Pérez-Llorca

Guía de buenas prácticas para aumentar la ciber-resiliencia en organizaciones

La Agencia Europea de Seguridad de las Redes y de la Información (**"ENISA"**) y el Equipo de Respuesta a Emergencias Informáticas de la Unión Europea (por sus siglas en inglés, **"CERT"**) publicaron el pasado 14 de febrero de 2022, una guía de buenas prácticas (la **"Guía"**) destinada a empresas públicas y privadas con la finalidad de garantizar un estándar mínimo de seguridad en sus redes y sistemas. En particular, la Guía establece las recomendaciones mínimas que toda empresa debería implementar de manera consistente y sistemática para mejorar su ciberseguridad y asegurar una respuesta resiliente ante un eventual ataque informático.

RECOMENDACIONES

1. **Implementar una autenticación multifactorial**[1] a través de redes privadas virtuales (VPN); portales corporativos externos o acceso a correo electrónico a través la web (por ejemplo, mediante *Outlook Web Access*). También se recomienda el despliegue de tokens resistentes al *phishing* como claves de seguridad FIDO2[2].

2. **Evitar que los usuarios reutilicen contraseñas**. Además de crear una cultura de concienciación en las organizaciones, las empresas pueden poner a disposición de sus empleados herramientas que permitan comprobar si sus credenciales han sido expuestas en brechas de seguridad. También recomienda la utilización de gestores de contraseñas corporativos que permitan:

   - El **almacenamiento** en entornos seguros
   - Su **cifrado**
   - La **identificación** de su filtración mediante la monitorización de la *dark web*

3. **Realizar actualizaciones periódicas de software.** En particular, se deberán priorizar aquellas actualizaciones y parches destinados a atajar vulnerabilidades altas y críticas. Es importante animar a los empleados a reiniciar los sistemas y establecer mecanismos que permitan comprobar si, efectivamente, los dispositivos corporativos han sido debidamente actualizados, obligando a su reinicio y actualización periódica.

4. **Controlar detalladamente los accesos de terceros a los sistemas de la empresa** mediante un registro que permita su identificación.

5. **Reforzar los entornos en la nube** antes de migrar elementos críticos a través de medidas de seguridad integrales que impidan a los atacantes saltar de un entorno a otro.

6. **Revisar la política interna de copias de seguridad y adoptar el enfoque conocido como "3-2-1"**, el cual consiste en mantener tres copias completas de los datos almacenados, dos de ellas a nivel local, pero en distintos medios y al menos una copia almacenada fuera de las instalaciones de la empresa[3].

1 La Agencia Española de Protección de Datos (**"AEPD"**) también recomienda la implementación de este patrón de diseño en su Guía de Privacidad desde el Diseño (https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf).

2 La Alianza FIDO (*Fast Identity Online*) ha sido creada por empresas tecnológicas de primer nivel y tiene como finalidad superar el uso de sistemas de autenticación tradicionales, basados en credenciales clásicas. En su lugar, FIDO2 propone métodos de autenticación basados en sistemas biométricos; empleo de factor múltiple; claves criptográficas que combinen claves almacenadas en el propio dispositivo *hardware* y claves almacenadas en el servicio online, etc.

3 El Instituto Nacional de Ciberseguridad (**"INCIBE"**), contempla esta estrategia de copias de seguridad en su Guía "Copias de seguridad una guía de aproximación para el empresario" (https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf).

7. Establecer sistemas que obliguen a **renovar las contraseñas periódicamente** e impedir la utilización de autenticación débil o autenticación obsoleta y vulnerable.

8. **Segmentar las redes y limitar el acceso de los empleados** únicamente a aquellas redes necesarias para el desempeño de sus funciones.

9. Proporcionar **formaciones periódicas** para garantizar que los administradores de sistemas conozcan la política de seguridad interna de la organización.

10. **Crear un entorno seguro en relación con el correo electrónico corporativo,** incluyendo la implementación de medidas anti-*spam*.

11. **Organizar eventos periódicos destinados a concienciar a los usuarios** sobre los ciberataques más comunes, como el *phishing*, y la forma de evitarlos[4].

12. **Proteger los activos web de la empresa de ataques de denegación de servicios** mediante el uso de redes de distribución de contenido que permitan distribuir los activos en distintos servidores.

13. **Bloquear o limitar el acceso a internet** de aquellos dispositivos que no se reinicien periódicamente.

14. **Garantizar una pronta respuesta ante incidentes** de seguridad y una comunicación fluida con el Equipo de Respuesta ante Emergencias Informática (CSIRT por sus siglas en inglés) de la empresa.

En la Guía se advierte de que las mencionadas prácticas no deben remplazar, sino complementar, aquellas recomendaciones publicadas por las autoridades nacionales, siendo responsabilidad de las propias empresas el priorizar la implementación de aquellas medidas que más se adapten a sus necesidades y modelo de negocio.

4 Precisamente, el CERT advertía en el Volumen 1 del Informe de Ciberamenazas publicado el 11 de junio de 2021, de que la principal vía de entrada de ataques *malware* es el *phishing* (https://media.cert.europa.eu/static/MEMO/2021/TLP-WHITE-CERT-EU-Threat_Landscape_Report-Volume1.pdf).

Para mas información contactar con:

Andy Ramos Gil de la Haza
Socio de Propiedad Intelectual, Industrial y Tecnología
aramos@perezllorca.com | +34 91 423 20 72

Nota realizada por:

Alicia Maddio Medina
Abogada de Propiedad Intelectual, Industrial y Tecnología
amaddio@perezllorca.com | +34 91 423 47 56