Les Services Secrets amÃ©ricains enquÃªtent sur la compromission des donnÃ©es
Internet
PostÃ© par : JulieM
PubliÃ©e le : 29/7/2010 15:00:00

Lâ□□Ã©dition 2010 du Verizon Data Breach Investigations Report, basÃ© pour la toute premiÃ¨re fois sur des **donnÃ©es des Services Secrets amÃ©ricains**, rÃ©vÃ¨le une hausse des compromissions de donnÃ©es liÃ©es Ã des menaces internes et Ã lâ□□utilisation dâ□□outils sociaux au cours de lâ□□annÃ©e 2009.

Les organisations criminelles restent Ã©galement trÃ¨s actives.

Les rÃ©sultats de cette enquÃªte, publiÃ©s ce jour, indiquent Ã©galement un dÃ©clin Â« prometteur Â» du nombre total dâ□□infractions Ã©tudiÃ©es lâ□□annÃ©e derniÃ¨re par rapport Ã 2008.

Le vol de droits dâ□□accÃ¨s apparaÃ®t comme le moyen le plus utilisÃ© pour accÃ©der illÃ©galement aux rÃ©seaux des entreprises en 2009, ce qui souligne une nouvelle fois la nÃ©cessitÃ© de rÃ¨gles de sÃ©curitÃ© strictes aux niveaux des entreprises comme des individus. Le crime organisÃ© Ã©tait Ã lâ□□origine de 85 % des vols de donnÃ©es lâ□□annÃ©e derniÃ¨re.

Une fois encore, les experts en sÃ©curitÃ© de Verizon Business considÃ¨rent que la plupart des compromissions auraient pu Ãªtre Ã©vitÃ©es si les principes Ã©lÃ©mentaires de sÃ©curitÃ© avaient Ã©tÃ© respectÃ©s. En effet, seuls 4 % des cas auraient nÃ©cessitÃ© des mesures de protection complexes et coÃ»teuses Ã mettre en place.

Une bonne prÃ©paration demeure la meilleure dÃ©fense contre les failles de sÃ©curitÃ©, indique ce rapport 2010. Or, de nombreuses entreprises peinent encore Ã dÃ©tecter les incidents et Ã y faire face. La majoritÃ© des infractions (60 %) continuent Ã Ãªtre dÃ©celÃ©es par des tiers externes aprÃ¨s un temps considÃ©rable. Alors que la faille est bien souvent signalÃ©e dans les journaux dâ□□Ã©vÃ©nements (logs) des victimes, elle est trop souvent ignorÃ©e, par manque de moyens humains, dâ□□outils ou de processus.

La collaboration des Services Secrets amÃ©ricains, annoncÃ©e en mai, a permis aux experts de Verizon Business dâ□□Ã©tablir un Ã©tat des lieux plus global des cas de violation de donnÃ©es

Ã©tudiÃ©s ces six derniÃ¨res annÃ©es. La combinaison des donnÃ©es Verizon Business et des informations sur les cas investiguÃ©s par les Services Secrets, chargÃ©s des enquÃªtes sur les dÃ©lits financiers, permet Ã cette Ã©dition 2010 de couvrir quelque 900 compromissions pour plus de 900 millions de donnÃ©es corrompues.

Â« *Nous avons pu cette annÃ©e Ã©largir notre champ dâ□□investigation afin dâ□□offrir une perspective plus large et approfondie des compromissions de donnÃ©es*Â», explique **Peter Tippett**, Vice-prÃ©sident chargÃ© des recherches et de la veille chez Verizon Business. Â« *En intÃ©grant les informations issues de la base de donnÃ©es des Services Secrets, nous amÃ©liorons notre comprÃ©hension des crimes informatiques et par consÃ©quent notre capacitÃ© Ã lutter contre les infractions.* Â»

Michael Merritt, Directeur adjoint chargÃ© des investigations au sein des Services Secrets amÃ©ricains, dÃ©clare : Â« Nouer des partenariats entre les diffÃ©rentes autoritÃ©s juridiques, les acteurs du secteur privÃ© et les chercheurs est un moyen efficace de protÃ©ger le cyberespace. Câ□□est cette collaboration qui aide notre agence Ã sensibiliser le public aux problÃ©matiques de sÃ©curitÃ© et Ã amÃ©liorer sans cesse ses mÃ©thodes de dÃ©tection et de prÃ©vention. Â»

Principaux rÃ©sultats du rapport 2010

Les constatations de cette annÃ©e confirment certaines conclusions de lâ□□annÃ©e passÃ©e tout en rÃ©vÃ©lant de nouvelles tendances. En voici quelques exemples :

â□¢ La plupart des compromissions de donnÃ©es Ã©tudiÃ©es sont le fait de sources externes. 69 % des infractions proviennent de sources extÃ©rieures et 11 % seulement sont le fait de partenaires. 49 % ont Ã©tÃ© causÃ©es par des sources internes, une hausse par rapport Ã 2008 principalement due Ã lâ□□inclusion des donnÃ©es et cas des Services Secrets amÃ©ricains.

â□¢ De nombreuses compromissions impliquent une utilisation abusive des droits dâ□□accÃ¨s. 48 % des infractions sont le fait dâ□□utilisateurs malintentionnÃ©s qui ont abusÃ© de leurs droits dâ□□accÃ¨s pour accÃ©der Ã des informations de leur entreprise. 40 % dâ□□entre elles sont attribuables Ã des pirates, tandis que 28 % se basent sur des outils sociaux et 14 % relÃ¨vent dâ□□attaques physiques.

â□¢ Certains constats sont communs Ã toutes les violations de donnÃ©es. Comme lors des annÃ©es prÃ©cÃ©dentes, pratiquement toutes les donnÃ©es dÃ©robÃ©es lâ□□ont Ã©tÃ© depuis des serveurs et applications en ligne. 85 % des failles Ã©taient simples Ã dÃ©tecter et 87 %

des victimes auraient pu repÃ©rer lâ□□infraction grÃ¢ce Ã leurs journaux dâ□□Ã©vÃ©nements, sans toutefois lâ□□avoir fait.

â□¢ La conformitÃ© Ã la norme PCI-DSS reste une nÃ©cessitÃ©. 79 % des victimes concernÃ©es par la norme PCI-DSS nâ□□Ã©taient pas totalement conformes lors de lâ□□infraction.

Etat des lieux des crimes informatiques en 2010

Selon le rapport, le dÃ©clin du nombre total de cas de compromissions de donnÃ©es peut sâ□□expliquer par diffÃ©rents facteurs, notamment Â« lâ□□efficacitÃ© des lois mises en place pour capturer les criminels Â». Cette explication est illustrÃ©e par lâ□□arrestation dâ□□Albert Gonzalez, lâ□□un des pirates informatiques les plus cÃ©lÃ¨bres au monde, qui a plaidÃ© coupable pour avoir participÃ© Ã la crÃ©ation dâ□□un rÃ©seau mondial responsable du vol de plusieurs centaines de millions de numÃ©ros de cartes de crÃ©dit et a Ã©tÃ© condamnÃ© lâ□□annÃ©e derniÃ¨re Ã 20 ans de prison.

Â« *La rÃ©duction du nombre dâ□□infractions est le signe que nous progressons dans la lutte contre les crimes informatiques*Â», indique **Peter Tippett**. Â« *GrÃ¢ce Ã la diffusion du framework de recherche en sÃ©curitÃ© VERIS, nous sommes maintenant en mesure de partager davantage dâ□□informations et de recouper nos donnÃ©es de sÃ©curitÃ© avec des sources telles que la base dâ□□investigation des Services Secrets. Nous sommes ainsi mieux armÃ©s que jamais pour doter les entreprises des meilleures pratiques, processus, outils et services dont elles ont besoin pour se protÃ©ger.* Â»

Les cas de compromission de donnÃ©es continuent de toucher tout type dâ□□entreprise.

Mais les services financiers, lâ□□hÃ©bergement et la vente de dÃ©tail reprÃ©sentent le trio de tÃªte des secteurs les plus ciblÃ©s (respectivement 33, 23 et 15 %) selon les donnÃ©es croisÃ©es de Verizon et des Services Secrets. Le pÃ©rimÃ¨tre des cas recueillis par Verizon place toutefois le secteur des technologies de pointe en 3Ã¨me position de ce classement, avant celui de la vente de dÃ©tail. Une part grandissante de cas et un pourcentage considÃ©rable (94 %) de toutes les donnÃ©es corrompues en 2009 concernent le secteur des services financiers.

Plus de la moitiÃ© des violations Ã©tudiÃ©es par Verizon en 2009 ont eu lieu en dehors des Etats-Unis, tandis que la majeure partie des cas Ã©tudiÃ©s par les Services Secrets concernait les Etats-Unis. Le rapport nâ□□indique aucune corrÃ©lation entre la taille dâ□□une entreprise et ses risques dâ□□Ãªtre victime dâ□□une violation de donnÃ©es.

Â« *Les voleurs orientent davantage leur choix de cible en fonction de la valeur des donnÃ©es et du coÃ»t de lâ□□attaque que de facteurs tels que la taille de lâ□□entreprise,* Â», indiquent les experts de Verizon.

Quelques recommandations pour les entreprises

Le Data Breach Investigations Report 2010 dÃ©montre, une fois de plus, que certaines mesures trÃ¨s simples, si elles sont appliquÃ©es convenablement et rÃ©guliÃ¨rement, peuvent sâ□□avÃ©rer trÃ¨s efficaces :

â□¢ Restreindre et surveiller les privilÃ¨ges accordÃ©s aux utilisateurs. Les donnÃ©es recueillies par les Services Secrets indiquent une augmentation sans prÃ©cÃ©dent du nombre dâ□□infractions commises par des sources internes. Les utilisateurs en interne, en particulier ceux disposant de droits Ã©tendus, peuvent Ãªtre difficiles Ã surveiller. La meilleure des stratÃ©gies est de nâ□□accorder ce type de droits quâ□□aprÃ¨s avoir rÃ©alisÃ© une enquÃªte avant embauche, de limiter les droits dâ□□accÃ¨s et dâ□□instaurer une sÃ©paration des fonctions. Lâ□□usage de droits Ã©tendus doit Ãªtre consignÃ© dans les logs (journaux dâ□□Ã©vÃ©nements) et les activitÃ©s effectuÃ©es dÃ©taillÃ©es dans des rapports destinÃ©s Ã la direction.

â□¢ Ne nÃ©gliger aucun cas de violation de politique de sÃ©curitÃ©. Les rÃ©sultats de cette enquÃªte permettent dâ□□Ã©tablir un lien entre les cas de violation de politique de sÃ©curitÃ© en apparence mineurs et les abus plus sÃ©rieux. Tous les cas de violation doivent donc Ãªtre pris en compte et traitÃ©s. Selon le rapport, la simple prÃ©sence de contenus illicites sur des systÃ¨mes utilisateur ou un comportement inappropriÃ© doivent alerter les entreprises. La mÃ©thode la plus efficace est encore de rechercher activement ces indicateurs.

â□¢ Instaurer des mesures pour contrer les vols de codes dâ□□accÃ¨s . EmpÃªcher lâ□□installation des logiciels de capture de droits dâ□□accÃ¨s malveillants sur les systÃ¨mes est une prioritÃ© absolue. Un double systÃ¨me dâ□□authentification peut constituer une solution efficace. Il peut Ã©galement sâ□□avÃ©rer utile, dans la mesure du possible, dâ□□instaurer des rÃ¨gles sur le temps dâ□□utilisation, dâ□□inscrire les adresses IP suspectes sur une liste noire et de restreindre les connexions administrateur.

â□¢ Surveiller et filtrer le trafic sortant. Le rapport dÃ©montre que lors de la plupart des violations de donnÃ©es, quelque chose (donnÃ©es, communications, connexions) emprunte le rÃ©seau de lâ□□entreprise pour rejoindre lâ□□extÃ©rieur. PrÃ©venir cette connexion sortante pourrait ainsi rompre la chaÃ®ne et stopper la fuite de donnÃ©es La surveillance, lâ□□analyse et le contrÃ´le du trafic sortant rÃ©duisent ainsi de maniÃ¨re significative les risques dâ□□attaque des entreprises.

â□¢ Adapter sa stratÃ©gie de surveillance des Ã©vÃ©nements et dâ□□analyse des logs.

La grande majoritÃ© des victimes dispose de la preuve de la compromission dans ses logs (journaux dâ□□Ã©vÃ©nements). La dÃ©tection des Ã©lÃ©ments problÃ©matiques et la mise en oeuvre dâ□□actions correctives adaptÃ©es sont Ã la portÃ©e du plus grand nombre. Les entreprises devraient accorder davantage de temps au contrÃ´le du traitement de leurs donnÃ©es et Ã lâ□□analyse de leurs logs. Il est important quâ□□elles veillent Ã disposer du personnel, des outils et des processus adÃ©quats pour dÃ©tecter et pallier les anomalies.

â□¢ Partager ses informations sur les incidents. Lâ□□efficacitÃ© dâ□□une entreprise Ã se protÃ©ger pleinement repose sur les informations dont elle dispose pour le faire. Verizon Business, pour qui la mise Ã disposition et le partage dâ□□informations sont indispensables Ã la lutte contre les crimes informatiques, fÃ©licite toutes les entreprises qui prennent part Ã cet effort, notamment par le biais de programmes de

partage de donnÃ©es tels que le framework VERIS.

Une version complÃ¨te du **Data Breach Investigations Report 2010** est disponible.