Dole Food Company

La empresa Dole Food Company protege su marca online y sus aplicaciones web críticas con XyberShield, una plataforma de seguridad en Internet basada en el comportamiento y ofrecida en forma de software-como-servicio

Visión general

Desafío

Dole.com, con sus más de 2 millones de sesiones web al mes, es un objetivo predilecto de actividades maliciosas en Internet. Mantenerse al día frente a los métodos de ataque en continua evolución constituía un desafío formidable, y las múltiples aplicaciones web de la compañía eran especialmente vulnerables.

Solución

Para proteger su sitio web, Dole utiliza XyberShield Enterprise Protection, que protege activamente contra la inyección SQL, la división de respuesta HTTP (HTTP Response Splitting) y otros ataques comunes definidos por el OWASP.

Ventajas

El sistema detectó y detuvo todos y cada uno de los ataques. No supone ninguna carga adicional al personal de Dole, a su infraestructura o al rendimiento de la red. Los visitantes habituales disfrutaron de un acceso íntegro al sitio. Se recopiló y analizó información forense sobre todos los intentos de ataque.

Dole Food Company, Inc. es una corporación multinacional agrícola estadounidense con sede en Westlake Village (California). La empresa es el mayor productor de frutas y verduras del mundo, y comercializa más de 300 productos en 90 países. Su alto perfil público y su activa presencia en línea señalan a los sitios web de la compañía como objetivos predilectos de actividades maliciosas en Internet.

La empresa implementó XyberShield con la intención de proteger sus aplicaciones web y, en el proceso, bloqueó cientos de ataques sin que ello supusiera ninguna carga adicional para su personal, infraestructura o rendimiento de la red.

Un blanco de alta notoriedad

En octubre de 2009, Dole comenzó a cotizar como empresa en la Bolsa de Nueva York. Además de cotizar en bolsa, la atención de los medios de comunicación hacia la empresa aumentó por varias campañas de marketing a nivel nacional. Este aumento de notoriedad pública se correspondió con un incremento de la actividad hacker en el sitio web corporativo principal, **www.dole.com**. Por ejemplo, la empresa sufrió hasta 100 ataques al día, varios de los cuales fueron intentos coordinados desde múltiples ubicaciones con la intención de alterar la apariencia del sitio, acceder y modificar datos confidenciales y descubrir información financiera. Los intentos de incursión más habituales fueron los ataques de inyección SQL, que se cuentan entre los ataques potencialmente más devastadores económicamente. Históricamente, un solo ataque de inyección SQL efectuado con éxito puede costarle a una empresa hasta 6,6 millones de dólares.

Con sus más de dos millones de sesiones de visitantes al mes, la protección del sitio web corporativo de Dole constituía un desafío formidable. Para complicar más el problema, la mayoría de ataques estaban dirigidos a los elementos de un sitio web que resultan normalmente más vulnerable según las protecciones tradicionales basadas en red: las aplicaciones web de la empresa.

"Dole.com es nuestra insignia corporativa; el principal punto de contacto entre los clientes y la marca Dole.

"XyberShield protege nuestro valor de marca defendiendo el sitio web contra las amenazas en línea y, a medida que mejoramos nuestra notoriedad en el sector y aumentamos nuestra presencia en línea, la protección se adapta para ajustarse a nuestro crecimiento. XyberShield es, sencillamente, la mejor forma de proteger la marca distintiva de Dole en Internet".

— Marty Ordman, vicepresidente de Servicios de Marketing de Dole Food Company, Inc.

Protección de aplicaciones Web

Una aplicación web es cualquier tipo de software interactivo que se ejecuta en un navegador web. Cualquier acción que realice un usuario en la web que no sea la lectura y la navegación básica requiere una aplicación web como, por ejemplo, calendarios en línea, correo electrónico basado en web, portales corporativos, perfiles personales en línea (LinkedIn, Facebook, eHarmony) y prácticamente todos los servicios de Google.

Los cortafuegos de red protegen redes e infraestructuras. Las protecciones de aplicaciones web protegen el comercio electrónico, el software y las bases de datos relacionadas con información valiosa. Aunque los cortafuegos de red son necesarios, los hackers han ido más allá de los ataques a nivel de red y se concentran cada vez en mayor medida en la información personal y confidencial de las personas.

Los clientes utilizan aplicaciones web para interactuar con el software y la información presente por debajo de la capa de red, y tales interacciones requieren un "agujero" intencional en la protección de la red. Estas aberturas intencionales requieren un tipo especial de protección.

Protección en tiempo real basada en el comportamiento

En el caso de Dole, XyberShield proporciona una eficaz y adaptativa protección de aplicaciones web. Cuando aumentó el número de ataques, XyberShield detectó y bloqueó con éxito todos y cada uno de ellos, impidiendo cualquier actividad maliciosa en el sitio web. Durante todo el mes de octubre de 2009, la página **www.dole.com** no experimentó ningún tiempo de inactividad ni sufrió ninguna consecuencia adversa pese al volumen de actividad hacker dirigido contra ella. Los más de 2 millones de visitantes legítimos del sitio disfrutaron de un acceso íntegro.

Actualmente, el sitio web corporativo de Dole recibe 2.215.170 sesiones de visitantes en un mes normal. En un intervalo de tiempo reciente, XyberShield ha detectado y evitado un total de 346 amenazas de alto nivel. Los ataques de scripting de sitios cruzados (Cross-site scripting) representaron 293 de los intentos de incursión, mientras que los 53 ataques restantes fueron ataques por inyección SQL.

A medida que los ataques se hacen más sofisticados, XyberShield aprende y evoluciona para enfrentarse al desafío. El sistema recopila información de cada amenaza potencial a través del análisis forense e informa constantemente a su motor de análisis y correlación de comportamiento (BACE) para ofrecer protección frente a las nuevas formas de ataque que puedan surgir. Esta experiencia adicional sobre las variantes de las amenazas hace posible que XyberShield reconozca y dé respuesta a las últimas técnicas de hacking generando alertas o deteniendo las sesiones web activas de forma inmediata, antes de que la actividad maliciosa pueda afectar al sitio web de alguna forma.

Industria agrícola

“En Dole, tomamos todas las medidas de seguridad necesarias en lo referente a nuestras aplicaciones web y datos en línea.

“La infraestructura basada en la nube de XyberShield, su análisis de comportamiento y sus capacidades de correlación son tremendamente eficaces. Desde que comenzamos a utilizar XyberShield en 2009, nos ha protegido a la perfección. XyberShield es la herramienta número uno para la protección de nuestras aplicaciones web”.

— Michael Contreras, director de Marketing Digital de Dole Food Company, Inc.

Protección a través de la nube global

Dado que XyberShield es un servicio auténticamente basado en la nube, se beneficia globalmente de las experiencias de cada uno de los usuarios del servicio, no solo de Dole Food Company. En cuanto se detecta información de nuevos tipos de comportamientos maliciosos en el sitio de un cliente y estos se detienen, todos los usuarios del servicio quedan protegidos. Sin ser conscientes de ello, las empresas que utilizan el servicio de XyberShield como, por ejemplo, Dole, se benefician mutuamente de las experiencias del resto.

La solución de seguridad se activa en minutos y se adapta dinámicamente para ajustarse a los requisitos cambiantes de la empresa. Las actualizaciones se realizan de manera invisible. Una auténtica solución de seguridad basada en la nube, al contrario de un dispositivo, no supone ninguna carga adicional para el personal de una empresa, su infraestructura o el rendimiento de la red.

Un obstáculo al que se enfrentan un gran número de soluciones de seguridad basadas en la nube es que requieren que el usuario redirija todo el tráfico web a los sistemas del proveedor de seguridad. Este sistema puede generar problemas de latencia, es decir, que sea necesario más tiempo para acceder al sitio web. Otros servicios basados en la nube requieren que el usuario aloje su sitio web y datos importantes en los servidores del proveedor del servicio, por lo que pierden cierto grado de control sobre sus propios datos y, posiblemente, infringen sus propias políticas de seguridad respecto a la salvaguarda de los mismos.

Al igual que la mayoría de empresas de la lista Fortune 500, Dole Food Company necesitaba mantener el control sobre sus propios datos y disminuir la latencia. Dole seleccionó XyberShield, una solución sin alojamiento, ni proxy, que utiliza un solo script de código denominado XyberObserver.

El observador permanente

Los usuarios de XyberShield instalan un pequeño fragmento de código, conocido como XyberObserver, en el nivel superior del servidor web. Este script se halla en constante comunicación con la plataforma del servicio global remoto de XyberSecure, donde se llevan a cabo todos los cálculos computacionales complejos.

Este enfoque ligero asigna todo el trabajo de protección a los recursos de XyberSecure, a la vez que permite que Dole mantenga el control absoluto sobre sus propios datos, al contrario que en una solución de alojamiento. No se redirige tráfico web para su filtrado (el problema de los proxys).

El script presente en el servidor de Dole analiza todas las acciones que se llevan a cabo en todas y cada una de las sesiones de uso del sitio web. En el instante en que se detecta actividad entrante maliciosa, el sistema de protección entra en acción advirtiendo al visitante, desviándolo a otro sitio web o directamente bloqueándolo.

Componentes de la solución:

- Servicio XyberShield Enterprise
- XyberFrames activos:

  Paquete OWASP
  Inyección SQL
  Inyección SSI
  División de respuesta HTTP
  (HTTP Response Splitting)

Además, XyberShield efectúa una correlación de la información procedente de todas las sesiones de cada uno de los sitios web protegidos por XyberObserver con el objeto de mejorar la seguridad de todos los usuarios de la solución, no solo de Dole Food Company.

En base a su experiencia, Dole decidió activar diversas opciones de seguridad que se encuentran disponibles en XyberShield.

XyberFrames Protección modular y adaptativa

Los módulos XyberFrames son módulos adaptativos que están diseñados para evitar determinados ataques a nivel de aplicación. **Dole.com** se encuentra protegido por el módulo XyberFrame de Inyección SQL. Entre el resto de módulos XyberFrames que están actualmente en activo en **www.dole.com**, se incluyen Abuso funcional, Abuso navegacional, Fuerza Bruta y el paquete OWASP.

La Fundación para la seguridad de aplicaciones web abiertas (OWASP, en inglés) es una organización mundial sin ánimo de lucro dedicada a mejorar la seguridad del software de las aplicaciones. El paquete XyberFrame específico de OWASP protege contra las diez actividades de Internet más peligrosas, de acuerdo con la definición de la OWASP, entre las que se incluyen el scripting de sitios cruzados (Cross-site Scripting), la falsificación de solicitudes de sitios cruzados (cross-site request forgery), la inyección SSI, la inyección SQL y la división de respuesta HTTP (HTTP Response Splitting).

Otros módulos disponibles responden a distintas necesidades específicas de la industria como, por ejemplo, PCI XyberFrame, que sirve de ayuda a los usuarios que deben cumplir con el estándar PCI.

Las brechas de seguridad a través de ataques a las aplicaciones web constituyen algunas de las amenazas más costosas y consumidoras de recursos de los negocios en línea. Desde la integración de XyberShield en su esquema de seguridad, Dole Food Company no ha sufrido ningún impacto negativo en su actividad por intentos de ataque a sus aplicaciones web.

Para más información

Póngase en contacto con su representante de ventas de XyberShield o con su distribuidor XyberSecure Business Partner, o visítenos en la dirección:

www.xybershield.com

Si desea más información sobre Dole Food Company, visite la dirección:
www.dole.com

Acerca de XyberShield, Inc.

XyberSecure, Inc. ofrece servicios de seguridad en las aplicaciones fáciles de implementar y soluciones inteligentes en tiempo real frente a las amenazas que afectan a los sitios web. XyberSecure utiliza una infraestructura global de nivel 1 con centros de operaciones tácticas en las dos costas de Norteamérica y con 55 puntos presenciales en 22 países. XyberSecure es una empresa de capital privado.

XyberSecure
575 Market Street, 40th floor
San Francisco, CA 94105
Estados Unidos

Desarrollado en Estados Unidos de América
Marzo de 2011