

## **PME et Grandes Entreprises face à la sécurité : Une analyse approfondie**

## Introduction

"PME" est l'un des sigles qui reviennent aujourd'hui le plus souvent dans le langage économique. La plupart des fournisseurs travaillant à la fois pour les Petites et Moyennes Entreprises et les Grandes Entreprises distinguent quant à eux ces deux catégories d'acteurs du marché en fonction de leur chiffre d'affaires annuel ou de leur effectif. Pour autant, lorsqu'il s'agit de sécurité informatique, aucune de ces deux approches ne correspond vraiment à une réalité. Plutôt que de tenter de leur attribuer une étiquette, les fournisseurs devraient consacrer davantage de temps et d'énergie à évaluer les besoins en sécurité de ces entreprises et les ressources dont elles disposent, de manière à leur apporter une solution sécurité répondant au mieux à leurs besoins spécifiques.

Le travail de sécurisation des actifs réseau des PME et des Grandes Entreprises cible des objectifs d'ampleur équivalente, mais le niveau d'expertise, les effectifs et le budget dont disposent les PME sont clairement sans commune mesure avec les ressources des grandes entreprises. Les fournisseurs de solutions de sécurité ont tendance à mettre en avant une "qualité professionnelle" dans leur argumentaire commercial à destination des PME, mais ce qu'ils leur proposent en réalité est trop partiel dans l'approche, manque de performance et de fonctionnalités par rapport à leur offre 'Grande Entreprise'.

### Un besoin de sécurité

Les menaces réseau se propageant par l'Internet, elles s'attaquent sans distinction aux PME et aux grandes entreprises. Aussi, quelle que soit leur taille, toutes les entreprises connectées à l'Internet devront faire face aux mêmes menaces. Elles doivent notamment s'attendre aux attaques véhiculées par le trafic HTTP entrant et sortant. De même, la quasi-totalité des entreprises actuelles ont recours au courrier électronique dans leurs communications quotidiennes à l'interne et à l'externe. Elles se retrouveront par conséquent confrontées à la grande diversité et au nombre croissant des menaces qui se propagent par e-mail. Si elles hébergent elles-mêmes un serveur e-mail ou un site Web, elles devront impérativement prendre des mesures de sécurité complémentaires pour les protéger.

Il en va de même pour les serveurs d'application de l'entreprise, pour ses bases de données, ou pour tout autre élément de son infrastructure réseau. Sans distinction de taille, toutes les entreprises, les PME au même titre que les grandes entreprises, doivent faire face aux attaques visant ces actifs critiques. La seule différence significative entre elles concerne le volume de leur activité.

### Des ressources fondamentalement inégales

Le principal aspect par lequel les PME diffèrent des grandes entreprises concerne le niveau de leurs ressources humaines et financières. Les PME partagent la plupart des besoins en sécurité des grandes entreprises, mais disposent de ressources nettement inférieures - et d'un débit réseau limité - pour pouvoir les gérer avec efficacité.

Une grande entreprise peut mettre en place un service informatique à temps plein, chargé notamment de gérer au quotidien les problématiques de sécurité de la structure. Cela implique de déployer des systèmes complexes afin de sécuriser efficacement l'ensemble des actifs réseau de l'organisation, sur chacun de ses sites. Il s'agit également de suivre au plus près le profil d'une menace en constante évolution, d'adapter si nécessaire les politiques de sécurité de l'entreprise aux risques émergents. Plus important encore, ce service informatique doit constamment garder la main sur le trafic réseau de l'entreprise, en analysant notamment les fichiers journaux pour y détecter tout évènement inhabituel. Une Grande Entreprise possède le potentiel financier nécessaire à l'acquisition de tels systèmes et à la mobilisation du personnel requis pour les faire fonctionner avec efficacité.

A l'inverse, une PME n'aura pas forcément affecté du personnel à temps plein à la gestion du parc informatique, et il est presque certain qu'elle ne comptera pas parmi ses collaborateurs un expert se consacrant exclusivement à la sécurité informatique. Il est plus probable qu'elle s'appuiera sur un seul salarié chargé de toutes les questions relatives à l'informatique dans l'organisation, y compris de la sécurité. D'autres encore externaliseront tout simplement l'intégralité de leurs besoins en informatique.

Les PME n'ont généralement ni le temps ni les ressources nécessaires à l'implémentation d'une solution de sécurité complexe et globale. Si une grande entreprise est prête à régler une facture considérable et à gérer un déploiement s'étendant sur plusieurs mois, une PME en revanche sera réticente ou incapable de faire face à une dépense d'une telle ampleur, et souhaitera obtenir des résultats quasi immédiats.

### Des décisions différentes en matière de sécurité

Avec de tels défis à relever, les PME devront naturellement prendre des décisions difficiles. Les grandes entreprises sont en mesure d'engager les investissements conséquents en temps et en argent que nécessite le déploiement d'un système de sécurité par couches successives proactif et réellement complet qui permette d'atteindre un niveau de sécurité maximal. Quant aux PME, avant de choisir un système, elles doivent tout d'abord évaluer les moyens qu'elles peuvent engager dans l'acquisition et la maintenance de ce système.

Le dispositif le plus sophistiqué du monde ne sera d'aucune utilité à une PME si sa mise en œuvre nécessite de nombreuses et fréquentes interventions humaines. Sans un ou plusieurs techniciens informatiques affectés à la sécurité, un système complexe générant un important volume d'informations, comme par exemple des fichiers journaux enregistrant les anomalies du trafic SNMP et HTTP, serait relativement sans intérêt, car le service informatique manquerait de temps pour analyser les données de ces journaux. De même, un système complexe dont l'implémentation prendrait des mois ne résoudrait pas le problème d'une PME, à la recherche d'une solution de sécurité opérationnelle en quelques jours, avec peu de personnel mobilisé.

En tenant compte de ces différents défis apparemment insurmontables et de la réputation qu'ont les PME de ne pas être pleinement conscientes des problématiques de sécurité, il est prévisible que les PME choisiront leur solution sécurité en fonction de son coût, de sa simplicité et de son degré d'automatisation plutôt que sur des critères de fiabilité et d'efficacité.

## L'offre Sécurité actuelle orientée PME

La plupart des fournisseurs habituels de solutions de sécurité sur le marché des entreprises s'avèrent encore incapable à ce jour de répondre correctement aux besoins de sécurité des PME. L'offre PME de ces fournisseurs intègre des composants matériels moins nombreux et moins puissants que ceux qui sont mis en œuvre dans l'offre conçue pour les grandes entreprises. Les produits PME seront donc bien moins performants. Ces vendeurs se contentent pour beaucoup de supprimer certaines caractéristiques et fonctionnalités de leurs produits grandes entreprises afin de les proposer sur le marché des PME à prix réduit. Par exemple, une solution de filtrage d'URL intégrant une liste noire de 50 millions d'adresses pourra en comporter uniquement 5 millions dans la version PME. De même, un moteur anti-malware pensé pour les grandes entreprises contiendra 500000 signatures de malwares quand la version PME n'en comptera que 3000... soit juste assez pour couvrir la "wildlist", la liste officielle de virus en circulation dans le monde, utilisée par les professionnels de la sécurité. Ou encore, une solution de filtrage e-mail orientée grandes entreprises, capable de détecter du spam ou autres malwares en fonction du contenu ou de l'apparence, pourra se contenter dans la version PME d'une simple liste noire dynamique de domaines connus classés comme spam.

Certains vendeurs limitent même considérablement la puissance et les fonctionnalités de leur produit. La version Grandes entreprises d'un système de sécurité pourra intégrer les logiciels les plus sophistiqués et le meilleur de la technologie tandis que la version PME devra se contenter d'un logiciel de sécurité open-source. La version PME pourra également se voir privée de certaines fonctionnalités, ce qui rendra le produit moins fiable, ou moins convivial pour l'utilisateur. Plus important encore, toutes ces restrictions finissent par créer pour la PME une exposition significative au risque sécurité, rendant son réseau bien plus vulnérable que celui d'une entreprise de plus grande taille.

## Les Besoins des PME

Globalement, e-mail et accès à Internet représentent la majeure partie des applications critiques à l'activité des PME. Une multitude de paramètres entre en jeu dans le processus de sélection d'un système de sécurité englobant l'e-mail par une organisation.

## Une protection complète pour toutes les entreprises

En matière de menace Internet, les petites et moyennes entreprises doivent faire face au même risque, relever les mêmes défis que les grandes entreprises. Les entreprises devraient rechercher un prestataire de solutions de sécurité présent dans le monde entier, capable d'analyser le trafic Web et e-mail jour et nuit afin d'identifier les menaces nouvelles qui s'y profilent. Auparavant, on attendait d'un fournisseur qu'il offre une protection 'J+zéro', c'est à dire une protection contre les menaces e-mail garantie dès le jour où celles-ci avaient été identifiées. Désormais, les organisations de toute taille exigent une protection 'H+zéro', une protection quasi-instantanée.

## Une solution Hautes Performances

Pour être efficace, l'analyse sécurité Web et e-mail se doit d'être rapide. Le plus souvent, les solutions de sécurité intervenant sur la passerelle Internet ont besoin de temps pour traiter les communications entrantes et sortantes, ce qui implique un impact négatif sur la réactivité des échanges et la frustration des utilisateurs du réseau.

## La continuité de l'activité

Une solution de sécurité efficace pour la passerelle Internet doit non seulement garantir une protection contre les menaces détectées, mais également constituer un rempart contre les menaces qui restent encore à identifier par les laboratoires de recherche antispam et anti malware.

## Une administration intuitive

Les petites et moyennes entreprises ne disposent pas du personnel informatique nécessaire pour réaliser une installation complexe, assurer la maintenance de plusieurs suites logicielles de sécurité, gérer les mises à jour, traiter la problématique des licences utilisateurs. Le déploiement et la maintenance de la solution doivent être suffisamment intuitifs pour l'utilisateur. La solution doit également inclure impérativement une interface de configuration pratique et des statistiques résumées présentées sous forme de graphiques.

## Conclusion

Lorsqu'il s'agit de sécuriser les actifs de leurs réseaux, PME et Grandes Entreprises ont les mêmes besoins, mais le niveau d'expertise et les ressources humaines et financières dont elles disposent les placent dans des catégories réellement opposées. En soi, "Solution professionnelle" est un argument convaincant, dans la mesure où il s'applique à une protection vraiment complète et puissante. Pour autant, cette expression ne devrait pas s'appliquer à la version édulcorée d'une solution destinée aux grandes entreprises. Les solutions PME devraient être conçues comme un produit à part, pensé pour répondre aux besoins spécifiques de ces acteurs économiques. Plus encore, les solutions PME devraient garantir un niveau de sécurité identique à celui dont bénéficient les Grandes Entreprises.

---

## NETGEAR ProSecure STM : Solution de management des menaces Web et E-mail

Le boîtier ProSecure STM fait appel à une technologie exclusive qui détecte et bloque les attaques de façon appropriée à la rapidité et à l'étendue de leur propagation. Par cette approche, il est possible de détecter le spam et les attaques de malwares dès leur apparition, et de bloquer en temps réel tous les messages associés.

Le boîtier ProSecure STM intègre la technologie Netgear de Stream Scanning (Scan à la Volée), en attente de brevet, qui permet d'analyser les flux de données au moment où ils entrent sur le réseau. Grâce à la technologie Stream Scanning, les boîtiers NETGEAR STM peuvent traiter un volume important de données en temps réel, une seule analyse suffisant pour identifier le spam, les malwares, les atteintes à la sécurité ou les applications inappropriées. Il est ainsi possible de garantir aux utilisateurs du réseau un contenu e-mail et Web sûr, sans temps d'attente.

Le boîtier ProSecure STM utilise un système de défense comportemental et proactif qui supprime l'intervalle existant jusqu'alors entre l'exploitation d'une vulnérabilité et sa correction. La solution NETGEAR intègre une analyse chirurgicale qui permet d'identifier les caractéristiques suspectes du trafic réseau entrant et sortant, et de les neutraliser jusqu'à ce qu'elles puissent être examinées de manière approfondie.