Cyber MSME

Ciberseguridad para PYMES

Mejora del plan de gestión de ciberseguridad - buenas prácticas

Creado por CTS Customized Training Solutions & CASE

Erasmus+

Índice– pulse para ir a la página correspondiente:

Puede mejorar su plan de gestion de ciber seguridad comenzando con los siguientes pasos:

1. Aplicar contraseñas seguras

Parece obvio que una contraseña segura es la primera línea para defendernos de los ataques. Cambiar las contraseñas de cuando en cuando ayuda a entorpcer el trabajo de los hackers.

Buenas prácticas para las contraseñas

Es posible que haya escuchado que la contraseña más segura contiene al menos una letra en mayúscula, al menos 1 número, y al menos un símbolo (como %, #, &). Debe contener más de 7 caracteres. Vea algunos ejemplos.

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.

Supongamos que nuestro perro se llama Rusty y que lo hemos adoptado en 2018. Así que la contraseña de nuestro portatil, de la nube y en nuestro email de trabajo es **Rusty-2018**. Fácil de recordar, ¿verdad?

Pues también es fácil de hackear.

Entonces, ¿qué hacemos?

Aprendamos a crear contraseñas seguras. Una buena contraseña, y difícil de hackear tiene que ser:

- **larga (no menos de 15 caracteres)**
- **Una mezcla de caracteres en mayúsculas y en minúsculas**
- **Que no sean substituciones habituales (por ejemplo, "h0m3" en vez de "home" es demasiado obvio)**
- **Que no sean combinaciones de teclado obvias (como "qwerty", "12345")**

Use administradores de contraseñas

Un administrador de contraseñas es un programa de ordenador, basado en la web, o un plugin que permite a los usuarios generar y gestionar sus contraseñas. Se pueden usar Keeper, LastPass, o DashLane.

Si no le gusta ninguno, puede leer más sobre varios gestores de contraseñas y sus especificaciones siguiendo este enlace:
https://en.wikipedia.org/wiki/List_of_password_managers

2. Usar frases como contraseñas en vez de palabras

Una **frase de contraseña** es una combinación de palabras y símbolos que forman una frase. Una frase no tiene por qué ser gramaticalmente correcta. Las frases de contraseña normalmente tienen más de 40 caracteres. La diferencia es que mientras las contraseñas no tienen espacios, las frases de contraseña si las tienen.

Erasmus+

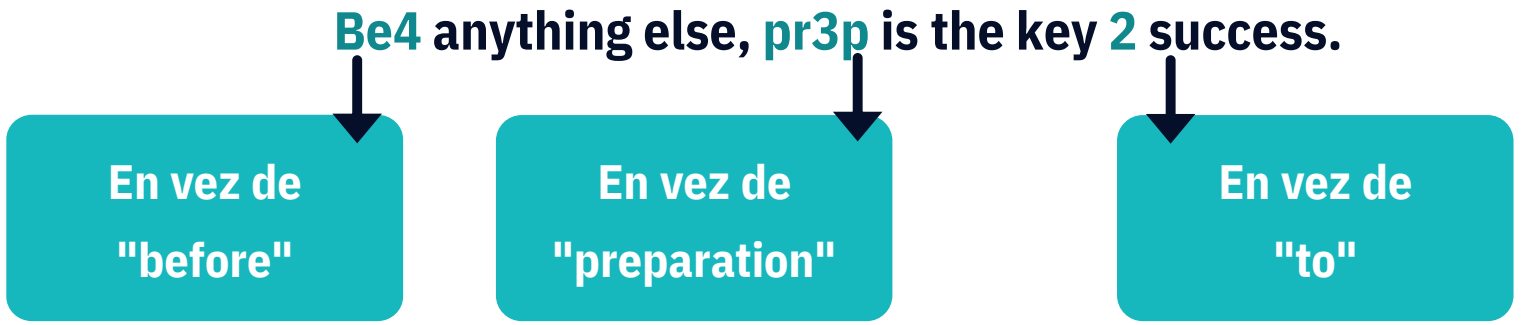
Buenas prácticas para crear frases de contraseñas

- Use una frase fácil de recordar, pero que no sea muy común.
- Use palabras no muy comunes y/o abreviadas.
- Añada espacios.
- Use mayúsculas (al principio de la frase o para palabras concretas).
- Cambie algunas letras por números.
- Añada signos de puntuación

Enlaces de relevancia: TechTarget > Frases de contraseña (https://searchsecurity.techtarget.com/definition/passphrase); John Carroll University > Contraseñas y frases de contraseña (https://password.jcu.edu/public/passphrase.php)

Erasmus+

Una frase de contraseña puede parecerse a una cita de Alexander Graham Bell:



O como palabras y números aleatorios:

Male h0rse 21, viLLag3 rAce.

Sea lo que sea que elijas, recuerda cambiar tu contraseña regularmente. No la escriba en ningún lugar donde otras personas puedan acceder a ella. Elija quien debería conocerla —
No todos los miembros del equipo deberían saber ni la contraseña ni la frase de contraseña.

Cyber MSME

3. Si es posible, usar más de un sistema de autenticación

Un pirata informático puede descifrar incluso una contraseña segura o una frase secreta. Por eso, siempre que se pueda, es bueno utilizar **la autenticación de dos factores (2FA)**. 2FA es una capa adicional de seguridad para su contraseña / frase de contraseña creada para garantizar que nadie, excepto usted, pueda acceder a su cuenta, incluso si alguien más conociera su contraseña.

¿Cómo funciona 2FA?

- Se pueden encontrar 2FA usando muchas apps y webs. En una primera fase usaremos nuestro usuario y contraseña o frase de contraseña como siempre.
- En un segundo momento, la app o web nos envía un código de verificación temporal (por ejemplo a nuestro número de móvil). Necesitaremos insertar este código en la app o web para acceder.
- Otra posibilidad 2FA son las huellas dactilares o faciales biométricas.

Erasmus+

4. Nunca escriba mensajes de texto o mande un email a nadie con su contraseña

En el caso que necesite compartir contraseñas o frases de contraseña con sus empleados, usar un gestor de contraseña tipo Keeper, LastPass, o DashLane.

5. Elija preguntas de seguridad difíciles de adivinar

Al crear cualquier cuenta es normal configurar un pregunta de seguridad si olvidamos la contraseña. La mayoría de estas preguntas son fáciles de encontrar en sus redes sociales (por ejemplo su película favorita, la fecha de su primera cita o el nombre de su primer gato, etc.).

Sea consciente de esto y elija con cuidado sus preguntas. Y aleccione a sus empleados y socios sobre este punto.

Enlaces de relevancia: Avast > Cómo crear una contraseña robusta (https://blog.avast.com/strong-password-ideas)

Erasmus+

6. Actualice regularmente todas sus apps

Asegúrese que su antivirus se actualiza regularmente. Escanee su ordenador al menos una vez a la semana. Recuerde que cualquier conexión a internet puede ser vulnerable y que usted posiblemente esté conectado varias horas diariamente.

Además, actualice también sistema operativo, navegadores, la nube, apps de comunication, etc. La vulnerabilidad más pequeña puede facilitar el acceso a los piratas para hackear su negocio.

7. Actualice regularmente sus dispositivos

Los empresarios a menudo se olvidan de actualizar los dispositivos que no son portátiles ni móviles. Sin embargo todos los negocios poseen más cosas pirateables por hackers. Un atacante puede hackear su router, impresora o máquina de fax. Asegúrese que su firmware esté actualizado en todos los dispositivos con conexión wifi — incluso el microondas y el horno de su cocina.

Erasmus+

8. Tenga cuidado cuando use wifis públicas

Las wifis públicas están disponibles en casi todos los sitios, con puntos de acceso listos para usarse en restaurantes, coffee shops, o aeropuertos. Como empresario, puede necesitar acceso a internet desde varios lugares. La pregunta es: ¿estamos seguros usando wifis públicas?

Siempre que sea posible, intente usar su proveedor habitual. Puede compartir la conexión de su móvil como hotspot o comprar un dispositivo dedicado, siempre será mucho más seguro que una wifi pública, que debido a su accesibilidad puede ser propensa a que un hacker husmee datos confidenciales

¿Qué puede protegerme a mi y a mi negocio si decido usar una WiFi pública?

La mejor opción y más accesible es unar una VPN para proteger nuestra privacidad.

Enlaces de relevancia : Kaspersky > **Seguridad en Wifis públicas** (https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi)

¿Qué es una VPN?

VPN significa **Red Privada Virtual**. Virtual significa que la red no existe realmente de una manera física, sino que está hecha por software. Privada se explica por sí mismo: es una red a la que no se puede acceder libremente en Internet. Por lo general, es mucho más seguro que una red pública porque restringe las conexiones y los piratas informáticos que se aprovechan de una red pública no pueden espiar los datos con facilidad.

¿Cómo conseguir un acceso VPN?

Puede configurar su propia VPN o usar una cualquiera de pago de los muchos proveedores de servicios existentes. Pero sea prudente. Puede encontrar VPN gratuitas en la red, pero usarlas puede ser incluso más peligroso que usar los wifi gratuitos de un aeropuerto. Todo depende de como funcionen esas VPN.

Enlaces de relevancia : Algo VPN > **Self hosted VPN solution** (https://github.com/trailofbits/algo)

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.

¿Cómo funciona una VPN?

Cuando accedemos a cualquier recurso en Internet, toda la comunicación se envía por paquetes. En resumen, un paquete es una pequeña porción de datos que pasan por distintos caminos para llegar a su destino final. Así sería la “vida" simplificada de un paquete sin usar una VPN:

Observe como sus paquetes viajan sin encriptación a través de una red wifi gratuita. Cualquier pirata con acceso a esta wifi gratuita puede interceptar y por tanto robar cualquier información confidencial que enviemos/recibamos.

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.

Ahora comparémoslo con la “vida" de un paquete con una VPN habilitada:

Como podemos ver, el paquete está encriptado hasta llegar al servidor VPN. ¿Cómo pasa esto? El cliente VPN instalado en su dispositivo encapsula el paquete original en otro encriptado. Ese paquete encriptado luego se envía a través del wifi gratuito y el proveedor de servicios de Internet al servidor VPN. Finalmente, el servidor VPN descifra el paquete original y lo envía al destino original. Comparando esto con el ejemplo anterior, incluso si los piratas informáticos se apoderan de los paquetes cifrados en la red gratuita, todavía tendrían que desencriptar el cifrado para leer sus datos.

Inconvenientes de usar una VPN

Por supuesto, como con todo, existen inconvenientes al usar una VPN. En primer lugar, la VPN que está utilizando debe ser de total confianza. Si bien es posible que alguien intente interceptar sus datos en una red pública, la VPN que está utilizando está diseñada para interceptar todos sus datos. Esto significa que las VPN configuradas con fines maliciosos son extremadamente peligrosas para su negocio.

En segundo lugar, los proveedores populares de VPN, debido a la seguridad que brindan, a menudo atraen a usuarios con malas intenciones. Es posible que se le prohíba el acceso a webs o recursos populares debido a que comparte la misma dirección IP final con alguien que la usó para un mal propósito en el pasado.

Por último, la velocidad. La capa adicional de protección generalmente limita la velocidad a la que accedemos a los recursos. Si bien esto es insignificante cuando usamos wifi gratuitas (donde la velocidad de Internet no es muy alta, para empezar), podría limitar el rendimiento de su red doméstica.

9. Cree un inventario

Hoy en día, ser dueño de una empresa requiere mucho más de usted y sus empleados que hace unos años. Necesita recordar varios nombres de aplicaciones, inicios de sesión, contraseñas, etc. ¿Qué pasa si alguien olvida sus credenciales? ¿Qué pasa si uno de sus empleados pierde su móvil? ¿Qué deberías hacer?

En primer lugar, prepare su negocio para todas las posibilidades creando un inventario. Su inventario debe incluir todos los datos sobre sus dispositivos y servicios online.

Usted o su experto en seguridad cibernética deben preparar un inventario y revisarlo periódicamente. En caso de cualquier incidencia, siempre dispondrá de todos los datos necesarios para implementar el plan de gestión de ciber crisis.

¿Cómo preparar un inventario?

Erasmus+

Ejemplo de inventario

- **Lista de dispositivos > modelo, memoria, almacenamiento, sistema operativo, IP,número de serie** > usuario habitual (nombre empleado) > fecha de entrada
- **Ajustes de configuración para especificar si el dispositivo está configurado de forma segura** > especificación, fecha de actualización> fecha de entrada
- **Conexiones de red, protecciones de red y VPN** > proveedor, ubicación, estado, configuración > fecha de entrada
- **Antivirus y otros programas de protección** > proveedor, estado, ubicación, fecha de actualización, versión de actualización > fecha de entrada

- **Lista de aplicaciones y software >** proveedor, versión de actualización > persona/ dispositivos con acceso autorizado > fecha de entrada
- **Lista de cuentas de usuarios, incluyendo inactivas, compartidas, locales, admins, etc.** > ubicación, estado> fecha de entrada
- **Backup** > estado > fecha de entrada
- **Lista de vulnerabilidades, brechas y ataques** > ubicación estado, respuesta y pasos de recuperación > fecha de entrada

Enlaces de relevancia : Verve Industrial > **¿Que es el inventario de activos OT/ICS y por qué es la base de un programa de seguridad cibernética?** (https://verveindustrial.com/resources/blog/what-is-ot-ics-asset-inventory-and-why-is-it-the-foundation-of-a-cyber-security-program/)

Erasmus+

¿Dónde guardar el inventario?

Las grandes empresas usan plataformas especiales como:

- **Otorio** (https://www.otorio.com)
- **Axonius** (https://www.axonius.com/platform)

Tienen una versión demo disponible que se puede probar de forma gratuita.

Es posible probar también una solución creada por la comunidad global de las TI:

- **Controles CIS** (https://www.cisecurity.org/controls/inventory-and-control-of-software-assets/)

Esta herramienta es gratuita y de código abierto. Se actualiza constantemente, y entre sus desarrolladores se encuentran empresas, agencias gubernamentales, instituciones y personas de cada parte del ecosistema (analistas cibernéticos, buscadores de vulnerabilidades, proveedores de soluciones, usuarios, consultores, formuladores de políticas, ejecutivos, académicos, auditores, etc.)

10. Desactive todos los servicios que no utilice

Gracias a un inventario, puede gestionar servicios, productos y aplicaciones que ya no usa que caducarán pronto o que ya caducaron. ¿Recuerda cuántas veces insertó sus datos de empresa, incluido el número de su tarjeta de crédito para activar una aplicación? Exactamente...
Por lo tanto, si no va a reactivar la cuenta, esa información seguirá disponible para un potencial pirata informático.

11. Revise las conexiones entre dispositivos

No todos los dispositivos de la empresa necesitan comunicarse entre sí o con la red. Revise todas las conexiones y decida cuáles son necesarias y cuáles no.

Si administra una enorme base de datos o transacciones financieras, tal vez sea mejor hacerlo en un ordenador concreto que no tenga conexión con otros dispositivos de la empresa.

12. Cree niveles de datos de acceso

Por otra parte, así como no todos los dispositivos necesitan comunicarse entre sí, no todos sus trabajadores necesitan tener acceso a todos los datos, cuentas y documentos. Si ya hemos creado el inventario, podemos controlar sus dispositivos y sus programas. Ahora es el momento de crear otro documento que nos ayudará a administrar la ciberseguridad: los niveles de acceso a los datos.

El nivel de acceso es un conjunto de permisos o restricciones que se proporcionan para acceder a los datos.

Si es un programador, simplemente puede codificar los niveles de acceso en la aplicación o la página web. Sin embargo, no solo los programadores deberían pensar en crear niveles de acceso. Incluso si no tiene experiencia en TI, usted también puede hacerlo.

¿Por dónde empezar?

Erasmus+

Principios de niveles de acceso de datos

Como dijimos, los niveles de acceso se basan en un conjunto de permisos o restricciones. En primer lugar, debemos categorizar todos los datos, incluidas apps y software, y luego debemos priorizarlos, por ejemplo:

categoría A	El mayor nivel de prioridad
categoría B	Alto nivel de prioridad
categoría C	Nivel medio de prioridad
categoría D	Nivel bajo de prioridad
categoría E	El menor nivel de prioridad

importancia

Erasmus+

Estos niveles son ejemplos, por supuesto. Depende de usted decidir cuántos de ellos serán necesarios. Lo más importante es saber qué empleados deben tener acceso a los datos y sobre qué base.

Por ejemplo, es posible que solo 2 personas que trabajan con datos de clientes todos los días puedan acceder a los datos confidenciales que se guardan en la base de datos de dichos clientes. En caso de crisis, se les unen otros 2 empleados. Así es como se implementa uno de los puntos del plan de gestión de crisis cibernéticas.

En realidad, solo unas pocas personas están al tanto de los datos. Piense en cómo esto facilita la gestión de crisis

— Si los datos mencionados anteriormente se comparten fuera de la empresa, será fácil localizar la fuga.

Tendremos 4 personas para controlar, así como sus dispositivos y su historial operativo. Eso es mucho más fácil que investigar a todos los empleados, socios y proveedores.

Puede crear una lista de niveles de acceso a los datos usted mismo o pedir ayuda a un experto en ciberseguridad. Elija lo que elija, recuerde informar a sus empleados sobre cual es el nivel que tienen. Fórmelos sobre lo que significan esos niveles en el trabajo diario y en la situación de cibercrisis.

Además, recuerde actualizar la lista con regularidad, especialmente cuando uno de sus empleados cambie de puesto, sea ascendido o deje la empresa. Actualizar esta lista puede ser una de las responsabilidades de las personas que responden a las crisis cibernéticas. Si gestiona un equipo más grande, puede asignar a una persona adicional a esta tarea.

Podría ser:

- Un experto en ciber seguridad
- Un consultr en ciber seguridad
- Un analista en ciber seguridad
- Un administrador de sistemas de TI.

13. No guarde todos sus datos en un sólo sitio

No queremos decir que no podamos mantener nuestros datos en una nube segura. La clave es que si algunos datos clave sobre nuestro negocio, como datos de clientes o datos financieros, se ven en una pantalla, esto le facilita a un atacante hacer una captura de pantalla en cuestión de segundos.

Estos datos también se pueden robar fácilmente haciendo una captura de pantalla con un smarphone. Así que hay que reconsiderar la política de tener smartphones en la empresa. Quizás no todos los necesiten, y quizás no en cualquier sitio.

Recuerde también que se puede hacer una captura de pantalla cuando usted o cualquier empleado esté trabajando en una cafetería, el vestíbulo de un hotel, un tren o un aeropuerto. Forme a sus empleados para que sepan que ni siquiera conectarse a través de una VPN los resguarda por completo contra la piratería de datos. Siempre necesitan protegerse.

14. Utilice protectores de pantalla TPU

Como hemos dicho, incluso un VPN no puede proteger nuestros datos en un lugar público. Por eso te recomendamos que utilices protectores de pantalla especiales fabricados con TPU (poliuretano termoplástico).

Este material es un plástico mejorado químicamente que incluye resistencia a los rayones, flexibilidad, protección contra aceite y grasa y mayor dureza. ¿Por qué creemos que necesitas esto?

Porque también se utiliza en la fabricación de protectores de pantalla con propiedades especiales. El TPU evita que el contenido de su pantalla sea visto por cualquier persona que lo mire lateralmente.

Para los demás, su pantalla será básicamente negra. No habrá forma de hacer una foto de ningún dato. Usted, por otro lado, podrá hacer su trabajo con normalidad - todo se verá correctamente.

Enlaces de relevancia : Viola Pan > **Tercera Parte: PET, TPU, o vidrio templado – todo lo que es necesario saber para elegir un protector de pantalla** (https://www.linkedin.com/pulse/part-three-pet-tpu-tempered-glass-all-you-need-know-choose-viola-vmax/)

15. Enseñe a los demás

Tenga en cuenta que la ciberseguridad no es una actividad que se haga en un paso. Es un plan a largo plazo que debe implementarse de manera progresiva y prudente. Requiere la participación de todos los empleados, aunque no necesariamente de la misma manera. Depende del plan de gestión de crisis cibernéticas de la empresa.

No olvide que las personas son el eslabón más débil de su sistema de ciberseguridad. Forme a sus empleados, infórmeles sobre cambios, actualizaciones y nuevos métodos de ingeniería social.

¿Está listo para empezar?

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.

¡Gracias por su 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.