Cyber MSME

Ciberseguridad para las micro, pequeñas y medianas empresas

Gestión de crisis – me hackearon, ¿y ahora qué?

Por CTS Customized Training Solutions & CASE

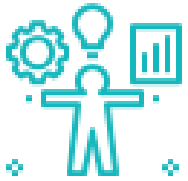
Erasmus+

Objetivos y metas

Al final de este modulo serás capaz de:

- identificar la crisis cibernética en el negocio
- identificar los potenciales riesgos y deficiencias
- evitar los errores más comunes en la crisis cibernética
- mejorar o crear el plan de gestión de crisis cibernética
- prepararse para la respuesta a la crisis cibernética y para la recuperación después de la crisis cibernética.

Indíce



Unidad 1: **Gestión de crisis cibernética**

Unidad 2: **Responder a la crisis cibernética**

Unidad 3: **Recuperación después de la crisis**

Unidad 1: Gestión de crisis cibernética

Sección 1.1: ¿Por qué necesitas la gestión de crisis cibernética?

Si gestionas una micro o pequeña empresa, probablemente no tienes bastante recursos ni personas para prevenir y combatir los crímenes cibernéticos.

Para las empresas medianas, es más realista delegar a unos especialistas para que trabajen en la ciber seguridad. Sin embargo, incluso los negocios más pequeños deberían sentirse obligados a mejorar los procedimiento de gestión de ciber seguridad.

Los protocolos de gestión de crisis cibernética consisten en 3 fases: 1) prevención, 2) **respuesta a la crisis,** y, por último, cuando pase la tormenta 3) **recuperación**.

En este módulo, puedes profundizar tu conocimiento sobre las fases 2 y 3.

Gracias a este módulo, mejorarás tus procedimientos de gestión de crisis cibernética con pasos que te ayudan a lidiar con el ataque del hacker.

Unidad 1: Gestión de crisis cibernética

Sección 1.2: Identificar la crisis

Primero que todo, necesitas saber lo que puede ser clasificado como crisis cibernética.

Una crisis cibernética es cualquier ciber evento que puede influenciar negativamente tu negocio.

Por ejemplo:

- Dispositivos hackeados
- Reproducción de pantallas de tus dispositivos
    - Correos copiados
- Datos de tarjetas de crédito robados
- Base de datos de los clientes robados
- Páginas web colapsadas
- Redes violadas
- Denegaciones de servicios, etc.

Erasmus+

Unidad 1: Gestión de crisis cibernética

Sección 1.2: Identificar la crisis

Todos los eventos cibernéticos sospechosos deben empezar su protocolo de crisis cibernética y lanzar la fase 2 — respuesta. Incluso si no estés 100 por cien seguro de lo que pasa, es mejor iniciar una acción.

Recuerda, no se trata solo de ti y de la situación actual de tu empresa. Tienes que tener cuidado también con:

- La seguridad de tus clientes y de los socios comerciales
- La rentabilidad de tu negocio
- La reputación segura de tu negocio

Erasmus+

Unidad 2: Responder a la crisis cibernética

Sección 2.1: El papel del tiempo

Tu reacción a la crisis cibernética tiene que ser rápida. A veces tienes unos segundos para hacer algo, y el peor escenario es que cunda el pánico. Ten en cuenta que el pánico y el miedo pueden costarte todo el negocio que has construido.

Los errores más comunes de las crisis cibernéticas en las MiPymes

- no nombrar a persona(s) responsable(s) de la respuesta a las crisis cibernéticas
- los contactos de proveedor no está disponibles
- no hay protocolo de comunicación sobre la crisis cibernética

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unidad 2: Responder a la crisis cibernética

Sección 2.1: El papel del tiempo

¿Por qué necesitas a una persona/as) responsable de la respuesta a la crisis cibernética?

La respuesta a la crisis cibernética es cualquier acción que puede ayudarte a gestionar un evento de crisis y proporcionar una actualización para los responsables de tu negocio.

La respuesta a la crisis cibernética es un plan que cumples en caso de un ataque. Cuando alguien te hackea, no hay tiempo para pensar quién hará qué. Cada uno necesita estar preparado. Esa es la razón que necesitas para una o varias personas responsables de la respuesta a la crisis cibernética.

Qué opinas: ¿la persona responsablede la respuesta a la crisis cibernética tienen que tener experiencia en el sector informático o no?

Unidad 2: Responder a la crisis cibernética

Sección 2.1: El papel del tiempo

¿No estás seguro de si las personas responsables de la respuesta a la crisis cibernética deberían tener experiencia en el sector informático? Bueno, podemos decirte que la experiencia en el sector TI no es el factor más importante. ¿Por qué? Para empezar, echamos un vistazo a las responsabilidades de la persona que se encarga de la respuesta a la crisis cibernética.

Responsabilidades de la persona que se encarga de la respuesta a la crisis cibernética:

- Conocer el plan de respaldo
- Supervisar todas las actividades dentro de una crisis
- Liderar la estrategia interna
- Implementar el protocolo de comunicación en caso de crisis cibernética

Unidad 2: Responder a la crisis cibernética

Sección 2.1: El papel del tiempo

Si la persona responsable de la respuesta a la crisis cibernética tiene experiencia en el sector informático, puede entender mejor todos los pasos a seguir. Sin embargo, sin el liderazgo y las competencias gestiónales que aquí son cruciales, una persona del sector TI no puede involucrar la respuesta a la crisis cibernética.

Si tienes una micro empresa, es obvio que necesitas prepararte a esa posibilidad. Puedes firmar también un acuerdo con el experto cibernético en el que confías. Las empresas pequeñas o medianas deberían nombrar a un líder para la fase de respuesta a la crisis cibernética.

Es bueno recordar que la respuesta a la crisis cibernética se puede implementar **remotamente**.

Unidad 2: Responder a la crisis cibernética

Sección 2.2: El plan de respaldo

En una mini pyme, el plan de respaldo puede variar dependiendo de la sucursal, tipo de negocio, etc.

Sin embargo, deberías considerar los siguientes pasos:

Conoce a tus proveedores

Mantén toda la información de contacto de tus proveedores (internet, nube, hosting, etc.) en un lugar seguro, desconectado. Ya que el ataque puede ser realizado desde tu red local, incluso si no estás conectado a internet, tu contraseña y tus datos confidenciales pueden ser robados.

Qué hacer:

Considera todos los posibles ataques antes que ocurran. Mantén todos los contactos no solo online, sino también en **versión impresa**.

Erasmus+

Unidad 2: Responder a la crisis cibernética

Sección 2.2: El plan de respaldo

Sigue el rastro

Si notas acciones sospechosas:

- En tu cuenta bancaria, llama el banco y bloquea todas las tarjetas de crédito;
- En tu nube empresarial, contacta con el proveedor (por teléfono o por correo).

Qué hacer:
Evita utilizar las aplicaciones/nubes que pueden estar infectados. Contacta directamente con el proveedor.

¡Desconecta el enchufe!

Algunas veces hay solo una manera de parar un ataque cibernético.

Qué hacer:
Si notas eventos sospechosos en tu ordenador/otros dispositivos o en los de tus empleados, simplemente desenchufa.

Unidad 2: Responder a la crisis cibernética

Sección 2.3: Protocolo de comunicación en caso de crisis cibernética

Pensando en la respuesta a la crisis cibernética, deberías considerar el protocolo de comunicación. Aquí, lo más importante es siempre el tiempo. Comunícate lo antes posible con las partes interesadas e infórmales sobre el problema. Deberías ser la fuente de los hechos — no los periódicos o las redes sociales.

Muestra a las partes interesadas que te preocupas por ellos, y que ya has tomado las medidas adecuadas para minimizar las consecuencias de la crisis cibernética.
Tienes que estar listo para dar este paso antes del ataque, prepara la lista de los principales interesados:

- clientes (especialmente si tienes una base de datos de los clientes)
- Socios empresariales, patrocinadores e inversores
- Tus proveedores
- vecinos / otros negocios en el edificio (a lo mejor el hacker ha hackeado también a ellos)

Erasmus+

Unidad 2: Responder a la crisis cibernética

Sección 2.3: Protocolo de comunicación en caso de crisis cibernética

Además tienes que pensar en hacer una declaración sobre tu página web/redes sociales o en otros medios de comunicación. Por supuesto, puedes delegar esta tarea a uno de tus empleados.

Es crucial actualizar tu declaración con frecuencia. Las partes interesadas y tus clientes necesitan estar seguros que te preocupes por sus datos. Recuerda que el resultado de un ataque cibernético puede ser el futuro de tu negocio.

¿Cómo hablar de crisis cibernéticas?

- ✓ Habla siempre claramente.
- ✓ Utiliza los hechos, no las opiniones.
- ✗ Evita las reacciones emotivas.
- ✓ Da respuestas claras a las preguntas.
- ✗ No acuses a nadie o no te disculpes hasta que no sepas lo que ha pasado.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unidad 3: Recuperación después de la crisis

Sección 3.1: ¿Cómo volver a la normalidad después de una crisis cibernética?

Después de una crisis cibernética, cada negocio necesita dar unos pasos para volver al funcionamiento normal.

Así es como llegamos a la tercera fase de gestión de la crisis cibernética llamada recuperación en caso de desastre.

La recuperación después de la crisis cibernética es el proceso que ayuda a las empresas a volver a las operaciones normales.

La recuperación después de la crisis cibernética incluye pasos que siguen al evento, como:

- evaluaciones (de los daños, las causas y la gestión)
- Lecciones aprendidas
- Mejoras previstas

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unidad 3: Recuperación después de la crisis

Sección 3.2: ¡Haz la evaluación!

La recuperación empieza después de la crisis cibernética. Para estar seguro que tu negocio estará “sanado” necesitas dar unos pasos radicales. Primero que todo, necesitas encontrar las deficiencia que pueden convertir el ataque en algo posible.

- Planea las reuniones de evaluación con tu equipo para hablar de los daños surgidos durante el ataque cibernético. Encuentra y entiende las causas. Si fuera necesario, pide apoyo a expertos externos.

- Evalúa tu plan de gestión cibernético. Habla de cada paso, de todas las medidas tomadas, para entender lo que salió mal.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unidad 3: Recuperación después de la crisis

Sección 3.3: Lección aprendida

Durante o después de la evaluación, crea una lista de las vulnerabilidades que hicieron el ataque cibernético más fácil. No lo tomes como algo personal. No pienses en ello como un fracaso. Lo más importante es aprender de este ataque.

Si eres el líder/ propietario del negocio, tu actitud tiene un impacto en los empleados. Si consideras el ataque como un fracaso o si acusas erróneamente a uno de tus empleados de ser el responsable, puede afectar el futuro de tu negocio.

Sólo ten en cuenta que cada movimiento y acción que tomas está influenciando no solo ese momento y este ataque cibernético, sino también tu reputación y rentabilidad futura.

Unidad 3: Recuperación después de la crisis

Sección 3.4: Planifica las mejoras

El último paso es analizar todas las deficiencias utilizando los hechos y los datos. Si descubres que hackearon tu negocio, porque uno de tus empleados descuidó su trabajo, es mejor evitar reacciones emotivas. Hay múltiples maneras de actuar en esta situación, porque cada caso es diferente.

Por cierto, puedes hacer un esfuerzo para crear objetivos a corto o largo plazo para colmar las lagunas. Cada laguna es un indicador verificado en el accidente. Cada objetivo supone la prevención de ataques similares en el futuro.

La recuperación después del ataque cibernético debe eliminar o minimizar las causas de dichos ataques. Si eso no ocurre, la lección no ha sido aprendida.

Unidad 3: Recuperación después de la crisis

Sección 3.5: Casos de estudio sobre la crisis cibernética

Puedes ser hackeado, no importa si tienes una empresa pequeña o grande. Poseer una empresa más grande no te hace más seguro o mejor preparado para enfrentar la crisis. Al menos no siempre. Échale un vistazo al caso de estudio a continuación.

Marriott International

El ataque cibernético

La conocida cadena hotelera, Marriott International, fue hackeada en enero de 2020, pero el ataque pasó desapercebido por la empresa hasta finales de febrero. Los hackers que obtuvieron las credenciales de acceso de los dos empleados de Marriott podían acceder a los datos del cliente. La empresa empezó su propia investigación.

Erasmus+

Unidad 3: Recuperación después de la crisis

Sección 3.5: Casos de estudio sobre la crisis cibernética

Respuesta

Marriott hizo una declaración según la cual los hackers podrían haber adquirido datos como nombres, fechas de nacimiento, números de teléfono, preferencias lingüísticas y cuentas de fidelización. Además, el hotel envió correos a los clientes involucrados; creó una página web dedicada y un call center para informar a los clientes. Marriott aseguró que tenía seguro, que incluía también la seguridad cibernética. Hasta ese momento, todo parecía profesional, sin embargo, al hacer la declaración la empresa no creía que sus costes totales, que estaban relacionados con este accidente, serían significativos.

Recuperación

En octubre de 2020, el organismo de control de privacidad de los datos de Reino Unido multó a la cadena de hoteles Marriott con 18.4 millones, por el incumplimiento que puede haber afectado hasta a 339 millones de clientes.

Unidad 3: Recuperación después de la crisis

Sección 3.5: Casos de estudio sobre la crisis cibernética

¿Cuál fue la lección aprendida?

Primero que todo, no fue el primer ataque cibernético que sufrió Marriott International. En 2014, los hackers atacaron el grupo de Hoteles Starwood que fue adquirido por Marriott dos años después. Como sabemos, la empresa no dio ningún paso de recuperación en aquel momento. Esa es la razón por la cual el siguiente ataque fue más fácil.

El primer ataque conocido públicamente tuvo lugar en 2018. Una vez más, el protocolo de gestión de crisis no fue implementado correctamente, por tanto, hasta aquel momento los hackers siguieron teniendo acceso a todos los sistemas afectados, incluso:

- Nombres
- Correos electrónicos
- Números de teléfono
- Números de pasaporte
- Información de llegada y de salida
- Estado VIP
- Números del programa de fidelidad

Unidad 3: Recuperación después de la crisis

Sección 3.5: Casos de estudio sobre la crisis cibernética

Esa es la razón por la cual Marriott fue multada por el organismo de control de privacidad de los datos de Reino Unido. La cadena de hoteles falló en proteger los datos personales, como requerido por la Regulación General de Protección de Datos (GDPR). Además, falló más que una vez. Los líderes responsables de la gestión de la crisis cibernética no identificaron ni analizaron los fallos profundamente.

¿Qué ayudó?

Marriott International está asegurado, incluida la seguridad cibernética. Eso ayudó a pagar las multas.

¿Qué puedes aprender de esto?

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unidad 3: Recuperación después de la crisis

Sección 3.5: Casos de estudio sobre la crisis cibernética

Lección aprendida:

- **Reconsidera tu gestión de crisis cibernética.**
- **Piensa si tienes bastante capacidad de liderazgo y gestión para implementar el plan de gestión de crisis cibernética.**
- **Si no, aprende más a través de nuestros otros cursos.**
- **Además, busca un experto de informática como apoyo.**
- **Piensa si necesitas el seguro cibernético.**

Unit 3: Recovery after the cyber crisis

Sección 3.6: Resumen

Hoy en día, la gestión de crisis cibernética es igual de importante tanto para las micro que las grandes empresas. La diferencia está en los recursos que tienes. Más pequeña es la empresa, mayores son las responsabilidades que tienes como propietario.

Recuerda que la crisis cibernética puede afectar a tu empresa, aunque no sea una típica empresa online (comercio electrónico). Cuando necesitas un portátil, un móvil, una impresora, un fax, un buzón, debes considerar la gestión de la seguridad cibernética.

Por último, ten en cuenta que la mala gestión puede intensificar la crisis o incluso crear otra más.

¡Mucha suerte!

Bibliografía y enlaces relevantes

The New Statesman > **How to tell your customers you've been hacked**

https://www.newstatesman.com/spotlight/2019/09/how-tell-your-customers-you-ve-been-hacked

Deloitte > **Cyber crisis management: Readiness, response, and recovery**

https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-cm-cyber-pov.pdf

Security Boulevard > **Marriott Data Breach 2020: 5.2 Million Guest Records Were Stolen**

https://securityboulevard.com/2020/04/marriott-data-breach-2020-5-2-million-guest-records-were-stolen/#:~:text=The%2520breach%2520was%2520identified%2520at,have%2520accessed%2520the%2520guest%2520details.

BBC News > **Marriott Hotels fined £18.4m for data breach that hit millions**

https://www.bbc.com/news/technology-54748843

Marriott International News Center > **Marriott International Notifies Guests of Property System Incident**

https://news.marriott.com/news/2020/03/31/marriott-international-notifies-guests-of-property-system-incident

Forbes > **What Businesses Are The Most Vulnerable To Cyberattacks?**

https://www.forbes.com/sites/theyec/2021/01/19/what-businesses-are-the-most-vulnerable-to-cyberattacks/?sh=1c1c8f663534

¡Gracias por tu atención!

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.