websense®

PREVENCIÓN DEL ROBO DE DATOS

LA CLAVE PARA LA SEGURIDAD, EL CRECIMIENTO Y LA INNOVACIÓN

PREVENCIÓN DEL ROBO DE DATOS

RESUMEN EJECUTIVO

Las herramientas y las mejores prácticas de seguridad de datos continúan evolucionando; aun así, las pérdidas atribuidas a las fugas de datos continúan sobrepasando las defensas de datos. En 2014, las fugas de datos comprometieron más de 700 millones de registros, con pérdidas financieras estimadas en al menos $400 millones. Aún más difícil de estimar es el daño causado a la marca y la reputación de una compañía después de que sus datos fueron robados. A pesar de las grandes inversiones en seguridad de datos, muchas organizaciones descubrieron, de la manera más dura, que las soluciones de punto actuales basadas en firmas hacen muy poco para detener los ataques cibernéticos avanzados.

Los líderes industriales y mundiales están recurriendo a las gerencias de primera línea y a los órganos del gobierno para impulsar el cambio tan necesario para hacer de la seguridad cibernética una prioridad. Al mismo tiempo, los líderes de seguridad necesitan mantener sus equipos enfocados en los objetivos generales de su inversión en seguridad cibernética. Obsesionarse con la última tecnología o distraerse con las amenazas más recientes promocionadas de manera exagerada en los medios no ayuda a los equipos de TI a elevar el nivel de seguridad de los datos de sus organizaciones.

Por el contrario, los equipos de TI necesitan adoptar un enfoque más holístico para proteger sus datos esenciales. La seguridad cibernética que ofrece una perspectiva de prevención del robo de datos tiene un alcance más extenso, una aplicación más inteligente y una mejor eficacia para defender sus datos esenciales. Una postura centrada en los datos como esta es una mejora de las defensas de datos, ya que garantiza que los datos estén seguros contra amenazas entrantes y salientes. De este modo, la prevención del robo de datos comprende una completa postura de seguridad, no simplemente la prevención de la pérdida de datos (DLP).

Además, los equipos de TI de las organizaciones deben alcanzar estos objetivos de seguridad de los datos y, al mismo tiempo, cumplir con los otros dos objetivos de TI, que son ayudar a la organización a crecer y a innovar. Con frecuencia, estos dos últimos objetivos se pierden en el esfuerzo por brindar protección contra el robo de datos. Pero la verdad es que TI, y los datos esenciales que TI administra y protege, existe para servir a la organización permitiéndole adoptar nuevas tecnologías, evolucionar los procesos y mantener sus ventajas competitivas en el mercado.

EN 2014,

LAS FUGAS DE DATOS COMPROMETIERON MÁS DE 700 MILLONES DE REGISTROS, CON PÉRDIDAS FINANCIERAS ESTIMADAS EN AL MENOS $400 MILLONES

EL AÑO DE LAS FUGAS DE DATOS Y MÁS

Las fugas de datos masivas de alto perfil que se produjeron el año pasado y provocaron costosos incidentes de robo de datos en importantes instituciones financieras, proveedores de atención de la salud, organismos de gobierno, comerciantes minoristas y otras organizaciones son solo el comienzo de una tendencia a largo plazo. El atractivo que brinda la facilidad y la considerable ganancia financiera, además de la explosión en la cantidad de participantes en el escenario de las amenazas, no hacen más que garantizar que esta costosa tendencia de robo de datos continuará. Y aunque sucedieron en industrias diferentes, los principales incidentes de robo de datos de 2014 se debieron una o más de las tres causas siguientes:

- Ataques maliciosos y robo de datos perpetrados por atacantes externos.
- Fugas accidentales de información esencial debido a errores de usuarios y procesos comerciales interrumpidos.
- Robo de datos interno con motivaciones financieras, políticas, vengativas o de otra índole.

Estas tres fuentes principales de amenazas a los datos han permitido que los atacantes alcancen un éxito desenfrenado en sus intentos de traspasar las defensas, incluso en las organizaciones que más dinero han invertido en seguridad. Los equipos de TI que se aferran a maneras de pensar antiguas sobre la defensa de los datos y las herramientas de seguridad estáticas simplemente están haciendo de sus datos esenciales un blanco aún más vulnerable para el robo. Esta realidad cuadra con la **encuesta de Pricewaterhouse** que informa que los incidentes de seguridad de datos aumentaron un 66 % en 2014.

LOS INCIDENTES DE SEGURIDAD
AUMENTARON UN 66 % EN 2014

Por ejemplo, los piratas informáticos encontraron maneras de explotar nuevas tecnologías y lograr acceso a través de terceros que resultan confiables y también mediante señuelos sofisticados diseñados para las redes sociales. Todos estos métodos destinados a violar la seguridad de los datos fueron exitosos en forma individual o combinados. Este nuevo desafío de las nuevas amenazas y los métodos de ataque altamente exitosos pone aún más presión en las defensas de TI para que incorporen análisis en tiempo real del tráfico entrante y saliente para detectar una potencial actividad de amenazas.

PREVENCIÓN DEL ROBO DE DATOS Y AMENAZAS INTERNAS

Sin embargo, si bien el panorama de amenazas externas se ha vuelto muy riesgoso, las amenazas internas presentan un riesgo aún mayor para sus datos esenciales. En comparación con los datos robados intencionalmente, el doble de datos esenciales se pierde en forma accidental. A menudo, simplemente se trata de empleados y/o socios confiables que inadvertidamente generan nuevos riesgos para sus datos esenciales al buscar soluciones alternativas y otros métodos de **'TI en la sombra'** para cumplir con sus responsabilidades.

Las amenazas internas varían considerablemente y tienen diferentes causas y fuentes. Algunas, sin duda, están motivadas por cuestiones financieras, o conflictos personales o políticos con la organización. Sin embargo, a menudo la fuga de datos se debe a que un empleado inadvertidamente tiene un comportamiento riesgoso por costumbre, ignorancia o ambas cosas. Cualquiera que sea la motivación o la causa, las amenazas internas continuarán provocando pérdidas de datos devastadoras en muchas organizaciones.

Pero el robo de datos producido por las amenazas internas no es solo culpa del usuario final. Lamentablemente, la pérdida de datos derivada de causas internas y socios a menudo es el resultado de la reputación de TI como el "departamento del NO". Esta dinámica de causa y efecto debe cambiar. Es necesario que las defensas de datos se adapten a la tecnología cambiante tanto como al panorama cambiante de amenazas para que los equipos de TI puedan decir 'SÍ' a la innovación y las oportunidades de crecimiento.

EN COMPARACIÓN CON LOS DATOS ROBADOS INTENCIONALMENTE,
EL DOBLE DE DATOS ESENCIALES
SE PIERDE EN FORMA ACCIDENTAL

La prevención del robo de datos brinda protección contra las amenazas internas mediante el uso de defensas digitales para monitorear el correo web, los medios sociales, las funciones de impresión y otros canales de intercambio de datos en busca de un potencial abuso. También utiliza defensas físicas para asegurar los puertos USB y otros medios extraíbles. Además, la prevención del robo de datos permite a los equipos de TI aprovechar el análisis de comportamiento anómalo para identificar a los usuarios de alto riesgo antes de que se produzca el robo de datos.

NO PERMITA QUE EL TEMOR ANULE EL CRECIMIENTO Y LA INNOVACIÓN

En esta era de ataques sofisticados, avances tecnológicos rápidos y amenazas internas, las organizaciones que no cuentan con un enfoque holístico de seguridad de datos tendrán dificultades para encontrar el equilibrio entre asegurar los datos y proporcionar un acceso apropiado. Con bastante razón, el temor a la pérdida de datos influye en la vacilación de las organizaciones frente a la adopción de nueva tecnología con la rapidez que lo harían en otras circunstancias. El fantasma y el costo de una fuga de datos pública del nivel de la de Sony, Home Depot, Target, Anthem y otros casos de robo de datos de alto perfil en los últimos años han tenido un efecto negativo en el uso de servicios en la nube como Office 365 y Box Enterprise, por ejemplo.

Aun así, las necesidades comerciales exigen que las organizaciones adopten nuevas tecnologías en forma regular si desean continuar innovando y creciendo. Si no lo hacen, corren el riesgo de ser superados por sus competidores, perder oportunidades de crecimiento y de participación en el mercado, o incluso la capacidad de sobrevivir. Este temor a la fuga de datos irónicamente también ha sido un factor que contribuyó a la aparición de 'TI en la sombra' en algunas organizaciones, donde de manera no oficial los empleados adoptan herramientas para hacer su trabajo, donde y cuando los departamentos de TI no responden a sus necesidades.

Como se mencionó antes, las demandas comerciales impulsan estas respuestas arriesgadas. Los usuarios de *roaming* tienen la necesidad de acceder a datos esenciales desde múltiples ubicaciones, como por ejemplo desde su oficina en el hogar, una cafetería o un aeropuerto. El personal necesita colaborar y compartir información confidencial internamente y con socios confiables. Los dispositivos móviles y el incipiente Internet de las cosas (IoT) necesitarán seguridad de datos para ser totalmente adaptables. La verdad es que la nueva tecnología realmente trae consigo nuevos riesgos, pero también nuevas oportunidades.

ADOPTE NUEVAS TECNOLOGÍAS CON CONFIANZA

La prevención del robo de datos le permite adoptar con éxito el cambio tecnológico y nuevas oportunidades, y al mismo tiempo reducir el riesgo al agregar tres elementos a su postura de seguridad:

- Seguridad adaptable y atenta al contexto.
- Protección de datos en todos lados.
- Elevación del coeficiente de inteligencia en seguridad de los equipos de TI y los empleados.

La implementación de seguridad adaptable es una respuesta obvia y necesaria para el panorama de amenazas que cambia rápidamente. Pero también debe adaptarse a las tecnologías cambiantes que se adoptan. Los servicios en la nube, como Office 365, dispositivos finales Mac y otras tecnologías, han estado en el mercado durante un tiempo; sin embargo, incluso en la actualidad, pocas soluciones proporcionan apoyo completo para asegurar los datos durante su uso.

Además, los trabajadores remotos necesitan trabajar con datos esenciales en cualquier lugar donde se encuentren. Pero la adopción de servicios en la nube y otras herramientas de colaboración pueden colocar sus datos fuera del perímetro de defensa. Sus datos esenciales deben estar protegidos en cualquier lugar donde residan o donde se acceda a ellos. Sus soluciones de seguridad de datos deben poder identificar, controlar y defender sus datos del robo en cualquier lugar y en todos los lugares.

Finalmente, hacer frente a los desafíos que presentan los atacantes incluye mucho más que soluciones tecnológicas solas. Las organizaciones deben invertir en la capacitación continua de profesionales en seguridad y prepararlos para contrarrestar el creciente déficit de habilidades. Afortunadamente, la generación actual de usuarios ha crecido con la tecnología, como teléfonos inteligentes y medios sociales, lo cual constituye la base para comprender los principios básicos de la seguridad. Sin embargo, aún deben recibir capacitación y actualizaciones regulares sobre mejores prácticas para usar los vehículos de ataque comúnmente explotados, como Wi-Fi, los medios sociales y el correo electrónico.

UN ENFOQUE HOLÍSTICO A LA SEGURIDAD DE DATOS

La prevención del robo de datos nos obliga a pensar más allá de la amenaza más reciente o la emocionante tecnología de seguridad. Si bien aún quedan lecciones por aprender derivadas de la conmoción que genera una

nueva e innovadora técnica de amenazas, las defensas deben ser siempre mantenidas para atacar cualquier amenaza, conocida o desconocida. Distraerse con una nueva y radiante tecnología de defensa de última generación nunca ha generado un retorno de inversión a largo plazo. Los delincuentes cibernéticos siempre encontrarán maneras de evadirlas o atravesarlas.

La prevención del robo de datos también cubre la necesidad de coordinar las defensas en las actividades entrantes y salientes. La defensa de actividades salientes no solo debe evitar que los datos confidenciales vayan a lugares que no deberían, sino también controlar las redes bot y otros tipos de tráfico saliente malicioso. Las defensas de actividades entrantes son el costado proactivo de la prevención del robo de datos, ya que identifican la actividad de amenazas indicativa de un ataque en progreso, e incluso sondeos y pruebas previos que realiza un atacante antes de un ataque. En un nivel más granular, TI debe aplicar la **cadena de avance de un ataque** como una herramienta para evaluar las capacidades actuales de la prevención del robo de datos, con la dimensión agregada de cómo las defensas comparten información en toda la cadena de avance de un ataque para identificar ataques altamente evasivos.

Esto requiere un cambio en la manera de abordar la seguridad en tres áreas principales:

- Seguridad web
- Seguridad de correo electrónico
- Prevención de la pérdida de datos (DLP)

Desde sitios web comprometidos hasta enlaces maliciosos en medios sociales, la web se ha convertido en un factor principal en las amenazas modernas. Pero dados los funestos antecedentes de un enfoque de detección de malware, brindar defensas contra amenazas en la web requiere de una defensa coordinada que pueda analizar códigos y contenido web en tiempo real, así como también verificar señuelos, redirecciones, kits de explotación y demás componentes numerosos de las amenazas avanzadas.

DEMASIADAS SOLUCIONES DE SEGURIDAD DE CORREO ELECTRÓNICO NO ESTÁN A LA ALTURA DE LAS CIRCUNSTANCIAS

Para la mayoría de las fugas importantes mencionadas anteriormente, los investigadores informaron que probablemente comenzaron con un mensaje de correo electrónico. En consecuencia, los ataques de phishing de esta naturaleza van en aumento simplemente debido a que son eficaces —el **informe sobre investigaciones de fugas de datos 2015 de Verizon** indica que el 23 % de los destinatarios abrió mensajes de phishing y el 11 % hizo clic en el enlace incluido en el mensaje. Para los que están preocupados por la prevención del robo de datos, es una prioridad detener una amenaza en la etapa más temprana, aún así demasiadas soluciones de seguridad de correo electrónico no están a la altura de las circunstancias.

Incluso la selección e implementación de la prevención de la pérdida de datos (DLP) juega un papel importante como parte de una estrategia completa de prevención del robo de datos. Las capacidades avanzadas, como el reconocimiento óptico de caracteres (OCR) y DLP por goteo, se convierten en requisitos básicos. Asegurar los dispositivos finales Mac es tan importante como un dispositivo final de Windows, y requiere las mismas capacidades cuando estén en la red y también fuera de las instalaciones. Y la verdadera prevención del robo de datos también requiere de capacidades para retener el control de los datos almacenados en servicios en la nube, como Office 365, Box Enterprise, Salesforce.com, etc.

Sin embargo, la eficacia completa de una estrategia de prevención del robo de datos solo se puede apreciar cuando la actividad de amenaza identificada en diversas etapas de un ataque está correlacionada. La inteligencia compartida proporciona una imagen general, de manera que se puedan correlacionar múltiples eventos 'sospechosos' para identificar una amenaza verdaderamente maliciosa. La validez de este enfoque holístico ante las amenazas persistentes avanzadas (APT) y otras amenazas avanzadas ha sido demostrada tanto por analistas como por organizaciones de evaluación independientes.

WEBSENSE® TRITON® APX Y LA PREVENCIÓN DEL ROBO DE DATOS

La prevención del robo de datos es un enfoque de seguridad centrado en los datos que conduce a la toma decisiones estratégicas, muy por encima del ruido de la última tecnología prometedora o la amenaza más reciente. Otorga poder a los empleados de la misma manera que asegura los datos en el corazón de la organización. La prevención del robo de datos comprende los productos, las personas y los procesos que tocan los datos de maneras tales que pueden hacer avanzar la organización. Sin ella, las organizaciones continúan en una posición de mayor riesgo de sufrir una fuga de datos.

Como defensa unificada, Websense TRITON APX es una plataforma de seguridad que proporciona una solución coordinada para la prevención del robo de datos. Monitorea múltiples canales en busca de actividad de amenazas en toda la cadena de avance de un ataque para identificar actividad maliciosa o sospechosa, entrante o saliente. También proporciona capacidades de defensa únicas en la industria, junto con soporte para tecnologías cada vez más populares, como Office 365 y dispositivos finales Mac, además de que eleva el coeficiente de inteligencia en seguridad de su equipo de TI y sus empleados.

Websense TRITON APX es la solución de prevención del robo de datos que le permite a su organización...

DESAFIAR AL NUEVO MUNDO.

OBTENGA MÁS INFORMACIÓN SOBRE LA PREVENCIÓN DEL ROBO DE DATOS EN www.websense.com/DTP

© 2015 Websense, Inc. Todos los derechos reservados. Websense y los logotipos de Websense, TRITON y ThreatSeeker son marcas comerciales registradas de Websense, Inc. en los Estados Unidos y varios países. Todas las demás marcas son propiedad de sus respectivos dueños. [DTP-WP-ESLA-8MAY15]