Fournisseur de services de sÃ©curitÃ© ? Cinq signes d'urgence
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 7/2/2017 13:00:00

Pour les PME, la gestion de la sÃ©curitÃ© rÃ©seau sâ□□apparente de plus en plus comme un chemin de croix. Selon une Ã©tude 2016 du cabinet Ponemon, 69% des PME aux Etats Unis ne disposent pas du budget ou du savoir-faire en interne pour sâ□□assurer un bon niveau en matiÃ¨re de cyber sÃ©curitÃ©.

En fait, plus de la moitiÃ© des PME interrogÃ©es dans lâ□□Ã©tude ont fait lâ□□objet dâ□□une attaque au cours de lâ□□annÃ©e passÃ©e, avec un prÃ©judice moyen de prÃ¨s de 900.000$. Ce nâ□□est pas surprenant.

Les cybers criminels attaquent dÃ©libÃ©rÃ©ment les PME car elles reprÃ©sentent des proies plus faciles, elles peuvent servir de relais pour attaquer des entreprises plus grosses, et parce que des changements dans le â□□dark webâ□□ ont rendu plus intÃ©ressante la vente de petits volumes de numÃ©ros de carte bancaire et dâ□□informations personnelles.

Himanshu Verma, Director of Product Management chez WatchGuard Technologies

Traditionnellement, les petites entreprises concentrent leurs faibles ressources informatiques sur tout sauf la sÃ©curitÃ© rÃ©seau. Pour rÃ©soudre ce problÃ¨me, beaucoup se sont dÃ©jÃ tournÃ©es vers le cloud et de petits fournisseurs locaux de services managÃ©s (MSPs) pour rÃ©pondre Ã leurs besoins informatiques.

En effet, de nouvelles solutions de sÃ©curitÃ© permettent dÃ©sormais aux MSPs traditionnels de rajouter facilement Ã leur offre en direction des PME des services de sÃ©curitÃ© tels que la prÃ©vention, la dÃ©tection et des capacitÃ©s de rÃ©ponse sous la forme dâ□□abonnements supplÃ©mentaires abordables et sans grandes difficultÃ©s techniques. Ceci a crÃ©Ã© un nouveau type de service â□□ celui offert par les fournisseurs de services managÃ©s de sÃ©curitÃ©, ou MSSP.

Mais comment les PME peuvent-elles savoir quand elles doivent se tourner vers un prestataire extÃ©rieur pour leurs besoins de sÃ©curitÃ© ? Voici cinq signes qui montrent quâ□□il serait temps de dÃ©crocher son tÃ©lÃ©phone et dâ□□appeler un MSSP :

1. Ressources et Savoir-faire LimitÃ©s au sein dâ□□une Organisation : Lâ□□organisation dispose dâ□□une Ã©quipe informatique limitÃ©e sans lâ□□expÃ©rience requise pour gÃ©rer les menaces Ã©mergentes dâ□□aujourdâ□□hui. Elle se retrouve souvent Ã gÃ©rer les incidents de sÃ©curitÃ© en mode rÃ©actif. De plus, elle nâ□□a pas les ressources pour configurer, contrÃ´ler et mettre Ã jour ses produits de sÃ©curitÃ© pour garantir une protection adÃ©quate sur la durÃ©e.

2. Restrictions de Budget : Lâ□□organisation ne possÃ¨de pas de budget allouÃ© Ã la sÃ©curitÃ© informatique. Dans la majoritÃ© des cas, la sÃ©curitÃ© ne figure pas dans le budget des PME (51 pour cent des PME interrogÃ©es rÃ©cemment par Experian nâ□□ont allouÃ© aucun budget Ã la protection contre les cybers attaques), et jusquâ□□Ã un passÃ© rÃ©cent, les services managÃ©s de sÃ©curitÃ© sont restÃ©s un luxe rÃ©servÃ© uniquement aux grandes entreprises.

Toutefois, avec lâ□□Ã©mergence de menaces croissantes ciblant directement les PME et lâ□□introduction de solutions de sÃ©curitÃ© conÃ§ues dans un souci de facilitÃ© de gestion et de contrÃ´le, des MSPs traditionnels ajoutent des services de sÃ©curitÃ© par abonnement (security as a service) Ã leur portefeuille de solutions pour rÃ©pondre aux besoins des petites entreprises.

3. Manque de VisibilitÃ© sur les Infrastructures IT : Lâ□□entreprise sait-elle exactement quelles donnÃ©es et quelles ressources informatiques elle utilise ? Les PME nâ□□ont souvent pas une visibilitÃ© suffisante sur les ressources quâ□□elles consomment, oÃ¹ celles-ci rÃ©sident, et comment elles communiquent entre elles. Quâ□□il sâ□□agisse dâ□□un ordinateur portable utilisant un logiciel bureautique, ou une solution de point de vente exploitant une application SaaS, la capacitÃ© Ã identifier quelles donnÃ©es sont effectivement utilisÃ©es, oÃ¹ ces donnÃ©es sont stockÃ©es, et comment elles sont traitÃ©es par les utilisateurs et les applications est essentielle pour garantir leur sÃ©curitÃ©.

Les PME ont Ã©galement tendance Ã adopter des pratiques telles que â□□Bring your own Deviceâ□□ et â□□Bring your own Identityâ□□ pour simplifier leurs relations avec leurs clients et aider leurs employÃ©s Ã Ãªtre aussi productifs que possible. Ceci mÃ¨ne Ã des procÃ©dures de contrÃ´le trÃ¨s souples qui crÃ©ent des risques de sÃ©curitÃ© et des complexitÃ©s imprÃ©visibles, et rendent encore plus difficile pour une entreprise de comprendre ses ressources informatiques.

Les MSSPs peuvent aider Ã identifier et remÃ©dier Ã ces nouveaux risques de sÃ©curitÃ© avec de nouveaux services de contrÃ´le et de reporting, mais aussi Ã concevoir une infrastructure qui garantisse la mise en Å□uvre des politiques de sÃ©curitÃ© adÃ©quates, tout en continuant Ã satisfaire les besoins en matiÃ¨re de productivitÃ© et de facilitÃ© dâ□□utilisation.

4. Un EcosystÃ¨me dâ□□Entreprise VulnÃ©rable : Une entreprise interagit avec de multiples fournisseurs et dâ□□autres organisations, et souvent ses applications rÃ©sident dans un Ã©cosystÃ¨me plus large. Si elle est en liaison permanente ou contractuelle avec une entreprise ou une organisation partenaire, par exemple dans la santÃ©, lâ□□hÃ´tellerie ou les services financiers, des criminels pourront tenter dâ□□atteindre son systÃ¨me informatique en lanÃ§ant une attaque sur lâ□□un de ses partenaires directs ou indirects. MÃªme si une entreprise est certaine que son activitÃ© ne prÃ©sente aucun intÃ©rÃªt pour des attaquants, lâ□□assistance dâ□□un MSSP lâ□□aidera Ã protÃ©ger ses relations avec ses partenaires.

5. ConformitÃ© â□□ Etre ou ne pas Ãªtre : Une entreprise respecte-t-elle les normes standards de sÃ©curitÃ© dans son domaine dâ□□activitÃ©, telles que PCI 3.0 ? La conformitÃ© et les rÃ©glementations sont gÃ©nÃ©ralement ce qui incite les entreprises Ã mettre en place des pratiques de sÃ©curitÃ©. Les MSSPs utilisent des techniques complÃ¨tes de reporting afin dâ□□identifier les rÃ¨gles de conformitÃ© et les manquements des entreprises en la matiÃ¨re. Si celles-ci ont des doutes sur les normes de sÃ©curitÃ© en vigueur dans leur industrie, faire appel Ã un expert dans ce domaine peut Ãªtre prÃ©fÃ©rable si cela permet dâ□□Ã©viter des investissements lourds.

Les PME sont dÃ©sormais des cibles de choix pour les cybers criminels. En 2016, nombre dâ□□entre elles ont fait lâ□□objet en particulier dâ□□attaques de â□□phishingâ□□ et touchant des points de vente. Pour relever ces dÃ©fis de sÃ©curitÃ©, elles doivent se montrer vigilantes dans la protection de leurs employÃ©s, de leurs clients et de leurs partenaires. Si elles sont confrontÃ©es Ã lâ□□un des cinq signes citÃ©s plus haut, elles doivent sÃ©rieusement envisager de sâ□□adresser Ã un partenaire extÃ©rieur pour assurer leur sÃ©curitÃ©.