KnowBe4
Human error. Conquered.

Siete amenazas de ingeniería social que el asesoramiento en tiempo real puede ayudar a mitigar

INTRODUCCIÓN

Fortalecer el firewall humano de su organización representa la última línea de defensa contra los ciberataques y las violaciones de seguridad de datos. La innovadora capacitación en concientización sobre seguridad es una de las mejores maneras de lograr esto.

Otra es el asesoramiento en tiempo real a los usuarios en respuesta a comportamientos de seguridad riesgosos mediante el envío de la educación adecuada en el momento de la acción riesgosa. Para lograr esto, una plataforma de asesoramiento en tiempo real como SecurityCoach de KnowBe4 consolida los datos de alerta de la pila de seguridad de su organización (gestión de terminales, correo electrónico/web, acceso a identidades, SIEM/SOAR, etc.), los analiza y determina qué amenazas ofrecen las mejores oportunidades para asesorar a sus usuarios. El asesoramiento en tiempo real ofrece a las organizaciones la oportunidad de fortalecer su firewall humano contra una gran cantidad de amenazas de ingeniería social.

SIETE AMENAZAS DE INGENIERÍA SOCIAL

A continuación, se describen siete de las amenazas de ingeniería social más comunes y cómo el asesoramiento en tiempo real puede ayudar a mitigarlas aprovechando los datos de alerta de su pila de seguridad existente.

Descargar archivos adjuntos potencialmente peligrosos
Muchos intentos de ingeniería social consisten en lograr que una víctima potencial descargue o abra un archivo adjunto peligroso, como un archivo EXE, DOC o HTML. Muchas de las herramientas de seguridad mencionadas anteriormente bloquearán la mayoría de las descargas de archivos de alto riesgo. Sin embargo, cuando se integran con el asesoramiento en tiempo real, estas acciones se pueden aprovechar para capacitar a los usuarios a fin de que no descarguen archivos potencialmente maliciosos.

Hacer clic en enlaces de alto riesgo
Muchos intentos de ingeniería social contienen URL maliciosas que simulan ser enlaces de confianza de un determinado proveedor o fuente confiable. Una vez más, muchas de las herramientas de seguridad antes mencionadas bloquearán estos enlaces falsos. Pero cuando se integran con el asesoramiento en tiempo real, estos datos de alerta se pueden utilizar para recordar a los usuarios que deben pasar el cursor sobre los enlaces URL para comprobar su legitimidad antes de hacer clic en ellos.

Filtrado de contenido
Muchas herramientas de seguridad bloquean el contenido censurable según lo definido en las políticas de contenido de una organización. Por ejemplo, un usuario puede intentar ver un video violento o ser engañado para que lea un contenido cuestionable o inapropiado. El acceso a este contenido se bloquea, y se puede mostrar al usuario un mensaje de advertencia para que evite contenidos similares porque van en contra de las políticas de una organización.

Ejecutar o instalar software no autorizado
A menudo, los usuarios intentan instalar software no aprobado por la organización. Un programa de control de aplicaciones de seguridad bloquearía la instalación o ejecución, mientras que el asesoramiento en tiempo real se podría usar para recordar a los usuarios que no deben instalar aplicaciones o servicios no autorizados, además de otra información relevante.

Iniciar conexiones salientes no autorizadas
Determinadas herramientas de análisis y monitoreo del tráfico de red identifican conexiones salientes no autorizadas a ubicaciones maliciosas conocidas. Cuando se combinan con una plataforma de asesoramiento en tiempo real, se podría recordar al usuario que no instale ni utilice software o servicios de comunicación no autorizados.

Intentar iniciar sesión en computadoras no autorizadas
En la mayoría de las organizaciones, los inicios de sesión entre computadoras son poco frecuentes. Una de las principales señales de actividad maliciosa son los inicios de sesión inesperados de una computadora a otra sin que haya un motivo legítimo. Muchas de las herramientas de seguridad mencionadas anteriormente bloquearán estas conexiones no autorizadas, y una plataforma de asesoramiento en tiempo real podría recordar a los usuarios que no intenten conectarse a computadoras que no están autorizados a utilizar.

Intentar eludir los requisitos de autenticación multifactor
Muchas organizaciones exigen a los usuarios que utilicen la autenticación multifactor (Multi-Factor Authentication, MFA) para iniciar sesión en las redes o computadoras de la organización. Los usuarios que intenten eludir la autenticación multifactor o utilizar una forma no autorizada de autenticación multifactor, por lo general, activarán un mecanismo de detección y bloqueo. Se podría utilizar una plataforma de asesoramiento en tiempo real para recordar a los usuarios que deben utilizar un inicio de sesión de autenticación multifactor aprobado por la empresa.

REDUZCA LOS RIESGOS Y MEJORE SU CULTURA DE LA SEGURIDAD

En definitiva, es más probable que las personas acepten corregir sus errores cuando estos se identifican de inmediato y se proporcionan prácticas recomendadas de seguridad en tiempo real.

El asesoramiento en tiempo real logra esto y permite a su organización hacer lo siguiente:

- Reforzar la capacitación en concientización sobre seguridad existente.
- Obtener información sobre los riesgos de seguridad mediante el seguimiento de las tendencias de la actividad riesgosa de sus usuarios a lo largo del tiempo.
- Reducir el riesgo humano y mejorar la cultura de seguridad general de su organización.
- Aumentar el valor de su pila de seguridad existente mediante la integración con las herramientas de seguridad comunes que ya utiliza.

Defenderse de los agentes de amenazas y sus tácticas maliciosas añadiendo asesoramiento de seguridad en tiempo real a su conjunto de herramientas de concientización sobre seguridad.

OBTENGA MÁS INFORMACIÓN **Cómo SecurityCoach puede fortalecer su firewall humano**

Recursos adicionales

Prueba de seguridad contra el phishing (PST) gratuita
Descubra qué porcentaje de sus empleados tienen predisposición para ser víctimas de phishing con la prueba de seguridad contra el phishing (PST) gratuita.

Automated Security Awareness Program gratuito
Cree un programa de concientización sobre seguridad personalizado para su organización.

Phish Alert Button gratuito
Ahora sus empleados tienen una forma segura de informar los ataques de phishing con un solo clic.

Email Exposure Check (EEC) gratuita
Descubra antes que los malhechores cuál de las direcciones de correo electrónico de sus usuarios está expuesta.

Domain Spoof Test gratuita
Descubra si los hackers pueden falsificar una dirección de correo electrónico de su propio dominio.

Acerca de KnowBe4

KnowBe4 es la plataforma integrada de capacitación en concientización sobre seguridad y phishing simulado más grande del mundo. Al constatar que se estaba descuidando seriamente el elemento humano en la seguridad, se creó KnowBe4 para ayudar a que las organizaciones manejen el problema de la ingeniería social con una metodología integral de capacitación sobre concientización de la nueva escuela.

Este método integra pruebas iniciales con simulacros de ataques del mundo real, capacitación interactiva y atractiva, y evaluación continua a través de informes simulados sobre la fortaleza empresarial para crear una organización con mayor capacidad de adaptación y que considere la seguridad como principal prioridad.

Decenas de miles de organizaciones en todo el mundo utilizan la plataforma de KnowBe4 en todas las industrias, incluidos los campos estrictamente regulados como las finanzas, la salud, la energía, el gobierno y los seguros, para movilizar a sus usuarios finales como última línea de defensa y permitirles tomar mejores decisiones de seguridad.

Para obtener más información, visite www.KnowBe4.com.

KnowBe4
Human error. Conquered.

En Brasil, somos El Pescador, una empresa KnowBe4 | Av. Ibirapuera, 2315 - 14º andar - SL. 142 CEP 04029-200 | São Paulo-SP | www.KnowBe4.com | Sales@KnowBe4.com

07D03K01