CUSTOMERONE

Symantec

Symantec Data Loss Prevention: Desde su Adopción hasta su Madurez

En el verano de 2015, un funcionario de Symantec de forma involuntaria violó la política interna cuando configuró su cuenta de trabajo para enviar de forma automática correos electrónicos a su cuenta personal. Posteriormente, un colega de trabajo envió por correo electrónico un fragmento del código fuente - otra violación de política, agraviada por el hecho que el código estaba siendo transmitido fuera de la empresa.

Ningún funcionario tuvo intenciones maliciosas, pero sus atajos podrían haber expuesto nuestro activo más valioso - nuestro código fuente - a varios delincuentes alrededor del mundo.

Afortunadamente, la solución Symantec Data Loss Prevention (DLP) estaba activa. Alertó a nuestro Centro de Operaciones de Seguridad que alguien estaba enviando el código fuente por correo electrónico. Un equipo de respuesta a incidentes entró en acción, investigó la actividad y la impidió antes de que se produjese cualquier daño.

Si no estuvieramos usando Symantec DLP, quizás no sabriamos de estas violaciones hasta algunos meses después o tal vez nunca lograriamos identificarlas. Por esa razón, hicimos de la solución una parte importante de nuestra estrategia de protección. Alerta a nuestro equipo de seguridad siempre que la información confidencial es enviada por correo electrónico, guardada en una unidad USB, o transmitida de otra forma por la red de forma sospechosa, permitiéndonos tomar medidas inmediatas y garantizar que ninguna política esté siendo violada.

Symantec Data Loss Prevention: Desde su Adopción hasta su Madurez fue escrito para informar a los CIOs, CTOs, CISOs y otros ejecutivos acerca de nuestra jornada para ayudar en la protección de nuestros datos. En este artículo explicamos los retos que enfrentamos, cómo los solucionamos y las valiosas lecciones aprendidas. También describimos nuestras mejores prácticas y las experiencias de nuestros funcionarios de TI a medida que desarrollaron e instalaron una de las soluciones más robustas para prevención de pérdida de datos en el segmento.

Data Loss Prevention – Encontrar la Estrategia Correcta

Todas las compañías poseen información que necesitan mantener en sigilo. Esa información puede ser el código fuente, datos de clientes o información de identificación personal, el precio a pagar es alto si los archivos confidenciales escapan de su red. Parte de la respuesta implica mantener a los delincuentes fuera de su red, pero si los hackers logran invadirla (tal vez a través del robo de credenciales de usuario de un funcionario), necesita garantizar que no consigan extraviar la información.

También necesitamos esta garantía. Y para ello, confiamos en Symantec DLP.

"Nuestra principal prioridad es proteger los activos más críticos de Symantec: código fuente, datos de clientes e información personal de identificación de nuestros funcionarios", dice Tim Fitzgerald, nuestro director de seguridad. "Una implantación amplia y creativa de Symantec DLP es una de las herramientas más poderosas que tenemos para ayudarnos a lograr nuestro objetivo".

El producto es altamente personalizable, entonces es importante ajustarlo para atender a las necesidades específicas de su propia empresa. Ese paso puede llevar algún tiempo - trabajamos durante dos años para establecer nuestra propia estrategia ideal, sin embargo, como lo podrá confirmar, nuestros resultados valdrán el esfuerzo.

Visión General Estratégica

Rastrear su información involucra cinco etapas:

1. Decida cuál es la información que desea rastrear
2. Marcar la información con una marca de agua u otro identificador secreto
3. Crear reglas para que reciba alertas cuando alguien mueve esas informaciones con marcas de agua en circunstancias inusuales
4. Garantizar que las alertas sean evaluadas y respondidas de forma inmediata
5. Refinar las reglas para minimizar falsos positivos

Historial

Symantec adquirió en 2007 su producto Data Loss Prevention. Como el principal objetivo de la empresa era fortalecer nuestro portafolio de productos, la idea de implementarlo internamente era apenas una prioridad secundaria.

En aquel momento, nuestro equipo de TI estaba tercerizando algunos de sus esfuerzos de infraestructura para un tercero. Cuando solicitamos al proveedor para configurar Symantec DLP en nuestra compañía, nuestro objetivo inicial era usarlo para proteger nuestra red y endpoints, y no necesariamente monitorear nuestro código fuente.

Reevaluamos la situación en 2012. Fue cuando internalizamos la administración de nuestras operaciones de TI. A partir de ese punto, decidimos aprovechar al máximo los recursos de Symantec DLP, instalándolo como parte fundamental de nuestra estrategia de protección de código fuente.

Navegar la Curva de Aprendizaje

Cuando implementamos Symantec DLP, nuestra idea inicial era correcta, pero descubrimos que habría una curva de aprendizaje. Nuestra empresa posee un extenso conocimiento en cómo ajustar Symantec DLP, pero nuestros equipos de TI, que conocían el producto hacía poco tiempo, crearon reglas muy amplias y no tan bien planeadas.

"Nosotros tratamos la solución como un software antivirus - basta apenas activarla y dejarla funcionar", dice Tim. "En retrospectiva, la solución Data Loss Prevention no funciona de esa forma. Es una herramienta de caza muy sofisticada, pero si no le informa lo que debe ser cazado, encuentra todo y no es útil".

Esa también es la principal reclamación que recibimos de los clientes. Ellos configuran reglas amplias para todo, desde números de tarjeta de crédito hasta números de documentos de identidad, y acaban con una avalancha de alertas tan grande que desisten y cancelan totalmente las reglas.

Aquí cómo evitarlo: antes de comenzar, su equipo ejecutivo y profesionales de seguridad necesitan tener un diálogo detallado acerca de la gestión de riesgos. Identifique los datos que necesita proteger y lo que considera como una amenaza, seguidamente, llame a sus ingenieros para desarrollar las políticas adecuadas.

Nosotros elaboramos ese proceso de forma contraria. Solicitamos que nuestros ingenieros crearan políticas y al recibir muchas alertas, reconfiguramos las reglas e intentamos nuevamente, un método de ensayo y error que duró más de un año.

Si hubiésemos creado inicialmente la estrategia, podríamos haber llegado al nivel de protección deseado en pocos meses.

En paralelo con la creación y pruebas de nuestras políticas, desarrollamos una forma secreta de marcar nuestro código fuente, de modo que la solución Symantec DLP pudiera acompañar la forma como el código fuente es transmitido. El proceso involucró la superación de algunos desafíos técnicos.

En primer lugar, teníamos decenas de millones de líneas de código para poner la marca de agua. También necesitábamos rastrear donde estaba todo nuestro código, pues no habíamos ofrecido a nuestros desarrolladores las mejores herramientas para almacenar su código en un área única, de ese modo muchos guardaban su trabajo en laptops y otros dispositivos no protegidos.

Entonces, iniciamos un proyecto ambicioso. Primero, consolidamos cerca de 750 repositorios de código fuente en todo el mundo y migramos sus contenidos hacia dos sistemas administrados de forma centralizada. Después, usamos tecnología propietaria para poner las marcas de agua en nuestro código. (Para más información, lea nuestra otra historia CustomerONE: "Modelo Symantec de Seguridad de Código Fuente.")

Proceso de Ajuste de Nuestras Alertas

Luego que nuestro código recibió las marcas de agua y fue protegido, elaboramos reglas para que sean usadas por el software DLP para detectar actividades sospechosas.

Los clientes se sorprenden cuando les decimos como ese paso consume tiempo. Tim Deese, un ingeniero de Symantec que ayudó a ejecutar nuestro proyecto de DLP, lo explica de esta forma: "Supongamos que desea rastrear actividades relacionadas a números de documentos de identidad". "Si crea una política para detectar números de nueve dígitos, cada número de nueve dígitos - números de productos, códigos postales, incluso algunos números de teléfono - activaran una alerta".

En este caso, necesitaría analizar cada alerta, determinar cuáles son falsos positivos y ajustar su regla para evitar que sean marcados. A continuación, necesitaría dejar que la nueva regla sea ejecutada por un período de tiempo y, enseguida, pasar otra semana reexaminando los resultados, y continuar el ciclo hasta que haya logrado acertar en el proceso. Mientras tanto, debe hacer lo mismo para todas sus otras reglas.

"Es una cantidad considerable de trabajo", dice Tim Deese. "El proceso es sencillo, pero representa un gran volumen de datos. Y usted debe analizar detenidamente estos datos para garantizar que no está excluyendo las verdaderas amenazas".

Es posible que también enfrente demandas corporativas conflictivas. Una unidad de negocios puede desear que una regla sea más flexible, incluso que genere más alertas, y otra unidad puede querer la misma regla más rígida. Eso puede llevar a una discusión administrativa que retrase el proceso.

Entonces, ¿cuál es la lección que ha aprendido? Dos cosas: Primero, configure reglas solamente para su información más crítica; segundo, tenga una jerarquía clara para aprobar políticas, así el proceso de ajustar reglas y políticas no se interrumpe por discusiones burocráticas.

Respuestas Adecuadas a las Alertas

No tiene sentido recibir una alerta si no se toma ninguna acción al respecto. Tuvimos ese problema cuando estábamos tercerizando nuestro monitoreo DLP a un tercero. Como no habíamos desarrollado políticas claras, hubo momentos en los que las alertas eran ignoradas porque nosotros y el proveedor creíamos que la otra parte las investigaría.

Logramos resolverlo al atribuir todas las responsabilidades de monitoreo a nuestro Centro de Operaciones de Seguridad en Virginia, EE.UU. Actualmente, cuando los funcionarios en el centro reciben una alerta, saben que son los responsables por investigarla. Si creen que una determinada actividad puede ser maliciosa, escalan el asunto en una jerarquía claramente definida. Si una alerta no esta escalada a ese nivel, como el ejemplo de nuestro funcionario que envió correos electrónicos de trabajo hacia una cuenta personal, el equipo trata la situación de acuerdo con la política interna.

Usted necesitará un proceso similar. Sepa en su empresa quienes deben recibir las alertas de datos y, enseguida, tenga un proceso claro que describa cuando las alertas deben ser escaladas y para quien.

Nos complacerá ayudarlo a elaborar esa estrategia.

Retos de Personal

Tim Deese ingresó a nuestro departamento de soporte en 2006. Cuando adquirimos el producto Data Loss Prevention, se ofreció para ser entrenado para utilizarlo, una decisión, que él bromea, que le garantizó estabilidad perpetua de empleo.

"Eso es real. Es un mercado activo, incluso dos a tres años después que DLP irrumpió en el mercado", dice él. "Cuando los clientes compran nuestro software y buscan ayuda para configurarlo, no hay muchas personas. Definitivamente, es un reto."

Symantec ofrecía servicios profesionales para ayudar en las instalaciones, pero descontinuamos ese modelo de negocios. Ofrecemos entrenamiento, algo que Tim realmente recomienda.

"Para que un cliente desarrolle la experiencia de forma interna, sugiero seleccionar algunas personas y ofrecerles nuestro entrenamiento y acceso a los recursos que tenemos", dice él. "En un período de tres a seis meses, pueden tornarse extremadamente competentes en la gestión de su solución instalada".

Mejores Prácticas

Recuerde que la solución Data Loss Prevention es apenas una parte de su estrategia general de protección de datos. Danny Graves, analista senior de seguridad de la información de Symantec, también recomienda las siguientes mejores prácticas:

- Establezca controles de contraseñas y autenticación fuerte
- Administre todas las políticas de forma centralizada para garantizar consistencia
- Si posee laboratorios de ingeniería, asegúrese de que los desarrolladores usen repositorios centralizados seguros y no sus propias soluciones individuales
- Use cifrado fuerte
- Mantenga un sistema ágil de gestión de parches
- Asegúrese de que la protección de endpoints esté actualizada y activada para todos en la red

"La mayoría de estas recomendaciones son obvias", dice Danny, "sin embargo son fáciles de olvidar o ignorar."

Nuestros Próximos Pasos

En 2016, iniciamos la comercialización de un nuevo servicio basado en la nube de Data Loss Prevention. Proporcionamos el hardware, mantenimiento y servicio, para que los clientes no necesiten administrar la infraestructura y seguridad física.

"Ese es un gran paso para nuestra empresa", dice Linda Park, gerente de marketing de productos de Symantec. "Esa es la tendencia que nuestro segmento y mercado están siguiendo."

Si bien los servicios están en la nube, los clientes necesitan sus propios funcionarios para responder a los incidentes.

También en desarrollo: una solución para ofrecer lo que CSO Tim Fitzgerald describe como el ítem más deseado cuando se trata de protección de código fuente: prevención. El primer paso es detectar cuando el código fuente está siendo movido de forma inadecuada – el próximo paso es prohibir este movimiento.

Ese es el camino que buscamos seguir.

El principal reto en la prevención es encontrar el equilibrio entre bloquear las acciones sospechosas e impedir el trabajo legítimo de nuestro equipo. Symantec está cerca de una solución, que debe ser lanzada en 2016. Esté atento.

Obtenga más Información con una Presentación Ejecutiva

Este documento tuvo como objetivo dar una visión amplia acerca de cómo utilizamos internamente la solución Symantec Data Loss Prevention. Su representante Symantec puede mostrarle como adaptar nuestro plan para tornar su propia jornada DLP mucho más tranquila.

Si desea una experiencia mucho más detallada, visite nuestros Centros de Reuniones Ejecutivas en nuestra sede en EE.UU. en Mountain View, California, o en Reading, en el Reino Unido.

Las presentaciones ejecutivas ofrecen una oportunidad exclusiva de aprender cómo las soluciones de Symantec pueden proteger sus entornos de negocios y red. Personalizaremos la presentación para atender a sus objetivos específicos, y también le mostraremos de forma anticipada nuestras nuevas tecnologías y retos futuros del sector.

SOLUCIONES Y PRODUCTOS SYMANTEC EN ESTE ARTÍCULO

Data Loss Prevention: DLP identifica donde están almacenados los datos en sus entornos en la nube, móviles e instalados localmente; monitorea como están siendo usados dentro y fuera de su red corporativa; y protege los datos de que sean divulgados o robados

customer_one@symantec.com

CustomerONE Team
350 Ellis Street
Mountain View, CA 94043
800-745-6054

El equipo de Symantec CustomerONE puede facilitar el diálogo entre nuestros profesionales de seguridad de TI y usted, para ayudarlo a resolver sus dudas y preocupaciones de seguridad. Contáctese directamente o por medio de su equipo de ventas Symantec.