

Fournisseur de services de sécurité ? Cinq signes d'urgence

Sécurité

Posté par : JPilo

Publié le : 7/2/2017 13:00:00

Pour les PME, la gestion de la sécurité réseau apparaît de plus en plus comme un chemin de croix. Selon une étude 2016 du cabinet Ponemon, 69% des PME aux Etats Unis ne disposent pas du budget ou du savoir-faire en interne pour assurer un bon niveau en matière de cyber sécurité.

En fait, plus de la moitié des PME interrogées dans l'étude ont fait l'objet d'une attaque au cours de l'année passée, avec un préjudice moyen de près de 900.000\$. Ce n'est pas surprenant.

Les cybers criminels attaquent directement les PME car elles représentent des proies plus faciles, elles peuvent servir de relais pour attaquer des entreprises plus grosses, et parce que des changements dans le "dark web" ont rendu plus intéressante la vente de petits volumes de numéros de carte bancaire et d'informations personnelles.

Himanshu Verma, Director of Product Management chez WatchGuard Technologies

Traditionnellement, les petites entreprises concentrent leurs faibles ressources informatiques sur tout sauf la sécurité réseau. Pour résoudre ce problème, beaucoup se sont tournés vers le cloud et de petits fournisseurs locaux de services managés (MSPs) pour répondre à leurs besoins informatiques.

En effet, de nouvelles solutions de sécurité permettent désormais aux MSPs traditionnels de rajouter facilement à leur offre en direction des PME des services de sécurité tels que la prévention, la détection et des capacités de réponse sous la forme d'abonnements supplémentaires abordables et sans grandes difficultés techniques. Ceci a créé un nouveau type de service qui est offert par les fournisseurs de services managés de sécurité, ou MSSP.

Mais comment les PME peuvent-elles savoir quand elles doivent se tourner vers un prestataire extérieur pour leurs besoins de sécurité ? Voici cinq signes qui montrent qu'il serait temps de décrocher son téléphone et d'appeler un MSSP :

1. Ressources et Savoir-faire Limités au sein d'une Organisation : L'organisation dispose d'une équipe informatique limitée sans l'expérience requise pour gérer les menaces émergentes aujourd'hui. Elle se retrouve souvent à gérer les incidents de sécurité en mode réactif. De plus, elle n'a pas les ressources pour configurer, contrôler et mettre à jour ses produits de sécurité pour garantir une protection adéquate sur la durée.
2. Restrictions de Budget : L'organisation ne possède pas de budget alloué à la sécurité informatique. Dans la majorité des cas, la sécurité ne figure pas dans le budget des PME (51 pour cent des PME interrogées récemment par Experian n'ont alloué aucun budget à la protection contre les cybers attaques), et jusqu'à un tiers, les services managés de sécurité sont restés un luxe réservé uniquement aux grandes entreprises.

Toutefois, avec l'émergence de menaces croissantes ciblant directement les PME et l'introduction de solutions de sécurité conçues dans un souci de facilité de gestion et de contrôle, des MSPs traditionnels ajoutent des services de sécurité par abonnement (security as a service) à leur portefeuille de solutions pour répondre aux besoins des petites entreprises.

3. Manque de visibilité sur les Infrastructures IT : L'entreprise sait-elle exactement quelles données et quelles ressources informatiques elle utilise ? Les PME n'ont souvent pas une visibilité suffisante sur les ressources qu'elles consomment, où celles-ci résident, et comment elles communiquent entre elles. Quand il s'agit d'un ordinateur portable utilisant un logiciel bureautique, ou une solution de point de vente exploitant une application SaaS, la capacité à identifier quelles données sont effectivement utilisées, où ces données sont stockées, et comment elles sont traitées par les utilisateurs et les applications est essentielle pour garantir leur sécurité.

Les PME ont également tendance à adopter des pratiques telles que «Bring your own Device» et «Bring your own Identity» pour simplifier leurs relations avec leurs clients et aider leurs employés à être aussi productifs que possible. Ceci mène à des procédures de contrôle très souples qui créent des risques de sécurité et des complexités imprévisibles, et rendent encore plus difficile pour une entreprise de comprendre ses ressources informatiques.

Les MSSPs peuvent aider à identifier et remédier à ces nouveaux risques de sécurité avec de nouveaux services de contrôle et de reporting, mais aussi à concevoir une infrastructure qui garantisse la mise en œuvre des politiques de sécurité adéquates, tout en continuant à satisfaire les besoins en matière de productivité et de facilité d'utilisation.

4. Un Ecosystème d'Entreprise Vulnérable : Une entreprise interagit avec de multiples fournisseurs et d'autres organisations, et souvent ses applications résident dans un écosystème plus large. Si elle est en liaison permanente ou contractuelle avec une entreprise ou une organisation partenaire, par exemple dans la santé, l'hôtellerie ou les services financiers, des criminels pourront tenter d'atteindre son système informatique en lançant une attaque sur l'un de ses partenaires directs ou indirects. Même si une entreprise est certaine que son activité ne présente aucun intérêt pour des attaquants, l'assistance d'un MSSP l'aidera à protéger ses relations avec ses partenaires.

5. Conformité à être ou ne pas être : Une entreprise respecte-t-elle les normes standards de sécurité dans son domaine d'activité, telles que PCI 3.0 ? La conformité et les réglementations sont généralement ce qui incite les entreprises à mettre en place des pratiques de sécurité. Les MSSPs utilisent des techniques complètes de reporting afin d'identifier les règles de conformité et les manquements des entreprises en la matière. Si celles-ci ont des doutes sur les normes de sécurité en vigueur dans leur industrie, faire appel à un expert dans ce domaine peut être préférable si cela permet d'éviter des investissements lourds.

Les PME sont désormais des cibles de choix pour les cybers criminels. En 2016, nombre d'entre elles ont fait l'objet en particulier d'attaques de «phishing» et touchant des points de vente. Pour relever ces défis de sécurité, elles doivent se montrer vigilantes dans la protection de leurs employés, de leurs clients et de leurs partenaires. Si elles sont confrontées à l'un des cinq signes cités plus haut, elles doivent sérieusement envisager de s'adresser à un partenaire extérieur pour assurer leur sécurité.