Le piratage informatique Ã des fins politiques et sociales
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 22/3/2012 13:30:00

En 2011, **58 %** des vols de donnÃ©es ont pu Ãªtre attribuÃ©s Ã du hacktivisme, confirme le rapport de Verizon. Une nouvelle tendance en rupture avec les pratiques de compromissions de donnÃ©es de ces derniÃ¨res annÃ©es, majoritairement du fait de **cybercriminels, essentiellement motivÃ©s par le gain financier.**

79 % des attaques analysÃ©es dans le rapport sont opportunistes. **96 %** de toutes les attaques nâ□□Ã©taient pas trÃ¨s difficiles Ã perpÃ©trer, dans le sens oÃ¹ elles ne nÃ©cessitaient ni compÃ©tences avancÃ©es, ni ressources importantes. Et **97 %** des infractions auraient pu Ãªtre Ã©vitÃ©es sans contre-mesures complexes, ni onÃ©reuses de la part de lâ□□entreprise. Le rapport fait ensuite Ã©tat de recommandations pour aider les entreprises grandes et petites Ã se protÃ©ger.

Lâ□□Ã©dition 2012 marque la cinquiÃ¨me annÃ©e de publication du rapport. C'est aussi la deuxiÃ¨me annÃ©e record, en termes de donnÃ©es perdues, depuis que les Ã©quipes Verizon RISK (Research Investigations Solutions Knowledge) ont commencÃ© Ã recueillir des informations en 2004.

Cette annÃ©e, cinq partenaires ont contribuÃ© au rapport par lâ□□apport de donnÃ©es Ã Verizon : les services secrets AmÃ©ricains, la Dutch National High Tech Crime Unit des Pays-Bas, la police fÃ©dÃ©rale Australienne, le service Irlandais Reporting & Information Security Service et la e-Crime Unit de la police centrale londonienne.

Â« GrÃ¢ce Ã la participation de multiples partenaires du monde entier, lâ□□Ã©dition 2012 de notre rapport Data Breach Investigations Report offre une vision de la cyber sÃ©curitÃ© la plus complÃ¨te possible Ã ce jour Â», explique **Wade Baker**, directeur de la gestion du risque chez Verizon. Â« *Notre objectif est dâ□□informer le plus grand nombre sur les pratiques de la cybercriminalitÃ© de sorte que lâ□□industrie de la sÃ©curitÃ© puisse lutter le mieux possible et que les administrations et entreprises dÃ©veloppent leurs propres plans de sÃ©curitÃ© en*

connaissance de cause. Â»

Les conclusions du rapport confirment la dimension internationale de la cybercriminalitÃ© : en effet, les infractions ont Ã©tÃ© perpÃ©trÃ©es depuis 36 pays, contre 22 pays lâ□□an dernier. PrÃ¨s de **70 %** des infractions proviennent dâ□□Europe de lâ□□Est et moins de **25 %** dâ□□AmÃ©rique du Nord.

Les infractions ciblant des donnÃ©es sont majoritairement perpÃ©trÃ©es de lâ□□extÃ©rieur, Ã **98 %** par des agresseurs externes. Il sâ□□agit dâ□□organisations criminelles, de groupes dâ□□activistes, dâ□□anciens employÃ©s, de pirates isolÃ©s, voire dâ□□organisations financÃ©es par dâ□□autres gouvernements. Avec lâ□□intensification des agressions externes, la part des incidents perpÃ©trÃ©s de lâ□□intÃ©rieur est de nouveau Ã la baisse cette annÃ©e (Ã **4 %**). Les partenaires commerciaux sont incriminÃ©s dans moins dâ□□1 % des cas de compromissions de donnÃ©es.

Concernant les mÃ©thodes, les actes de piratage et dâ□□infection par des programmes malveillants sont en hausse. Le piratage est Ã lâ□□origine de **81 %** des compromissions de donnÃ©es et de **99 %** des pertes. Les programmes malveillants sont impliquÃ©s dans **69 %** des infractions et dans **95 %** des dossiers compromis. Le piratage et les programmes malveillants sont les mÃ©thodes prÃ©fÃ©rÃ©es des agresseurs externes, qui peuvent ainsi cibler Ã distance plusieurs victimes en mÃªme temps. Beaucoup dâ□□outils de piratage et de diffusion de programmes malveillants, plutÃ´t simples Ã utiliser, sont mis Ã la disposition des cybercriminels.

Enfin, le dÃ©lai entre la compromission et sa dÃ©tection se mesure toujours en mois, voire en annÃ©es, et non en heures ou en journÃ©es. Enfin, ce sont des tiers qui dÃ©tectent la majoritÃ© des infractions (**92 %**).

Voici dâ□□autres conclusions de lâ□□analyse de 2012 :

â□¢ Lâ□□espionnage industriel , le vol de secrets de fabrication et lâ□□accÃ¨s Ã des informations de propriÃ©tÃ© intellectuelle intÃ©ressent de plus en plus les criminels. Cette tendance, quoique moins frÃ©quente, peut avoir de graves consÃ©quences et des rÃ©percussions sur la sÃ©curitÃ© des donnÃ©es des entreprises, surtout si elle venait Ã se confirmer.

â□¢ Les attaques externes se multiplient. Le hacktivisme Ã©tant prÃ©sent dans plus de la moitiÃ© des infractions, les attaques sont surtout le fait dâ□□agresseurs externes. Seules 4 % des attaques impliquent des employÃ©s.

â□¢ Le piratage et les programmes malveillants dominent. Le recours au piratage et aux programmes malveillants augmente en 2011 de mÃªme que les attaques de lâ□□extÃ©rieur. Le piratage est prÃ©sent dans 81 % des infractions (contre 50 % en 2010) et les programmes malveillants dans 69 % des infractions (contre 49 % en 2010). Ces deux mÃ©thodes sÃ©duisent les agresseurs externes car elles leur permettent dâ□□accÃ©der Ã des donnÃ©es confidentielles en exploitant les failles de sÃ©curitÃ©.

â□¢ Les donnÃ©es dâ□□identification personnelle sont un vrai jackpot pour les criminels. Ces informations, Ã savoir le nom dâ□□une personne, ses coordonnÃ©es, son numÃ©ro de sÃ©curitÃ© sociale, sont de plus en plus recherchÃ©es. En 2011, 95 % des dossiers perdus comportaient de telles informations personnelles contre seulement 1 % en 2010.

â□¢ La conformitÃ© ne garantit pas forcÃ©ment la sÃ©curitÃ©. Les programmes de mise en conformitÃ©, comme le PCI DSS (Payment Card Industry Data Security Standard), offrent des recommandations utiles pour renforcer sa sÃ©curitÃ©, mais la conformitÃ© PCI ne protÃ¨ge pas pour autant les entreprises des attaques.

Â« *A en croire le rapport, bon nombre dâ□□entreprises ignorent quelles procÃ©dures appliquer pour se protÃ©ger des infractions ciblant leurs donnÃ©es* Â», constate **Wade Baker**. Â« *Cette annÃ©e, nous avons distinguÃ© les recommandations Ã lâ□□attention des grandes et plus petites entreprises en espÃ©rant que nos suggestions seront mieux comprises et plus suivies. Nous sommes Ã©galement convaincus quâ□□une plus grande sensibilisation du public aux cyber attaques, de mÃªme que lâ□□information et la formation des utilisateurs sont vitales pour lutter contre la cybercriminalitÃ©.* Â»

Quelques recommandations pour les groupes et grandes entreprises :

1. Supprimer les donnÃ©es inutiles. Sauf rÃ©el motif pour stocker ou transmettre des donnÃ©es, dÃ©truisez-les. Surveillez toutes les donnÃ©es quâ□□il est impÃ©ratif de conserver.

2. Instaurer les contrÃ´les de sÃ©curitÃ© indispensables. Les entreprises doivent veiller Ã ce que des contrÃ´les de sÃ©curitÃ© appropriÃ©s soient effectivement en place et contrÃ´ler rÃ©guliÃ¨rement leur bon fonctionnement.

3. Accorder lâ□□importance quâ□□ils mÃ©ritent aux journaux dâ□□Ã©vÃ©nements . Surveillez les journaux dâ□□Ã©vÃ©nements Ã la recherche dâ□□activitÃ©s suspectes ; câ□□est gÃ©nÃ©ralement ainsi que lâ□□on identifie les infractions.

4. Fonder la stratÃ©gie de sÃ©curitÃ© sur les prioritÃ©s identifiÃ©es. AprÃ¨s avoir Ã©valuÃ© leur exposition aux menaces, les entreprises ont intÃ©rÃªt Ã sâ□□appuyer sur les conclusions pour articuler leur propre stratÃ©gie de sÃ©curitÃ© autour des prioritÃ©s.

Quelques recommandations pour les petites entreprises :

1. Utiliser un pare-feu. Installez un pare-feu au niveau de vos services dâ□□accÃ¨s Ã Internet pour protÃ©ger vos donnÃ©es. Les pirates ne peuvent pas voler ce Ã quoi ils nâ□□ont pas accÃ¨s.

2. Modifier systÃ©matiquement les codes dâ□□accÃ¨s par dÃ©faut. Les terminaux de paiement sur les point de vente (POS systems) et dâ□□autres Ã©quipements sont vendus avec des codes dâ□□accÃ¨s par dÃ©faut. Changez-les systÃ©matiquement pour Ã©viter tout accÃ¨s non autorisÃ©.

3. ContrÃ´ler ses propres fournisseurs. Souvent ce sont des tiers qui gÃ¨rent les pare-feu et les terminaux de paiement sur les points de vente. Les entreprises doivent donc vÃ©rifier que ceux-ci observent bien les recommandations de sÃ©curitÃ© applicables, rÃ©pertoriÃ©es prÃ©cÃ©demment.