué voire dangereux pour la plupart des entreprises. Pourtant cette démarche n'est pas si complexe et est parfois même nécessaire.

PARTIE 2

PARTIE 2

1 FAIRE SAUTER LES FREINS

Etes-vous réellement satisfait de la solution que vous avez actuellement ? Une question simple que vous devez probablement entendre souvent. Mais en prenant le temps d'y réfléchir, gardez-vous votre actuelle solution parce qu'elle vous convient ou parce vous vous y êtes habitué ? Certaines entreprises s'accrochent à leur solution même si elles n'en sont pas satisfaites, parce qu'elles ne savent pas qu'elles peuvent avoir mieux ni où le trouver, se sentent prisonnières de leur éditeur ou sont rebutées parce qu'elles pensent qu'un changement de solution est trop compliqué. Alors si la réponse à la question posée plus haut est « non » ou « moyennement » c'est qu'il est probablement temps de changer.

TROUVER MIEUX

Il est vrai qu'il peut parfois être difficile de distinguer le bon du mauvais parmi toutes les offres qui existent aujourd'hui. Et à en croire tous les éditeurs d'antivirus du marché, tout le monde semble être LE leader incontesté dans le domaine. C'est pourquoi il existe des comparateurs indépendants comme AV-Test ou AV-Comparatives qui vous permettent de comparer différents éditeurs de solutions antivirales selon des critères spécifiques.

ENGAGE MAIS PAS MARIE

L'engagement avec un éditeur d'antivirus n'est pas une limite infranchissable. Et le modèle d'engagement a tellement été malmené et décrié ces dernières années que la plupart des éditeurs d'antivirus proposent des engagements sur un an. Mais il n'est pas rare de rencontrer des entreprises qui trainent un engagement de cinq ans comme un boulet enchaîné à leur pied. Il faut bien avoir conscience qu'un engagement peut être rompu avec un éditeur. Certes, il faut accepter de ne pas utiliser un service pour lequel on a déjà payé. Cependant, il est toujours possible de trouver un arrangement avec le nouvel éditeur que vous ciblez pour limiter (voire supprimer) cet impact financier.

MIGRER N'EST PAS COMPLIQUE...

...Par contre nous avons conscience que ce n'est pas non plus une partie de plaisir. Techniquement, une migration ne demande pas beaucoup de travail en tant que tel. Pour les entreprises, il suffit de bien identifier les différents terminaux et éléments du système d'information à protéger. Pour le reste, vous pouvez bénéficier du soutien de votre nouvel éditeur pour vous accompagner dans la migration et notamment :

La désinstallation de l'ancienne solution

Le déploiement de la nouvelle solution

L'installation de la console d'administration

Le paramétrage de la nouvelle solution

Est-ce que vous voulez vraiment garder un antivirus qui ne vous convient plus ? Le jeu en vaut-il la chandelle ?

PARTIE 1

2 EVOLUER AU MEME RYTHME QUE LES MENACES

Vos salariés ne se posent pas la question de savoir si oui ou non leur entreprise possède la solution antivirale qui garantira la sécurité maximum de l'organisation quels que soient leurs comportements. A part peut-être les plus zélés.

VOS SALARIES VOUS FONT CONFIANCE

85% des employés français estiment que leur entreprise est bien protégée contre les hackeurs. Ce score diffère toutefois suivant la taille de l'entreprise : il grimpe à 90% dans les grandes entreprises mais n'atteint que 75% dans les PME[3].

Autant d'employés qui considèrent pouvoir avoir des comportements à risque au travail. Ou qui n'ont peut-être pas non plus conscience d'avoir des comportements à risque. Ou qui ont intentionnellement des comportements à risque. La plus grande menace aujourd'hui vient de l'intérieur, comme l'a encore montré récemment l'attaque contre TV5MONDE.

ANTICIPER LES RISQUES

D'après PwC, la principale source des failles de sécurité provient des actuels employés. Ils représentent 32.73% des incidents en Europe (toutes tailles et tous secteurs d'activité confondus). Suivis de très près par les anciens employés (29.58%) et les hackeurs n'arrivent qu'en troisième position (24.78%).

Une partie de l'enjeu pour une solution antivirus aujourd'hui, c'est donc d'être en mesure de prévenir ces risques et permettre aux entreprises d'avoir un meilleur contrôle sur leurs politiques de sécurité. C'est-à-dire donner les clés pour réduire le rôle du facteur humain, auparavant jugé incontrôlable, dans les incidents de sécurité. Notamment par un meilleur contrôle de l'utilisation du web.

Principales sources des failles de sécurité

32.73%
les actuels employés

29.58%
les anciens employés

24.78%
les hackeurs

Autant éviter qu'un malheur n'arrive avant de changer de solution, non ? Pouvez-vous garantir ces contrôles aujourd'hui ?

PARTIE 1

3 AVOIR CONSCIENCE DU DANGER

Si une entreprise se sent vulnérable ou exposée au danger c'est qu'elle l'est probablement... Et certainement que la confiance qu'elle accorde à sa solution de protection commence à décliner.

NE SOYEZ PAS UNE CIBLE FACILE

La première étape vers une sécurisation adaptée et performante, c'est la prise de conscience du danger que représentent les menaces informatiques. Entre la perte de crédibilité auprès des clients ou partenaires, les pertes d'argent liées au vol ou la destruction de données et la perte de temps pour réparer les dégâts, les conséquences sont souvent désastreuses. Et pourtant...

... Pourtant un chiffre nous fait penser que nous n'avons probablement pas assez insisté auprès des PME sur la nécessité de ne pas s'exposer au danger et de ne pas être une cible facile : 26% d'entre elles ne disposeraient pas d'un anti-virus[1]. C'est environ 26% de trop, surtout compte tenu des différentes sources de menaces.

26%
ANTIVIRUS

AVOIR CONSCIENCE C'EST BIEN, AGIR C'EST MIEUX

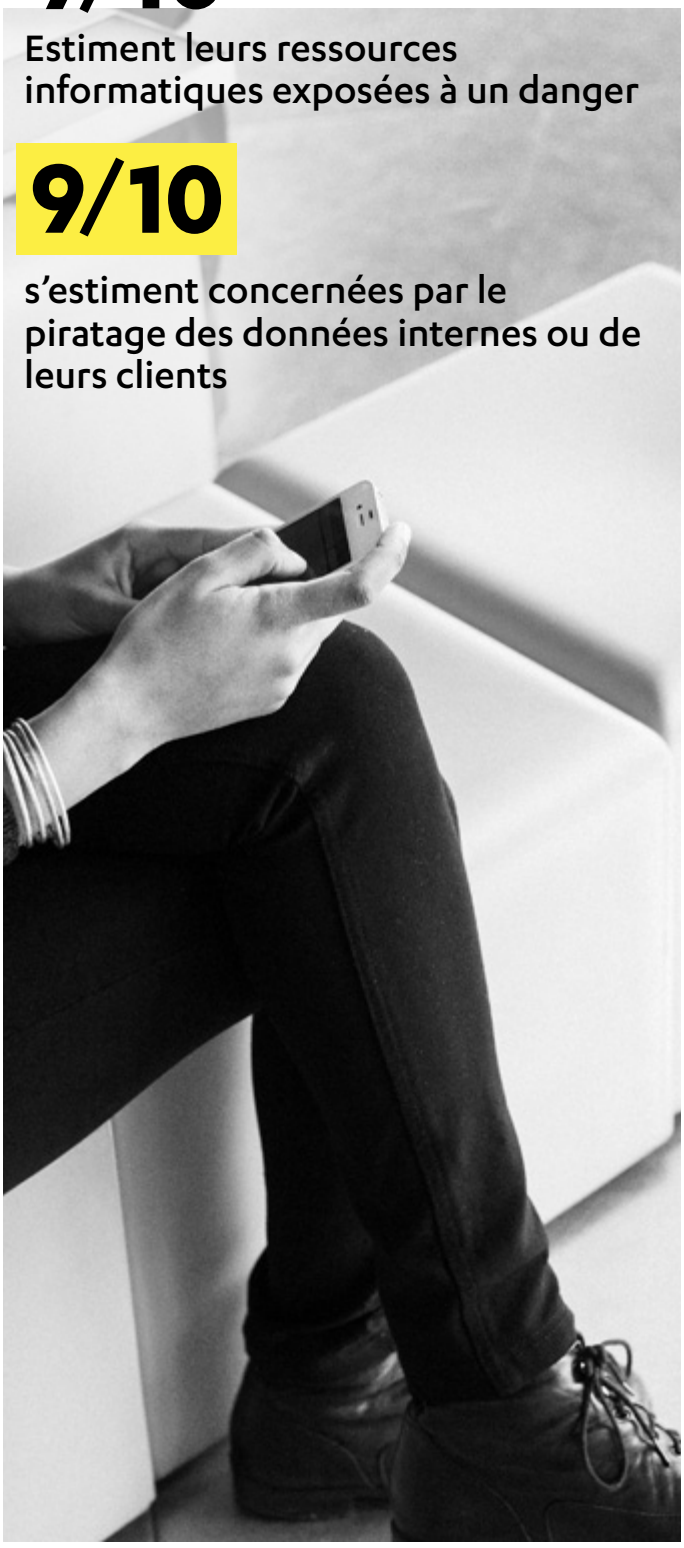
Aujourd'hui, 9 entreprises sur 10 s'estiment exposées à une usurpation des mots de passe et à une utilisation frauduleuse ou malveillante de leurs ressources informatiques[1]. Parallèlement, 7 entreprises sur 10 s'estiment concernées par le piratage des données internes à la société ou de leurs clients par exemple[1].

Si la majeure partie des entreprises sont conscientes d'être exposées aux menaces, pourquoi ne pas prendre les devants ? Comme on dit souvent, la meilleure défense, c'est l'attaque. Entamer une démarche proactive de lutte contre les menaces informatiques représente souvent le meilleur moyen de se protéger et de diminuer le sentiment d'insécurité. Et peut-être que celle-ci doit passer par un changement de solution.

Vous sentez-vous exposé en dépit de votre solution de protection ?

7/10
Estiment leurs ressources informatiques exposées à un danger

9/10
s'estiment concernées par le piratage des données internes ou de leurs clients



REJOIGNEZ LE MOUVEMENT SWITCH ON FREEDOM

communications-france@f-secure.com

01 77 54 94 00

www.f-secure.fr/business

fr.business.f-secure.com

SOURCES ET REFERENCES

(1) Enquête Ipsos pour le fournisseur de solutions réseau Navista (janvier 2015)
(2) Etude Ponemon Institute de novembre 2014
(3) Etude Opinionway/Capgemini réalisée en mai 2015