1r Congrés
Seguretat Informàtica UOC.
Ciberseguretat i Ciberespionatge

UOC

Juny 2013

Senyores i Senyors,
Amigues i amics,

Sigueu benvinguts al Ir. Congrés de Seguretat Informàtica de la UOC.

Recents esdeveniments sobre fuites d'informació, notícies d'atacants informàtics trencant tecnologies de seguretat, fallades de seguretat que han tingut lloc tant al sector públic com el privat, són arguments suficients per fer veure que estem en un nou escenari de riscos i amenaces, on la informació s'ha convertit en una arma estratègica i tàctica, que pot arribar a qüestionar la governabilitat d'una organització o d'una nació.

Sense anar gaire lluny, aquest cap de setmana la premsa informava de l'aprovació per part del govern de l'Estat (amb el suport del principal partit de l'oposició) de l'Estratègia de Seguretat Nacional, que inclou controls preventius d'Internet en vista de la ciberguerra, fa referència a ciberatacs "de grups terroristes, xarxes de crim organitzat, empreses, Estats o individus aïllats" i proposa l'adopció de "mesures preventives de vigilància de l'ús de la Xarxa".

La figura, fins ara opcional, de la seguretat de la informació comença a esvair-se i a agafa, avui, una rellevància estratègica, en un escenari on la informació és "moneda fonamental" per a generar i desenvolupar posicions privilegiades de persones, empreses i nacions.

Quan portem aquesta reflexió a nivell d'estats i països, trobem múltiples vistes per a comprendre els riscos i amenaces en front de la informació i els seus impactes que generen confusió i desconfiança. Ara bé, els fets i els esdeveniments que s'han presentat, mantenen l'atenció dels governs sobre aquests perills i permeten mesurar la capacitat de reacció d'un estat.

Cap al febrer de 2010 es podia llegir al Washington Post el següent titular: "Els Estats Units estan avui per avui combatent una ciberguerra, i l'estem perdent". Aquesta notícia no tindria més importància si no fos que la deia el vicealmirall Mike McConnel, que va ser Director de la NSA (Agència Nacional de Seguretat) entre 1992 i 1996 amb el president Clinton. I que va ser després Director de la Intel·ligència Nacional amb George Bush, del 2007 al 2009.

McConnel indicava que una simulació feta sobre un allau de Ciber-Xoc (Ciber Shock Wave) mostrava el que ja temien feia temps aquells que estaven relacionats amb la política nacional de seguretat, que era, ni més ni menys, que les qüestions més elementals sobre Ciber-Conflictes estaven encara pendents de resoldre.

Deia McConnel que aquestes batalles simulades no eren de cap manera hipotètiques. I posava com a exemple la xarxa i les infraestructures de Google, que havien estat hackejades en un atac començat el desembre 2009 i que procedia de la Xina.

«Per McConnel la simulació havia revelat el que tothom relacionat amb les polítiques de seguretat nacional temien des de feia temps: que fins ara tots els documents i les estratègies s'havien centrat en la guerra tradicional i que ara calia tenir en compte i respondre les preguntes relacionades amb el ciberconflicte.»

A partir de l'incident amb Google, que posteriorment es va anomenar com Operació Aurora i que va acabar afectant d'altres companyies, com ara Adobe o Juniper, han començat a proliferar moltes altres manifestacions d'atacs d'aquest tipus.

Potser la més notable, també per ser la primera a gran escala, va ser Stuxnet. El primer cuc informàtic que era capaç d'espiar i reprogramar sistemes industrials, en concret sistemes SCADA de control i monitoratge de processos, i que podia afectar a infraestructures crítiques. Companyies com Kaspersky Labs el descrivien com "un prototip funcional i aterrador d'arma cibernètica". La investigació va concloure que la majoria d'ordinadors infectats estaven a l'Iran i que l'objectiu més probable d'aquest cuc eren les infraestructures d'alt valor de l'Iran. Alguns mitjans com The New York Times afirmaven que l'objectiu era endarrerir la posada en funcionament de la planta nuclear de Bushehr (Iran).

Posteriorment aquest tipus d'eines s'han anat sofisticant, moltes d'elles aprofitant forats de seguretat coneguts com "Dia Zero" o Zero Day. És a dir atacs contra sistemes aprofitant errors de seguretat desconeguts pel públic en general i pel fabricant del sistema o de l'aplicació.

«Això denota també l'alt grau d'especialització i coneixement dels programadors d'aquest malware i la infraestructura econòmica amb què compten.»

Darrerament ha aparegut un nou concepte que forma part de l'èxit d'aquests tipus d'atacs. Es tracta de les Amenaces Persistents Avançades o Advanced Persistent Threats, que es poden definir com un tipus d'atac en xarxa que guanya l'accés a un sistema no detectat durant un període llarg de temps.

«La intenció d'aquests tipus d'atacs és robar dades més que no pas causar danys en el sistema. Solen tenir com a objectiu aquelles organitzacions amb un valor estratègic elevat per la informació que tenen. Per exemple la defensa nacional o la indústria financera.»

Tot sovint els atacants utilitzen l'anomenat spear-phishing (o suplantació dirigida), un tipus d'enginyeria social que tracta d'utilitzar persones amb un nivell d'influència o de privilegis molt alt com a vector d'accés per instal·lar el programari maliciós en el sistema.

Hi ha una frase molt coneguda del criptògraf i expert mundial en seguretat informàtica, Bruce Schneier, que diu:

«En el ciberespai, la balança de poder està en el costat de l'atacant. Atacar una xarxa és molt més fàcil que defensar-la ...»

Això podria canviar i l'atac cibernètic ser l'equivalent de la guerra de trinxeres, on el defensor té l'avantatge natural. Però no s'espera que passi en el curt termini.

És per tot això, doncs, que la UOC organitza aquest Ir. Congrés de Seguretat Informàtica, i el dedica a la ciberseguretat i al ciberespionatge.

Volem que totes aquelles persones que estant investigant i treballant en Seguretat Informàtica i que habitualment no participen exposant les seves idees, les seves investigacions, tinguin a partir d'ara el fòrum idoni.

Desitjo que tingueu una bona jornada i una bona feina.

Moltes gràcies.

Josep A. Planell