KnowBe4

El excelente retorno de la inversión de PhishER Plus

Mi nombre es Stu Sjouwerman. Soy el fundador y director ejecutivo de KnowBe4, mi quinta *startup*. Llevo más de 40 años en TI, los últimos 25 en seguridad de la información. En mi última empresa, creamos un motor antivirus desde cero, y lo combinamos con detección y prevención de intrusiones y un firewall. Pero nos encontramos con un problema persistente que pocas organizaciones estaban abordando: los usuarios finales son manipulados por malhechores. Por eso fundé KnowBe4: para ayudar a los profesionales de TI a gestionar el continuo problema de la ingeniería social. En abril de 2021, salimos a bolsa en el NASDAQ y en 2023, pasamos a ser privados.

Cómo combatir el tsunami de phishing

El 91 % de los ciberataques comienzan con un ataque de spear-fishing (suplantación de la identidad específica), y el phishing es responsable de dos tercios de las infecciones de ransomware. Dados los avances en IA que hacen que los sofisticados ataques de phishing se vuelvan exponencialmente más eficaces, es crucial que dote a sus equipos de seguridad de la información y TI con las herramientas necesarias para mitigar de forma rápida y minuciosa las amenazas de phishing ANTES de que den el golpe.

> “PhishER es un componente natural de nuestro negocio. Reduce significativamente nuestro riesgo, ahorra muchísimo tiempo a nuestros equipos técnicos y es muy fácil de configurar y personalizar.”
>
> – George Schneider, gerente de Seguridad de la información

Si su organización está combatiendo las amenazas de phishing con flujos de trabajo manuales, está aumentando drásticamente el riesgo de que su organización sea víctima de phishing. Estos procesos obsoletos crean cuatro desafíos principales:

- **SOBRECARGA DE ALERTAS**

  Los equipos de seguridad de la información y TI que dependen de los flujos de trabajo manuales tardan, en promedio, 27 minutos en clasificar manualmente un correo electrónico de phishing,[1] lo cual aumenta drásticamente el riesgo de que su organización sea víctima de phishing.

- **EQUIPOS DE TI CON POCOS RECURSOS Y MUCHA PRESIÓN**

  El 61 % de las organizaciones de tamaño mediano no cuentan con un experto dedicado a la ciberseguridad dentro de su personal, y en promedio, por cada 10 empleados de TI de una organización, solo uno se dedica a la ciberseguridad.[2]

- **INCAPACIDAD PARA DETENER EL TSUNAMI**

  Cada vez mayores porcentajes de correos electrónicos de phishing cruzan las puertas de enlace de correo electrónico seguro y llegan a las bandejas de entrada de sus usuarios: El 56 % de los ataques basados en correos electrónicos eludieron los filtros tradicionales de seguridad en 2022,[3] y el 18,8 % de los correos electrónicos de phishing eludieron Microsoft Exchange Online Protection y Defender.[4]

- **RESPUESTA LENTA ANTE ATAQUES DIRIGIDOS**

  La incapacidad de mitigar un ataque de phishing dirigido, como una campaña de spear phishing (suplantación de identidad específica), en tiempo real hace que su organización se vuelva vulnerable. Es probable que varios usuarios reciban los mismos correos electrónicos de phishing y que su organización no pueda ponerlos en cuarentena desde las bandejas de entrada antes de que se haga clic en un enlace malicioso.

[1]The Business Cost of Phishing, 2022 Report (Informe de 2022, El costo comercial del phishing)
[2]State of Cybersecurity for Mid-Sized Businesses, 2023 (El estado de la ciberseguridad para las medianas empresas)
[3]ArmorBlox
[4]Equipo de investigación de correo electrónico de Check Point

Por eso, es fundamental implementar el producto de orquestación, automatización y respuesta de seguridad (SOAR) de KnowBe4, diseñado específicamente para gestionar las amenazas de phishing y responder a ellas: PhishER Plus.

Los beneficios y el retorno de la inversión de PhishER Plus/PhishER de KnowBe4

Estos son los ahorros de costos, aumentos de productividad y beneficios comerciales que obtuvo una organización empresarial al implementar PhishER de KnowBe4, según el Forrester Total Economic Impact de KnowBe4.[5]

Gracias al uso del Phish Alert Button de KnowBe4, los empleados de la organización denuncian hasta 2000 correos electrónicos sospechosos en PhishER por mes. Cerca del 88 % de estos correos electrónicos denunciados por los usuarios son correos no deseados (spam) o amenazas. Esto ayuda a la organización a gestionar, derivar y corregir estos grandes volúmenes mediante la función de cuarentena de correos electrónicos de PhishRIP a fin de poner en cuarentena y eliminar automáticamente los correos electrónicos de phishing denunciados desde las casillas de correo de los usuarios afectados.

Se calcula que el ahorro de tiempo gracias a las notificaciones de alerta de correo electrónico y las respuestas automatizadas tiene un valor de $411 302.

PhishER Plus le ahorra al equipo de respuesta ante incidentes de la organización un promedio de 25 minutos de trabajo de investigación y corrección por cada correo electrónico.

La colaboración creciente entre los usuarios y el equipo de operaciones de seguridad permite responder de forma proactiva ante las amenazas y reducir los tickets en el servicio de asistencia de TI, así como la necesidad de realizar trabajos de corrección de TI.

Las respuestas automatizadas le permiten comunicarse rápidamente con los empleados en relación con los correos electrónicos que requieren para seguir trabajando.

Otras organizaciones que ahorran tiempo:

- **Organización de infraestructura crítica con base en los EE. UU.**

  Ahorra al equipo de TI el equivalente a 7 semanas por año gracias a que investiga, pone en cuarentena y elimina automáticamente los correos electrónicos maliciosos.

- **Empresa de marketing**

  Redujo la cantidad de correos electrónicos sospechosos que se debían investigar manualmente de aproximadamente 70 a 20 por mes, lo que se tradujo en un ahorro de al menos 12,5 horas por mes.

- **Organización de tecnología**

  Utiliza el análisis de PhishER impulsado por IA para identificar automáticamente el 70 % de todos los correos electrónicos denunciados por los usuarios, lo que permite asignar personal y presupuesto a otros equipos de TI.

- **Organización sin fines de lucro**

  Mejores tiempos de respuesta ante los ataques de phishing y más personal y recursos de TI disponibles para otras prioridades de seguridad.

- **Instituciones de educación superior**

  PhishER eliminó más de 150 000 correos electrónicos maliciosos de las bandejas de entrada de los usuarios antes de que tuvieran la oportunidad de hacer clic en ellos.

Más de 65 000 organizaciones en todo el mundo lo utilizan con éxito.

Obtenga más información

[5] Forrester Total Economic Impact of KnowBe4 (Impacto económico total de KnowBe4 según Forrester)

KnowBe4 Brazil | Av. Ibirapuera, 2315, Indianópolis, CEP 04029-200 | São Paulo-SP | Tel: +55 (0800) 761-2668 | www.KnowBe4.com | Correo electrónico: Sales@KnowBe4.com
