Symantec : PrÃ©visions annuelles 2013 dans la sÃ©curitÃ© informatique
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 29/11/2012 13:00:00

Alors que la fin d'annÃ©e approche, **Symantec publie ses prÃ©visions annuelles pour 2013** dans le domaine de la sÃ©curitÃ© informatique. Symantec s'est basÃ© sur des chiffres et des donnÃ©es factuelles, son expertise mÃ©tier, en ajoutant une dose de prospective et de nombreux discussions et Ã©changes avec les experts de lâ□□entreprise et externes Ã celle-ci.

Ces prÃ©visions sont ainsi basÃ©es sur des Ã©lÃ©ments factuels, et sont le fruit de nos annÃ©es d'expÃ©rience, de notre comprÃ©hension de l'Ã©volution des menaces et de notre connaissance des tendances passÃ©es dans le domaine de la cybersÃ©curitÃ©. Ces prÃ©visions peuvent Ãªtre classÃ©es en trois catÃ©gories, en fonction du type de menace attendu et des tendances technologiques montantes.

1/ Types de menace :

Les Â« cyberconflits Â» vont devenir monnaie courante

En 2013 et par la suite, les conflits opposant les pays, organisations et individus joueront un rÃ´le dÃ©cisif dans le monde de la cybercriminalitÃ©. LÃ oÃ¹ il y aura des diffÃ©rends, qu'ils soient politiques ou Ã©conomiques, il y a aura des risques d'attaques ou d'espionnage en ligne. Sur ce point, des programmes trÃ¨s sophistiquÃ©s visant Ã dÃ©rober des donnÃ©es, tels que Flamer devraient faire parler d'eux courant 2013.

Les ransomware s'imposent

Les programmes de type ransomware dÃ©passent le stade de la tromperie ; leurs auteurs cherchent Ã intimider leur victimes en les harcelant. Si ce Â« modÃ¨le Ã©conomique Â» n'est pas nouveau, il a toujours rencontrÃ© les mÃªmes limites que le kidnapping physique, en ne trouvant pas de mÃ©thode efficace pour rÃ©cupÃ©rer l'argent. Les cybercriminels ont quant Ã eux trouvÃ© la parade idÃ©ale : le paiement en ligne. Ils peuvent ainsi forcer leurs victimes Ã payer, au lieu de faire usage de la simple intimidation.

L'intÃ©gritÃ© des donnÃ©es menacÃ©e

ParallÃ¨lement aux risques pesant sur le vol de donnÃ©es, un autre type devrait se dÃ©velopper qui menace l'intÃ©gritÃ© de ces informations. Le principe consiste Ã les modifier, changeant du mÃªme coup les actions qu'elles sont censÃ©es dÃ©clencher dans le monde rÃ©el. Stuxnet, qui fut le tout premier programme de ce type, devrait faire des Ã©mules en 2013. Symantec a rÃ©cemment mis au jour Narilam, un programme trÃ¨s sophistiquÃ© conÃ§u dans le but de modifier des bases de donnÃ©es d'entreprises. Les infrastructures critiques d'un pays peuvent ainsi Ãªtre menacÃ©es, ou bien encore les rouages du secteur financier.

L'usurpation d'identitÃ© sous les projecteurs

L'utilisation de fausses identitÃ©s est une pratique trÃ¨s rÃ©pandue, utilisÃ©e principalement pour des particuliers. Elle l'est moins pour des objets connectÃ©s. Avec le boom des terminaux et des objets reliÃ©s au Net, on risque d'assister Ã l'usage de certificats corrompus, conÃ§us Ã des fins malveillantes et susceptibles de causer des dysfonctionnements de ces appareils. Les entreprises et organisations qui mettent au point ces derniers et les commercialisent doivent donc adopter des procÃ©dures de sÃ©curitÃ© ad hoc.

2/ RÃ©seaux sociaux :

La monÃ©tisation des rÃ©seaux sociaux voit apparaÃ®tre de nouveaux risques

Symantec s'attend Ã une augmentation des attaques utilisant des programmes malveillants dans le but de voler des coordonnÃ©es bancaires, via les rÃ©seaux sociaux. En succombant Ã la technique du leurre, les internautes peuvent aussi Ãªtre poussÃ©s Ã fournir ces informations financiÃ¨res ou d'autres tout aussi sensibles prÃ©sentant un intÃ©rÃªt pour les attaquants, via de fausses pages imitant en tous points celles des rÃ©seaux sociaux. Pour attirer leurs victimes, ils leur envoient des notifications faisant Ã©tat d'un prÃ©tendu cadeau ou des mails demandant leur adresse et d'autres informations personnelles. Si le fait de fournir des donnÃ©es sans caractÃ¨re financier peut sembler inoffensif, les attaquants les vendent ensuite ou se les Ã©changent pour disposer de fiches complÃ¨tes sur une personne. Ils ont alors entre leurs mains des Ã©lÃ©ments exploitables pour accÃ©der aux autres comptes de la victime.

RÃ©seaux sociaux d'entreprise : risques potentiels de passerelles vers l'extÃ©rieur et de brÃ¨ches de sÃ©curitÃ©

Le risque de voir des informations rÃ©cupÃ©rÃ©es pour Ãªtre transmises Ã l'extÃ©rieur de l'entreprise est rÃ©el. Plusieurs raisons Ã cela : les entreprises sont de plus en plus nombreuses Ã dÃ©ployer des rÃ©seaux sociaux internes, qui permettent de limiter la taille d'un groupe selon les critÃ¨res de postes ou de services. Des rÃ©seaux rapidement adoptÃ©s par les salariÃ©s, qui n'abandonnent pas pour autant leurs pratiques habituelles sur les rÃ©seaux sociaux publics, faisant de fait courir un risque de diffusion des informations hors de l'entreprise, via la passerelle des rÃ©seaux sociaux. Qu'il s'agisse d'erreur humaine ou d'acte intentionnel, les donnÃ©es confidentielles peuvent fuiter et Ãªtre exploitÃ©es Ã l'extÃ©rieur.

3/ La mobilitÃ© et le Cloud :

Alors que les entreprises et les particuliers adoptent le mobile et Cloud, les attaquants leur emboÃ®tent le pas.

Les attaquent suivent les utilisateurs, et la tendance se vÃ©rifie avec les terminaux mobiles et le cloud.

Sans surprise, les plates-formes mobiles et les services de cloud seront en 2013 des cibles

Ã©videntes pour des attaques et tentatives de brÃ¨ches. Une prÃ©cision confirmÃ©e par l'explosion des programmes malveillants sur les terminaux sous Android en 2012.

Des terminaux mobiles Ã©chappant au contrÃ´le des entreprises ne cessent d'accÃ©der Ã leurs rÃ©seaux, puis de se dÃ©connecter, rÃ©cupÃ©rant au passage des informations qui finissent pas Ãªtre stockÃ©es sur d'autres nuages. Des pratiques qui peuvent ouvrir des brÃ¨ches et motiver des attaques ciblant les donnÃ©es prÃ©sentes sur les terminaux mobiles. Les utilisateurs tÃ©lÃ©chargent, Ã leur insu, des programmes malveillants sur leur tÃ©lÃ©phone en mÃªme temps que des programmes licites dÃ©sirÃ©s.

2013 Ã©prouvera aussi les limites des infrastructures mobiles. L'essor de l'informatique mobile va leur mettre la pression, rÃ©vÃ©lant un problÃ¨me de taille : l'activitÃ© Internet sur les navigateurs mobiles n'est pas protÃ©gÃ©e par un certificat de sÃ©curitÃ© SSL. Plus inquiÃ©tant encore, la plupart des usages mobiles reposent sur des applications insuffisamment sÃ©curisÃ©es, pouvant servir de tremplin Ã des tentatives d'interception de donnÃ©es de type Â« man-in-the-middle Â».

La publicitÃ© sur mobile : une nuisance dangereuse

La publicitÃ© sur mobiles ou Â« madware Â» est source de nuisance dans la mesure oÃ¹ elle perturbe l'expÃ©rience de l'utilisateur et peut mettre Ã portÃ©e de pirates ses coordonnÃ©es postales et GPS, ainsi que des Ã©lÃ©ments d'identification de son terminal. Au cours des 9 derniers mois seulement, le nombre d'applications intÃ©grant de la publicitÃ© mobile relativement agressive a augmentÃ© de 210 %. Une tendance qui devrait se confirmer dans l'annÃ©e qui vient.