Economías sumergidas

El capital intelectual y los datos confidenciales de las empresas, los nuevos objetivos de la ciberdelincuencia

McAfee | SAIC

Economías sumergidas

El capital intelectual y los datos confidenciales de las empresas, los nuevos objetivos de la ciberdelincuencia

Contenido

Prólogo de Simon Hunt, CTO y Vicepresidente de la división Endpoint Security de McAfee

La globalización y el uso masivo de las tecnologías de la información han llevado a las empresas a aumentar la cantidad de información confidencial corporativa que almacenan en Internet. Mientras se producía este cambio, los ciberdelincuentes han descubierto nuevas formas de atacar estos valiosos datos, desde dentro y desde fuera de la empresa.

Antes, el objetivo principal de los ciberdelincuentes era la información personal, como números de tarjetas de crédito y de documentos de identidad, que después vendían en el mercado negro. Ahora, esos delincuentes se han dado cuenta de que pueden generar mayores beneficios a través de la venta de información confidencial de una empresa a competidores y gobiernos extranjeros. Por ejemplo, la venta de los documentos jurídicos de una empresa puede ser mucho más lucrativa que la de una lista de tarjetas de crédito de clientes.

El nuevo objetivo de la cibereconomía sumergida es el robo de capital intelectual de las empresas, que se define por el valor que genera una compañía gracias a su propiedad intelectual, incluida la información confidencial, los planes de comercialización, los resultados de la investigación y desarrollo, e incluso el código fuente. Por ejemplo, Operación Aurora, un ataque selectivo contra Google y, al menos, contra otras 30 empresas, fue un ataque sofisticado destinado al robo de capital intelectual.

Más recientemente, hemos descubierto los ataques de "Night Dragon" contra compañías petroleras y de gas en todo el mundo, que durante varios meses filtraron de manera silenciosa e insidiosa gigabytes de información interna de naturaleza altamente confidencial, incluidos datos protegidos sobre operaciones de campo, financiación de proyectos y documentación sobre licitaciones. Si bien estos ataques se centraron de manera específica en el sector energético, las herramientas y técnicas utilizadas pueden emplearse con éxito contra cualquier otro sector industrial.

En un contexto en el que las amenazas provienen tanto del interior como del exterior de la empresa, las soluciones de protección de datos cobran más importancia que nunca. WikiLeaks, por ejemplo, supone una nueva amenaza para las empresas, ya que el personal interno con acceso a información privilegiada se siente cada vez más tentado a revelar los secretos de su empresa para conseguir algún beneficio económico o tecnológico, para aumentar el nivel de transparencia de las empresas o para sacar a la luz lo que consideran malas prácticas. La enorme repercusión pública que ha tenido WikiLeaks ha llevado a las empresas a examinar detenidamente lo que debe considerarse confidencial, público y lo que debe protegerse. Con la progresiva disolución de los perímetros de la red, debido a que las empresas amplían las operaciones a los dispositivos móviles, al "cloud computing" y a terceros, cada vez resulta más difícil contener los vectores de intrusión. Una vez que se ha conseguido traspasar el perímetro de la red, los ciberdelincuentes saben muy bien cómo extraer y rentabilizar los datos.

Al tiempo que las inversiones de TI aumentan para impedir estos robos de capital intelectual, también aumenta la sofisticación de los ataques, haciendo necesarias tecnologías y soluciones avanzadas para mitigar las amenazas, así como más formación y directivas. La implementación de directivas es importante, pero no es suficiente para resolver el problema.

Este informe evalúa el estado actual de la seguridad en las empresas a nivel global, que parece que no cuentan con la protección necesaria contra los sofisticados ataques generados por la cibereconomía sumergida. Asimismo, intenta determinar si las empresas han adaptado sus directivas y enfoques en consecuencia. El informe concluye con iniciativas para proteger el capital intelectual con el fin de contener las pérdidas y sacar el máximo partido de la recuperación económica que se vislumbra en el horizonte.

Introducción

Hace dos años, McAfee elaboró el informe "Economías Desprotegidas", el primer estudio mundial sobre la seguridad de las economías de la información. Ese estudio (basado en un sondeo entre empresas de todo el mundo) desveló que, en total, las compañías habían perdido más de 1 billón de dólares en 2008 como consecuencia de las fugas de datos, el coste de la recuperación y el daño causado a su reputación. En la actualidad, cuando la economía mundial comienza a recuperarse, las empresas de todo el mundo revisan su capital intelectual y evalúan las pérdidas como consecuencia de la fuga de datos y de los ciberataques. El capital intelectual se define por el valor que genera una empresa gracias a su propiedad intelectual, incluida la información confidencial, los planes de comercialización, los resultados de la investigación y desarrollo, e incluso el código fuente.

Internet ha dinamitado las fronteras geográficas y las empresas tienen gran parte de su valor en información intangible que se almacena de forma virtual. Cuando los ciberdelincuentes buscan nueva información de la que apoderarse, tienen en cuenta cuestiones como el almacenamiento en el extranjero, que ha permitido la prevalencia del robo de capital intelectual y, al mismo tiempo, ha dificultado la acción de la justicia. Dado el grado de sofisticación de los tipos de técnicas utilizadas por los ciberdelincuentes, con frecuencia, las empresas ni siquiera perciben que se está produciendo un robo de su información.

Aunque la ubicación geográfica y la cultura tienen su peso, en particular, en países en los que las líneas entre empresas y gobierno son difusas, es el valor de los datos lo que determina a quién y qué se ataca. El objetivo y la motivación son casi siempre económicos.

En 2011, muchos de los interrogantes son similares a los que se planteaban hace dos años, pero la recuperación económica, frente a una situación de recesión, hace que el contexto sea diferente. ¿Cuál será el impacto de una recuperación económica en la capacidad de las empresas para proteger la información vital? ¿Qué países representarán la mayor amenaza para la estabilidad económica de otros países?

¿Cómo atacarán los ciberdelincuentes a las empresas de cualquier punto del planeta? ¿En qué medida la protección de los activos digitales ayudará o dificultará la recuperación económica mundial el próximo año?

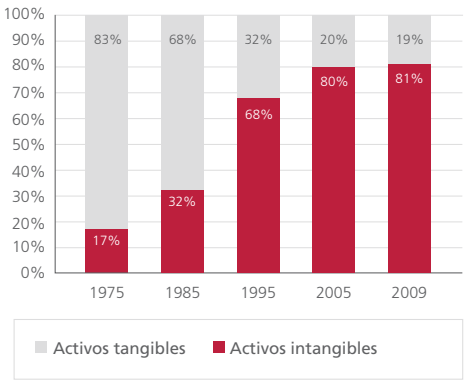
En colaboración con expertos de los sectores de la protección de datos y la propiedad intelectual, McAfee y Science Applications International Corporation (SAIC), una empresa de aplicaciones tecnológicas, científicas y de ingeniería que pertenece a FORTUNE 500®, han examinado en profundidad estas cuestiones.

A través de una encuesta realizada entre más de 1.000 responsables de TI en EE. UU., Reino Unido, Japón, China, la India, Brasil y Oriente Medio, McAfee, junto con SAIC, ha desarrollado un estudio sobre este tema. Dicho estudio, dirigido por el investigador internacional Vanson Bourne, revela los cambios en las actitudes y percepciones de la protección de la propiedad intelectual en los dos últimos años.

Sección 1: Cómo cambia la economía y el valor del capital intelectual

La economía ha dado un giro en los últimos veinte años; antes los activos físicos eran la representación principal del valor de una empresa y ahora, en cambio, el capital intelectual es el grueso del valor corporativo. Un reciente análisis de Ocean Tomo Intellectual Capital Equity estima el valor de los intangibles en torno al 81% del valor de las empresas del índice S&P 500, una parte importante del cual está representada por tecnología patentada, información confidencial, documentación corporativa, procesos empresariales y planes de comercialización.

Componentes del valor de mercado de S&P



FUENTE: OCEAN TOMO

A menudo resulta complicado cuantificar el capital intelectual, ya que normalmente no se mide. Puede ser el fruto de años de inversión directa e indirecta, y la demanda de la economía sumergida le atribuye un precio que no suele reflejar correctamente su valor para la empresa a la que pertenece. Por ejemplo, es posible que, para un competidor, la fórmula de la Coca-Cola actual no sea tan valiosa como el plan de la corporación Coca-Cola para su nueva línea de productos. ¿Qué suponen unos cuantos millones de dólares si la empresa competidora puede ahorrarse miles de millones en investigación y desarrollo gracias al robo de información confidencial de Coca-Cola? Marcel van den Berg, de la empresa Team Cymru, plantea la amenaza de la siguiente manera: "todo lo que puede convertirse en dinero es susceptible de ser objetivo de la ciberеconomía

"todo lo que puede convertirse en dinero es susceptible de ser objetivo de la cibereconomía sumergida. Los datos van desde credenciales bancarias de personas a bases de datos de empresas del índice Fortune 100."

Marcel van den Berg, Team Cymru

sumergida. Los datos van desde credenciales bancarias de personas a bases de datos de empresas del índice Fortune 100".

Hay casos en los que los gobiernos fomentan el robo de información comercial confidencial y en algunos países la línea entre lo público y lo privado es difusa. Si los costes de I+D son mínimos o inexistentes, las empresas pueden comercializar los productos más rápidamente y generar grandes beneficios aprovechando las inversiones de otra empresa. El robo de capital intelectual puede llevar a la "muerte lenta y dolorosa" de una empresa, y esto debería ser motivo de preocupación para las empresas de todo el mundo.

En 2009, el funcionario alemán Walter Opfermann, un experto en protección contra el espionaje del estado de Baden-Württemberg, afirmó que China estaba utilizando una serie de métodos sofisticados para interceptar conversaciones telefónicas y, cada vez más, Internet, para apoderarse así de documentación confidencial[1]. Entre los sectores más afectados por los ataques se encuentran fabricantes de coches, compañías de energías renovables, empresas químicas, de comunicaciones, ópticas, de tecnología de rayos x, de maquinaria, de investigación de materiales y armamentísticas. De este modo, los ciberdelincuentes recopilan información sobre investigación y desarrollo, técnicas de administración y estrategias de marketing.

El robo de capital intelectual puede llevar a la "muerte lenta y dolorosa" de una empresa, y esto debería ser motivo de preocupación para las empresas de todo el mundo.

En Italia, en septiembre de 2010, Nigel Stepney, un antiguo ingeniero de Ferrari, fue condenado a 20 meses de cárcel por su implicación en la fuga de datos corporativos que se produjo en 2007. Stepney fue declarado culpable de "sabotaje, espionaje industrial, fraude deportivo y daños graves" por haber entregado datos técnicos de Ferrari al equipo rival McLaren[2].

El capital intelectual es cada vez más vulnerable debido a la convergencia entre las actividades empresariales y las tecnologías de la información. La información confidencial y documentos corporativos residen en bases de datos y se comparten a través del correo electrónico e Internet. Los objetivos de la economía sumergida han cambiado de manera significativa en los dos últimos años. Si bien la compraventa de tarjetas de crédito robadas sigue siendo rentable, últimamente el capital intelectual se ha convertido en la nueva fuente de importantes y rápidas ganancias.

Sin duda, los vectores y objetivos de los ataques virtuales contra la sociedad de la información en red se multiplican. El comité para delitos tecnológicos de la asociación brasileña de abogados (Sección de Sao Paulo), los resume de la siguiente manera: "estamos detectando la actividad de grupos especializados en el sabotaje de redes, servicios e infraestructuras básicas mediante ataques de denegación de servicio distribuido (DDoS) más sofisticados, que provocan pérdidas de beneficios y

un enorme daño a la imagen de grandes empresas. Por otro lado, hay grupos centrados en el reconocimiento de información confidencial y en el espionaje industrial. Las fugas de datos de los gobiernos serán una constante".

En la actualidad, a los ciberdelincuentes les interesa el contenido con fines económicos, y actúan con una gran rapidez y flexibilidad para conseguir sus objetivos. Una vez que se identifica una vulnerabilidad, pueden poner en marcha una gran operación en cuestión de días. Desarrollan un exploit y roban la mayor cantidad de datos posible en un corto período de tiempo. Entonces utilizan "mulas" para enviar sus beneficios (tras adjudicarse una comisión) a los dirigentes de la red clandestina.

El aspecto económico del almacenamiento de datos en el extranjero cobra peso en las decisiones relativas a la gestión de la información, ya que resulta más barato y las empresas son conscientes del beneficio que puede suponer en el futuro. Más de la mitad de las organizaciones que participan en el estudio están volviendo a evaluar los riesgos de procesar la información fuera de sus países debido a la crisis económica. En 2008 sólo cuatro de cada diez lo hacían.

Las firmas corporativas incluidas en los correos electrónicos, los manuales para el empleado y las patentes son los tipos de datos menos protegidos. Una cuarta parte de las organizaciones afirman que dedican muy poco o ningún presupuesto a la protección de dichos documentos. Los datos de clientes y proveedores, la información de los empleados y la información sensible son los datos mejor protegidos, aunque ataques como Operación Aurora (y otros) ponen de manifiesto que la información confidencial más preciada carece de la protección necesaria frente a un agresor sofisticado, a pesar de las protecciones de seguridad.

Tanto el valor de la información como el importe dedicado a protegerla han descendido en los últimos dos años. En 2008, las empresas gastaron aproximadamente 3 dólares estadounidenses en la protección de 1 dólar de datos. Esta cantidad ha aumentado proporcionalmente hasta los 4,80 dólares en seguridad por cada dólar de datos almacenados en el extranjero, debido a que las empresas han disminuido la cantidad de datos almacenados de esta forma, manteniendo el mismo nivel de protección. Al mismo tiempo, aproximadamente un tercio de las empresas están considerando aumentar la cantidad de información confidencial que almacenan en el extranjero, respecto a hace dos años, cuando lo hacían una de cada cinco.

En algunos países los procesos para el almacenamiento de información en el extranjero son más sencillos, gracias a que sus legislaciones en materia de privacidad y notificación son menos estrictas. El 80% de las empresas que almacenan información confidencial en el extranjero tienen en cuenta las leyes de privacidad que obligan a la notificación de las fugas de datos a los clientes. Al mismo tiempo, el 70% de las empresas almacenan información confidencial en países en los que las leyes otorgan un nivel más amplio de autonomía.

Las decisiones que se toman para proteger la información confidencial tienen el objetivo de cumplir las normativas del país. Sin embargo, sólo poco más de un tercio de las empresas piensan que el cumplimiento de las normativas que imponen sus países de origen es muy útil y se centran en lo fundamental para proteger el capital intelectual de su empresa.

Aproximadamente un tercio de las empresas están considerando aumentar la cantidad de información confidencial que almacenan en el extranjero.

Sección 2: La protección de la información confidencial

La cibereconomía sumergida evoluciona al igual que lo hace el tipo de datos atacados. Además, la creciente sofisticación de los ataques ha llevado a un cambio del enfoque en materia de protección de datos. En la actualidad, las empresas no solo tienen que preocuparse del robo de su capital intelectual por parte de la competencia, sino también de la filtración de información confidencial o clasificada a los medios de comunicación, como en el caso de WikiLeaks.

En julio de 2010, Gordon M. Snow, Director Adjunto del FBI, testificó ante el subcomité judicial de la Cámara estadounidense sobre delincuencia, terrorismo y seguridad nacional.

"El impacto de la ciberdelincuencia sobre las personas y los comercios puede ser considerable, y puede ir de una simple molestia a la ruina económica. La perspectiva de obtener considerables beneficios económicos atrae a jóvenes delincuentes y ha contribuido a la creación de una gran cibereconomía sumergida. La cibereconomía sumergida es un mercado invasivo, dominado por unas reglas y una lógica muy próximas a las que rigen el mundo empresarial legítimo, es decir, un idioma único, unas expectativas sobre el comportamiento de sus miembros, así como un sistema de estratificación basado en los conocimientos, las aptitudes, las actividades y la reputación".

Las nuevas amenazas se caracterizan por su persistencia y sofisticación, y los ataques se llevan a cabo a escala mundial. En noviembre de 2010, Postmedia News reveló que el 86% de las grandes empresas canadienses había sufrido ataques, según un informe secreto del gobierno canadiense. El informe también indicaba que, en dos años, el ciberespionaje en el sector privado se había duplicado.

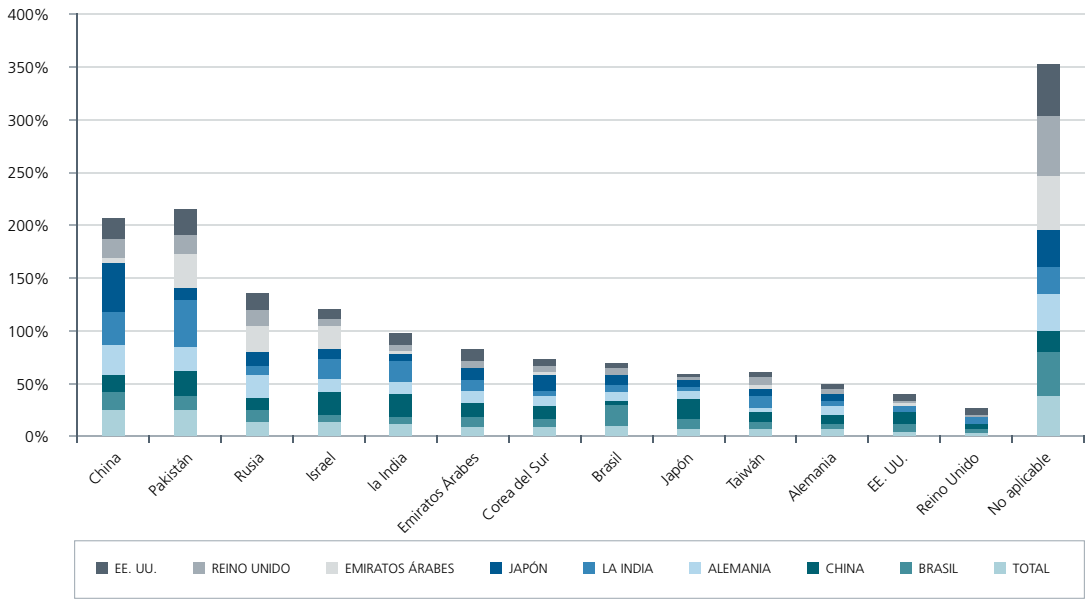
Un informe de Forrester Research elaborado en marzo de 2010 reveló que la documentación corporativa y la información sensible son dos veces más valiosas que otros documentos, que es necesario conservar y proteger, como los datos médicos o la información de tarjetas de crédito y de clientes.

"La documentación confidencial representa dos tercios del valor del total de información de las empresas. A pesar del aumento de normativas a las que tienen que hacer frente

las empresas, los datos protegidos no son los activos más valiosos. Sin embargo, el conocimiento corporativo y la documentación confidencial tienen un valor dos veces superior. Como ponen de manifiesto los recientes ataques contra empresas, la documentación sensible es el objetivo principal"[3].

A pesar de que el 90% de las empresas que almacenan datos en el extranjero llevan a cabo un análisis formal de riesgos, lo que supone un aumento desde 2008, hay algunas que continúan almacenando datos en países de alto riesgo. Si bien es difícil atribuir la responsabilidad de un ataque a un país específico, China, Rusia y Pakistán son considerados como los menos seguros para almacenar datos. Estos tres países ya tenían esta consideración en 2008. Los países considerados más seguros en 2008 eran el Reino Unido, Alemania y Estados Unidos, y lo seguían siendo en 2010.

Figura 1 – ¿Ha evitado su empresa las relaciones comerciales con estos países?



"Más de un cuarto de las empresas evalúan las amenazas o los riesgos a los que están expuestos sus datos dos veces al año o incluso con una frecuencia menor."

Comité de delitos de alta tecnología, asociación brasileña de abogados (Sección Sao Paulo)

Son muchas las empresas que no evalúan las amenazas y los riesgos con la frecuencia que deberían. Más de un cuarto de las empresas evalúan las amenazas o los riesgos a los que están expuestos sus datos dos veces al año o incluso con una frecuencia menor. Más de la mitad de las empresas fijan ellas mismas la frecuencia de estas evaluaciones de riesgos, en lugar de seguir las recomendaciones de los auditores o los requisitos normativos.

Según el comité de delitos de alta tecnología de la asociación brasileña de abogados (Sección de Sao Paulo): "la amplia mayoría de las empresas de distintos sectores carece del control sobre sus directivas de seguridad de la información e incluso grupos de distintas áreas de la empresa, a menudo, tardan en comunicarse entre ellos cuando se producen estos incidentes de seguridad. De hecho, las directivas no son objeto de auditorías regulares por parte de los responsables, lo que multiplica las posibilidades de cometer acciones ilegales. Parecería como si no se sancionaran los actos maliciosos en el seno de las empresas. Las empresas deben mejorar en este punto, concretamente mediante una formación permanente encaminada a proteger su capital intelectual".

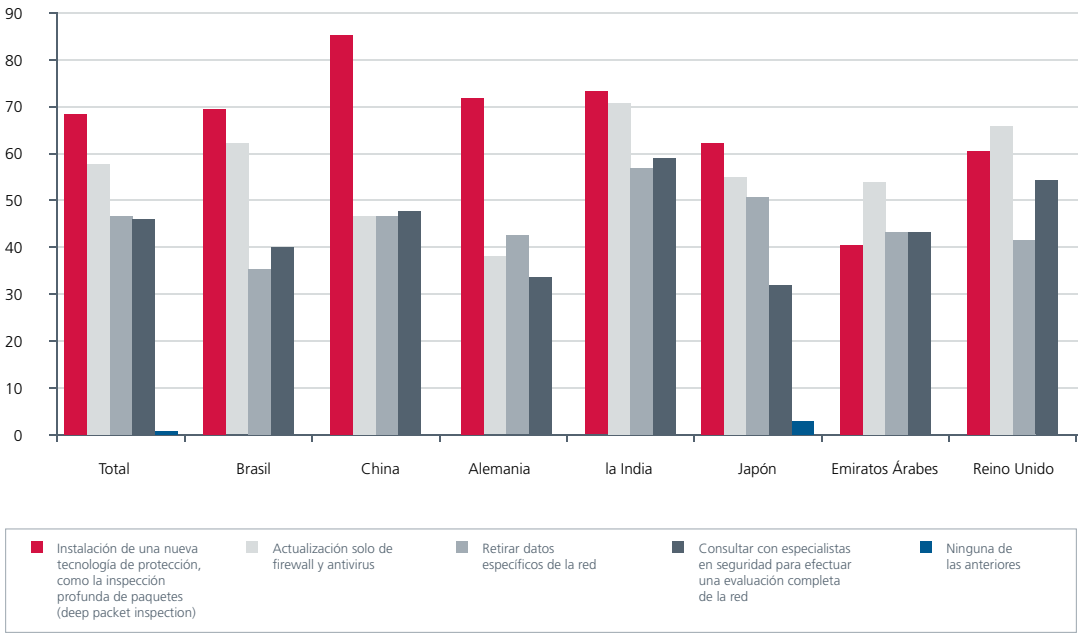
De hecho, las directivas no son objeto de auditorías regulares por parte de los responsables, lo que multiplica las posibilidades de cometer acciones ilegales.

En China, Japón, Reino Unido y Estados Unidos, las empresas dedican de media más de 1 millón de dólares al día en tecnologías de la información (TI).

En China, Japón, Reino Unido y Estados Unidos, las empresas dedican de media más de 1 millón de dólares al día en tecnologías de la información (TI). En Estados Unidos, China y la India, dedican de media más de 1 millón de dólares a la semana en proteger la información confidencial almacenada en el extranjero. Aproximadamente la mitad de las empresas entrevistadas prevén aumentar las partidas dedicadas a la seguridad de TI en ampliaciones de hardware y de software, así como en el alojamiento externo de datos y de otros servicios. Casi un 50% de las mismas estiman que su inversión en la protección de la información confidencial irá en aumento, y sólo un 5% piensa reducir sus gastos.

A pesar del aumento del gasto en seguridad de TI, las soluciones implementadas son, con frecuencia, reactivas. Cuando las empresas deciden tomar medidas de protección, son más propensas a instalar nuevas tecnologías, como la inspección profunda de paquetes (deep packet inspection), según admiten más de dos tercios de las compañías encuestadas. Las soluciones más populares para la protección de los datos confidenciales siguen siendo el software antivirus, los firewalls y los sistemas de prevención/detección de intrusiones (IDS/IPS), implementadas por cuatro de cada cinco empresas.

Figura 2 – Medidas adoptadas para corregir y proteger los sistemas en el futuro



Es interesante destacar que casi la mitad de los encuestados afirmaron estar preparados para "retirar de la red determinados datos" para evitar su fuga. Aquí, la seguridad de los datos se considera más importante para la empresa que la disponibilidad o uso de los mismos.

La protección de los dispositivos móviles sigue siendo un reto para el 62% de las empresas. A la hora de administrar la seguridad de la información, el mayor problema al que se enfrentan las empresas es la naturaleza cambiante de los ataques, seguido muy de cerca por la proliferación de los dispositivos y servicios, como soportes extraíbles, smartphones y sitios web de redes sociales. La movilidad sigue facilitando la productividad y la eficacia de los empleados, una tendencia que no deja de aumentar. Paralelamente, las empresas se interesan cada vez más por las redes sociales para aprovechar sus múltiples ventajas. Estas dos tendencias representan un aumento astronómico del nivel de riesgo al que se enfrentan las empresas en lo relacionado con la fuga de datos. Si a esto unimos la necesidad de las organizaciones de compartir datos críticos con partners estratégicos, resulta imperativo reforzar el enfoque tradicional sobre las necesidades en materia de ciberseguridad."Es muy probable que los ciberdelincuentes se centren particularmente en el desarrollo de técnicas para atacar los smartphones debido a su omnipresencia y a su funcionalidad. Los servicios basados en Internet también pueden representar un nuevo objetivo, no sólo para el robo de datos, sino porque representan recursos e infraestructura barata para cometer actividades ciberdelictivas", afirma Marcel van den Berg de Team Cymru.

La protección de los dispositivos móviles sigue siendo un reto para el 62% de las empresas.

Los servicios basados en Internet también pueden representar un nuevo objetivo, no sólo para el robo de datos, sino porque representan recursos e infraestructura barata para cometer actividades ciberdelictivas

Sección 3: Aumento del impacto de las ciberamenazas en las actividades empresariales

La amplia cobertura mediática de determinados incidentes ha contribuido al aumento de la preocupación sobre la pérdida de información confidencial, especialmente cuando es provocada por el personal interno. En 2008, tres personas fueron condenadas por el robo de planes comerciales de Coca-Cola[4] y un año después, un antiguo programador informático de Goldman Sachs fue detenido por robar código informático de la compañía[5].

"Un solo error cometido por un empleado incauto puede tener terribles consecuencias", explica Dinesh Pillai, CEO de Mahindra Special Services Group, una importante empresa india de consultoría de riesgos para la seguridad. "Un empleado víctima de un ataque de ingeniería social puede dar lugar a fugas de datos fundamentales, pérdidas financieras y daños para la imagen de la empresa, o interrupciones de la actividad comercial. La mayor parte de las tecnologías actuales emplean algoritmos precargados para detectar posibles anomalías. Sin embargo, el mundo clandestino es muy superior en cuanto a capacidad y aptitudes tecnológicas, lo que permite a los agresores identificar fácilmente los medios y formas para irrumpir en los sistemas".

Además, según el comité de delitos de alta tecnología de la asociación brasileña de abogados (Sección de Sao Paulo), es extraño que las amenazas internas sean meramente "accidentales": "según nuestros propios análisis, la amenaza interna más importante proviene de profesionales que podemos considerar "intrusos". Estos profesionales desempeñan funciones de segundo orden y llevan a cabo prácticas de apropiación de datos confidenciales y de ingeniería social.

"Algunas empresas someten a sus empleados directos e indirectos a un control más estricto. En muchos casos, hay profesionales que sufren presiones de bandas de delincuentes que actúan en sus comunidades. A cambio de seguridad de sus familias, estas bandas reclaman a los empleados datos confidenciales, como fechas de entrega de mercancía, terminales electrónicos, planes de distribución, contraseñas de seguridad internas y externas, así como otros datos de la empresa".

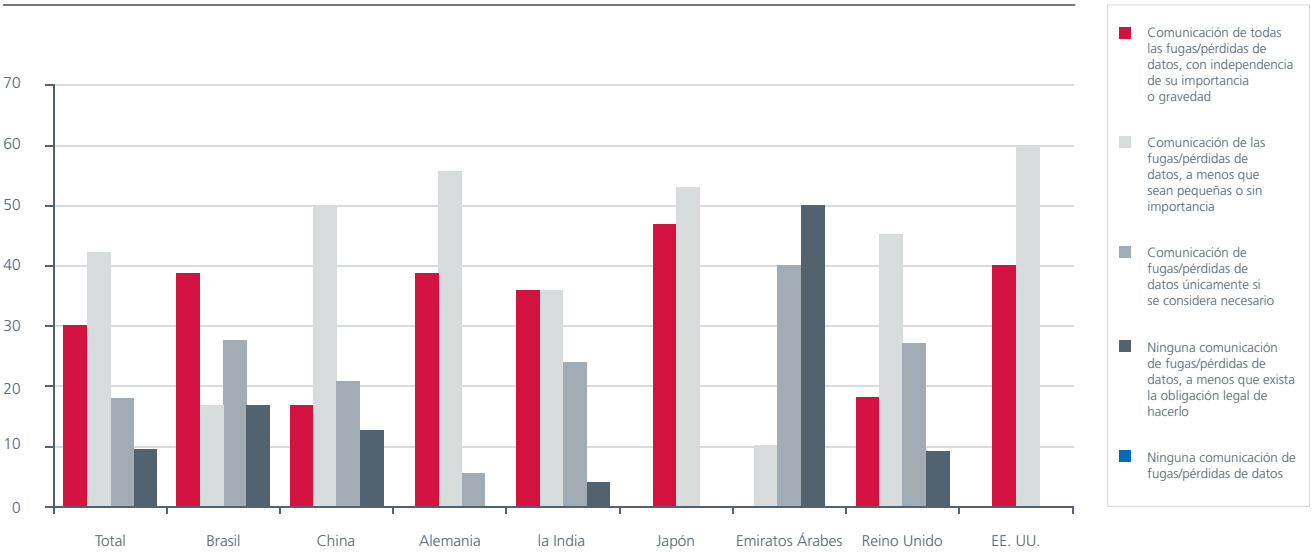
Como resultado, al igual que ocurría en el estudio anterior, el daño a la reputación es la principal preocupación de las empresas. Aproximadamente la mitad de las empresas lo consideran su mayor preocupación cuando se produce una fuga de datos confidenciales o de propiedad intelectual. En la actualidad, una empresa pública que pierda una fórmula secreta, un plan de lanzamiento al mercado o cualquier otro secreto capital, es reticente a informar del hecho por la alarma que el hecho puede provocar entre sus clientes y en su accionariado, y por la reacción desfavorable de los mercados. La divulgación de una filtración de datos en los medios de comunicación puede afectar a la imagen de marca y a su valor en el mercado, por lo que en escasas ocasiones sale a la luz.

Una de cada siete empresas ha evitado informar sobre fugas y/o pérdidas de datos a las autoridades o agencias gubernamentales externas, o a los accionistas. Sólo tres de cada diez empresas comunican todos los casos de fugas o pérdidas de datos que han sufrido, mientras que una de cada diez únicamente comunica estos incidentes cuando tiene obligación legal de hacerlo. En la actualidad, seis de cada diez empresas "eligen" los casos de fuga o pérdida de datos que comunican.

La admisión de una vulnerabilidad importante podría llamar la atención de otros agresores, así que son pocas las empresas que hacen públicas las pérdidas de capital intelectual.

Las actividades asociadas a fusiones y adquisiciones, alianzas y comercialización de productos son víctimas potenciales de robo por parte de redes de delincuentes de la cibereconomía sumergida. Aproximadamente un

Figura 3 – Comunicación de fugas de datos



25% de las empresas ha visto interrumpida o ralentizada una fusión y adquisición o el lanzamiento de nuevos productos o soluciones, debido a una fuga de datos o a la amenaza creíble de una fuga de datos. Casi la mitad de las empresas han experimentado alguna pequeña pérdida de datos y casi un cuarto han sufrido filtraciones de información el año pasado, unos porcentajes superiores a los de 2008.

Además, las fugas de datos resultan caras. De media, los datos perdidos/filtrados han costado a las empresas más de 1,2 millones de dólares, frente a menos de 700.000 dólares en 2008.

Es posible que esto explique por qué sólo un 25% de las empresas realiza análisis a posteriori de una fuga o pérdida, y sólo la mitad toman medidas para solucionar y proteger los sistemas en el futuro tras producirse una brecha o una tentativa de intrusión. Más de la mitad de las empresas han decidido, en algún momento de su historia, no perseguir o investigar un incidente de seguridad debido al coste que ello implicaría. Con más frecuencia, las empresas analizan o investigan las fugas de datos poco importantes internamente, en lugar de buscar ayuda externa. Esta ausencia de investigación significa que los posibles vectores de ataque no se han circunscrito y que la amenaza persiste o que sigue siendo posible una nueva intrusión en el futuro. Si no se ha identificado al personal interno implicado y no se han investigado las causas de los incidentes anteriores, no será posible identificar una futura amenaza más importante. La ausencia de medidas que lo solucione expone a las empresas al riesgo de fugas en el futuro.

La amenaza más importante que han comunicado las empresas en relación a la protección de la información confidencial es la fuga de datos provocada de manera accidental o intencionada por los empleados. El cumplimiento de los procedimientos de seguridad por parte de los empleados es el reto más importante para la seguridad de la información en las empresas. Este factor pesa más que otros, como el uso de varios sistemas dentro la organización o la inseguridad de los sistemas de partners de la cadena logística. Parece claro que las medidas implementadas no han puesto freno a las fugas de datos, lo que ha obligado a las empresas a elegir soluciones tecnológicas robustas e innovadoras para reforzar sus políticas.

Una de cada diez únicamente comunica estos incidentes cuando tiene obligación legal de hacerlo.

Sección 4: Las soluciones y las directivas van de la mano

Para muchas empresas, las decisiones en materia de gestión de riesgos y de seguridad se basan en el estricto respeto de las normas de cumplimiento, no sólo en la protección de su capital intelectual. Estas empresas no son siempre conscientes de que una fuga de datos puede tener un gran impacto en la actividad comercial y en la productividad, y que puede traducirse en una ralentización del desarrollo de productos o de un procedimiento de fusión y adquisición.

Es necesario que directivas y soluciones avanzadas vayan de la mano para que la situación cambie realmente. Estas directivas deben implementarse junto con tecnologías de inspección profunda de paquetes (deep packet inspection), de prevención de la fuga de datos, de supervisión de amenazas avanzadas, de análisis forense e incluso de medidas tales como retirar determinados datos de la red.

Además, la distinción entre amenazas internas y externas está desapareciendo. "Los agresores sofisticados pueden infiltrarse en una red, apoderarse de credenciales válidas y disponer de una gran libertad de acción, igual que lo haría un empleado. Disponer de estrategias defensivas contra estas amenazas internas combinadas es esencial, y las empresas necesitan herramientas específicas capaces de predecir estos ataques", afirma Scott Aken, Vicepresidente de la división Cyber Operations en SAIC.

Tom Kellermann, Vicepresidente de la división Securiry Awareness de Core Security Technologies, cita la ausencia de calendarios bien definidos para las pruebas de intrusiones y de medidas adecuadas como el punto débil de las estrategias de ciberseguridad de muchas empresas. Además, una autenticación débil, una seguridad inalámbrica permeable y una tecnología de detección de intrusiones inadecuada contribuyen a agravar el problema.

Según Kellermann, es necesario evaluar regularmente las funciones de análisis forense y de intervención en caso de incidente. "Las amenazas persistentes avanzadas ponen de manifiesto la necesidad de que el sistema de respuesta a incidentes incluya un mapa de rutas de ataque. Los proveedores de servicios gestionados de terceros, como las empresas de alojamiento y proveedores de infraestructura basada en la nube deben comprometerse formalmente a probar su estado de seguridad y a cumplir las normativas más exigentes sobre ciberseguridad, para evitar convertirse en brechas enormes por las que puedan infiltrarse todo tipo de depredadores", añade Kellermann.

"La mayoría de las empresas siguen considerando la seguridad como un problema asociado al perímetro. Sin embargo, puesto que el perímetro se sigue ampliando con la llegada de dispositivos móviles y el "cloud computing", el trabajo de un departamento de ciberseguridad se hace cada día más complicado", añade Aken.

A continuación se enumeran algunas tendencias emergentes que cambian los métodos mediante los cuales las empresas se protegen de los ataques sofisticados y de las fugas internas:

Inspección profunda de paquetes (DPI – Deep Packet Inspection): se trata de una solución muy flexible que viene a complementar la arquitectura de seguridad existente, a través del análisis completo de paquetes en línea casi en tiempo real de todos los paquetes (niveles 2-7), es decir, sin pérdida de paquetes. Las aplicaciones de software instaladas sobre el hardware permite la implementación de cualquier tipo de estrategia basada en reglas para retirar determinados datos de los paquetes que abandonan la red, así como para impedir todo tipo de exploit de tráfico entrante.

Seguridad de red basada en el comportamiento humano: estas son soluciones que están un paso por delante de los hackers internos o externos que detectan las intenciones mediante un análisis de las actividades que se llevan a cabo en la red. No utilizan firmas, detección de anomalías ni análisis heurístico, sino los comportamientos humanos comunes en todas las acciones engañosas de una red, con el fin de detenerlos antes de que los datos abandonen la red.

Herramientas de detección de amenazas internas: innovaciones recientes en tecnologías contra amenazas internas han permitido crear suites de herramientas que se pueden implementar en los sistemas para supervisar miles de usuarios internos de forma simultánea, realizando un seguimiento de sus actividades e identificando características inherentes que provocan alertas. Mediante la creación de perfiles de actividades sospechosas en tiempo real, estas soluciones pueden interrumpir las conexiones en caso de eliminación no autorizada de datos o de actividades inusuales y críticas.

Análisis forense avanzado: cada dispositivo digital, ordenador o teléfono móvil deja una huella digital que se pueden rastrear a través de sofisticados análisis de ordenadores y redes. Las herramientas y servicios de software ayudan a descubrir y extraer el contenido crítico e identificar los comportamientos de los usuarios y las características exclusivas. Conocer los fallos y vulnerabilidades que llevan a un ataque es el primer paso en la prevención del siguiente ataque.

Análisis de malware avanzado: ahora es posible descubrir malware de tipo zero-day que utilizará o que utiliza exploits de red para atacar una red. Una vez descubierto, el malware puede capturarse con fines de análisis y respuesta.

Conclusión

Aunque es imposible eliminar completamente los fallos de la ciberseguridad, las empresas pueden reducir enormemente los riesgos asociados a la fuga de datos confidenciales. Las empresas buscan soluciones para supervisar los movimientos de información confidencial y detener las pérdidas potenciales de datos, ya sean intencionadas o no. Estas soluciones existen.

Se pueden instalar dispositivos en la red para grabar y clasificar todas las interacciones con Internet. Además, hay equipos capaces de explorar los datos estructurados y no estructurados almacenados, de manera que las empresas puedan buscar y descubrir dónde se guardan los datos confidenciales. Si bien estos dispositivos no son nuevos, se amplían continuamente e incorporan más funciones predictivas basadas en el comportamiento humano. Tecnologías como la inspección profunda de paquetes (deep packet inspection), el análisis del comportamiento humano y el cifrado son soluciones que serán cada vez más utilizadas y efectivas en los próximos años.

En la actualidad, las empresas van más allá del cumplimiento de normativas y se esfuerzan en proteger los datos confidenciales –como documentos de diseño, esquemas técnicos, planes de lanzamiento de productos, fórmulas farmacéuticas–, en definitiva, su capital intelectual. Estos documentos son mucho más complejos que simples números de documentos de identidad o de tarjetas de crédito, y requieren soluciones de protección avanzadas.

Scott Aken cree que la protección de la empresa empieza por la concienciación y por conocer qué es lo que se debe proteger.

"La mayoría de las empresas gastan enormes sumas de dinero en proteger las partes menos críticas de su red, mientras que lo esencial, su capital intelectual, permanece desprotegido. El análisis riguroso de los recursos que residen en la red, junto con una profunda estrategia de defensa eficaz, todo ello implementado por un equipo adecuadamente formado, son clave a la hora de proteger los datos de una empresa".

Colaboradores

Scott Aken, Vicepresidente de la división Cyber Operations, SAIC

Jenifer George, Directora de Cyber Portfolio, SAIC

Marcel van den Berg, Jefe de equipo del proyecto Business Intelligence, Team Cymru

Simon Hunt, Vicepresidente y CTO de la división Endpoint Security, McAfee

Tom Kellermann, Vicepresidente de la división Security Awareness, Core Security Technologies

Dinesh Pillai, CEO, Mahindra Special Services Group

Erasmo Ribeiro Guimarães Junior, Secretario y miembro del comité de delitos de alta tecnología, asociación brasileña de abogados (Sección Sao Paulo)

Marco Aurélio Pinto Florêncio Filho, Vicepresidente del comité de delitos de alta tecnología, asociación brasileña de abogados (Sección Sao Paulo)

Coriolano Aurélio de Almeida Camargo Santos, Presidente del comité de delitos de alta tecnología, asociación brasileña de abogados (Sección Sao Paulo)

Referencias:

1 *http://www.guardian.co.uk/world/2009/jul/22/germany-china-industrial-espionage*

2 *http://f1grandprix.motorionline.com/condannato-nigel-stepney-patteggia-1-anno-e-8-mesi/*

3 *http://www.rsa.com/products/DLP/ar/10844_5415_The_Value_of_Corporate_Secrets.pdf*

4 *http://www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf*

5 *http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aSDxSdMlPTXU*

McAfee

McAfee, empresa subsidiaria propiedad de Intel Corporation (NASDAQ:INTC), es líder en tecnología de seguridad. McAfee tiene el firme compromiso de afrontar los más importantes retos de seguridad. La compañía proporciona servicios y soluciones probados y proactivos que ayudan a proteger redes, dispositivos móviles y sistemas en todo el mundo, permitiendo a los usuarios conectarse a Internet, navegar por la Web y realizar compras online de forma más segura. Gracias a la tecnología Global Threat Intelligence (Inteligencia Global de Amenazas), McAfee proporciona protección en tiempo real mediante sus soluciones de seguridad, permitiendo a las empresas, usuarios particulares, organismos públicos y proveedores de servicios cumplir con la normativa, proteger datos, prevenir interrupciones, identificar vulnerabilidades y controlar cualquier tipo de amenaza que pueda poner en peligro su seguridad. En McAfee enfocamos todos nuestros esfuerzos en la búsqueda constante de nuevas soluciones y servicios que garanticen la total seguridad de nuestros clientes.

www.mcafee.com/es

SAIC

SAIC es una empresa FORTUNE 500® especializada en aplicaciones tecnológicas, científicas y de ingeniería, que utiliza su profundo conocimiento de dominios para resolver problemas de vital importancia para EE. UU. y para el mundo, en materia de seguridad nacional, energía y medio ambiente, infraestructuras críticas y salud.

SAIC: From Science to Solutions®
Para obtener más información, visite www.saic.com

SAIC

McAfee

McAfee,
Avenida de Bruselas nº 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8535
www.mcafee.com/es