

En United Bank, el ransomware no es rentable

United Bank utiliza Malwarebytes para impedir que los programas de malware y los exploits realicen cobros ilegales

SECTOR

Servicios financieros

DESAFÍO COMERCIAL

Impedir los ataques de malware y ransomware

ENTORNO DE TI

Centro de datos con firewalls, control de red y antivirus VIPRE

SOLUCIÓN

Malwarebytes Endpoint Security, que incluye Anti-Malware, Anti-Exploit y la consola de administración

RESULTADOS

- Identificación satisfactoria de amenazas y bloqueo de exploits
- Minimización del riesgo de interrupción asociado al malware o al ransomware
- Mayor tranquilidad

Perfil de la empresa

La atención de United Bank se centra en proporcionar un servicio de calidad al cliente ofreciendo soluciones financieras innovadoras además de prácticas en aquellas comunidades en las que realiza operaciones. Con 17 oficinas repartidas por el área metropolitana de Atlanta, el banco quiere ser práctico en lo que se refiere a evitar el malware y el ransomware.

El mundo de las amenazas cada vez está peor y los malos se hacen cada vez más inteligentes. Este es justo el tipo de riesgos que no queremos correr. Malwarebytes nos garantiza que esto sea así.

—Russell Heelan, administrador de red, United Bank

Desafío comercial

Evitar ataques desde el principio

El equipo de TI de United Bank había utilizado, y posteriormente descartado, muchas soluciones antivirus con el tiempo. Las soluciones probadas resultaban ser «excesivas», con características que el banco no necesitaba, además de muy costosas, o bien simplemente eran ineficaces. Hace poco, el banco probó el antivirus VIPRE para combatir los virus y el malware. Sin embargo, esta solución necesitaba mucho trabajo informático en los PC de los empleados. Si un usuario detectaba un sitio web malicioso o un fragmento de malware, el rendimiento bajaba considerablemente. Y, a pesar de todo, el malware continuaba llegando. Por ejemplo, los usuarios se encontraban a menudo con programas de seguridad falsos, como falsos antivirus, inundando sus pantallas de mensajes.

«Era solo cuestión de tiempo que el ransomware o el extortionware apareciera», afirma Russell Heelan, administrador de red, United Bank. «No íbamos a cruzarnos de brazos a esperar que eso sucediera».



La solución

Malwarebytes Endpoint Security

Heelan comenzó a buscar una solución para sustituir el antivirus existente y añadir protección adicional contra el malware. Su anterior experiencia con Malwarebytes le había impresionado, así que decidió adoptar una postura proactiva frente al malware y al ransomware con Malwarebytes Endpoint Security.

«Malwarebytes siempre se ha mostrado proactivo a la hora de anticiparse a las amenazas», resalta Heelan. «Pensamos que era mejor utilizarlo desde el principio».

Endpoint Security ofrece una potente defensa en varias capas diseñada para eliminar el malware más reciente y peligroso, incluido el ransomware. Incluye Malwarebytes Anti-Malware, Anti-Exploit y la consola de administración en una completa solución. Malwarebytes Anti-Malware permite detectar y eliminar malware de hora cero, troyanos, gusanos, rootkits, adware y spyware en tiempo real. Permite detener las amenazas en seco, eliminando la necesidad de que United Bank tenga que quitar manualmente el malware de los terminales. Malwarebytes Anti-Exploit permite añadir cuatro capas adicionales de protección para bloquear los exploits e impedir que se reciban cargas maliciosas.

Todo queda a la vista

Heelan implementó el software mediante la consola de administración de Malwarebytes y lo instaló en cerca de 400 terminales. Según Heelan, fue un proceso sencillo que se llevó a cabo en menos de una semana.

«La consola de administración nos muestra todo: informes, número y tipo de amenazas y los orígenes de las mismas», indicó. «Un análisis en profundidad nos revela exactamente lo que está entrando y cómo lo maneja Malwarebytes. Los informes nos ayudan definitivamente a ver lo que está sucediendo para que podamos ser aún más proactivos».

Malwarebytes identificó rápidamente los programas potencialmente no deseados (PUP) y bloqueó los sitios maliciosos. También bloqueó cuatro exploits distintos, cualquiera de ellos podría haber afectado seriamente a la productividad de los empleados y a las operaciones del banco.

Protección proactiva y rendimiento mejorado

«El mundo de las amenazas cada vez está peor y los malos se hacen cada vez más inteligentes», asegura Heelan. «Este es justo el tipo de riesgos que no queremos correr. Malwarebytes nos garantiza que esto sea así».

El poco espacio que ocupa Malwarebytes en los PC de los usuarios también garantiza que la productividad de estos no se verá interrumpida. Heelan realiza un análisis rápido en toda la red a diario y, además, efectúa un análisis en profundidad dos veces por semana. De esta forma, se asegura de que todo está limpio.

«Afortunadamente, no hemos tenido ningún problema desde que implementamos Malwarebytes», asegura. «No tengo palabras para transmitir qué gran solución es. Nos sentimos mucho mejor con Malwarebytes en acción».

Acerca de

Malwarebytes ofrece soluciones de software anti-malware y anti-exploit diseñadas para proteger a empresas y usuarios frente a las amenazas de día cero que continuamente escapan a la detección de los antivirus tradicionales. Malwarebytes Anti-Malware obtuvo una calificación de Sobresaliente otorgada por los editores de CNET, es el programa favorito de los editores de PCMag.com y fue el único software de seguridad que obtuvo una puntuación perfecta en desinfección de malware según AV-TEST.org. Ese es el motivo por el que más de 38 000 PYMES y empresas globales confían en Malwarebytes para proteger los datos. Fundada en 2008, Malwarebytes tiene su sede principal en California, mantiene varias oficinas en Europa y emplea a un equipo global de investigadores y expertos.



Santa Clara, CA



malwarebytes.com



corporate-sales@malwarebytes.com



1.800.520.2796