La sÃ©curitÃ© des entreprises nâ□□est pas assurÃ©e
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 18/11/2013 15:00:00

Les incidents de sÃ©curitÃ© dÃ©tectÃ©s ont augmentÃ© de 25% par rapport Ã lâ□□annÃ©e derniÃ¨re dans le monde
La 15Ã¨me Ã©dition de lâ□□Ã©tude PwC sur la sÃ©curitÃ© de lâ□□information et la protection des donnÃ©es rÃ©vÃ¨le que les entreprises ont enregistrÃ© une hausse de 25% du nombre dâ□□incidents de sÃ©curitÃ© dans le monde. Si les entreprises ont augmentÃ© leur budget de sÃ©curitÃ© de 51% par rapport Ã lâ□□annÃ©e derniÃ¨re, il reste trop limitÃ© et leur stratÃ©gie peu adaptÃ©e. Elles s'appuient encore trop souvent sur des outils et des postures obsolÃ¨tes qui ne leur permettent pas de se dÃ©fendre contre les menaces internes et externes, toujours plus innovantes.

Un coÃ»t des incidents de sÃ©curitÃ© dÃ©cuplÃ© pour les mauvais Ã©lÃ¨ves Les incidents de sÃ©curitÃ© dÃ©tectÃ©s ont augmentÃ© de 25% par rapport Ã lâ□□annÃ©e derniÃ¨re. Une hausse qui sâ□□explique par deux faits : une augmentation des attaques toujours plus sophistiquÃ©es, mais aussi une amÃ©lioration de la capacitÃ© des organisations Ã dÃ©tecter les intrusions dans leur systÃ¨me dâ□□information.

Une prise en compte de la sÃ©curitÃ© dans les entreprises qui se traduit par une augmentation du budget moyen de sÃ©curitÃ© de 51% par rapport Ã 2012, pour atteindre 4,3 millions de dollars cette annÃ©e. Une croissance qui doit nÃ©anmoins Ãªtre relativisÃ©e : les dÃ©penses liÃ©es Ã la sÃ©curitÃ© ne reprÃ©sentent que 3,8% de lâ□□ensemble des dÃ©penses IT en 2013, ce qui reste un investissement trop faible.
Une nÃ©cessitÃ© dâ□□autant plus forte que lâ□□Ã©tude souligne une hausse du coÃ»t des incidents. Ainsi, le nombre de rÃ©pondants ayant dÃ©clarÃ© une perte de plus de 10 millions de dollars a augmentÃ© de 51% depuis 2011. Dâ□□autre part, si le coÃ»t moyen dâ□□un incident de sÃ©curitÃ© est Ã©tabli Ã 531$, il Ã©volue selon le niveau de sÃ©curitÃ© de lâ□□entreprise. Ainsi les organisations ayant Ã©tÃ© identifiÃ©es comme leaders dans lâ□□Ã©tude enregistrent un coÃ»t moyen de 421$, quand les entreprises les moins prÃ©parÃ©es reportent un coÃ»t moyen de 635$ par incident.
Â« Ces chiffres montrent combien il est urgent pour les entreprises de prendre conscience de lâ□□impact dâ□□une stratÃ©gie de sÃ©curitÃ© non adaptÃ©e. Les entreprises les moins bien prÃ©parÃ©es devront, Ã court et moyen terme, faire face Ã des risques toujours plus Ã©levÃ©s et des coÃ»ts associÃ©s exorbitants, qui affecteront Ã terme leur compÃ©titivitÃ© Â», dÃ©clare Philippe Trouchaud, AssociÃ© PwC spÃ©cialiste de la sÃ©curitÃ© de lâ□□information.

Les salariÃ©s, une menace sous-estimÃ©e par les entreprises La premiÃ¨re source dâ□□incident demeure externe. Ainsi, 32 % des dirigeants attribuent les incidents de sÃ©curitÃ© aux hackers, soit une augmentation de 27 % par rapport Ã l'annÃ©e derniÃ¨re. En revanche, si les attaques menÃ©es par des Etats Ã©trangers sont trÃ¨s mÃ©diatisÃ©es, elles ne reprÃ©sentent que 4% des incidents dÃ©tectÃ©s.
Cependant, les dirigeants interrogÃ©s nous disent que la menace est souvent plus proche de lâ□□entreprise : ainsi, 31% des incidents de sÃ©curitÃ© sont attribuÃ©s Ã des employÃ©s, 27% Ã des anciens collaborateurs (27%) et 16% Ã des prestataires de lâ□□entreprise.

Une menace interne souvent sous-estimÃ©e par les entreprises, qui ne la considÃ¨rent pas comme un rÃ©el risque.

Â« *Cette situation sâ□□explique notamment par le fait que de nombreux collaborateurs et prestataires ont accÃ¨s au rÃ©seau interne de lâ□□entreprise et bÃ©nÃ©ficient dâ□□un niveau de confiance trÃ¨s Ã©levÃ©, voire trop Ã©levÃ©. Il est temps que les entreprises prennent en compte ce risque interne dans la sÃ©curisation de leurs informations* Â», prÃ©cise **Philippe Trouchaud.**

Ces incidents ciblent en prioritÃ© les donnÃ©es des collaborateurs (35%) et des clients (31%), qui sont les plus simples Ã rÃ©cupÃ©rer. Des fuites qui suggÃ¨rent que les efforts de protection de ces donnÃ©es ne sont pas assez efficaces ou ne se concentrent pas sur les bons risques.

L'Europe en retard face aux autres rÃ©gions du monde Depuis quelques annÃ©es, lâ□□Asie-Pacifique a investi massivement en matiÃ¨re de sÃ©curitÃ©. Le budget de la rÃ©gion a ainsi progressÃ© de 85% lâ□□annÃ©e derniÃ¨re, et la Chine se rÃ©vÃ¨le particuliÃ¨rement bien Ã©quipÃ©e. Lâ□□AmÃ©rique du sud investit Ã©galement beaucoup et sâ□□avÃ¨re la rÃ©gion dans laquelle le top management communique le plus sur lâ□□importance de cet enjeu.

A lâ□□opposÃ©, lâ□□Europe connaÃ®t un retard important sur de trÃ¨s nombreux volets. Le budget europÃ©en a ainsi dÃ©clinÃ© de 3% lâ□□annÃ©e derniÃ¨re, alors que les pertes financiÃ¨res dues aux incidents de sÃ©curitÃ© ont cru de 28%.

Lâ□□Europe est plus particuliÃ¨rement en retard sur les aspects suivants : la mise en place de plans de continuitÃ© dâ□□activitÃ©, la formation des collaborateurs et la politique de sÃ©curitÃ© liÃ©e Ã lâ□□usage du mobile.

Les entreprises utilisent les armes d'hier pour combattre les menaces d'aujourd'hui

Des mutations technologiques rapides qui ne sont pas prises en compte Lâ□□usage grandissant des smartphones et tablettes, le recours croissant au Cloud et les frontiÃ¨res de plus en plus floues entre la sphÃ¨re professionnelle et personnelle ont dÃ©multipliÃ© les points dâ□□entrÃ©e et fragilisÃ© les organisations. Pourtant, seules 42% des entreprises ont une stratÃ©gie de sÃ©curitÃ© mobile et 18% dâ□□entre elles ont dÃ©ployÃ© une stratÃ©gie adaptÃ©e Ã lâ□□utilisation du Cloud.

Au-delÃ de ces mutations, on observe une diversification des attaques, notamment via le social engineering (usurpation dâ□□identitÃ©, arnaque au prÃ©sidentâ□¦) qui se base sur la dÃ©stabilisation ou la manipulation des collaborateurs, ainsi que sur la rÃ©cupÃ©ration dâ□□informations disponibles sur Internet (rÃ©seaux sociaux notamment). Ainsi, les attaques deviennent de plus en plus ciblÃ©es, avec un objectif prÃ©cis (gain financier, support Ã des causes) et prennent un caractÃ¨re permanent.

Pourtant, une majoritÃ© dâ□□entreprises adoptent encore des stratÃ©gies de sÃ©curitÃ© basÃ©es essentiellement sur des dÃ©fenses pÃ©rimÃ©triques et passives (pare-feu, antivirus). Ainsi 52% des rÃ©pondants nâ□□ont pas dÃ©ployÃ© de techniques de dÃ©tection des comportements anormaux pour identifier les risques. De plus, certaines technologies Ã©tablies qui sont essentielles Ã la protection des informations sensibles sont sous-utilisÃ©es : 42% n'utilisent pas dâ□□outils de prÃ©vention de perte de donnÃ©es. Aujourdâ□□hui, il est nÃ©cessaire de mettre au point des outils qui permettent dâ□□adopter une posture plus proactive.

Recommandations PwC : une nouvelle approche de la sÃ©curitÃ© basÃ©e sur lâ□□identification des vulnÃ©rabilitÃ©s et la riposte active

Pour faire face Ã ces mutations, PwC recommande aux entreprises dâ□□adopter dâ□□une nouvelle approche en complÃ©tant leur stratÃ©gie de protection dÃ©fensive (interdire, bloquer, freiner) par une stratÃ©gie dâ□□identification et de riposte proactive : il faut dÃ©sormais analyser les menaces liÃ©es aux nouveaux usages et utiliser de nouveaux outils, quâ□□ils relÃ¨vent de solutions techniques ou de comportements.

Les entreprises doivent donc sâ□□Ã©quiper dâ□□outils modernes, technologiques et innovants afin de : â□¢ rÃ©colter et analyser toutes les informations de leurs infrastructures,

â□¢ identifier la typologie des donnÃ©es critiques pour leur activitÃ© et ainsi pouvoir repÃ©rer et bloquer les donnÃ©es jugÃ©es sensibles avant quâ□□elles ne sortent de lâ□□entreprise,

â□¢ assurer un suivi rÃ©gulier des informations clÃ© de lâ□□entreprise afin de pouvoir dÃ©celer

les comportements anormaux et les modÃ¨les qui se reproduisent afin dâ□□anticiper les attaques. Au-delÃ , il est clÃ© de crÃ©er une vÃ©ritable culture interne de la sÃ©curitÃ© qui soit adaptÃ©e aux usages, portÃ©e par le top management et dÃ©ployÃ©e auprÃ¨s de lâ□□ensemble des collaborateurs.