Guide
des bonnes pratiques des entreprises en matière de protection de données

Point de vue
des RSSI

Sommaire

GENESE

Historiquement, les entreprises ont fait des choix de solutions antivirus au gré des besoins et des projets déployés, et, la plupart du temps, les critères de choix étaient à caractère technique :

- performance du produit ;
- facilité de déploiement ;
- souplesse d'évolution ;
- gestion locale et à distance ;
- gestion multi-environnement ;
- terminaux fixes, nomades.

Aujourd'hui, beaucoup d'entreprises appréhendent plus précisément les enjeux liés à la sécurité, et les critères de choix sont devenus plus complexes.
Pour tous, les risques encourus dépassent les critères techniques et d'autres éléments tout aussi importants doivent être pris en compte lors du choix d'une solution, citons pour exemple :

- une solution mal administrée ;
- le temps de travail des équipes informatiques ;
- une crise mal gérée par manque de support ;
- un maillon faible non détecté dans l'environnement global ;
- une solution dépassée liée au choix d'un éditeur en retard de 6 mois en matière de technologie.

C'est à partir de ces questions que nous avons mené cette étude, en rencontrant vingt RSSI d'entreprise de tout secteur d'activité et de toute taille (cf annexe 28).

Les différentes pratiques des RSSI des entreprises françaises en matière de protection des données sont mises en avant et illustrées par de nombreux retours d'expérience, intéressants pour tout responsable qui envisage de mener un tel projet ou qui s'interroge sur les choix qu'il a réalisés.

1. LES ENJEUX LIES A LA PROTECTION DES DONNEES DE L'ENTREPRISE

1.1. Les enjeux de la sécurité

- Evolution de la cybercriminalité

Le marché de la cybercriminalité a beaucoup évolué ces dernières années, les menaces se sont transformées, passant d'attaques massives visant un grand nombre de PC, à des menaces plus ciblées, à profil polymorphe pour être difficilement détectables. En même temps, les cybercriminels se sont professionnalisés, leur objectif n'est plus d'infecter une machine pour le plaisir mais plutôt d'utiliser toute la panoplie d'attaques : ver, virus, bot… avec pour unique objectif : le vol et la revente d'informations, le chantage aux entreprises… Ces cybercriminels adoptent des techniques croisées faisant intervenir le spam, le courrier électronique et les applications. Par exemple, une menace combinée se sert de messages électroniques pour inciter les destinataires à se rendre sur des URL contrefaites ou même sur des URL saines connues, contaminées par du code malveillant afin de capturer les mots de passe de messagerie et d'implanter des logiciels enregistreurs de frappe ou des chevaux de Troie. Les courriers indésirables qui ne cessent de croître sont de plus en plus élaborés et une forme de confiance s'est installée dans l'esprit des utilisateurs qui ne s'attendent plus à recevoir de mails malveillants dans leur boîte mail. En conséquence, tout élément qui parvient à passer entre les mailles du filet est d'autant plus dangereux.

- La course à l'innovation sans fin des éditeurs

Confrontés à cette évolution sans répit des menaces, les éditeurs de solutions de protection des données doivent sans cesse innover pour faire face à l'intelligence complexe des malwares, tout en n'impactant pas les performances des postes de travail, ou des serveurs informatiques.

- Des employés 2.0

Internet est une plateforme d'échange au sein de l'entreprise, approches SaaS (logiciel en tant que service), applications Web, lieux de travail distants et partenariat étendu… la « Toile » est omniprésente et les employés ne peuvent plus s'en passer. La génération d'employés 2.0 a entraîné l'apparition d'un nouveau type de salarié connecté en permanence, où qu'il se trouve. Ceci pose d'autant plus de difficultés aux entreprises qui, jusqu'à présent, verrouillaient leurs applications, leurs recherches internes, leurs états financiers par le biais de serveurs sécurisés ou de segments réseau isolés. Ces informations essentielles commencent à circuler librement, à l'intérieur et à l'extérieur du périmètre de l'entreprise.

- Bien des malveillances viennent de l'interne

Une récente étude souligne l'importance des salariés dans le piratage ou le vol des données de l'entreprise, beaucoup d'entreprise investissent dans les infrastructures serveurs et postes de travail en négligeant l'aspect humain pour former les employés à la sécurité, et les rendre capables de détecter un comportement normal ou anormal.

- les RSSI savent-ils qu'ils ont été visités ?

Les malwares les plus dangereux sont les chevaux de Troie multifonctions qui effectuent des contaminations ciblées, lesquelles passent totalement inaperçues au sein de l'entreprise et installent des portes grandes ouvertes « invisibles » vers l'extérieur.

La question est alors : les RSSI savent-ils qu'ils ont été visités ? de plus, comme il n'y a ni preuves ni traces, aucun recours n'est possible.

1.2. Les enjeux perçus par les RSSI

Sur le terrain, l'approche est beaucoup plus pragmatique, les RSSI rencontrés dans le cadre de notre étude sont unanimes dans la hiérarchisation des enjeux perçus. La préoccupation principale des entreprises est la continuité de service.

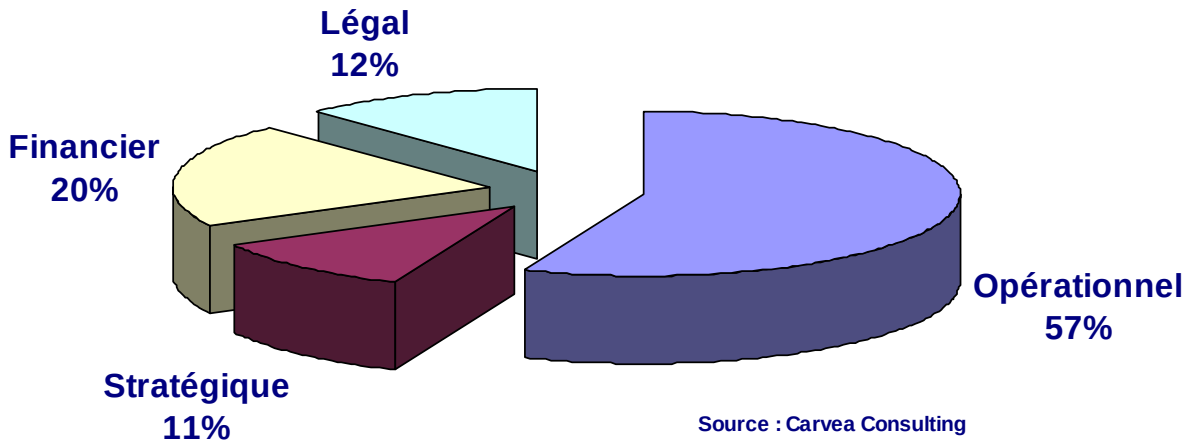

Figure 1 : Enjeux perçus par les RSSI concernant la protection des données

N°1 : Enjeu opérationnel : continuité de service

Opérationnel : il s'agit avant toute chose d'assurer la continuité de service et d'éviter une perte temporaire d'une partie de l'activité, un arrêt ou un ralentissement de la production de l'entreprise.

Voici quelques citations de RSSI rencontrés pour illustrer l'enjeu opérationnel :

- Dans la grande distribution : *« Si un virus provoque l'arrêt de notre SAP, tous nos magasins s'arrêtent de vendre. »*
- Au sein d'une activité de formation : *« Une attaque de virus paralyse notre activité. »*
- Une compagnie d'assurance : « *Un cas d'incident sur notre périmètre critique et nous ne pouvons plus vendre de contrats via nos agents.* »
- Un industriel de la construction fournissant une matière première : « *Nous sommes comme une usine et nous devons fournir notre produit 24 heures sur 24 et 7 jours sur 7 , en cas de problème c'est toute la filière aval qui est pénalisée.* »

N° 2 : Enjeu financier : perte des moyens d'exploitation

Financier : La perte des moyens d'exploitation est constituée essentiellement par la perte de postes de travail, qui demande du temps (et par conséquent de l'argent) pour les reconfigurer, et la destruction d'informations que ce soit des bases de données clients pillés par des tiers.

- *« La perte d'un PC, c'est une demi-journée de travail »,* précise un RSSI d'un groupe industriel.
- « *Nous estimons le coût total de perte d'un PC entre 20 K€ et 50 K€ en prenant en compte la perte des données et le travail de remise en fonction »,* précise un autre RSSI.

N° 3 : Enjeu stratégique : image de l'entreprise ou de la marque

Stratégique : L'enjeu stratégique est principalement lié à l'impact sur l'image de l'entreprise et concerne les entreprises ou la marque est un élément important du patrimoine. Les incidents les plus fréquemment cités sont l'image de l'entreprise dégradée suite à des spams sur carnet d'adresses d'employés et la propagation de fausses informations via les serveurs de l'entreprise.

N° 4 : Enjeu légal : obligation d'intégrité vis-à-vis des tiers

Légal : au-delà des obligations de conformité légales, réglementaires ou contractuelles telles que la Loi Informatique et Libertés, Sarbanes-Oxley… c'est principalement l'obligation d'intégrité qui est citée. Beaucoup d'entreprises ont des obligations légales pour assurer l'intégrité des informations qu'elles fournissent à des tiers, c'est le cas des administrations vis-à-vis du grand public et des tiers, mais aussi des banques et des industriels vis-à-vis de leurs partenaires.

1.3. Les enjeux par secteur

Toutes les entreprises placent en premier la continuité des services ; les critères sectoriels, la taille de l'entreprise, interviennent ensuite dans la perception et l'évaluation des enjeux et des risques.

- Le secteur bancaire est contraint par des obligations de conformité (Sarbanes-Oxley…) et doit lutter contre la fraude.
- Les industriels mettent en seconde priorité la protection du patrimoine informationnel.
- La grande distribution et les fournisseurs de produits de consommation attachent une très grande importante à l'image de marque.
- Le secteur public considère la continuité de service comme une obligation et se fait un devoir d'être exemplaire dans ce domaine.

2. LES PRATIQUES DES RSSI

2.1. Introduction

Les trois remarques de RSSI suivantes marquent le changement qui s'est opéré ces dernières années :

- *« Les virus n'apparaissent pratiquement plus sur nos remontées de statistiques, et ce sont les spywares qui nous posent problème. »*
- *« Aujourd'hui, on ne parle plus de virus mais de malware.»*
- *« Les problèmes liés aux virus représentent 2 % des incidents ; c'est combattre les spam qui nous demandent beaucoup d'énergie. »*

La menace est à la fois complexe et diversifiée : vers, chevaux de Troie, publicités indésirables, détournements de programmes légaux (keyloggers, systèmes d'administration à distance), spam à caractère divers allant jusqu'à l'escroquerie, phishing pour escroquerie financière, attaques de réseau et rackets…

2.2. Historique des solutions antivirus au sein de l'entreprise

Par le passé donc, la plupart des entreprises (80 %) ont eu, en même temps, plusieurs solutions d'antivirus, généralement liées à des modifications de périmètre des entreprises (acquisition, fusion), des zones géographiques différentes, ou des structures juridiques autonomes (filiales minoritaires). Pour des raisons économiques et de rationalisation, le choix d'une solution unique pour les postes de travail s'est imposé pour la majorité d'entre elles.
Seulement 20 % des entreprises ont conservé la même solution antivirus depuis plusieurs années. Ces entreprises sont globalement satisfaites ou du moins n'ont pas de projet d'évolution.

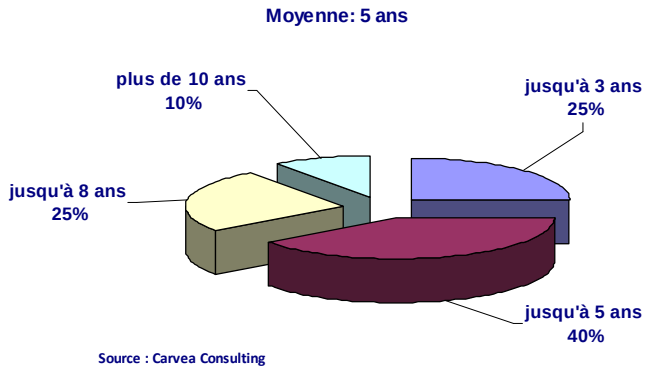

Figure 2 : Durée de remise en cause d'une solution

Lorsqu'une solution est choisie par les entreprises, sa remise en cause est en moyenne de 5 ans
Note : Dans notre échantillon, la moyenne est tirée vers le bas par les entreprises du public (23 %) qui ont des obligations de 3 ans.

Rien de surprenant pour des entreprises, en effet, difficile de changer de produit en quelques mois, les imbrications techniques et organisationnelles liées à la solution mise en place sont fortes. Par ailleurs, lorsqu'une solution est performante pourquoi changer .

2.3. Du gadget au projet d'entreprise

Depuis quelques années, les éditeurs de solutions ont mis l'accent sur les fonctions de supervision et de management du parc de stations de travail. Il est désormais possible de gérer plusieurs milliers de PC à partir d'un point central unique. Dès lors, la coexistence de solutions différentes au sein d'une entreprise devient incompatible avec une visibilité globale sur le parc ou pour disposer de statistiques consolidées. Seule une solution unique et globale permet d'offrir cette vision d'ensemble.
Aujourd'hui, la mise en œuvre d'une solution de protection des données est traitée véritablement comme un projet d'entreprise par les RSSI.

Quelques citations de RSSI résument très bien leur sensibilité :

- *« Nous ne parlons plus de solutions antivirus, mais de solutions de protection des données offrant des fonctionnalités plus élargies. »*

- *« Si, jusqu'à présent, les solutions disponibles pouvaient être considérées comme un gadget dont on pouvait faire l'économie – auparavant nous avions des virus sur le master et on ne le savait pas –, c'est aujourd'hui réellement un outil indispensable du RSSI, voire critique lorsqu'il s'agit des postes de travail éclatés partout au sein des grandes entreprises. »*

- *« Avec les fonctions d'administration et de supervision, c'est devenu un projet d'entreprise qui intègre les outils, mais aussi l'organisation de gestion et de supervision, le reporting d'incidents, et les cellules de crise en cas d'attaque. »*

2.4. Défense en profondeur multiniveau

De notre étude, il ressort que toutes les entreprises pratiquent la défense en profondeur multiniveau. Cette pratique, issue des théories militaires, consiste à sécuriser chaque sous-ensemble d'un système, estimant que la sécurisation de la périphérie n'est pas suffisante.
Le concept de défense en profondeur suppose également que les différents éléments d'un système d'information ne font pas confiance aux autres composants avec lesquels ils interagissent et que chacun des composants est autonome pour garantir sa sécurité.

Dans la pratique, la majorité des entreprises met en place une protection de sécurité multiniveau allant de la périphérie au centre, en choisissant les solutions les plus performantes pour chacun des niveaux.

La périphérie est constituée des passerelles Internet et des pare-feu, et le centre est constitué des postes de travail et des serveurs.

Ces différents niveaux de protection allient plusieurs mécanismes complémentaires :

- une stratégie de blocage des flux au niveau du pare-feu ;

- le moteur antivirus tient les virus à distance ;

- la solution antispyware protège les données sensibles et les performances système ;

- le moteur antispam bloque les attaques contre la messagerie électronique ;
- le filtre d'URL joue également un rôle, en empêchant les utilisateurs d'aller sur des sites corrompus.

Le poste de travail constitue le centre et est « le dernier rempart ». C'est aussi le plus complexe car le plus dispersé dans l'entreprise, et c'est celui qui nécessite le plus d'attention de la part des RSSI.

Postes de travail et serveurs de fichiers bureautiques

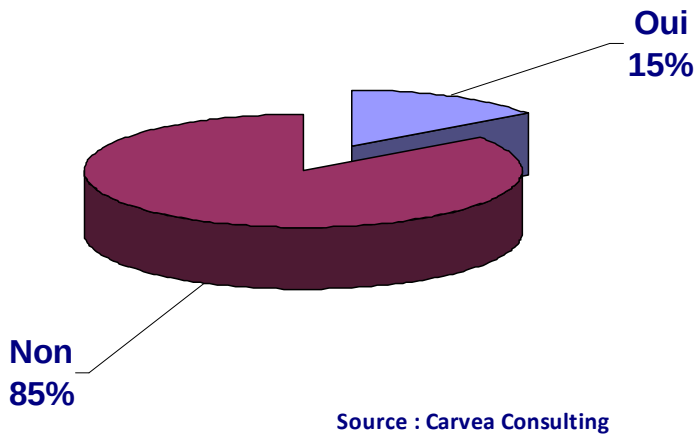

Figure 3 : Solutions différentes sur postes de travail et serveurs

85 % des entreprises disposent de la même solution antimalware sur les postes de travail et les serveurs de fichiers bureautiques.

Pour les autres qui utilisent un produit différent pour protéger les serveurs bureautiques et les postes de travail, l'objectif est de diversifier les produits afin de dresser un rempart supplémentaire aux attaques. De l'avis des RSSI concernés, c'est beaucoup de complexité pour une plus-value faible, car les solutions de détection sont performantes et aujourd'hui sensiblement équivalentes en terme de détection.

Un RSSI précise : « *Nous choisissons la solution la plus simple en terme de gestion, ce qui conduit à avoir la même solution pour les serveurs et les postes de travail*. »

Un autre RSSI d'une assurance précise : *« Mettre plusieurs antivirus en cascade coûte plus cher et nous ne sommes vraiment pas persuadés d'avoir une meilleure efficacité. »*

Serveurs de production

Les serveurs de production sont rarement traités au sein d'une politique globale, mais plutôt gérés par les responsables de la production informatique par rapport à leurs propres exigences de sécurité, de leurs systèmes d'exploitation (Linux…) et de leurs principes d'exploitation des serveurs.

Un DSI précise : *« Les fausses détections sont inacceptables et hypersensibles car nous avons beaucoup de développements maison et certains produits basés sur l'analyse comportementale réagissent mal à nos applications ; par exemple, l'antivirus bloque des flux et met nos serveurs actifs en buffer overflow et crée des incidents de production*. »

Un RSSI d'un hébergeur d'applications précise : *« Nous n'avons pas trouvé de solution très performante sous Linux, et nous préférons ne pas mettre d'antivirus pour ces serveurs, nous savons que nous hébergeons des malwares, mais nous n'avons pas de virus. »*

Remarque : *Une exception concerne les petites entreprises qui globalisent la protection de tous les serveurs par un même antivirus.*

Sécurité de la messagerie

Pour la messagerie, l'approche est double en fonction de la stratégie des RSSI.

Gestion interne ou externalisée (SaaS)

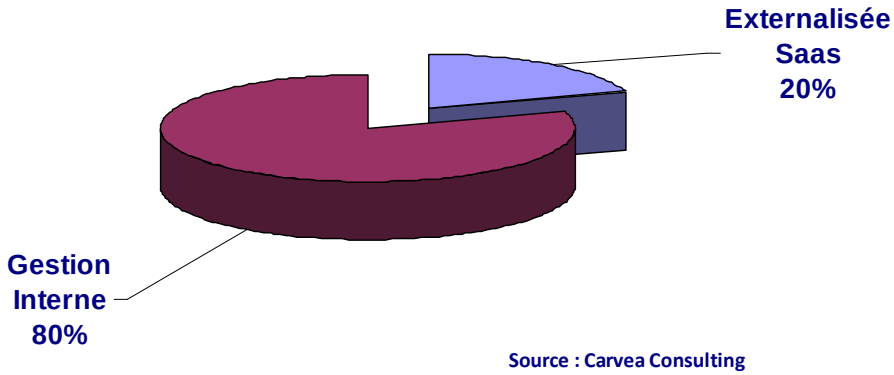

Figure 4 : Protection de la messagerie

80% des entreprises consultées choisissent de gérer elles-mêmes la solution et choisissent essentiellement un produit pour ses performances d'anti-spam, l'impact sur les performances de l'équipement est moins critique, car les serveurs peuvent disposer des ressources suffisantes
Les autres entreprises gèrent la sécurité de la messagerie en mode SaaS (Software as a Service), le service est le plus souvent intégré et proposé par un hébergeur ou l'opérateur de messagerie.

Beaucoup de fournisseurs utilisent, en cascade, plusieurs antivirus et anti-spam pour assurer une bonne qualité de détection. Le RSSI d'un organisme financier précise : « Pour les VIP qui sont très attaqués, 30 antivirus en cascade sont utilisés par l'hébergeur pour garantir un bon niveau de protection. »

Sécurité des passerelles Internet

Pour les passerelles Internet, c'est la capacité de la solution à empêcher un téléchargement « malicieux » sans perturber continuellement l'utilisateur par des avertissements non justifiés. Les technologies de réputation sont testées lors de benchmark en situation réelle : « *Savoir qu'un fichier est récent, qu'il n'a jamais été utilisé par d'autres utilisateurs, ou par peu de personnes, qu'il n'existe pas de versions antérieures connues, permet de fournir des avertissements et d'empêcher des téléchargements dangereux* », précise un RSSI.

2.5. Environnement logiciel des entreprises

Sans surprise, toutes les entreprises sont en environnement Windows, avec très peu de systèmes d'exploitation Linux, et de plus en plus souvent quelques Mac apparaissent dans l'univers des postes de travail.

Remarque : *Une chose nous a surpris lors d'entretiens avec quelques RSSI: c'est la confiance qui est accordée aux systèmes Linux et Mac, sur la soi-disant non-existence d'attaques de virus. Il est vrai que nombre de virus pour Linux et Mac OS est faible au regard du nombre considérable de programmes malicieux pour les systèmes Windows, mais cette tendance est en train de changer et le véritable problème des entreprises est « le maillon faible et la porte d'entrée » que représentent les systèmes Mac et Linux pour l'accès au système d'information de l'entreprise.*

2.6. Nomadisme

PC Nomade

En fonction du secteur d'activité, le nombre d e PC nomades varie de 10 % à 35 % du parc de PC.

Presque tous les nomades de type PC se connectent au réseau de l'entreprise, *via* des accès distants sécurisés, pour réaliser les mises à jour des solutions de sécurité. La principale difficulté rencontrée concerne le temps de téléchargement lorsqu'un utilisateur ne s'est pas connecté au réseau d'entreprise depuis longtemps.

Un RSSI dans le domaine pharmaceutique, qui a équipé les forces de vente en LapTop précise : *« Nos visiteurs médicaux ne sont pas souvent connectés au réseau de l'entreprise, et la mise à jour de base de données virales est difficile et très longue* via *les réseaux mobiles 3G/GPRS ; les solutions de type « cloud » pourraient être une bonne alternative. »*

Un autre RSSI d'un groupe international nous précise : *« Lors du choix de la solution antivirale, nous avons porté une attention particulière aux nomades, car nous avons beaucoup de voyageurs à travers le monde, et seuls quelques produits savaient localiser la station nomade pour télécharger les mises à jour à partir du site le plus proche de façon à optimiser ce temps toujours trop long pour l'utilisateur. »*

Verrouillage du poste de travail nomade

Même si un grand nombre d'entreprises « lock » les postes de travail pour empêcher les téléchargements de logiciels, une part importante d'entreprises autorise les postes nomades à modifier les configurations, pour paramétrer une imprimante à la maison. Dans ce cas, les solutions antivirus doivent être très efficaces et en permanence à jour.

SmartPhone :

Aujourd'hui, aucun SmartPhone n'est géré par les solutions de sécurité de l'entreprise. Un RSSI précise : *« Le problème n'est pas les virus mais la confidentialité en cas de vol ou de perte, et nous avons mis en place une solution de prise en main à distance. »*

Les BlackBerry sont extrêmement utilisés par les entreprises (70 %) pour leur VIP et leurs salariés et appréciés des RSSI. Un d'eux nous précise : *« C'est la seule solution envisageable, car l'offre est capable de gérer une politique d'entreprise, et parce que la solution est « fermée », elle est beaucoup plus sécurisée. »*
Un autre RSSI nous précise : *« Nous avons des BlackBerry pour les VIP, mais ce n'est pas officiel. »*

D'autres solutions Windows Mobile, Iphone… sont présentes mais ne sont jamais intégrées au niveau de la sécurité de l'entreprise.
Tous les RSSI savent qu'ils vont devoir traiter à moyen terme cette problématique de la sécurité de SmartPhone, mais aujourd'hui les SmartPhones sont gérés au cas par cas.

2.7. Statistique et reporting

Les outils de supervision sont un des facteurs de motivation pour changer de solution, et pour construire un projet d'entreprise. Quels sont les usages faits des informations de reporting et de statistique remontées par les outils ?

De l'avis général, le plus important à propos du reporting, c'est de pouvoir disposer d'une vision globale et à jour du parc de l'entreprise.

Comité technique

La quasi-totalité des entreprises consultées réalise un reporting technique à minima une fois par mois aux responsables opérationnels, au DSI ou au RSSI, en utilisant les informations remontées par les solutions de protection de données.

Restitution au management

Les entreprises les plus avancées synthétisent les informations importantes au chef de service ou à la direction générale afin que ceux-ci puissent disposer des éléments de décision pour agir ou non en matière de sécurité.
La plupart du temps, ces informations sur la protection des données sont consolidées avec d'autres informations liées à la sécurité en général, ou à la disponibilité des services proposés aux utilisateurs.

Besoin de granularité des statistiques

Pour ceux qui réalisent un reporting à destination du management, le plus important est de pouvoir disposer d'un bon niveau de granularité dans les statistiques afin de pouvoir communiquer le bon niveau d'informations aux bonnes personnes sans avoir à retravailler trop l'information brute produite par l'éditeur. L'objectif est de fournir au chef de service des rapports synthétiques faciles et rapides à lire, en travaillant les informations issues du logiciel de protection de données pour que celles-ci soient « digestes » associées à une série d'indicateurs visuels et de recommandations opérationnelles si besoin. En fonction des différents cas, les rapports sont mensuels ou annuels.

2.8. Comportement vis-à-vis des utilisateurs

Transparent et non intrusif

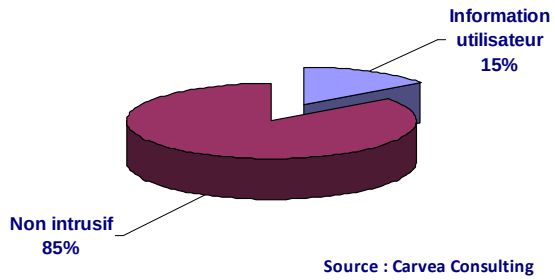

Figure 5 : Comportement vis-à-vis des utilisateurs

Pour une grande part des entreprises (85%), les RSSI ne souhaitent absolument pas être « intrusifs » vis-à-vis des utilisateurs que ce soit pour les scanning du poste de travail, les messages d'alerte, les mises à jour et la configuration du poste.
La solution doit être :

« Transparente et non intrusive. »

Ils ne souhaitent pas remonter d'informations liées à la sécurité aux utilisateurs, quelques propos de RSSI illustrent ce point de vue :

- « *La solution doit être transparente pour l'utilisateur aussi bien en ce qui concerne l'impact sur les performances que celui sur les avertissements de détection de virus et sur les statistiques*. »
- « *La solution doit être transparente et la moins intrusive possible pour l'utilisateur.* »
- « *Nous préférons laisser un virus plutôt que de bloquer le poste de travail, nous ne voulons pas de détection de virus inopportune.* »
- « *Certaines solutions affichent des messages qui perturbent l'utilisateur, car ils sont trop techniques et incompréhensibles.* »
- « *Nous ne remontons aucune information à l'utilisateur, mais lorsqu'il a 15 jours de retard dans ses mises à jour, nous lui envoyons un message*. »

Utilisateur « responsable »

Pour les 10 % d'entreprises qui n'ont pas choisi cette logique de transparence, le reporting à l'utilisateur se fait au fil de l'eau avec l'information brute, en l'informant de risques potentiels dès qu'ils apparaissent, considérant que l'utilisateur est responsable.

Un RSSI d'une mutuelle précise : *« Nous tenons à être non intrusifs pour ne pas demander à l'utilisateur d'agir, et pour ne pas bloquer son poste, mais nous ne cachons pas les informations remontées par l'antivirus aux utilisateurs, afin de le sensibiliser à la sécurité. »*

Remarques : *Seules les petites structures (50-500 postes) ou des structures publiques, telles qu'un conseil général, laissent l'utilisateur aux prises avec les messages d'alerte. Ces entreprises n'ont généralement pas d'autres moyens de sensibiliser les utilisateurs, et peu de ressources pour mettre en forme des rapports synthétiques et des plans d'action.*

2.9. Taille des équipes

La taille des équipes en charge de la gestion des solutions de protection de données est très variable, sans rapport avec le nombre de PC, allant de 10 personnes pour 100 000 PC à aucune personne de dédiée pour des parcs allant jusqu'à 1 500 postes de travail.

Exploitation et support du parc

La charge de travail « visible » et bien identifiée au sein de l'entreprise est celle liée à l'exploitation du parc de poste de travail, que ce soit pour le déploiement, les mises à jour, et le support utilisateur en cas de problème. La charge de gestion de solution de sécurité varie de 1 à plusieurs ETP (équivalent temps plein) et est étroitement liée à l'organisation de l'entreprise en matière d'exploitation.

Management de la sécurité

La taille des équipes en charge de gérer la sécurité dépend de la maturité de l'entreprise en matière de sécurité au sens large et n'est pas liée à une solution. Les entreprises les plus avancées ont des correspondants sécurité au sein d'entités métiers, des comités techniques, des comités stratégiques, des cellules de crise, et des entités de gestion des risques.
Les moins avancées ont un RSSI unique multifonction, qui fait donc tout.

2.10. Faire ou faire faire

Gérer soi-même les solutions de protection des données ou les confier à un tiers ?
Les avis sont partagés et c'est généralement une question de culture d'entreprise. La réponse est différente en fonction des domaines couverts.

Type de défense	Type de solution externalisée
Solution poste de travail	Dans le cas d'externalisation, la solution est mise en œuvre en interne et c'est la gestion qui est confiée à un prestataire ou un GIE appartenant au groupe.
Messagerie	Le plus souvent la solution est celle de l'hébergeur ou de l'opérateur de l'entreprise.
Passerelle Internet	L'externalisation se fait majoritairement avec des solutions en mode SaaS, c'est-à-dire une plateforme gérée et mutualisée par un fournisseur.

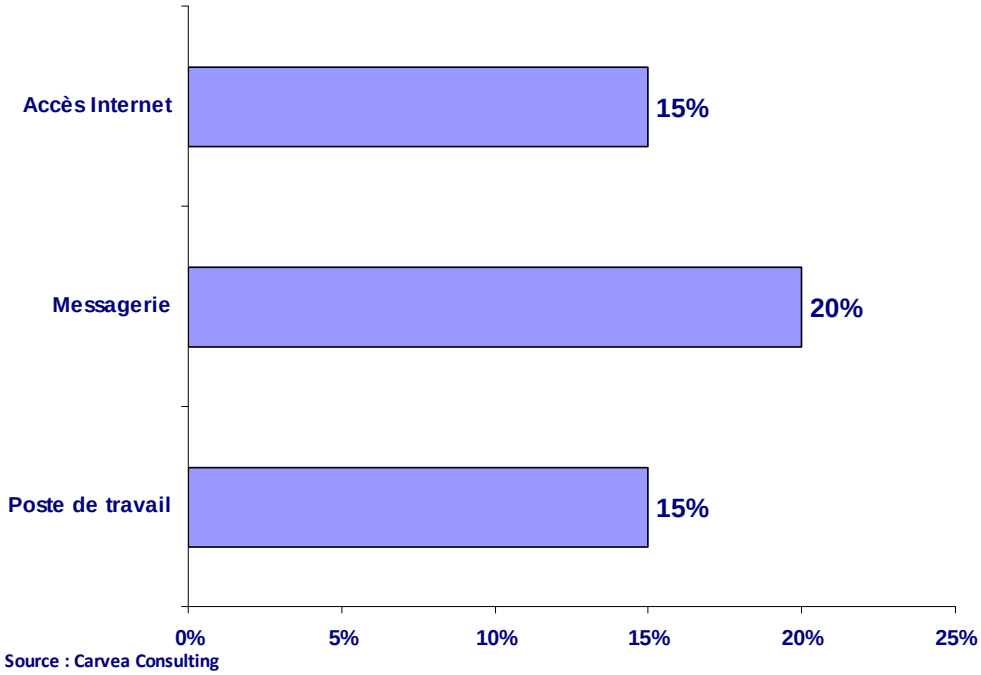

Figure 6 : Pourcentage des entreprises qui externalisent la protection des données

Pour ceux qui n'externalisent pas, la raison est souvent organisationnelle, car les coûts de gestion interne liés à la sécurité sont intégrés dans une gestion globale des processus de sécurité, ou d'exploitation des systèmes.

Un RSSI d'un groupe international nous confie : *« Le mode SaaS rassure les métiers, car ceux-ci n'ont pas toujours confiance dans les infrastructures internes, et avec ce mode seul les messages « propres » circulent au sein de l'entreprise, l'élimination étant faite à l'extérieur. »*

Note : Les RSSI rencontrés ayant fait ce choix sont en général très satisfaits de la performance des menaces détectées (spam, virus…) et de la flexibilité organisationnelle que cela apporte.

3. CRITERES DE CHOIX D'UNE SOLUTION

3.1. Hiérarchisation des critères de choix

Il a été demandé aux RSSI de hiérarchiser les critères de choix d'une solution de protection de données. Le graphe ci-dessous représente les réponses pondérées et rapportées sur une échelle de 100 %.

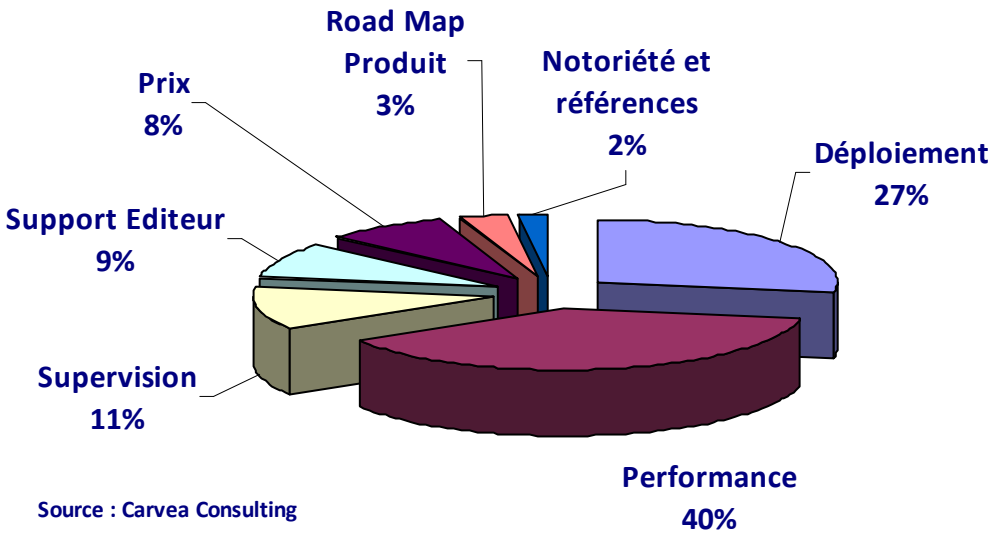

Figure 7 : Critères de choix pour une solution de protection des données

3.2. Facilité de déploiement de la solution

Les RSSI rencontrés pour cette l'étude n'ont pas tous participé à la mise en place du produit actuel, mais tous ceux qui sont en cours de réflexion pour choisir un nouveau produit retiennent comme priorité la facilité de déploiement.

Un RSSI résume très bien les attentes : *« Le produit doit être simple à installer la première fois, et tout aussi simple pour les mises à jour des bases de données virales, et les évolutions de version. »*

Désinstallation

Le point souvent cité concerne la désinstallation des antivirus existants qui est souvent source de problèmes et qui perturbe le déploiement d'un nouveau produit.

Un RSSI précise : *« L'éditeur en place nous demandait 40 000 € pour désinstaller son produit sur notre parc, alors qu'un éditeur en compétition offrait de base avec le produit la fonction de désinstallation de tous les produits existants. »*

Facilité d'intégration au sein de l'environnement

La plupart des problèmes rencontrés lors de déploiement sont liés à des difficultés d'intégration des produits avec l'environnement : systèmes, réseaux, prise en compte d'Active directory, application maison.

Centralisation de la gestion

Pouvoir piloter un déploiement à partir d'un poste central est un des points clefs des attentes des RSSI *: « Nous avons créé une task force pour piloter le déploiement, superviser les opérations, et répondre aux demandes des utilisateurs. »*
Un RSSI nous précise : *« Le fait de pouvoir effectuer la mise à jour des correctifs depuis un poste central est un atout considérable. »*

Déploiement à chaud

La capacité de déploiement à chaud, sans avoir à rebooter le système de certains éditeurs, nous a été citée plusieurs fois comme apportant une grande souplesse dans le déploiement d'une solution.

3.3. Performances

Performances de détection

Parmi les éléments de performance arrivent en premier :

- La performance de détection de tous les codes malicieux quelle que soit la situation : virus à signature connue ou non.
  Pour 70 % des RSSI, la base de signatures n'est plus suffisante, considérant que le modèle basé sur les signatures, même s'il est indispensable, n'est plus assez efficace à l'heure où les menaces sont de plus en plus ciblées et changeantes. Les éditeurs apportent des solutions très différentes pour neutraliser les nouvelles menaces inconnues des bases de signatures, protéger l'utilisateur lorsqu'il surfe en détectant les sites malveillants, ou détecter les fichiers téléchargés suspects.
  De l'avis de tous les RSSI, il est très difficile de comparer la performance des éditeurs sur ces critères et la manière la plus efficace est la mise en place d'un test en conditions réelles.

- Le temps de réaction de mise à jour des correctifs est très important aussi bien pour la découverte d'un nouveau virus que pour contrer les attaques avant qu'elles ne se répandent. Les attaques *" Zero Day "* inquiètent les RSSI et ceux-ci portent une attention particulière à la rapidité de distribution d'un *patch.*

- La pertinence de la détection est un critère souvent cité, celui-ci n'est pas seulement une question de paramétrage du logiciel, mais surtout lié à la qualité des algorithmes et des technologies mis en œuvre pour qualifier la présence d'un code malicieux avec certitude.

  Un RSSI nous confie : *« Les équipes passent parfois plus de temps sur les problèmes liés à la solution antivirus avec un poste de travail bloqué… que sur les véritables problèmes d'attaque. »*

Impact sur les performances du poste de travail

Dans un second temps, les éléments pris en compte sont :

- la consommation mémoire ;
- l'occupation des ressources CPU ;
- le temps de scanning des disques durs.

Note : *Le temps de scanning est de moins en moins critique car les analyses sont activées en tâche de fond pendant des périodes de faible occupation. Par ailleurs, les éditeurs commencent à proposer des techniques d'analyse différentielle qui consistent à n'analyser que ce qui a changé, et qui sont très rapides sauf lors de la première analyse.*

L'impact sur les performances des machines est affaire de compromis et est très dépendant de la vétusté du parc. C'est très important pour un parc vieillissant et non significatif pour les nouvelles générations de PC.
Un RSSI précise : *« Si le parc de PC est récent cela ne pose pas de problème, mais dans notre entreprise le parc est vieillissant, et c'est un élément clef. »*
Pour ces entreprises, il s'agit d'ajuster la meilleure sécurité au regard de l'impact des performances.

Contrôle des périphériques

Le contrôle des périphériques, notamment des clefs USB, est un point souvent abordé, car complexe : pour certains, les clefs USB sont interdites ; pour d'autres, la sécurité repose sur la solution anti-virus pour analyser les clefs USB et assurer la protection.

« Notre éditeur nous a proposé l'achat de clefs USB avec un identifiant pour chaque clef de façon à pouvoir l'authentifier, et cela est très pratique et permet de répondre efficacement aux demandes des utilisateurs », témoigne un RSSI.

Défense pro-active

Un RSSI nous confie : « *Chez nous des défenses pro-actives sont sur les clefs USB et sur les modifications de répertoires ; de base, les ports USB sont désactivés, et sont activés en fonction d'une stratégie dépendant du profil utilisateur configuré au sein de l'Active Directory.* »

Les systèmes de prévention et de détection sont très perfectionnés, mais difficiles à mettre en œuvre au sein d'une grande organisation. Un RSSI nous explique : *« La défense pro-active de type IPS (Intrusion Prevention System) nous paraissait indispensable, mais trop perturbante en raison des blocages intempestifs qu'elle occasionne. Nous nous sommes donc concentrés sur un IDS « Intrusion Detection System » ; il faut alors une équipe pour analyser les rapports produits par le système, mais notre organisation est telle qu'aucun responsable ne prend la décision de couper un flux applicatif suite à une détection, car il ne dispose pas des informations d'impacts d'une telle action. »*

3.4. Gestion et supervision

D'une façon générale, lors d'un choix, la recherche de souplesse est un des points prioritaires toujours cités et celui de la gestion/supervision revient de façon prioritaire pour tous les RSSI.
En effet, l'exploitation, la supervision, le suivi des mises à jour, constituent une charge de travail importante pour l'entreprise, et coûtent cher.

Console de supervision

La console de supervision doit être centralisée, ergonomique et simple d'utilisation.

Un RSSI nous confie : *« La solution que nous avons choisie , très performante, nous permet d'avoir une vision de nos 20 000 PC, mais il nous faut quatre fois plus de compétence et de temps pour gérer la solution, car celle-ci est très complexe, et cela nous a demandé de faire monter en compétence nos équipes. »* Un autre RSSI nous précise : *« La solution doit être intuitive pour être certain de paramétrer correctement l'outil. »*

Gestion à plat ou hiérarchisée

Plusieurs entreprises ayant plus de mille postes à gérer nous ont précisé que la supervision fonctionnait très bien dans un modèle « à plat » alors que d'autres utilisent les fonctions de distribution et construisent une véritable architecture hiérarchisée avec des serveurs distribués pour « coller » au plus près de l'organisation.
Un RSSI d'un groupe international précise : *« En me connectant au portail de l'éditeur, je peux visualiser la situation de mes 3500 PC de n'importe quel point du globe. »*

3.5. Le support technique de l'éditeur en cas de problème

Le support de l'éditeur est un élément clef des critères de choix, car c'est la crédibilité de l'équipe sécurité qui est mise en cause si elle n'arrive pas à gérer des incidents et le support technique s'avère, pour beaucoup, indispensable.

- Un RSSI d'une entreprise publique précise : « *Nous attendons un support technique de bon niveau et avons exigé un contact direct avec l'éditeur pour le support, même si notre intégrateur reste notre interlocuteur privilégié. »*

- Un autre RSSI précise : *« Nous évaluons la capacité de l'éditeur à nous aider en cas de problème. »*

- Un RSSI d'un groupe industriel précise : *« Nous avons un accord avec notre éditeur, car il nous arrive fréquemment de détecter de nouveaux virus issus des différentes zones géographiques du monde, nous lui soumettons le code malicieux et il nous répond dans la demi-journée comme il s'y est engagé, c'est très rassurant. »*

3.6. Road map « produit » et notoriété de l'éditeur

Compte tenu des évolutions et concentrations des éditeurs sur le marché, la notoriété est importante.

Un RSSI précise : *« Nous regardons la road map produit : ce qui est livré aujourd'hui est important mais ce qui existera demain l'est encore plus. »*

Les menaces sont en constante évolution et les cybercriminels débordent de créativité et de capacité d'innovation pour déjouer les parades des solutions de protection. C'est une course sans fin que mènent les éditeurs de solution antimalware pour garantir à leurs clients d'être toujours efficaces.

Quel moteur sous le capot ?

Ces éditeurs doivent sans cesse innover, développer de nouvelles stratégies de défense, être extrêmement réactifs à toute nouvelle forme d'attaque tout en minimisant l'impact sur les performances du poste de travail et en restant transparent vis-à-vis de l'utilisateur.

- Un RSSI bancaire précise : « *Difficile de choisir en fonction des fonctionnalités car un jour un éditeur est en avance et six mois plus tard c'est un autre qui sort une nouvelle technologie plus performante. »*

- Un autre RSSI : *« Nous avions constaté que la solution que nous avions choisie avait toujours six mois de retard, ce n'est pas très rassurant, on ne peut s'empêcher de penser que pendant ce temps une porte reste ouverte.* »

L'exercice de comparaison des moteurs et des technologies utilisés pour le scanner, la détection de virus, l'analyse comportementale… est extrêmement complexe car les éditeurs développent des savoir-faire qui leur sont spécifiques.

- Un RSSI nous confie : *« Avec la précédente solution, il fallait attendre de 6 à 8 mois pour que la prochaine release intègre les innovations de détection ; lors d'une comparaison, nous avons trouvé une solution qui, grâce à un moteur dynamique, met à jour de façon instantanée le moteur à chaque nouveauté. »*

- Un autre RSSI précise : *« Nous avons choisi notre éditeur actuel parce que son moteur de détection et d'analyse est embarqué en OEM dans plusieurs autres produits du marché, ce qui pour nous est un gage de qualité et de pérennité. »*

- Un autre RSSI : *« Certains éditeurs sont plus visionnaires que d'autres et c'est cela le plus important car nous nous engageons avec la solution longtemps et espérons ne pas avoir à changer. »*

4. ECLAIRAGE SUR LE MARCHE

4.1. Microsoft

Microsoft propose des solutions de sécurité antivirale pour les particuliers et les entreprises.

Quasiment toutes les entreprises interrogées sont en environnement Microsoft, la perception des RSSI vis-à-vis de la solution de protection de données de Microsoft est d'autant plus intéressante.

Pour 75 % des RSSI, faire confiance au même éditeur pour pallier les défaillances/failles des systèmes d'exploitation et pour les corriger ne paraît pas raisonnable.
Les propos sont identiques :

- *« Il ne faut pas mettre tous les œufs dans le même panier ! »*

Mais certains ont un point de vue contradictoire :

- *« Qui mieux que l'éditeur lui-même peut pallier les failles de sécurité de son système »* ou bien *«La solution présente l'avantage d'être gratuite et de pouvoir être mise à jour en même temps que les patchs des systèmes et des applications. »*

Pour d'autres RSSI la méfiance est de rigueur :

- *« Microsoft a déjà tenté une présence sur ce marché il y a trois ans avec un produit grand public sans grand succès. »*

- *« On ne peut pas être bon partout, c'est une affaire de spécialistes. »*

Si nous devions conclure, l'attentisme et l'observation sont la tendance générale :

- *« Attendons de voir ce que donne la solution avec le temps »,* précise un RSSI.

5. DEMARCHE DES ENTREPRISES

5.1. Source d'information des RSSI

Comment apprécier un éditeur et sa solution ? Pour 75 % des entreprises, la démarche la plus fréquente est d'effectuer une phase exploratoire constituée d'entretiens ou de workshops avec des éditeurs : les éditeurs ou intégrateurs viennent présenter leur produit de façon à ce que l'entreprise puisse se faire une idée des produits et de ce qu'ils peuvent apporter.

Les RSSI ont une certaine méfiance vis-à-vis des publications des laboratoires de test et les comparatifs techniques, imaginant que les éditeurs ont toujours des actions de lobbies vis-à-vis de ces tests même si les laboratoires sont réellement indépendants. Un RSSI précise : *« Nous savons pertinemment que les éditeurs pilotent certains tests faits en laboratoire. »*

Par ailleurs, ces tests sont d'une très grande complexité à mener et les résultats varient de façon importante d'un semestre à l'autre. Le RSSI d'une grande banque précise : *« Un éditeur est bon à un instant donné et quelques mois après c'est un autre qui le dépasse, alors que, nous, nous choisissons une solution pour plusieurs années. »*

Constitution d'une short list

Que l'entreprise soit publique ou non, tous les RSSI procèdent par un appel d'offre sur la base d'une short list de 3 à 5 éditeurs maximum.

Priorité à l'existant pour constituer la short list

La démarche est de reprendre systématiquement les éditeurs présents dans l'entreprise pour constituer une short list, y associer les éditeurs connus par le bouche-à-oreille ou *via* les clubs liés à la sécurité, la liste est composée de 3 à 5 éditeurs maximum dans la majorité des cas sur les 6 ou 7 éditeurs présents en France et disposant de produits dédiés aux entreprises.

Un RSSI nous confie : *« Nous n'avons pas le temps de voir tout le monde, nous challengeons ceux qui sont déjà référencés chez nous. »*

Note : *Lorsque le RSSI est satisfait de la solution en place, la priorité au sortant est importante.*

5.2. Motivation pour changer de solution

Les motivations sont multiples, mais nous pouvons les hiérarchiser de la façon suivante :

- La migration des logiciels d'exploitation du parc de PC qui entraîne une réflexion sur les logiciels associés dans les solutions de protection de données.
- Les besoins de management de sécurité des PC, généralement initiés par l'attrait des consoles de supervision proposées par les fournisseurs.

- Assez rarement le mécontentement.
- Et pour le secteur public, la mise en concurrence obligatoire au bout de trois ans.

Impact de la maison mère

De façon inattendue, les RSSI qui dépendent des choix d'une maison mère sont les plus affutée et sont ceux qui analysent en détail les caractéristiques des solutions et, la plupart du temps, c'est pour choisir une solution différente.

5.3. Test en configuration réelle

Dans 80 % des cas, des tests en configuration réelle sont mis en œuvre pour évaluer les performances des différentes solutions en short list.
Ces tests généralement réalisés en interne prennent en compte :

- les performances de détection ;
- les performances d'installation/ désinstallation des produits existants ;
- la capacité de supervision, et l'ergonomie de la console ;
- les performances impactant le poste de travail.

6. SYNTHESE « LES DIX BONNES PRATIQUES A RETENIR »

① Concevoir une défense en profondeur multiniveau

Toutes les entreprises mâtures en matière de sécurité pratiquent une défense en profondeur multiniveau, c'est-à-dire de la périphérie constituée des passerelles Internet et des pare-feu, et du centre constitué des postes de travail et des serveurs. *(cf page 10)*

② Porter une attention particulière aux postes de travail

Le poste de travail constitue « le denier rempart » ; il est le plus complexe à gérer car le plus dispersé dans l'entreprise, il est par conséquent nécessaire d'y porter une attention particulière. *(cf page 11)*

③ Prévoir un test de performances en situation réelle

Seuls les tests réalisés, en interne en conditions réelles, permettent de se faire une idée des performances adaptées au contexte de l'entreprise en fonction des architectures mises en œuvre, de la vétusté des postes de travail et du contexte en général. *(cf page25)*

④ Mettre en place un véritable projet d'entreprise

Les solutions de protection des données proposent aujourd'hui des consoles de supervision qui permettent de piloter les déploiements, de superviser à partir d'un lieu central plusieurs milliers de postes de travail et des outils de statistiques pour disposer d'une vision globale et précise de la sécurité d'une entreprise.
Dès lors, tous les éléments sont disponibles pour gérer, améliorer et optimiser les outils et les processus liés à la sécurité et en font un véritable projet d'entreprise intégrant aussi bien les dimensions techniques, sécurité, économiques, et processus d'exploitation au service de la stratégie sécurité de l'entreprise. *(cf page10)*

⑤ Analyser les fonctions de supervision en fonction de sa propre organisation

Les fonctions de supervision confortent le rôle des RSSI dans l'élaboration d'une stratégie sécurité en mettant à sa disposition un outil de pilotage « de la protection des données » et lui permettent d'optimiser le travail et l'organisation des ressources sécurité. *(cf page 14)*

⑥Analyser les fonctions de reporting et de statistique en fonction de sa politique interne

Le reporting et les statistiques peuvent être techniques, ou synthétiques pour être restitués aux exploitants, au management à haut niveau, au RSSI ou au fil de l'eau aux utilisateurs. Ceci dépend essentiellement de sa politique interne, et l'outil de reporting doit être adapté, et suffisamment paramétrable pour minimiser le travail de transformation de l'information à communiquer. *(cf page 14)*

⑦ Choisir son éditeur de solution sur son potentiel à rester performant

Un projet de protection des données est structurant et engagement sur le long terme ; lorsqu'on choisit un éditeur il faut donc analyser ses performances actuelles, mais aussi sa pérennité financière et technologique, les produits de la road map à venir, et sa vision de la sécurité de demain. *(cf page 22)*

⑧ Regarder sous le capot avant de faire confiance à un éditeur

L'innovation est au cœur des stratégies de défense élaborées par les éditeurs, pour choisir un produit il faut « regarder » sous le capot, c'est-à-dire comprendre les technologies qui ont été développées, les principes de fonctionnement du « moteur ». C'est certainement l'exercice le plus difficile à mener lors d'un choix. *(cf page 22)*

⑨ Privilégier le retour d'expérience des autres pour se forger une opinion

La comparaison des produits de protection de données est très complexe à mener : posséder un bon « background » technologique sur le sujet, et le retour d'expérience des autres RSSI (dont ce guide est inspiré) constituent une des meilleures façons de conforter ses choix. *(cf page 24)*

⑩ Prévoir la gestion des smartphones

Aujourd'hui, à l'exception des « BlackBerry » les smartphones sont gérés au cas par cas de façon isolée. Nous sommes convaincus que les terminaux mobiles vont prendre une position prépondérante dans les 3 à 5 ans à venir, et que les RSSI doivent s'y préparer. *(cf page 13)*

7. ANNEXES

7.1. Echantillon d'entreprises rencontrées dans cette étude

Nous avons rencontrés vingt RSSI d'entreprises françaises, de taille moyenne à de très grands comptes, représentatifs de tous les secteurs d'activité.

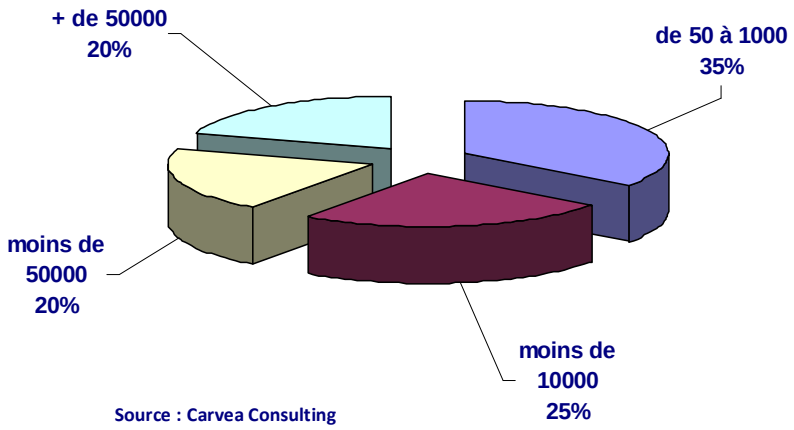

Figure 8 : Nombre de postes de travail de l'échantillon d'entreprises rencontrées

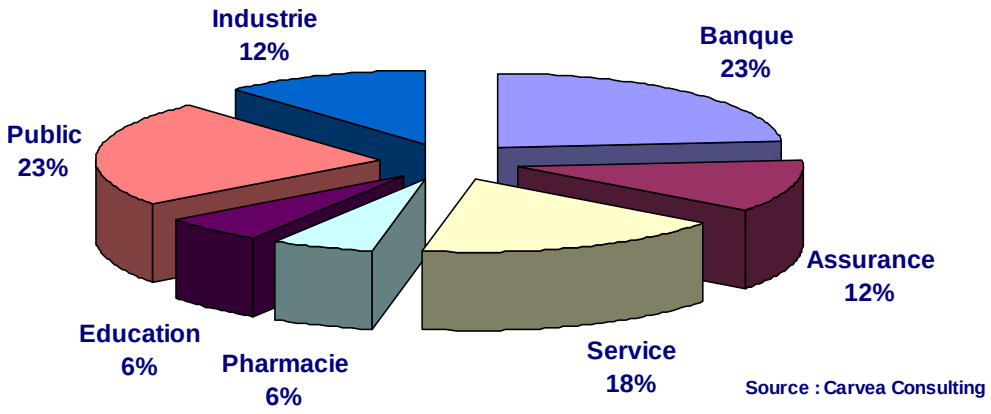

Figure 9 : Répartition sectorielle de l'échantillon d'entreprises rencontrées

TABLE DES ILLUSTRATIONS