Menaces internes : les ignorer câ□□est sâ□□exposer
Internet
PostÃ© par : JulieM
PubliÃ©e le : 12/12/2017 13:00:00

Face Ã lâ□□hypermÃ©diatisation des plus grandes menaces informatiques touchant les entreprises au niveau mondial, on peut lÃ©gitimement penser quâ□□elles Ã©manent toutes de logiciels de pointe malveillants ou de hackers commanditÃ©s par des Ã□tats. Mais si on pose la question Ã un professionnel de la sÃ©curitÃ©, il rÃ©pondra que la vÃ©ritable menace est bien plus proche quâ□□on ne le pense.

Il y a tout juste quelques mois, Verizon et Bupa - deux marques Ã la rÃ©putation mondiale - ont dÃ» faire face Ã des fuites de donnÃ©es considÃ©rables, affectant des millions de clients. Toutefois, dans les deux cas, lâ□□auteur nâ□□Ã©tait pas extÃ©rieur Ã lâ□□entreprise, mais bel et bien une ressource localisÃ©e en interne, possÃ©dant un accÃ¨s autorisÃ© Ã des donnÃ©es sensibles.

Dans le cas de Bupa, un employÃ© mÃ©content a dÃ©libÃ©rÃ©ment divulguÃ© plus de 500â□□000 dossiers clients en ligne.

Pour Verizon, câ□□Ã©tait une simple erreur de configuration dâ□□un collaborateur qui a entraÃ®nÃ© lâ□□exposition des informations personnelles de plus de 6 millions de clients.

Les entreprises restent focalisÃ©es sur les menaces externes

Le dÃ©fi des menaces internes rÃ©side dans la multiplicitÃ© des facettes qui les caractÃ©risent et qui rend toute protection complexe.

Les employÃ©s en interne, les sous-traitants et autres parties prenantes ont souvent besoin dâ□□accÃ©der Ã des ressources sensibles pour accomplir leur travail.

Il est, de fait, beaucoup plus difficile de se protÃ©ger des actes accidentels et malveillants que de mettre ces donnÃ©es en danger. Et mÃªme si la menace interne est claire, la majoritÃ© des entreprises continuent Ã la sous-estimer.

Dans une rÃ©cente enquÃªte menÃ©e au salon de la sÃ©curitÃ© Security BSides London, 71 % des professionnels de la sÃ©curitÃ© ont indiquÃ© considÃ©rer que les entreprises devraient sâ□□inquiÃ©ter davantage des menaces internes que ce quâ□□elles ne font actuellement.

En outre, 47 % des participants ont Ã©tÃ© jusquâ□□Ã dire que les menaces internes et les utilisateurs non Ã©duquÃ©s constituent la menace de sÃ©curitÃ© la plus nÃ©gligÃ©e par les entreprises. PrÃ¨s de la moitiÃ© des professionnels de la sÃ©curitÃ© considÃ¨rent que les menaces les plus fortes sont celles provoquÃ©es par les Ã□tats-nations comme la CorÃ©e du Nord ou la Russie.

MalgrÃ© leurs inquiÃ©tudes Ã lâ□□Ã©gard des menaces internes, 92 % des participants reconnaissent que lâ□□industrie dans sa globalitÃ© continue de dÃ©ployer bien plus de ressources pour contrer les menaces externes.

Cette approche de type Â«â□□chÃ¢teau fortâ□□Â» de la cybersÃ©curitÃ© prÃ©vaut depuis des annÃ©es, et les fournisseurs proposent de plus en plus de couches de dÃ©fense du pÃ©rimÃ¨tre pour aider Ã construire des murailles plus hautes et Ã creuser des douves plus profondes. Mais quelle est lâ□□utilitÃ© de ces dÃ©fenses si la menace est dÃ©jÃ Ã lâ□□intÃ©rieurâ□□?

Dans le cas de lâ□□attaque rÃ©cente de Verizon, un tiers, qui transfÃ©rait des donnÃ©es client vers un nouvel espace de stockage Cloud, a commis une erreur de configuration dâ□□accÃ¨s, ce qui a engendrÃ© un accÃ¨s externe accidentel. Si la menace interne Ã©tait vue comme un risque rÃ©Ã©l, elle serait vÃ©ritablement prise au sÃ©rieux.

Mais cela ne semble pas Ãªtre le cas dans la plupart des conseils dâ□□administration. Dans lâ□□enquÃªte Security BSides London, seuls 9 % des interrogÃ©s ont indiquÃ© trouver que la direction supÃ©rieure de leur entreprise prenait de bonnes dÃ©cisions pour la stratÃ©gie et les dÃ©penses de sÃ©curitÃ©.

Menaces internes : comment rÃ©duire les risques ?

Comme pour de nombreux problÃ¨mes de sÃ©curitÃ©, il nâ□□est pas toujours nÃ©cessaire dâ□□investir beaucoup pour rÃ©duire considÃ©rablement la menace. Des investissements stratÃ©giques dans deux domaines essentiels peuvent faire la diffÃ©rence :

Ã□ducation et information : le moyen de dÃ©fense le plus efficace contre les menaces internes accidentelles rÃ©side dans une Ã©ducation et une information permettant dâ□□Ã©veiller les

consciences. La grande majoritÃ© des fuites de donnÃ©es accidentelles ont lieu parce que les employÃ©s ne sont tout simplement pas conscients des consÃ©quences de leurs actes.

Une formation rÃ©guliÃ¨re sur la sÃ©curitÃ© des donnÃ©es contribue Ã rÃ©duire les cas de nÃ©gligence et Ã sâ□□assurer que les employÃ©s rÃ©flÃ©chissent avant dâ□□agir dÃ¨s que des donnÃ©es sensibles sont en jeu. Dans cette optique, il est important de fournir des rappels rÃ©guliers pour informer les employÃ©s des nouvelles procÃ©dures ou technologies de donnÃ©es mises en Å□uvre.

Une approche de la sÃ©curitÃ© plus centrÃ©e sur les donnÃ©es : malheureusement, toutes les menaces internes ne sont pas intentionnelles, comme lâ□□illustre la rÃ©cente fuite de donnÃ©es de Bupa.

Dans ces circonstances, une couche de technologie supplÃ©mentaire peut aider Ã empÃªcher la fuite de donnÃ©es sensibles.

Si lâ□□Ã©ducation et lâ□□information ne suffisent pas, les Ã©quipes sÃ©curitÃ© doivent pouvoir comprendre et visualiser lâ□□utilisation des donnÃ©es, afin de pouvoir repÃ©rer rapidement toute activitÃ© inhabituelle pouvant indiquer un risque. De plus, des politiques automatiques concernant lâ□□accÃ¨s aux donnÃ©es, voire qui empÃªchent les employÃ©s de copier, transfÃ©rer ou supprimer des donnÃ©es sensibles, peuvent aider Ã contrer les fuites ou actes malvaillants.

MalgrÃ© lâ□□accumulation des preuves attestant des risques engendrÃ©s par les menaces internes pour les entreprises modernes, les personnes qui dÃ©cident des dÃ©penses de sÃ©curitÃ© restent obstinÃ©ment focalisÃ©es sur les risques externes.

Â Bien que cela reprÃ©sente une source de frustration croissante pour les professionnels de la sÃ©curitÃ©, la bonne nouvelle est quâ□□il nâ□□est pas nÃ©cessaire dâ□□investir des fortunes pour amÃ©liorer considÃ©rablement la protection contre les menaces internes.

Des dÃ©penses stratÃ©giques focalisÃ©es sur lâ□□Ã©ducation et lâ□□information, combinÃ©es Ã des technologies tenant compte des donnÃ©es, peuvent contribuer Ã dÃ©courager les employÃ©s les plus malveillants ou insouciants, et Ã garantir que les donnÃ©es sensibles nâ□□arrivent jamais entre de mauvaises mains.

*Lâ□□enquÃªte, parrainÃ©e par Digital Guardian, a collectÃ© les rÃ©ponses de 187 professionnels de lâ□□industrie de la sÃ©curitÃ© travaillant Ã plein temps qui participaient au salon Security BSides London le 7 juin 2017.

Thomas Fischer, Global Security Advocate chez Digital Guardian