La grande migration de la sécurité informatique dans le « Cloud »

Comment les petites et moyennes entreprises peuvent gérer leurs risques informatiques tout en se conformant à la réglementation et avec un personnel et un budget minimes.

Assurer la sécurité et le bon fonctionnement des ressources informatiques dans le respect de la réglementation semble presqu'impossible, surtout pour les petites et moyenne entreprises (PME). Il y a de nombreuses explications à cela. Mais, heureusement, des tendances technologiques récentes évitent désormais cette fatalité.

- **Les cybermenaces et la réglementation ne se soucient guère de la taille de l'entreprise**
  La plupart des pirates ne se préoccupent pas de savoir s'ils attaquent une entreprise figurant au CAC 40 ou un petit fabricant en région qui emploie 25 personnes. Ce qui motive les cybercriminels ce sont les données et les identités à voler et à vendre. De leur côté, les organismes chargés de la réglementation exigent des PME le même investissement que les grandes entreprises en matière de sécurité. Prenons le cas des différentes lois en vigueur qui imposent aux entreprises de divulguer les atteintes à l'intégrité de leurs données. Elles ne s'appuient pas sur la taille de l'entreprise, mais sur le volume et le type de données clients qui ont été pillées. Et, même s'il peut y avoir de légères différences dans la manière dont la réglementation (HIPAA, PCI DSS et autres) affecte les entreprises de petite et moyenne taille, leur impact global reste le même.

- **Failles logicielles : une préoccupation toujours plus importante**
  Le nombre de vulnérabilités logicielles annoncé chaque jour ne montre aucun signe de fléchissement. Selon la liste Common Vulnerabilities and Exposures commanditée par la National Cyber Security Division du département américain de la sécurité intérieure, plus de 3500 failles ont été rapportées au cours des trois premiers trimestres de l'année 2010, soit plus de 10 nouvelles failles logicielles annoncées chaque jour. Et, ces vulnérabilités, qui permettent à un grand nombre de codes malveillants et de pirates d'accéder à des systèmes protégés, sont également nuisibles aux entreprises de grande et petite taille. Ce ne sont pas uniquement les systèmes d'exploitation du poste client, les serveurs et les logiciels qui sont concernés. Mais aussi les applications Web. Selon une récente étude publiée par le cabinet Dasient spécialisé dans la sécurité sur le Web, plus d'un million de sites Web ont été affectés par des codes malveillants en l'espace de 3 mois en 2010.

- **Extension du risque métier aux partenaires, fournisseurs et autres parties prenantes**
  Toutes les entreprises sont sous pression interne et externe. De plus en plus, les entreprises exigent de voir les plans de gestion de la sécurité et des risques de ceux avec qui elles travaillent beaucoup. Elles souhaitent connaître leurs procédures de reprise après incident et de continuité de l'activité. Elles veulent savoir comment sont gérés les moyens de défenses. Et elles souhaitent savoir comment leurs informations confidentielles sont protégées.

QUALYS®

Malheureusement, même si menaces de sécurité et contraintes de conformité à la réglementation affectent toutes les sociétés, ce sont les petites et moyennes entreprises qui ne disposent souvent pas du personnel ou du budget approprié pour combattre efficacement les menaces et garantir la conformité. Le rapport rédigé par Applied Research et publié par Symantec indique que les PME consacrent chaque année deux tiers du temps alloué à l'administration informatique et 51 000 dollars aux problèmes de sécurité. Soit deux fois plus de temps et 27,5% de budget de plus que ce qu'elles consacrent à d'autres domaines ayant trait à l'informatique. C'est tout simplement beaucoup trop cher payé pour la sécurité.

> Les entreprises de petite et moyenne taille consacrent aujourd'hui 66% du temps d'administration informatique à la sécurité.

Et nos clients nous disent la même chose. Ils nous expliquent qu'ils perdent trop de temps à installer, mettre à jour et administrer des logiciels et du matériel dans le cadre des initiatives de sécurité qu'ils prennent. Le présent article explique comment les entreprises avec un budget restreint et peu de ressources peuvent réduire les risques et se conformer à la réglementation de manière simple, fiable et économique.

POURQUOI LES APPROCHES TRADITIONNELLES DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION ÉCHOUENT

Pour tenter de maintenir ces coûts au niveau le plus bas possible, nombre d'entreprises se tournent vers les logiciels Open Source et les logiciels commerciaux les moins coûteux qu'elles peuvent trouver. Même si cela leur permet d'économiser quelques euros sur leur budget, ces économies de coût ne sont en fait qu'une illusion. En effet, ce n'est généralement pas l'achat du logiciel qui induit des coûts sur le long terme, comme nous l'avons vu précédemment, mais les moyens, notamment humains, mobilisés à cette fin. Bâtir et maintenir l'infrastructure, mettre à jour et adapter l'application et exécuter les logiciels coûte effectivement cher.

Le résultat net ? Les initiatives de sécurité échouent : les outils s'avèrent difficiles à administrer, ils exigent des équipes d'experts dédiées et les rapports produits fournissent des résultats contradictoires et trop souvent imprécis. Ainsi, les objectifs en matière de conformité et de sécurité ne sont pas atteints et les logiciels s'avèrent trop onéreux à maintenir et difficiles à utiliser. Et au bout du compte, les outils contraignants ne sont pas utilisés. Si bien que les évaluations et la remédiation des vulnérabilités ne sont pas réalisées, que les politiques des firewalls ne sont pas mises à jour et que les failles sur des serveurs Web s'accumulent au fur et à mesure. Enfin, les failles de sécurité et le nombre d'attaques réussies contre l'entreprise augmentent tandis que l'obligation de conformité n'est pas respectée.

LA GRANDE MIGRATION VERS L'INFORMATIQUE DANS LE CLOUD

C'est notamment pour éviter les coûts et la complexité des logiciels traditionnels que de nombreuses entreprises se tournent vers des solutions dans les nuages (Cloud) et des logiciels fournis sous la forme de services (SaaS). La plupart d'entre nous connaissent désormais les avantages du Cloud et du SaaS : économie, rentabilité rapide, souplesse et paiement en fonction de l'utilisation. Par exemple, contrairement au déploiement de correctifs réalisé par chaque entreprise et qui implique nécessairement de répéter l'opération pour chaque système et chaque installation, toutes les entreprises bénéficient instantanément des

correctifs lorsque les fournisseurs SaaS mettent à jour leurs applications logicielles. Sont ainsi résolus la plupart des problèmes de sécurité, notamment les problèmes de correctifs et de configurations logicielles, qui entravent aujourd'hui les systèmes technologiques de l'entreprise. Ce n'est donc plus à l'utilisateur mais au fournisseur de services logiciels qu'incombe l'essentiel du maintien de la sécurité d'une application.

Les avantages pour l'activité, les économies de coût et la simplification sont trop importants pour que les entreprises les ignorent. C'est pourquoi toujours plus d'applications de gestion de la sécurité et des risques migrent vers le Cloud. Cela concerne aussi bien la messagerie que le filtrage du contenu, la reprise après incident que la continuité de l'activité ou encore la gestion des vulnérabilités et bien d'autres processus et technologies. Tirer parti d'une gestion des risques en pleine mutation est l'une des plus importantes mesures qu'une entreprise peut prendre pour gérer des coûts informatiques en hausse constante.

Cette tendance aux applications dans le Cloud et SaaS est nourrie par la nécessité d'innover, de simplifier et de réduire les coûts.

Cette tendance aux applications dans le Cloud et SaaS est nourrie par la nécessité d'innover, de simplifier et de réduire les coûts. Grâce à cette conception à la demande de la sécurité et de la conformité des ressources informatiques, des entreprises de toute taille sont en mesure de gérer de manière cohérente les vulnérabilités et la conformité aux politiques.

L'une des principales caractéristiques de la sécurité dans le Cloudest l'absence d'équipements ou de logiciels à déployer à travers l'entreprise. En effet, c'est le fournisseur SaaS qui héberge ces ressources dans des centres de données sécurisés. En outre, sans coûts d'investissement, l'entreprise peut contrôler ses coûts. Les autres avantages de la sécurité fournie via le Cloud et des services SaaS pour les PME sont notamment :

- **Un minimum de matériel**
  Puisque peu voire aucun équipement n'est nécessaire sur site, les entreprises peuvent déployer le service dans le Cloudavec une relative aisance.

- **Aucun tracas**
  L'informatique dans le Cloud peut être opérationnelle en quelques minutes ou quelques heures et l'utilisation du Web comme moyen de communication vers les centres de données du fournisseur augmente réellement la disponibilité du service pour l'entreprise. En outre, chaque fois que l'entreprise sollicite du service, le fournisseur lui envoie automatiquement les dernières mises à niveau fonctionnelles et améliorations apportées au service.

- **Paiement en fonction de l'utilisation**
  L'application dans le Cloud ne s'exécute que lorsqu'elle est demandée, ce qui permet à l'entreprise de maîtriser parfaitement les coûts grâce au modèle de règlement en fonction de l'utilisation du service.

- **Fourniture des toutes dernières informations disponibles sur les menaces**
  Identifier les vulnérabilités les plus récentes, les codes malveillants ou un site Web non conforme nécessite une équipe de chercheurs dédiée pour identifier la menace et actualiser le processus d'inspection de la sécurité. L'approche dans les nuages fournit les informations les plus récentes chaque fois que l'entreprise utilise le service.

SOLUTIONS QUALYS À LA DEMANDE POUR LA GESTION DES RISQUES DE SÉCURITÉ INFORMATIQUE ET DE LA CONFORMITÉ

Reconnu comme le principal fournisseur de solutions à la demande pour la gestion des risques de sécurité informatique et de la conformité, Qualys permet aux entreprises de toute taille de garantir facilement, et à moindre coût, la sécurité et la conformité à la réglementation de leurs systèmes technologiques métier. En outre, avec Qualys, les entreprises peuvent renforcer la sécurité de leurs réseaux et de leurs applications et réaliser des audits de sécurité automatisés pour garantir la conformité à la réglementation et l'application des politiques de sécurité internes.

Qualys est le seul fournisseur à proposer ces solutions via une plate-forme unique de logiciels fournis sous la forme de services (SaaS) : QualysGuard. Déployables en quelques heures seulement partout dans le monde, toutes les solutions Qualys à la demande fournissent une vue immédiate de l'état de la sécurité et de la conformité des entreprises utilisatrices. QualysGuard est la solution de sécurité à la demande la plus déployée à travers le monde avec plus de 500 millions d'audits IP par an.

S'appuyant sur une plate-forme SaaS novatrice, QualysGuard® Security and Compliance Suite comprend le service de gestion des vulnérabilités à la pointe du marché de Qualys ainsi qu'une puissante solution de mise en conformité de l'activité informatique, une analyse complète des applications Web et des services de détection des codes malveillants. Ainsi, où que se trouvent les vulnérabilités ou les menaces, QualysGuard est là pour renforcer l'infrastructure et atténuer les menaces.

Pour plus d'informations, rendez-vous sur http://www.qualys.com

QualysGuard IT Security & Compliance Suite pour les PME

Tout ce dont une entreprise a besoin pour gérer les risques de sécurité pour le réseau et les applications ainsi que la conformité aux politiques.

La suite QualysGuard automatise le processus de gestion des vulnérabilités et de conformité aux politiques en fournissant la découverte et la cartographie du réseau, la classification des actifs par priorité, le reporting de l'évaluation des vulnérabilités ainsi que le suivi de la remédiation, le tout en fonction du risque pour l'activité de l'entreprise. Grâce aux fonctionnalités de conformité aux politiques, il est possible d'auditer, d'appliquer et de renseigner la conformité aux politiques de sécurité interne et à la réglementation externe.

Les principaux composants de QualysGuard Security and Compliance Suite sont :

QualysGuard Vulnerability Management
Gestion évolutive des risques de sécurité et des vulnérabilités déployable à l'échelle mondiale

QualysGuard Policy Compliance
Définition, audit et renseignement sur la conformité de la sécurité informatique

QualysGuard PCI Compliance
Validation automatisée de la conformité PCI pour les commerçants et les acquiring banks

QualysGuard Web Application Scanning
Évaluation et reporting automatisés de la sécurité des applications Web

Qualys SECURE Seal
Service de test de sécurité et sceau de sécurité pour sites Web qui analyse les vulnérabilités, les codes malveillants et valide le certificat SSL

QUALYS®