RESUMEN DE LA SOLUCIÓN

Amplíe su perímetro de defensa con el servicio de capacitación y concientización sobre seguridad de Fortinet

Proteja su organización creando una fuerza laboral con conciencia cibernética

Resumen ejecutivo

La prevalencia del ransomware sigue creciendo. Según el Informe global del panorama de amenazas del T1 de 2021 de FortiGuard Labs, el ransomware creció un 1070 % entre julio 2020 y junio 2021. Mientras que numerosos incidentes de alto perfil acaparan los titulares internacionales, el impacto real lo sufren decenas de miles de organizaciones, desde empresas hasta pequeños negocios y desde agencias federales hasta gobiernos locales.

Los empleados se convirtieron en activos de alto valor para los cibercriminales: no se puede olvidar el factor humano de la ciberseguridad. Hoy en día, la mayoría de las organizaciones siguen enfrentándose a una escasez de competencias. Aunque la concientización y la capacitación son fundamentales, algunas organizaciones pueden tener dificultades para definir, implementar y administrar un programa eficaz.

Proteger a una organización del creciente volumen de actores del Estado-nación, organizaciones de cibercriminales, ciberterroristas y hackers solitarios es cada vez más difícil. Los empleados son ahora objetivos de alto riesgo. Es necesario un esfuerzo continuo de capacitación para impulsar una concientización efectiva y un cambio de comportamiento.

Desarrollado por los mejores expertos en capacitación en ciberseguridad, el servicio de capacitación y concientización sobre seguridad de Fortinet ofrece una solución llave en mano que brinda una concientización oportuna y actual sobre las amenazas de ciberseguridad de hoy en día, y ayuda a construir una cultura de conciencia cibernética que está informada y capacitada para ayudar a proteger la organización.

Orientada al mercado y con capacidad de respuesta

Dado que el panorama de las amenazas cambia rápidamente y es cada vez más malicioso, los programas de capacitación y concientización sobre seguridad deben evolucionar al mismo tiempo para garantizar que están al día con las amenazas actuales. La expansión de la superficie de ataque impulsada por la transformación digital, la fuerza laboral híbrida que trabaja desde cualquier lugar y la pandemia mundial convierten a los empleados en objetivos importantes para los ciberdelincuentes.

Una solución de capacitación y concientización sobre seguridad debe contribuir a una cultura de seguridad global. Para ello, aplicar una casilla de verificación a un enfoque de cumplimiento de la capacitación no fomentará una cultura de concientización, ni responderá al panorama de amenazas en constante cambio.

"De hecho, las personas afectan directamente a los resultados de seguridad más que la tecnología, las políticas o los procesos. En los últimos 12 meses, el "elemento humano" intervino en el 85 % de las violaciones, y en casi la mitad de ellas (36 %), la suplantación de identidad fue el principal modo de ataque. En consecuencia, un programa de concientización sobre la seguridad debe considerarse un elemento crítico para ofrecer un programa de seguridad empresarial de defensa en profundidad, o de varias capas".

— Gartner®, Market Guide for Security Awareness Computer-Based Training, Richard Addiscott, Claude Mandy, William Candrick, 26 de julio 2021

En el informe Fortinet Cybersecurity Insiders: 2021 INFORME DE SEGURIDAD DE APLICACIONES, se les preguntó a 344 profesionales de la ciberseguridad: "¿Cuál de las siguientes barreras impide a su organización defenderse adecuadamente contra las ciberamenazas?" El cuarenta y tres por ciento eligió la poca conciencia de seguridad entre los empleados como un problema clave.

Los elementos de un sólido programa de capacitación sobre concientización de la seguridad incluyen:

- Capacitación relacionada con el contexto y el contenido
- Contenidos atractivos que no abrumen al estudiante
- Capacidad de volver a involucrar a los estudiantes para asegurarse de que la información se refuerza
- Capacitación basada en funciones para impartir la capacitación correcta a las personas adecuadas
- Aprendizaje fragmentado y comprensible para mantener la atención del estudiante
- Medición y análisis para pruebas y mejoras

La implementación de un servicio eficaz de concientización y capacitación, y el fomento de una cultura de concientización sobre las ciberamenazas ayudan a las organizaciones a cumplir con los requisitos de cumplimiento y a proteger sus inversiones tecnológicas, la reputación de su marca y sus finanzas.

El servicio de capacitación y concientización sobre seguridad de Fortinet es una oferta de software como servicio (SaaS) que puede integrarse con FortiPhish para proporcionar una solución. La capacitación entregada en múltiples formatos, incluyendo video, texto, audio, imágenes y animación, satisface los diferentes estilos de aprendizaje para asegurar que la capacitación se entienda y se aplique. Las extensiones más pequeñas y fáciles de adquirir, como el microaprendizaje y el nanoaprendizaje, junto con los recursos de comunicación, permiten a las organizaciones aumentar su capacitación para ayudar a reforzar las lecciones clave.

Capacitación de alta calidad

Los cursos están diseñados para un aprendizaje óptimo, con módulos de introducción de aproximadamente 8 minutos y micromódulos de reactivación de aproximadamente 2 minutos.

Capacitación basada en funciones para usuarios finales, gerentes y ejecutivos.

A lo largo de la capacitación, los exámenes interactivos y las verificaciones de conocimientos mantienen a los estudiantes comprometidos e interesados, lo que les permite a los gerentes evaluar los niveles de conocimiento.

Recursos de comunicación y refuerzo

Refuerce las enseñanzas clave de los módulos del curso con videos y otros activos. Mezcle y combine activos con diferentes cursos y utilícelos para llevar a cabo campañas específicas sobre las principales amenazas oportunas.

- Nanovideos
- Pósteres
- Protectores de pantalla
- Pancartas
- Hojas de sugerencias

Administración y manejo fáciles de usar

El servicio ofrece varios recursos para ayudar a los administradores a implementar y administrar el servicio, entre ellos:

- Videos de planificación e implementación
- Guía de implementación de la campaña de concientización sobre la seguridad
- Informe trimestral sobre las principales señales de amenaza para los administradores (desarrollado por FortiGuard Labs)

Además, el inicio de sesión único, la autenticación de dos factores y la integración LDAP facilitan el aprovisionamiento y la administración de los usuarios.

Monitoreo e informes activos

El portal de administración ofrece un panel actualizado de la actividad del usuario. Los informes están disponibles en formato pdf:

- Informe individual de campaña
- Informe semanal, mensual o al finalizar la campaña
- Informe de campaña para ejecutivos
- Resumen de todas las campañas
- Tasa de culminación total
- Progreso de todas las campañas

Marca personalizada y marca compartida

Los socios pueden personalizar su marca y ofrecer un servicio completo de capacitación y concientización sobre seguridad a sus clientes. Con el soporte jerárquico basado en roles y múltiples tenencias, los socios pueden administrar toda la experiencia, desde el aprovisionamiento de usuarios hasta la generación de informes para sus clientes y el empaquetamiento y la venta de servicios de consultoría adicionales con la solución.

Simulación de suplantación de identidad

Integre el servicio de capacitación y concientización sobre seguridad con FortiPhish y ponga a prueba la concientización y la vigilancia de sus usuarios mediante ataques de suplantación de identidad simulados en el mundo real, al tiempo que refuerza las prácticas adecuadas en el punto de clic.

Los administradores pueden crear reglas dinámicas con acciones de capacitación basadas en los resultados de la simulación de suplantación de identidad para proporcionar capacitación de corrección cuando sea necesario.

La capacitación instruye a su fuerza laboral sobre las ciberamenazas actuales, tales como suplantación de identidad, ingeniería social y ataques de ransomware y cómo protegerse contra ellos. El servicio de capacitación y concientización es adecuado para toda fuerza laboral, desde empleados técnicos y no técnicos hasta contratistas.

Cuando lo completen, entenderán:

- Los malos actores que están detrás de los ataques y qué los motiva
- Los métodos que se utilizan para los ataques
- Cómo protegerse a sí mismos y a la información a la que tienen acceso
- Términos clave de ciberseguridad

Cumplimiento y protección

Los materiales de los cursos de capacitación de Fortinet abordan la capacitación para la concientización de los usuarios que se describe en GDPR, PCI DSS, SOC 2, PIPEDA, CCPA e ISO. Creados específicamente para cumplir con los requisitos de capacitación y concientización sobre seguridad, tal como se indica en NIST 800-50 y NIST 800-16, los módulos de capacitación de Fortinet se centran en las necesidades de las organizaciones actuales y responden al mercado. A diferencia de otras soluciones que proporcionan un volumen abrumador de contenidos sin un plan claro para su implementación, el servicio de capacitación y concientización sobre seguridad de Fortinet proporciona la capacitación adecuada que puede impartirse en cualquier momento.

Ampliación de la protección

La arquitectura de malla de ciberseguridad del Fortinet Security Fabric, que trabaja junto con la capacitación y concientización sobre seguridad, les da a las organizaciones la capacidad de responder a las amenazas en cualquier lugar y en todas partes. El servicio de capacitación y concientización sobre seguridad amplía la protección proporcionada por las tecnologías de Fortinet Security Fabric para capacitar a los empleados para que sean conscientes y se comprometan con la protección de la organización, fortificando y ampliando así el perímetro de defensa.

julio 29, 2022
1407610-0-0-ES