SÃ©curitÃ© : PME, comment faire face aux nouvelles mÃ©thodes de piratage
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 31/3/2011 11:00:00

Les grands secteurs stratÃ©giques sont confrontÃ©s Ã des **vagues dâ□□attaques ciblÃ©es** de plus en plus sophistiquÃ©es qui viennent dÃ©frayer la chronique et **causer de sÃ©rieux prÃ©judices** : fuite de documents confidentiels, dÃ©tournements, espionnage politique et industrielâ□¦

Les exemples ne manquent pas et viennent chaque mois montrer Ã quel point les Ã©tats et les grands groupes stratÃ©giques sont vulnÃ©rables aux assauts dâ□□une cybercriminalitÃ© toujours plus difficile Ã apprÃ©hender.

Lâ□□attaque ayant frappÃ© de plein fouet les services du MinistÃ¨re des Finances au mois de mars en est le parfait exemple. En dÃ©pit des lourds investissements rÃ©alisÃ©s, les moyens de sÃ©curitÃ© dÃ©ployÃ©s nâ□□ont pas semblÃ© Ã mÃªme de contenir une attaque dâ□□un niveau professionnel.

Il paraÃ®t donc lÃ©gitime de sâ□□interroger sur le niveau dâ□□adÃ©quation entre les outils de protection systÃ¨me les plus utilisÃ©s aujourdâ□□hui â□□ technologiquement proches dâ□□outils grand public â□□ et les menaces auxquelles font face les secteurs stratÃ©giques sensibles â□□ des assaillants professionnalisÃ©s, structurÃ©s et appuyÃ©s par des moyens matÃ©riels considÃ©rables.

Ce document a pour objectif de prÃ©senter un Ã©tat des lieux des mÃ©canismes de sÃ©curitÃ© systÃ¨me traditionnellement utilisÃ©s, de mettre en lumiÃ¨re le type de menaces existantes et de donner un certain nombre de pistes et de bonnes pratiques Ã intÃ©grer.

Contexte

Rappelons dâ□□abord que cet article se place dans le contexte trÃ¨s particulier des organisations et entreprises nationales stratÃ©giques. Il sâ□□agit avant tout des acteurs publics ou privÃ©s liÃ©s plus ou moins directement Ã la dÃ©fense, au secteur de lâ□□Ã©nergie et des acteurs gÃ©rant les infrastructures vitales. On y ajoutera les grandes organisations telles que les ministÃ¨res et les institutions financiÃ¨res publiques. Naturellement, sont exclues les entreprises â□□classiquesâ□□ ou non vitales dâ□□un point de vue gÃ©ostratÃ©gique. Ces derniÃ¨res doivent Ã©videmment se protÃ©ger, et elles le font, mais sont peu susceptibles dâ□□Ãªtre la cible spÃ©cifique dâ□□un groupe de pirates. Elles font plus classiquement face au â□□prÃªt Ã porterâ□□ des attaques, Ã©quivalentes Ã celles visant le grand public, et se protÃ¨gent en consÃ©quence.

Les menaces

Malheureusement, les organisations et entreprises nationales stratÃ©giques subissent une menace dâ□□une tout autre envergure : la â□□haute coutureâ□□ du piratage, professionnalisÃ©e, structurÃ©e et parfois Ã©tatique, Ã©labore minutieusement des offensives sur mesure, trÃ¨s sophistiquÃ©es et ciblant spÃ©cifiquement leur victime. Le dÃ©ploiement de moyens que nÃ©cessitent une telle conception est justifiÃ© par la trÃ¨s grande valeur du rÃ©sultat escomptÃ© : informations confidentielles, mise hors service dâ□□infrastructure etc. Le rayon dâ□□action de lâ□□attaque est volontairement faible : en ne ciblant quâ□□une organisation, en Ã©vitant toute diffusion massive de lâ□□attaque, les assaillant sâ□□assurent que les outils de protection systÃ¨me classiques â□□ notamment les antivirus â□□ ne sourcilleront pas. Ces logiciels ne sont en effet efficaces que sur les attaques massives â□□ le â□□prÃªt Ã porterâ□□. Leur rÃ´le nâ□□est en aucun cas dâ□□adresser les attaques ciblÃ©es dÃ©crites plus haut.

Les protections systÃ¨me en place

Or ces logiciels, qui sâ□□appuient sur le concept ancien de reconnaissance par signatures, restent la pierre angulaire de la sÃ©curitÃ© des systÃ¨mes dans lâ□□immense majoritÃ© des entreprises et organisations stratÃ©giques. Le fossÃ© qui sÃ©pare ces protections gÃ©nÃ©ralistes et les attaques ultrasophistiquÃ©es dont elles sont victimes est abyssal, et continue Ã se creuser. Pour autant, inutile de sâ□□offenser de lâ□□inefficacitÃ© de lâ□□antivirus dans ce genre de contexte. Ces logiciels ne sont pas Ã blÃ¢mer. Ils sont tout simplement conÃ§us pour autre chose, pour un autre type de menace quâ□□ils adressent par ailleurs trÃ¨s correctement : lâ□□attaque massive Ã grande Ã©chelle, celle dont souffre le particulier et lâ□□entreprise non stratÃ©gique. La question quâ□□il convient plutÃ´t de se poser est pourquoi des intÃ©rÃªts nationaux gÃ©ostratÃ©giques se contentent-ils de ces outils gÃ©nÃ©ralistes ? Pourquoi, prenant la mesure de la menace, ces organisations ne sâ□□Ã©quipent-elles pas dâ□□outils spÃ©cialisÃ©s ?

Les parades existent

Car ces outils existent. Se basant gÃ©nÃ©ralement sur des analyses bas niveau de lâ□□activitÃ© des systÃ¨mes dâ□□exploitation, ces logiciels hautement spÃ©cialisÃ©s permettent de dÃ©tecter et de bloquer bon nombre dâ□□attaques ciblÃ©es. CouplÃ©s Ã des services dâ□□expertise â□□ de vraie expertise sur ce sujet â□□ ils permettent aux entreprises de bloquer mais aussi de comprendre les modes opÃ©ratoires des attaques afin de faire Ã©voluer les bonnes pratiques internes au fil de lâ□□eau.

En effet, lâ□□Ã©ducation des collaborateurs Ã lâ□□utilisation sÃ»re des outils informatiques est primordiale. Nombre dâ□□attaques pourraient Ãªtre contrÃ©es grÃ¢ce Ã la vigilance des

utilisateurs : ne pas ouvrir les courriers provenant dâ□□inconnus, Ã©viter les programmes exotiques et mal maintenus, se mÃ©fier des messages reÃ§us en doubles etc. Lâ□□expÃ©rience montre cependant que mÃªme les entreprises les plus pointilleuses sur ces aspects ne peuvent, et on le comprend bien, transformer chaque professionnel en un expert de la sÃ©curitÃ©.

Quelques exemples

Les exemples dâ□□attaques ciblÃ©es, capables de passer au travers de ces protections gÃ©nÃ©ralistes sont nombreux : avant la rÃ©cente attaque du ministÃ¨re des finance, le trÃ¨s suspect StuxNet visait Ã rendre inopÃ©rante des infrastructures industrielles vitales (majoritairement en Iran). Sa dÃ©tection par les antivirus ne dÃ©buta que lorsque le rÃ©seau de machines infectÃ©es a pris une ampleur impossible Ã ignorer. En 2009, des universitaires Canadiens mettent au jour lâ□□opÃ©ration GhotNet : lancÃ©e depuis la Chine, elle aurait infiltrÃ© des systÃ¨mes stratÃ©giques dans le monde entier, y compris le Pentagone. Plus tÃ´t, en 2007, lâ□□Estonie, alors en plein crise politique avec la Russie, faisait lâ□□expÃ©rience douloureuse de la mise en incapacitÃ© de ses services publics. On nâ□□ose imaginer le nombre dâ□□attaques passÃ©es sous silenceâ□¦ ou non dÃ©couvertes !

Conclusion

La cybercriminalitÃ© bÃ©nÃ©ficie aujourdâ□□hui de ressources et de moyens importants (humains, organisationnels et financiers). Il est donc du devoir des Etats et des organismes stratÃ©giques de ne pas rester passifs et de faire Ã©voluer en profondeur leur politique de sÃ©curitÃ©. Câ□□est Ã cette unique condition que ces organisations pourront prÃ©server la confidentialitÃ© des donnÃ©es quâ□□elles dÃ©tiennent ou se prÃ©munir dâ□□actes de piratage pouvant engendrer de vÃ©ritables bouleversements politiques ou Ã©conomiques.

Â

JÃ©rÃ´me Robert, Responsable Marketing Produit SkyRecon Systems

Â