Universitat Oberta de Catalunya

uoc.edu

Guía de prevención y respuesta frente a ataques de ransomware

Anexo III. Formación en ciberseguridad como prevención

Carlos Alberto Crego Sánchez
Master en Ciberseguridad y Privacidad
Privacidad

Albert Jové Canela
Cristina Pérez Sola

28 de diciembre del 2021

Índice

Anexo III. Formación en ciberseguridad

La ciberseguridad se ha convertido en un tema importante de discusión en los últimos años debido en parte a los ataques de ransomware.

Desde el 2016 y durante cada año hasta la actualidad hemos sido testigos de ciberataques que o bien exponían millones de registros de clientes y credenciales o bien resultaban en la infección de buena parte de la red corporativa de grandes empresas y organismos públicos.

Los ciberdelincuentes se han vuelto cada vez más sofisticados y las organizaciones empresariales y las agencias gubernamentales se han dado cuenta de la importancia de educar a sus empleados en ciberseguridad.

Desde la rápida explosión del ransomware en 2016, todos los estudios relacionados con las amenazas de ciberseguridad concluyen que el factor humano sigue siendo y seguirá siendo el eslabón más débil, por tanto, implementar un programa de formación en ciberseguridad es vital para la supervivencia de las organizaciones y se considera la mejor manera de prevenir ataques de ransomware y otras amenazas.

Un buen programa de formación en ciberseguridad educará a los empleados sobre las diferentes amenazas de ciberseguridad a las que se pueden enfrentar y les enseñara a identificar los puntos de entrada que pueden usar los atacantes para acceder a la red corporativa y qué medidas de precaución deben tomar para evitar el acceso no autorizado a los activos digitales de la organización.

Una parte del programa de formación en ciberseguridad consiste en hacer cumplir las reglas de la política de seguridad corporativa y aclarar la responsabilidad de los empleados de IT de acuerdo con su función laboral en la protección de los activos digitales de la organización y de los sistemas de IT.

En algunos sectores, la formación en ciberseguridad se ha vuelto obligatoria para cumplir con las leyes gubernamentales o con otros organismos de cumplimiento no oficiales que trabajan por promover las mejores prácticas de seguridad en el sector.

Por ejemplo, en Estados Unidos, la ley de transferencia y responsabilidad del seguro médico (HIPAA) exige que todas las organizaciones que trabajan en el sector de la salud implementen un programa de formación en ciberseguridad para todos los miembros del personal a fin de proteger la información del paciente.

En este capítulo, se analiza la importancia de que todas las organizaciones tanto públicas como privadas cuenten con un programa de formación en ciberseguridad, así como los temas que deben incluirse en dicho programa.

Importancia de la formación en ciberseguridad

Todos los empleados, proveedores de servicios de IT y terceros que tengan acceso al sistema de IT corporativo o que dispongan de una cuenta de correo electrónico deben recibir una formación adecuada en ciberseguridad.

Dicha capacitación es importante para proteger a la organización de ciberdelincuentes que intentan obtener acceso no autorizado a sus datos, a continuación, se enumeran los principales beneficios de realizar una formación sobre concienciación en ciberseguridad.

Reducción de incidentes

Diversos informes apuntan a que los empleados negligentes son el punto débil de pequeñas y medianas empresas cuando se trata de amenazas de ciberseguridad, especialmente cuando se trata de ransomware.

Educar a los empleados sobre los peligros de abrir archivos adjuntos de correo electrónico de fuentes desconocidas y hacer clic en enlaces sospechosos en correos electrónicos no deseados reducirá en gran medida el número de incidentes.

Mejora la seguridad general de la organización y su reputación

Cuando los empleados están formados en los diferentes vectores de ataque y en cómo evitarlos, la organización estará menos expuesta a ciberataques y a la exposición de información confidencial, lo que en consecuencia aumentará su reputación y hará que los clientes estén más dispuestos a depositar su confianza.

Aumenta la efectividad de las defensas tecnológicas

El hecho de que una organización use firewalls, sistemas de prevención de intrusiones (IPS), software antivirus, programas antimalware y otras soluciones de seguridad es insuficiente para protegerse contra ciberataques sin capacitar a los empleados en conciencia en ciberseguridad.

Por ejemplo, el sistema operativo del equipo de un usuario puede solicitarle que instale las actualizaciones de seguridad necesarias, sin embargo, si tales advertencias son ignoradas, el resto de las soluciones de seguridad adoptadas pueden acabar por resultar inútiles.

Evita pérdidas por incidentes de seguridad

Un ataque de ransomware exitoso puede costarle a la organización afectada una cantidad considerable de dinero si se ve obligada a interrumpir su actividad para recuperar y restaurar su operativa habitual.

Aun pagando el rescate, las empresas pueden dañar su reputación si se hace público que han sido víctimas de un ataque de ransomware, lo que se traduce en una pérdida de confianza por parte de potenciales clientes.

Aumenta la satisfacción de los empleados

Llevar a cabo una formación de concienciación en ciberseguridad aumentará la satisfacción de los empleados, haciéndolos más dispuestos a permanecer en su empresa actual, mejorar su carrera, sentirse seguros y asegurar su privacidad digital personal fuera del trabajo.

Buenas prácticas en programas de formación

A continuación, se enumeran los principales aspectos a considerar a la hora de crear un programa general de formación en ciberseguridad.

Crear el equipo de concienciación sobre seguridad

El programa de capacitación supone un esfuerzo continuo que requiere seguimiento y actualizaciones periódicas.

El primer paso es establecer un equipo de liderazgo responsable de desarrollar, hacer seguimiento e implementar el programa de capacitación, este equipo debe estar formado por diferentes departamentos e incluir personal con diferentes perfiles de IT, desde principiantes hasta profesionales para garantizar que el programa cubra todos los niveles.

Determinar los roles

El programa de capacitación en ciberseguridad debe estar dirigido a todos los empleados, desde el director ejecutivo hasta el personal de IT.

Es importarte considerar que no todo el personal tiene el mismo nivel de conocimiento o experiencia en informática, ni encara el mismo tipo de amenazas, por tanto, la capacitación debe ser distinta para un ingeniero de redes que para alguien del departamento de marketing ya que el ingeniero de redes debe estar capacitado para responder a una mayor variedad de ciberataques dada la naturaleza de su función laboral.

Por ejemplo, podemos dividir los empleados en 4 grupos basándonos en el rol que desempeñan dentro de la organización y de los activos digitales a los que tienen acceso:

- **Nivel ejecutivo**: Las personas en este nivel, no suelen tener un conocimiento tecnológico profundo y suelen tener acceso a información muy confidencial, la mayor amenaza a la que se encuentran expuestos, son los ataques de ingeniería social, por tanto, la capacitación debe estar especializada en este tipo concreto de ciberataque.

- **Personal de IT**: La capacitación para las personas en este nivel debería ser técnica y centrada en mitigar y responder a ciberataques.

- **Personal de administración**: La capacitación para personas de este nivel debería ser general y centrarse sobre todo en las políticas de seguridad corporativas.

- **Todo el personal**: Independientemente del nivel, todo el personal debería estar capacitado para mitigar y responder a los ciberataques más comunes, principalmente el phising y seguir las políticas de seguridad cuando usen los equipos de usuario para acceder a la red, consultar el correo electrónico o conectar dispositivos USB.

Determinar los temas a cubrir

Los materiales deben cubrir todos los aspectos de la ciberseguridad relevantes para la función laboral de cada usuario. A continuación, se proporciona una lista de los temas principales que deberían cubrirse:

- **Introducción**: En esta sección se debe explicar brevemente por qué es importante la ciberseguridad tanto para las personas como para las empresas, así como identificar las amenazas actuales y los diferentes vectores de ataque empleados.

- **Seguridad personal**: Este tema debe ocuparse de educar a los usuarios sobre las mejores prácticas para proteger sus cuentas personales y equipos de usuario e incluir aspectos como el uso de contraseñas seguras, ataques de fuerza bruta o diccionario, ataques de ingeniería social y cómo mitigarlos, riesgos asociados con el uso de redes sociales o sitios web de medios que revelen información confidencial sobre el trabajo y la vida personal que podrían ser explotados por los atacantes.

- **Seguridad informática**: En esta sección, el usuario debe aprender a diferenciar los diferentes tipos de malware así cómo se pueden introducir en la red corporativa, también sobre las soluciones de seguridad más comunes como, por ejemplo, antivirus, antimalware y firewalls para proteger los equipos y sobre la importancia de crear copias de seguridad. La seguridad en la nube también debe introducirse en esta sección.

- **Seguridad en Internet**: Este tema debe incluir los riesgos de seguridad derivados del uso del navegador web y el correo electrónico y cómo evitarlos mediante la instalación de complementos de seguridad, también debe abordarse el uso de redes privadas virtuales (VPN) y comprender cómo los atacantes pueden aprovechar las vulnerabilidades del navegador web para obtener acceso no autorizado.

- **Seguridad móvil**: En esta sección, los empleados deben comprender cómo los intrusos pueden explotar las redes WiFi para obtener acceso no autorizado, conocer los riesgos asociados con el uso de la tecnología móvil y los dispositivos de IoT, comprender la política de seguridad de una organización con respecto al uso dispositivos móviles, como proteger los dispositivos móviles y utilizar las redes WiFi de forma segura.

Ataques de ingeniería social

La ingeniería social, no es otra cosa que manipular psicológicamente a las víctimas con objeto de que proporcionen la información que los ciberdelincuentes necesitan para realizar accesos no autorizados a sus equipos.

A grandes rasgos, existen 2 tipos de ataques de ingeniería social, el primero y el más común, consiste en el envío de correos electrónicos, a esta técnica se la conoce como phising y el segundo consiste en realizar llamadas telefónicas suplantando la identidad de una persona o compañía para conseguir información confidencial de las víctimas, a esta técnica se la conoce como vishing.

Tanto el phising como el vishing son términos informáticos que distinguen un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza para manipularla y hacer que lleve a cabo acciones que no debería realizar.

Obviamente, esto dificulta la predicción de este tipo de ataques, ya que nadie puede predecir el comportamiento humano en tales casos, por tanto, es muy importante que los programas de formación en ciberseguridad incorporen las amenazas derivadas del uso de técnicas de ingeniería social, especialmente el phising.

Por esta razón, es importante estar siempre alerta y desarrollar en los empleados una conducta responsable cuando utilicen dispositivos que se encuentren conectados a la red corporativa.

La importancia de reconocer un ataque de phising

Los correos electrónicos de phising tienen como objetivo la adquisición de información confidencial de la víctima, sobre todo, sus credenciales de banca online, redes sociales, credenciales corporativas de inicio de sesión y cuentas de almacenamiento en la nube.

Una vez que el atacante obtiene las credenciales de acceso, puede usarlas para chantajear a la víctima o realizar acciones no autorizadas, por ejemplo, en el caso de obtener las credenciales de banca online, realizar compras sin el consentimiento de la víctima.

En un contexto empresarial, los ataques de phising se emplean para obtener un punto de entrada a la red corporativa que permita superar todos los perímetros de seguridad de la red para infectar y propagar ransomware o para obtener acceso a otros segmentos de la red.

La formación en defensa contra el phishing es un componente esencial en cualquier programa de formación en ciberseguridad ya que sigue siendo el vector de ataque número uno, por tanto, es primordial que los usuarios aprendan a reconocer las diversas técnicas empleadas en los correos electrónicos de phising.

Bibliografía

Nihad A. Hassan
Ransomware Revealed
Apress, 2019