infoblox

ESTUDIO DE CASO

Stupp Bros. refuerza la seguridad con Infoblox Threat Defense™

RESUMEN

La empresa con sede en St. Louis (Missouri) Stupp Bros. es un destacado proveedor de materiales y servicios esenciales para la construcción de infraestructura crítica en todo Estados Unidos.

La empresa fabrica acero estructural utilizado en puentes, rascacielos, hospitales, centros de convenciones, estadios deportivos y recintos de entretenimiento de costa a costa. Además de su actividad principal, Stupp Bros. ofrece una amplia gama de servicios, entre los que se incluyen la banca regional, la captura de datos que permite a las industrias con procesos intensivos cumplir la normativa, y la prestación de servicios de banda ancha residenciales y comerciales.

> *"Threat Defense es el foso que rodea nuestro castillo. Hay que cruzarlo antes de poder causar ningún daño a las murallas exteriores".*
>
> **John Roosa,**
> **Director de Informática,**
> **Stupp Bros.**

LA SITUACIÓN

Establecer una mentalidad de defensa en profundidad

Stupp Bros., fundada hace más de 165 años, se centraba principalmente en mejorar los métodos de fabricación y ampliar los mercados para sus materiales de construcción de alta calidad. Sin embargo, a medida que en las últimas décadas las operaciones de la empresa se han ido conectando digitalmente, la ciberseguridad se ha convertido en una de sus principales prioridades.

A mediados de la década de 1990, John Roosa era consultor y ayudaba a la empresa a optimizar sus redes en los inicios de internet, cuando apareció el virus Melissa. "Ese fue mi toque de atención", afirma. El incidente de 1997 le mostró lo drásticamente que había cambiado el panorama de la seguridad y lo poco preparadas que estaban las redes informáticas para esa nueva realidad.

Roosa ha sido firme defensor de la ciberseguridad integral desde entonces. Como director de Informática de Stupp Bros. durante los últimos 18 años, ha supervisado la construcción de un enfoque de defensa en profundidad diseñado para proteger a la empresa y sus más de 350 empleados frente a las amenazas modernas.

STUPP BROS., INC.
ESTABLISHED 1856 | ST. LOUIS, MISSOURI

Para alcanzar esos objetivos, Roosa y sus compañeros han implementado una pila de seguridad que consta de cortafuegos de última generación (NGFW) y otras medidas de protección de endpoints, respaldadas por Microsoft Sentinel, la plataforma de gestión de eventos y seguridad de la información (SIEM) basada en la nube de Microsoft, y las herramientas asociadas.

Aunque esas implementaciones han sido muy eficaces, no han podido abordar adecuadamente un grave problema de seguridad: los empleados que, sin darse cuenta, ejecutan conductas arriesgadas en internet.

EL DESAFÍO

Donde van los usuarios en línea, las amenazas los siguen

Desde el punto de vista de Roosa, los retos que plantea la conducta de los usuarios han evolucionado drásticamente desde que asumió el cargo de director de Informática en 2007. “Era mucho más sencillo en aquel entonces. Los riesgos no eran ni de lejos tan complejos”. En aquella época, los usuarios tenían menos dispositivos, las aplicaciones empresariales se ejecutaban principalmente en ordenadores de sobremesa y la tecnología en la nube apenas asomaba. Aunque existía el riesgo de los empleados, “era más fácil mitigarlo desde el punto de vista informático que hoy en día”, señala Roosa.

En la actualidad, todos los empleados de Stupp Bros. tienen teléfonos inteligentes u otros dispositivos que les proporcionan acceso instantáneo a internet dondequiera que vayan. Cada vez más, gran parte del trabajo que se desarrolla en la fabricación moderna de acero, la construcción y la banda ancha de fibra óptica depende del correo electrónico, los mensajes de texto y el acceso a aplicaciones y recursos en la nube.

Sin embargo, con tantas formas de conectarse, a Roosa y a su equipo les resulta cada vez más difícil controlar adónde acceden los empleados y qué hacen en internet. A diferencia de las grandes empresas, Stupp Bros. no cuenta con los recursos necesarios para proporcionar dispositivos bloqueados o implementar escritorios gestionados a todos los empleados. Como resultado, los empleados a veces hacían clic en enlaces de phishing o visitaban sitios con anuncios publicitarios sospechosos que los redirigían a sitios web maliciosos o, lo que es peor, iniciaban la descarga de virus.

En opinión de Roosa, la formación de los empleados era fundamental para mitigar esos riesgos. En general, esas iniciativas han sido muy eficaces, pero no siempre lo suficientemente oportunas. Por ejemplo, las alertas de seguridad se dispararon cuando Stupp Bros. adquirió una nueva unidad de negocio sin que sus empleados hubieran recibido la formación adecuada en materia de seguridad.

Roosa estaba decidido a evitar que esas situaciones se repitieran en el futuro. Pero incluso los usuarios más expertos pueden ser víctimas de contenidos maliciosos en línea hábilmente camuflados como legítimos. Inevitablemente, las alertas de virus llegaron a los NGFW y otras herramientas de seguridad de los endpoints de Stupp Bros., lo que obligaba a los equipos de seguridad a dedicar horas a investigar y corregir problemas.

Para hacer frente a este reto, Stupp Bros. necesitaba una solución integral que redujera los riesgos asociados a las actividades inseguras en línea y, al mismo tiempo, mejorara su postura de seguridad, con un impacto mínimo en los empleados y el personal de seguridad.

LA SOLUCIÓN

Aprovechar el poder de la seguridad proactiva del DNS

Roosa se dio cuenta de que la mejor manera de evitar que los empleados hicieran clic en enlaces peligrosos era impedírselo en primer lugar. Por ello, Stupp Bros. implementó una serie de productos de filtrado web, todos ellos con resultados insatisfactorios. “Eran los típicos productos torpes, del tipo "permitir este tema sí y este no"”, explica Roosa.

Cliente: ***Stupp Bros.***
Sector: ***construcción***
Ubicación: ***St. Louis, Missouri***

OBJETIVOS:

- Mitigar los riesgos asociados a una conducta insegura en internet
- Optimizar la gestión del filtrado web para reducir el esfuerzo manual
- Reducir el volumen de alertas de virus y el tiempo necesario para resolverlas

RESULTADOS:

- Implementación de la solución de seguridad del DNS en la nube en 15 minutos
- Bloqueo proactivo de interacciones digitales maliciosas en toda la red
- Eliminación casi total de las alertas de virus, reduciendo drásticamente el ruido de las alertas
- Reducción del 50 % en el tiempo medio para investigar amenazas

PRODUCTOS:

- Infoblox Threat Defense™

Estas soluciones también imponían a Roosa y a su personal la carga de identificar manualmente los temas y los destinos web que debían añadirse a las listas de bloqueo, una tarea que requería mucho tiempo y que exigía investigación y una configuración continua. Sin embargo, el mayor inconveniente era el defecto fundamental de diseño que presentaban estas herramientas de filtrado. "No me gusta nada dedicarme a controlar el uso de internet, porque entiendo cómo funciona y lo fácil que es eludir muchos de esos filtros", afirma Roosa.

Roosa tuvo conocimiento de Infoblox mientras buscaba opciones de gestión de DHCP para el departamento de fibra óptica de su empresa. Durante su búsqueda, descubrió Infoblox Threat Defense™ y su innovador enfoque de la seguridad basada en el DNS. "Infoblox fue una revelación para mí", afirma. "El DNS es donde empieza todo".

Con Threat Defense, Roosa se dio cuenta de que podía "matar dos pájaros de un tiro". En primer lugar, resolvía el problema de determinar qué destinos web eran maliciosos. En segundo lugar, al operar en el plano de control del DNS, bloqueaba por completo el acceso de los usuarios a esas ubicaciones, eliminando los métodos alternativos que son posibles con otras opciones de filtrado. "Por fin encajaban las piezas del puzle", continúa Roosa. "Si puedo controlar el DNS en las búsquedas de nombres, puedo detener mucha actividad antes de que se inicie".

Roosa y sus equipos desplegaron fácilmente la solución basada en la nube en solo 15 minutos. La implementación fue sencilla, transparente para los usuarios finales y funciona en toda la infraestructura, tanto local como híbrida, y en entornos multinube. Threat Defense protege a todos los empleados de Stupp Bros. en la red, independientemente de su ubicación o dispositivo. Bloquea de forma proactiva la comunicación de los usuarios con dominios web asociados a riesgos potenciales, como la descarga automática de malware y virus, el robo de credenciales y la exfiltración de datos, entre muchos otros riesgos.

Las avanzadas capacidades de filtrado web de Threat Defense son altamente personalizables. Además, se actualizan continuamente con los últimos dominios implicados descubiertos por Infoblox Threat Intel, el grupo de investigación líder del sector que se centra en las amenazas emergentes basadas en el DNS. Esta inteligencia se complementa con algoritmos basados en IA para exponer indicadores de amenazas en dominios que otros métodos de seguridad no pueden detectar.

En Stupp Bros., Threat Defense funciona junto con otras implementaciones de seguridad, como Microsoft Sentinel y herramientas relacionadas, que se encargan de los dispositivos comprometidos y de su corrección. Mientras que estas implementaciones son principalmente de naturaleza reactiva, ya que solo activan una respuesta una vez que las herramientas de seguridad de los endpoints detectan una amenaza, Threat Defense detiene las amenazas de forma proactiva, antes de que lleguen al perímetro de la red. Se trata de una capacidad vital que el director de Informática valora enormemente. "Threat Defense es nuestra primera línea de defensa para todo", señala Roosa.

EL RESULTADO

Forjar una postura de seguridad más sólida

En materia de defensa contra amenazas, Stupp Bros. encontró una solución elegante para proteger a los empleados de las amenazas que explotan las interacciones digitales modernas. Al impedir el acceso a sitios web maliciosos mientras se está conectado a la red, se eliminan conductas arriesgadas en línea. "Si Infoblox dice que hay peligro, no se puede acceder", afirma Roosa.

Las capacidades de filtrado de la solución no requieren ninguna intervención por parte de los empleados. También les facilita enormemente a Roosa y a su equipo la tarea de determinar qué destinos deben prohibirse, ventaja que él considera un importante argumento de venta. "Ahora no tengo que preocuparme de qué hay que bloquear. Threat Defense se encarga de ello".

Dado que Threat Defense detiene las amenazas en el plano de control del DNS, ha reducido significativamente la carga de las defensas perimetrales de Stupp Bros. Como explica Roosa: "Eliminamos la mayor parte del tráfico malicioso incluso antes de que nos alcance. Eso genera mucho menos ruido en nuestra plataforma de análisis".

Esta reducción del ruido, combinada con una tasa de falsos positivos extremadamente baja, de apenas el 0,0002 %, se traduce en que el personal de seguridad tiene que gestionar muchas menos alertas. Por ejemplo, desde que se implementó Threat Defense, las notificaciones de virus —antes habituales— han desaparecido casi por completo. Según Roosa, gracias a la reducción del volumen de alertas que posibilita Infoblox, los equipos de seguridad han reducido a la mitad el tiempo de investigación de amenazas, lo que les permite centrarse en iniciativas estratégicas que refuerzan la postura de seguridad general de la organización.

Threat Defense también le ha devuelto un tiempo valioso a Roosa, que tiene la seguridad de que las interacciones peligrosas que la plataforma detiene en seco se sustentan en la inteligencia más actualizada del sector sobre las amenazas basadas en el DNS, que evolucionan rápidamente. “Eso es lo mejor de este producto”, afirma. “Puedo afirmar con toda sinceridad que no he perdido tiempo gestionándolo, ocupándome de él ni nada parecido”.

Además de aprovechar las avanzadas capacidades de filtrado web de Threat Defense, Stupp Bros. pronto activará funciones adicionales, empezando por integrar los datos de Infoblox en su ecosistema de seguridad de Microsoft. Roosa prevé que la telemetría en tiempo real de la actividad de amenazas del DNS mejore significativamente los esfuerzos de clasificación y corrección de la empresa. “Podremos ver mucho más con Threat Defense”, explica.

En términos más generales, Roosa no se anda con rodeos al resumir el valor de la implementación de Infoblox: “Threat Defense es el foso que rodea nuestro castillo. Hay que cruzarlo antes de poder causar ningún daño a las murallas exteriores. Desactivamos al enemigo antes de que se acerque”.

Sede corporativa
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054 (EE. UU.)

+1.408.986.4000
www.infoblox.com/es

Versión: 20250620v1