proofpoint

CASO DE CLIENTE

Un fabricante mundial de componentes de automoción se beneficia de servicios gestionados para Proofpoint Security Awareness Training

La solución integral de Proofpoint reduce drásticamente los ataques de phishing dirigido

EL DESAFÍO

- Reducir los mensajes de correo electrónicos fraudulentos y los ataques de phishing dirigidos.
- Aumentar el nivel de concienciación de los empleados sobre las estafas por correo electrónico y fomentar su participación en las iniciativas de seguridad.
- Mejorar la productividad del equipo de ciberseguridad automatizando el proceso de clasificación.

LA SOLUCIÓN

- Proofpoint Email Protection con Targeted Attack Protection (TAP) y Threat Response Auto-Pull (TRAP)
- Servicios gestionados para Proofpoint Managed Security Awareness
- Proofpoint Closed-Loop Email Analysis and Response (CLEAR)

LOS RESULTADOS

- Bloqueo de prácticamente la totalidad de ataques de correo electrónico maliciosos contra los empleados.
- Implicación de los empleados como defensores activos de la seguridad de la empresa.
- Mejora importante de la productividad del equipo de ciberseguridad.

La empresa

Esta empresa de capital público con sede en Estados Unidos es un destacado fabricante y distribuidor de piezas de repuesto para automóviles. Durante décadas, la empresa se ha labrado una sólida reputación basada en la calidad y la fiabilidad. Esto le ha permitido ganarse la confianza y lealtad de partners y clientes en todo el mundo.

El desafío

Permanecer a la vanguardia en un entorno de ciberseguridad en constante evolución

Una de las principales frustraciones de los expertos en ciberseguridad, responsables de proteger a sus empresas contra los ataques basados en el correo electrónico, es su dificultad para adelantarse a los ciberdelincuentes que intentan eludir sus numerosas capas de seguridad. Tan pronto como un equipo de seguridad identifica, analiza y consigue bloquear un tipo de phishing malicioso o malware, los ciberdelincuentes han creado uno nuevo diseñado específicamente para eludir los métodos de detección existentes. Aprovechar las bibliotecas compartidas de ataques recientes proporcionadas por Proofpoint y otros puede ayudar a las empresas a reducir el tiempo de respuesta a las nuevas amenazas. Pero, por definición, este proceso es reactivo en lugar de proactivo.

Este fabricante de recambios para automóviles, cliente de Proofpoint durante casi siete años, conoce bien esta frustración.

"Es como tratar de alcanzar lo inalcanzable, dijo el CISO. "Cada vez que aparece un nuevo ataque de phishing, lo encontramos y lo detenemos. Pero inmediatamente, aparece algo nuevo y en ocasiones logra superar las defensas".

La empresa comenzó a trabajar con Proofpoint en respuesta a la avalancha de correo no deseado que recibían sus empleados todos los días. Las conversaciones con los ingenieros de Proofpoint convencieron al equipo de seguridad de la información de que necesitaban una protección de correo electrónico más amplia de la que podía proporcionar un filtro de spam. Con el tiempo, la empresa ha implementado una variedad de productos de Proofpoint en un esfuerzo constante de ir un paso por delante de los atacantes. Además de Proofpoint Email Protection, la empresa instaló Proofpoint Targeted Attack Protection (TAP), Proofpoint Threat Response Auto-Pull (TRAP), Proofpoint Encryption y Proofpoint Email Data Loss Prevention (DLP). Estas soluciones bloquearon con éxito casi todos los ataques de phishing y malware, lo que aumentó significativamente la productividad de TI y de los empleados.

Para proteger aún más a la empresa de los ataques de phishing, el equipo de seguridad se dio cuenta de que debían capacitar a sus empleados para identificar mensajes potencialmente maliciosos. Su objetivo era involucrar a todos los usuarios de correo electrónico como participantes activos en la seguridad de la empresa. El equipo de seguridad buscaba proporcionar a sus usuarios las herramientas necesarias para responder correctamente en tales situaciones.

"Somos clientes de Proofpoint desde hace aproximadamente siete años. Hemos invertido mucho en Proofpoint y nunca nos hemos arrepentido. Sus soluciones son de una fiabilidad absoluta.

Jefe de seguridad de la información (CISO)

Inicialmente, la empresa había contratado a otro proveedor para ofrecer la formación de concienciación sobre el phishing. Si bien el equipo de seguridad vio los beneficios de un programa de formación gestionado, a lo largo de un año encontraron fallos críticos en la solución que afectaron no solo a los empleados, sino que también requirieron tiempo y esfuerzo adicionales de parte del equipo de seguridad".
El "buzón de correo de phishing sospechoso" recibía hasta 45 mensajes "sospechosos" al día, y cada uno requería entre quince minutos y una hora de análisis manual para resolverse. Además, la falta de información completa y coherente que los empleados proporcionaban complicaba todavía más la investigación. Pronto, el equipo necesitó una persona a tiempo completo para hacer frente a la carga.

La solución

Servicios gestionados para Proofpoint Security Awareness Training con CLEAR

El equipo de seguridad se reunió con Proofpoint para discutir los problemas a los que se enfrentaban. Estaban comprometidos con un modelo de formación de seguridad gestionado, pero necesitaban una solución más eficiente y automatizada. El equipo también deseaba una integración total con su inversión existente en Proofpoint.

Proofpoint propuso una solución: servicios gestionados para Proofpoint Security Awareness Training (mPSAT) junto con Proofpoint Closed-Loop Email Analysis and Response (CLEAR). Esta combinación no solo ampliaría sus iniciativas de formación para los empleados, sino que también automatizaría el proceso de denuncia de mensajes sospechosos, el análisis de esos mensajes y el proceso de corrección una vez finalizada la investigación.

Por su experiencia con Proofpoint, el equipo de seguridad tenía la seguridad de que mPSAT podría satisfacer sus necesidades de formación. Sin embargo, resultó que CLEAR fue un factor crítico en la decisión de la empresa de cambiar de su proveedor anterior a Proofpoint. La solución integrada proporcionó un programa de formación y concienciación gestionado mucho más amplio que el proveedor inicial.

CLEAR está compuesto por tres piezas clave. En primer lugar, un botón "PhishAlarm", incorporado en todos los clientes de correo electrónico para equipos de sobremesa y móviles, permite a los usuarios enviar los mensajes de correo electrónico sospechosos de phishing directamente a una bandeja de abuso con todos los encabezados y archivos adjuntos intactos, lo que proporciona información coherente para el análisis. En segundo lugar, un módulo llamado "PhishAlarm Analyzer" recibe los mensajes sospechosos, los analiza en función de diversos factores de riesgo y los clasifica según su probabilidad de contener contenido malicioso. Este proceso inteligente reduce el tiempo de evaluación necesario cada día de horas a minutos. En tercer lugar, PhishAlarm Analyzer pasa la información a Proofpoint TRAP para su corrección manual o automática.

Esta solución analiza los mensajes denunciados respecto a múltiples sistemas de inteligencia y reputación y comparte los resultados con el equipo de seguridad de mensajes. Proofpoint TRAP puede eliminar automáticamente o poner en cuarentena los mensajes que superen un umbral de riesgo determinado, o puede proporcionar al equipo de seguridad la información necesaria para tomar una decisión de forma manual. Un ingeniero de seguridad puede ejecutar la decisión adecuada con un solo clic. Una vez que el análisis determina que un mensaje es malicioso, Proofpoint TRAP elimina automáticamente todo el contenido malicioso, dondequiera que se encuentre. Además, puede rastrear los mensajes reenviados o las listas de distribución hasta sus destinatarios finales. Incluso si un empleado hace clic en un enlace malicioso y luego se da cuenta de que ha cometido un error, solo tiene que hacer clic en PhishAlarm. PhishAnalyzer y Proofpoint TRAP tomarán todas las medidas necesarias para eliminar el contenido malicioso del sistema.

Además, Proofpoint CLEAR se incluyó en la licencia existente de Proofpoint TRAP de la empresa y, por lo tanto, no precisó inversión adicional. La combinación de estos factores hizo que la decisión de pasar a una solución integral de Proofpoint fuera sencilla.

Como parte del esfuerzo global de mPSAT, el CISO también quería un administrador que pudiera supervisar y coordinar todo el programa de concienciación y formación en materia de seguridad de la empresa. El administrador de mPSAT asume los desafíos de diseño, ejecución e informes, necesarios para que un programa de educación en seguridad tenga éxito. Un administrador dedicado es un profesional experimentado que puede liberar al CISO y al equipo de seguridad, para centrarse en nuevos proyectos y otras prioridades. Este innovador programa de formación proporciona a los empleados los conocimientos, la formación y las herramientas que necesitan para desempeñar un papel activo en la protección tanto de sí mismos como de la empresa. El resultado es una reducción en los "clics" en mensajes de correo electrónico de phishing y una identificación y denuncia más temprana de mensajes sospechosos.

Los resultados

mPSAT con CLEAR logró una mejora inmediata en el nivel de concienciación y de participación de los empleados.

Según el CISO, la transición desde el proveedor de formación anterior de la empresa a mPSAT de Proofpoint fue completamente fluida. "El administrador de mPSAT ha demostrado ser excelente y ha aligerado de manera importante la carga de trabajo administrativo en mi área. Y el modelo de formación gestionada de Proofpoint nos ha demostrado los beneficios de usar un único proveedor para proteger las comunicaciones de nuestros empleados".

El equipo de mPSAT comenzó con pruebas mensuales, enviando mensajes a todos los empleados utilizando los últimos métodos de ataque. Si una prueba señalaba áreas específicas que necesitaban mejoras, el administrador diseñaba una campaña específica para abordar el problema, trabajando tanto con equipos como con individuos para proporcionar la formación adicional que fuera necesaria. Los resultados han sido cuantificables y significativos, reduciendo drásticamente el número de "clics" en los enlaces maliciosos incrustados en los mensajes de correo electrónico de prueba.

Proofpoint CLEAR ha superado las expectativas del equipo de seguridad. Cuando un empleado hace clic en el botón PhishAlarm, recibe respuesta inmediata de que su mensaje ha sido recibido, lo que les convierte en participantes activos de la seguridad de la empresa. En menos de seis meses, el número de empleados que hicieron clic en PhishAlarm en un caso de prueba aumentó cinco veces, del 5 al 25 %. El CISO atribuye el mejor rendimiento en las pruebas al uso del refuerzo positivo.

"PSAT es un programa educativo", explicó el CISO. "Queremos recompensar a las personas por tomar la decisión correcta, no criticarlas por cometer un error. Queremos que nuestros empleados sean parte de la solución. No son solo nuestra última línea de defensa, sino nuestra primera línea de defensa contra los nuevos tipos de mensajes de correo electrónico maliciosos".

El proceso automatizado de Proofpoint CLEAR también ha reducido el tiempo necesario para recibir, analizar y corregir los mensajes sospechosos. Si antes se necesitaba un empleado a tiempo completo para gestionar el volumen diario de mensajes sospechosos ahora puede hacerse en cuestión de minutos por cualquier miembro del equipo de seguridad, con el consiguiente aumento de la productividad.

"Llevamos aproximadamente siete años siendo clientes de Proofpoint", resumió el CISO. Hemos invertido mucho en Proofpoint y nunca nos hemos arrepentido. Sus soluciones son de una fiabilidad absoluta.

MÁS INFORMACIÓN

Para obtener más información, visite **proofpoint.com/es**.