FireEye™

Informe

Protección de los datos, la propiedad intelectual y la marca frente a ciberataques

Guía para CIO, CFO y CISO

Contenido

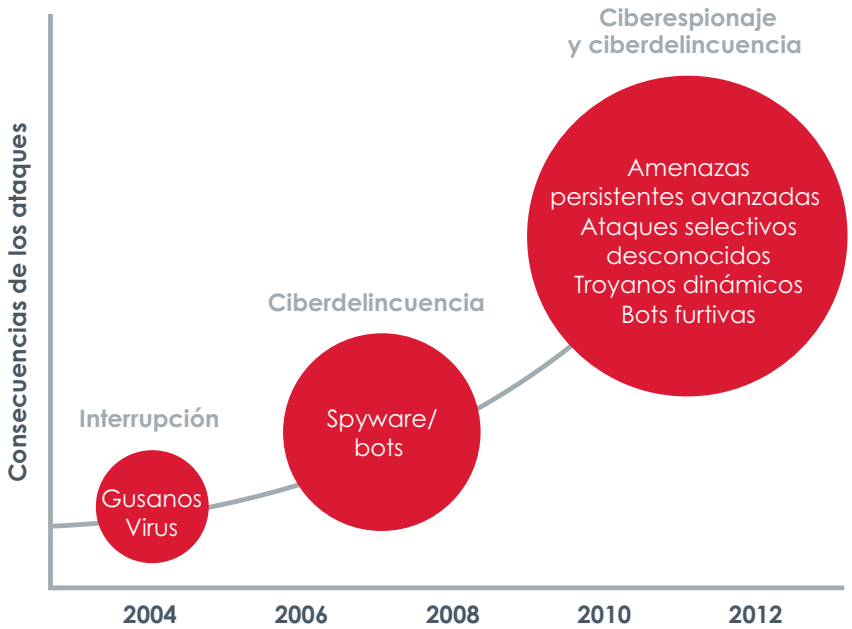
El problema

En la actualidad, tanto empresas como organismos públicos están constantemente en riesgo de ataques. Algunos de estos ataques, como los dirigidos contra RSA, Global Payments, ADP, Symantec, el Fondo Monetario Internacional y otras organizaciones, han salido a la luz pública, pero, sin duda, hay muchísimos más que no hemos llegado a conocer. Se han descubierto ciberataques, como Flame y Stuxnet, entre otros, que han establecido nuevos estándares en cuanto a complejidad y sofisticación.

Estos cambios dejan claro básicamente que los ciberdelincuentes, los países y los hacktivistas que están detrás de estos ataques emplean métodos cada vez más sofisticados y más eficaces a la hora de conseguir sus objetivos: robar y sabotear. Mediante el empleo de malware dinámico, mensajes de correo electrónico de phishing selectivo, complejos ataques web y otras tácticas, estos criminales saben cómo sortear los mecanismos de defensa tradicionales, como firewalls y firewalls de próxima generación, soluciones IPS, antivirus y puertas de enlace. ¿Cree que su empresa es inmune? Si es así, es una excepción: el 95% de las empresas son víctimas de ataques frecuentes, siendo cada vez más habituales los incidentes relacionados con el robo de propiedad intelectual, registros de clientes y otros datos confidenciales.

Un informe de 2012 elaborado por Gartner describe esta situación de la siguiente manera: "Todo el mundo parece estar de acuerdo en que los ataques avanzados están sorteando nuestros controles de seguridad tradicionales basados en firmas y permanecen en nuestros sistemas, sin detectarse, durante largos períodos de tiempo. La amenaza es real. Su empresa ha sufrido ataques, lo que ocurre es que no lo sabe".

¿Por qué no son eficaces las defensas de seguridad actuales? Para esta lucha, sus equipos de seguridad se sirven de un arsenal obsoleto: plataformas de seguridad antiguas que emplean tecnología diseñada hace muchos años, basada en el uso de firmas. Estas herramientas son eficaces para bloquear malware básico conocido y documentado, como virus; sin embargo, son incapaces de identificar los ciberataques dinámicos y multifase actuales, conocidos normalmente como malware avanzado o amenazas persistentes avanzadas (APT).



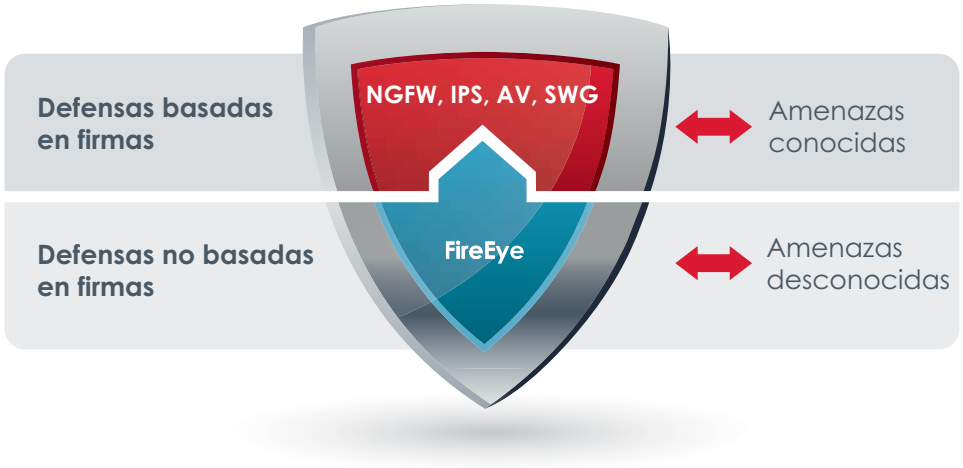
Razones para preocuparse

Si su empresa es como la mayoría, estará gastando una gran cantidad de dinero (puede que entre un 10 y un 20% de su presupuesto de TI anual) en seguridad. Sin embargo, este esfuerzo no da resultados contra la nueva generación de ciberataques. Si no le parece una razón de peso, piense en lo que supondría para su empresa perder la batalla de la seguridad:

- **Pérdida de competitividad.** Si los ciberdelincuentes consiguen sortear sus defensas, puede que sus secretos comerciales, patentes, registros de clientes y actividades de fusiones y adquisiciones queden expuestos al público, con el consiguiente perjuicio para su posición frente a la competencia.
- **Incumplimiento de normativas.** Si su empresa no cuenta con la protección necesaria contra fugas de datos, es posible que sea incapaz de cumplir las normativas y regulaciones correspondientes. Tanto si pertenece al sector financiero y debe garantizar la seguridad de los datos de tarjetas de crédito, así como cumplir la norma PCI DSS, como si su negocio se rige por las normas HIPAA, NERC, FISMA, las relacionadas con la privacidad o cualquier otra normativa de aplicación internacional, las fugas de datos pueden dar lugar a multas, pérdida de negocio y otras muchas sanciones.
- **Daño en la reputación.** La confianza del cliente y la cuota de mercado son activos de gran valor. Una fuga importante puede ser suficiente para acaparar titulares y que esos activos, que tanto trabajo ha costado cosechar, se esfumen rápidamente. Se estima que las fugas de información en las empresas han generado pérdidas que van desde algunos millones hasta los 200 millones de dólares.
- **Pérdida de productividad.** Si su equipo de seguridad descubre las fugas una vez que se han producido, tendrá que lidiar con los análisis forenses, corregir las vulnerabilidades, evaluar si hay en el sistema de seguridad otras brechas similares, recomponer los sistemas dañados, etc. El tiempo empleado en estas tareas es tiempo que su empresa no recupera y que no puede dedicar a otras iniciativas más estratégicas.

La solución

Para luchar contra las tendencias y riesgos mencionados, muchas empresas están incorporando un nuevo nivel de seguridad que complemente sus tecnologías de seguridad existentes y permita a los equipos de seguridad identificar y neutralizar de manera eficaz los ciberataques que se despliegan en la actualidad. Gracias a este nivel adicional, los equipos de seguridad pueden detectar, en tiempo real, si el código es realmente malicioso y si ha conseguido atravesar todas las demás defensas.



FireEye ofrece soluciones que proporcionan este nivel de defensa necesario y que, como se ha demostrado, pueden detectar y bloquear las ciberamenazas avanzadas a las que se enfrenta su empresa. FireEye, mencionada en Forbes, Businessweek, The Wall Street Journal y otras importantes publicaciones, ayuda a su empresa a protegerse de manera eficaz contra los ataques avanzados actuales, con el fin de evitar los daños financieros, de marca y competitivos que generan. Además, gracias a la automatización de la detección del malware avanzado, FireEye permite a su equipo de seguridad centrarse en otras tareas, con el consiguiente ahorro en costos operativos. La solución FireEye elimina también los falsos positivos y negativos, lo que ahorra más tiempo a su personal. Con todas estas ventajas, un estudio independiente calculó que la rentabilidad media que obtienen los clientes por la inversión en soluciones FireEye es de 16.517.000 dólares.

Esto explica que, aproximadamente un 20% de las empresas del índice Fortune 500 sean clientes de FireEye. Dichos clientes proceden de diversos sectores, como el financiero, el sanitario, el de fabricación y el energético, así como de más de 60 organismos públicos.

A continuación se incluyen comentarios de algunos responsables de la toma de decisiones que eligieron FireEye:

"Pensamos en FireEye porque las herramientas tradicionales que utilizábamos —firewalls, antivirus, prevención y detección de intrusiones— se basan fundamentalmente en firmas y, por lo tanto, eran sencillamente ineficaces frente a los ataques selectivos y desconocidos (zero-day)".

—Jerry Archer, SVP y CSO, Sallie Mae

"Los ataques selectivos y desconocidos que eluden las defensas más sencillas son los que imponen el uso de un producto de próxima generación como FireEye. Hemos analizado las soluciones de otros proveedores, pero FireEye se distingue por su capacidad para detectar estas amenazas avanzadas y garantizar nuestra seguridad".

—Tony Spinelli, SVP y CSO, Equifax

"Hemos disfrutado de las ventajas de los dispositivos FireEye, que nos ayudan a protegernos contra la filtración de la propiedad intelectual. Además, el personal de FireEye atendió rápidamente todas nuestras solicitudes y dudas. No se han limitado a actuar como un proveedor, sino que han demostrado ser un extraordinario aliado a la hora de ayudarnos a abordar nuestros problemas de protección del perímetro de la red".

—Leslie Lambert, CISO, Juniper Networks

Acerca de FireEye

FireEye es líder en la lucha contra ataques selectivos avanzados que utilizan malware avanzado, exploits desconocidos (*zero-day*) y tácticas de amenazas persistentes avanzadas. Las soluciones de FireEye complementan los firewalls tradicionales y de próxima generación, las soluciones de prevención de intrusiones, los antivirus y las puertas de enlace, que son incapaces de detener las amenazas avanzadas, dejando vacíos de seguridad en las redes. FireEye ofrece la única solución del sector que detecta y bloquea ataques que llegan a través de la Web y el correo electrónico, así como el malware latente que se hospeda en los recursos compartidos. Actúa en todas las fases del ciclo de vida de un ataque con un motor que no emplea firmas y que utiliza análisis con información de estado para detectar las amenazas desconocidas. Con sede en Milpitas, California, FireEye cuenta con el respaldo de destacados socios financieros, como Sequoia Capital, Norwest Venture Partners y Juniper Networks.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408.321.6300 | LATAM@FireEye.com | www.FireEye.com