

Nuevas protecciones ante nuevas amenazas



Alfonso XI “el Justiciero” (1311-1350), fue un rey español que describía con asombro cómo en una batalla contra los benimerines, se “tiraban muchas bolas de hierro que las lanzaban con truenos, de los que los cristianos sentían un gran espanto, ya que cualquier miembro del hombre que fuese alcanzado, era cercenado como si lo cortasen con un cuchillo”.

Estaba describiendo el impacto que la pólvora estaba causando entre sus tropas. Soldados que en el siglo XIV no podían imaginarse una batalla que no fuera con espadas, sables, flechas, escudos... De repente, un arma nueva para la que la tecnología de seguridad de aquella época no podía.

Lo mismo pudo pasar cuando el carro de combate Mark I entró en combate en la Batalla del Somme en 1916. Las trincheras preparadas para proteger a los soldados no servían de nada, los proyectiles de las armas ligeras de los soldados rebotaban ante aquella mole metálica. De nuevo, no existía tecnología para enfrentarse a una nueva amenaza.

Sin tener que recurrir a este tipo de enfrentamientos bélicos, los hombres también nos hemos visto ante situaciones en los que el concepto de seguridad debe cambiar: ¿servían de algo los pañuelos que se colocaban en la cara las personas que luchaban contra la “gripe española” en 1918? No, era inútil: los virus causantes de la gripe son tan pequeños que un pañuelo no puede llegar a filtrarlos. Hubo que desarrollar filtros especiales que retengan virus propagándose por el aire.

Y hoy en día, también nos encontramos con problemas en los sistemas de seguridad, en este caso los informáticos. Cuando en los albores de la informática personal los virus empezaron a desarrollarse, los usuarios se vieron expuestos a una amenaza para la que no estaban preparados. La tecnología no servía, y hubo que desarrollar programas que fueran capaces de detener a los virus: los “antivirus”.

Sin embargo, poco después, hicieron falta sistemas más avanzados de protección. Los virus cada vez eran más, y los laboratorios de las empresas a duras penas se bastaban para generar todas las vacunas. Se estaba lanzando una batalla en la que la calidad del malware ya era casi lo de menos, se estaba intentando que los fabricantes se saturaran. De detectar apenas un par de decenas de virus al día en el año 2000 se pasó a detectar cientos, incluso miles.

Las tecnologías de detección proactiva de nuevos códigos cumplen su función, pero de nuevo nos encontramos con nuevas armas que superan a las técnicas proactivas, que ni siquiera han podido desarrollar muchas empresas todavía.

En muchas empresas (y también en ordenadores domésticos) están empezando a florecer ataques dirigidos por hackers. Software utilizando técnicas de ocultación especiales (los rootkits, por ejemplo), creaciones únicas dirigidas a un solo ordenador con información vital... son nuevas armas. El negocio que supone tener, por ejemplo, un troyano espiando a la competencia es tan grande que ha hecho renunciar a los hackers a su fama personal.

Nuevas protecciones ante nuevas amenazas



Mientras estos ataques dirigidos cosechan información privilegiada, siguen llegando masivamente nuevos ejemplares de malware a los laboratorios, tal y como vemos en las películas de batallas épicas: cientos o miles de soldados lanzados al sacrificio, mientras un general observa desde una colina cómo un grupo de especialistas atacan por otro sitio al enemigo sin llamar la atención.

La tecnología debe volver a diseñarse. Ya no sirven esos clásicos “antivirus residentes”, las tecnologías reactivas no son suficientes. La situación ha vuelto a cambiar, y la estrategia de protección debe cambiar. Las tecnologías antiguas nos sirven para tanto como un escudo medieval ante un fusil de asalto.

Hoy en día mientras un técnico de laboratorio pone en marcha un ordenador para investigar un determinado código malicioso, pasa un tiempo que es suficiente como para que se pueda producir una infección masiva. El récord en este campo lo tiene el gusano SQLSlammer, algunas fuentes citan que le bastaron 15 segundos.

Para poder establecer un sistema de protección contra nuevas amenazas, debemos establecer en cada uno de los sistemas conectados a Internet (me da igual que sea un puesto de trabajo en una red empresarial que un ordenador doméstico) una capa de protección inteligente. Es decir, un sistema que sea capaz de analizar qué está pasando en el ordenador para poder detectar movimientos peligrosos, y poder frenarlos antes de que sea demasiado tarde.

Este tipo de tecnología de detección de amenazas desconocidas (y no hablo de sistemas heurísticos clásicos, sino de tecnologías inteligentes) pueden encontrarse fácilmente en algunos fabricantes de soluciones domésticas. ¿Y dónde queda esta protección en redes corporativas? ¿Tienen que renunciar a la protección contra amenazas desconocidas los administradores de cientos o miles de equipos?

Fernando de la Cuadra
Editor Técnico Internacional
Panda Software (<http://www.pandasoftware.com>)
E-mail: Fdelacuadra@pandasoftware.com