ESCAPE:

Preparing healthcare professionals for cyberattacks

Puzzles para estudiantes

¿Estás preparado para afrontar los ciberataques?

ESCAPE: Preparing healthcare professionals for cyberattacks	
¿Estás preparado para afrontar los ciberataques?	
Idioma	Español

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.

ESCAPE: Preparing healthcare professionals for cyberattacks	
¿Estás preparado para afrontar los ciberataques?	
Idioma	Español

Índice

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.

ESCAPE: Preparing healthcare professionals for cyberattacks	
¿Estás preparado para afrontar los ciberataques?	
Idioma	Español

1) ¿Estás preparado para afrontar los ciberataques?

Este rompecabezas consta de 5 preguntas relacionadas con los diferentes ataques que puede sufrir su centro de salud. Elija con cuidado para proteger adecuadamente sus valiosos datos de los ciberdelincuentes.

2) Clasificación

Category	Mark if applies
Sector	☑ Cuidado de la salud
	☐ General
Temas cubiertos	☑ Ciberseguridad
	☑ Protección de datos
Tipo de situación	☑ Prevención
	☐ Impacto (es decir, cuando está ocurriendo o ha ocurrido) en el cuidado del paciente.
	☑ Impacto en todas las demás actividades que no impliquen atención directa al paciente.
Idioma de los materiales originales	☐ Holandés
	☑ Inglés
	☐ Alemán
	☐ Italiano
	☐ ESpañol
Tipo de material	☑ Preguntas de cuestionario

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.

ESCAPE: Preparing healthcare professionals for cyberattacks	
¿Estás preparado para afrontar los ciberataques?	
Idioma	Español

	☐ Juegos
	☐ Aplicaciones y vídeos interactivos
	☐ LIstas de verificación

3) Preguntas de cuestionario

1) Usted está a cargo de la gestión de una clínica dental privada. Un empleado abrió un documento adjunto, supuestamente enviado por un cliente, y el equipo se bloqueó inmediatamente con un mensaje emergente que le instaba a pagar para restaurar el acceso y los datos. En caso de un ataque de ransomware a su clínica, ¿cuál de las siguientes medidas no se recomienda para prevenirlo o mitigarlo?
    a) Cambie todas las contraseñas, incluida la contraseña de administrador del sitio web y la contraseña de Wi-Fi, como medida de precaución..
    b) Haga clic en el archivo adjunto del correo electrónico accediendo a él desde otra computadora que no esté conectada a la red.
    c) Retire las unidades infectadas para desinfectarlas y ver si se pueden recuperar los datos.
    d) Restaure las copias de seguridad en nuevas unidades y reanude el trabajo.

Respuesta correcta: Haga clic en el archivo adjunto del correo electrónico accediendo a él desde otra computadora que no esté conectada a la red.

Comentarios: Aunque parezca conveniente, es posible que se almacenen datos maliciosos en esa nueva computadora. Debe contactar con su servicio de soporte informático o con organismos oficiales (policía, instituciones de ciberseguridad, etc.) para encontrar la mejor manera de resolver el problema.

2) Uno de los empleados de su laboratorio recibió una llamada instándolo a proporcionar las contraseñas de administrador de la página web para realizar tareas críticas de mantenimiento del servidor. Como parecía confiable, las proporcionó. Como resultado, la página web relacionada con su laboratorio fue redirigida por ciberdelincuentes. Se trató de un intento de phishing en el que los delincuentes buscan obtener los nombres de usuario, las contraseñas o las cuentas bancarias de sus clientes redirigiendo su página web a su entorno malicioso. ¿Cuál de estas acciones no es útil para mitigar el problema?
    a) Realizar una copia encriptada (para enviar a la policía junto con el informe) de los registros del servidor donde se pueden ver los intentos de acceso de los ciberdelincuentes y las potenciales víctimas.
    b) Solicitar al proveedor de alojamiento web que desconecte el sitio web.
    c) Despedir al empleado para que no vuelva a suceder.
    d) Restaure las copias de seguridad en nuevas unidades y reanude el trabajo.

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.

Respuesta correcta: Despedir al empleado para que no vuelva a suceder.

Comentarios: La mejor solución para estar bien protegido en estos escenarios es la educación adecuada, la capacitación del personal y el aprendizaje de los errores. Despedir al empleado no mitigará el problema ni capacitará al resto del personal para evitar este tipo de ataques.

3) Trabajas en una farmacia como auxiliar de farmacia y teletrabajas dos veces por semana junto con otros empleados que, finalmente, han tenido varias sustituciones. De la noche a la mañana, los datos clínicos de algunos pacientes de tu farmacia aparecieron en la red oscura, y las autoridades locales te llamaron para comprobar qué estaba pasando. ¿Cuál de las siguientes opciones podría explicar mejor esta filtración de datos?
    a) Se olvidó quitar el acceso remoto al personal temporal de su farmacia una vez que haya terminado su trabajo.
    b) Utilice una conexión VPN segura para acceder a los registros de los pacientes mientras trabaja desde casa.
    c) Implementar políticas de contraseñas seguras y autenticación de dos factores para todas las cuentas del personal.
    d) Actualice y aplique parches periódicamente a todos los sistemas de la farmacia para corregir vulnerabilidades de seguridad conocidas.

Respuesta correcta: Se olvidó quitar el acceso remoto al personal temporal de su farmacia una vez que hayan terminado su trabajo.

Comentarios: Si bien el teletrabajo tiene ventajas innegables, es fundamental garantizar la protección de sus datos para evitar filtraciones. Una de las medidas es garantizar que solo el personal autorizado tenga acceso a estos datos protegidos. Todas las demás opciones son, sin duda, buenas medidas para evitar esta filtración.

4) Trabajas como auxiliar de enfermería en una clínica privada de atención a personas mayores y estás a cargo del inventario de suministros médicos generales. Tras regresar de vacaciones, observas varios pagos a proveedores desconocidos, y no hay recepción del material ni recibo. Al hablar con los contables, te encuentras con un mensaje de tu jefe solicitando sus credenciales para proceder con las transferencias. Tras revisarlo detenidamente, descubres que la dirección del remitente era falsa. ¿A qué tipo de problema nos enfrentamos?
    a) Ciberataques.
    b) DDos.
    c) Ingeniería social.
    d) Software no actualizado.

Respuesta correcta: Ingeniería social.

Retroalimentación: La ingeniería social es una técnica de ataque que se basa en la manipulación psicológica para engañar a las personas y lograr que revelen información confidencial, otorguen acceso no autorizado o realicen acciones que comprometan la seguridad. En lugar de explotar vulnerabilidades técnicas, la ingeniería social se aprovecha de la confianza, la curiosidad, el miedo o la urgencia de las personas para evadir las medidas de seguridad.

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.

5) Usted está a cargo de la red de un hospital privado en Barcelona, España. Recibe una llamada del gerente de una gran corporación que informa que su sitio web ha quedado inoperativo debido a un volumen masivo de tráfico de red procedente de los servidores de su empresa. La investigación revela un servicio DNS interno expuesto, la ausencia de firewall perimetral y que un atacante probablemente ha instalado malware para registrar sus equipos en una botnet controlada remotamente que luego envía tráfico a la víctima. ¿Qué tipo de ataque se describe?
   a) Inyección SQL.
   b) Ataque de intermediario (MitM).
   c) Ataque de denegación de servicio distribuido (DDoS).
   d) Ransomware.

Respuesta correcta: Ataque de denegación de servicio distribuido (DDoS).

Comentarios: El escenario describe el uso de numerosos hosts infectados (una botnet) para enviar grandes volúmenes de tráfico a un objetivo, saturando su servidor web y dejando el sitio indisponible. Esta es la definición de un ataque de denegación de servicio distribuido (DDoS). La exposición del servicio DNS y la falta de firewall explican cómo el atacante pudo comprometer las máquinas internas y utilizarlas para generar el tráfico. Las opciones A, B y D describen diferentes tipos de ataque que no se corresponden con el comportamiento de la botnet, que implica tráfico masivo e impacto en la disponibilidad, en este escenario.

6) Más información

Estas preguntas han sido inspiradas y adaptadas al sector salud por los escenarios presentados por INCIBE en la siguiente web https://www.incibe.es/empresas/formacion/juego-rol-pyme-seguridad. Este material se publica en español, ya que INCIBE es una institución española.

Co-funded by the European Union

El proyecto "ESCAPE: preparing healthcare professionals for cyberattacks" está cofinanciado por la Unión Europea. Las opiniones y puntos de vista expresados en este material sólo comprometen a sus autores (ESCAPE consortium) y no reflejan necesariamente los de la Unión Europea ni los del Servicio Español para la internacionalización de la educación (SEPIE). Ni la Unión Europea ni la agencia nacional sepie pueden ser considerados responsables de ellos.