Caja de herramientas de ciberseguridad de la GCA: documento guía para las herramientas de «Copias de seguridad y recuperación»

Cuanta más información tenemos en línea, más importante resulta crear copias de seguridad, tanto en el caso de las empresas como de los particulares. Estas copias de seguridad son fundamentales para la continuidad del negocio.

Son muchas las razones por las que pueden perderse los datos. En esta presentación, vamos a centrarnos en las pérdidas de datos provocadas por un ciberataque, pero las copias de seguridad también resultan útiles para recuperarse de un error del disco duro, del robo de equipos, de errores humanos, de daños accidentales, de inundaciones, etc.

La gran dependencia que tenemos de los equipos informáticos y el mundo en línea hace que la productividad y rentabilidad de una empresa puedan verse seriamente afectadas si se pierden los datos o hay periodos de inactividad. En el caso de los particulares, la pérdida de fotografías con gran valor sentimental de un dispositivo doméstico, por ejemplo, también podría causar mucha angustia.

Piense, por ejemplo, en el impacto que tendría desde una perspectiva financiera y reputacional si su negocio:

- No pudiera realizar su actividad o usar los sistemas informáticos durante un día.
- Perdiera una propuesta clave para conseguir un contrato importante.
- No pudiera acceder a los archivos de los clientes o estos estuvieran dañados.
- Le impidieran acceder a su información a menos que pague un rescate.

Tener copias de seguridad es fundamental para poder recuperarse rápidamente y reanudar la actividad.

Ransomware
El ransomware es un tipo de malware que bloquea el acceso a un sistema, dispositivo o archivo hasta que se paga un rescate, por lo general en criptomonedas, como bitcoin, ya que son más difíciles de rastrear que las transferencias tradicionales.

Este tipo de ataque ha ido ganando popularidad y ha estado detrás de diversos ataques importantes. Algunos ejemplos de ataques de ransomware son:

- WannaCry: WannaCry aprovechó una vulnerabilidad del sistema operativo Windows en 2017. NHS, Renault y FedEx se vieron afectados.

- Petya (2016) y NotPetya (2017): Petya se extendió oculto dentro de un PDF adjunto a un correo electrónico (por ejemplo, un currículo maligno enviado a un departamento de Recursos Humanos) y evolucionó a NotPetya, que aprovechó en parte la misma vulnerabilidad que WannaCry.
- A comienzos de 2020, TravelEx, una multinacional que se dedica al intercambio de divisas, fue víctima de un ataque de ransomware que mantuvo a la organización desconectada más de dos semanas y provocó el caos entre millones de viajeros.

Aunque puede resultar tentador pagar el rescate, la recomendación más extendida es que NO se haga.

Para protegerse del ransomware:

- **Asegúrese de que todos los sistemas estén actualizados:** mantener una buena higiene, instalar parches, realizar actualizaciones automáticas y utilizar un software antivirus en tiempo real le ayudará a evitar este tipo de ataque.
- **Evite los mensajes de phishing o spam:** para ello, habilite los filtros adecuados e instruya a los usuarios para que no hagan clic en enlaces ni abran archivos adjuntos de fuentes que no sean de confianza.
- **Realice copias de seguridad periódicas en sitios externos:** de este modo, podrá recuperarse más fácilmente si se convierte en víctima de un ataque de ransomware (también de malware o si los datos se pierden o dañan por otro motivo).

Existen diferentes maneras de hacer copias de seguridad:

- **Copias de seguridad sin conexión:** son almacenes de datos locales y sin conexión, como un disco duro externo, una unidad USB, una tarjeta de memoria, etc. Estos dispositivos deben desconectarse y guardarse en un lugar ajeno al dispositivo.
- **Copias de seguridad en línea:** al igual que las copias de seguridad en la nube, los datos se guardan fuera de las instalaciones en servidores seguros que están *en la nube*.

Las copias de seguridad en línea se pueden configurar automáticamente para que guarden los datos a intervalos regulares, lo que, en muchos casos, puede ayudar a recuperar la información (en caso de robo o inundación, por ejemplo). Hay que tener cuidado y recibir un asesoramiento adecuado al recuperar los datos tras un ciberataque o un ataque de ransomware para evitar que la copia de seguridad también se vea afectada. Es conveniente adoptar una directiva que incluya copias de seguridad tanto en línea como sin conexión.

Piense en el impacto que tendría perder los datos y elabore una política de copias de seguridad que tenga esto en cuenta. Para proteger la información confidencial, debería utilizarse el cifrado de datos.

- Implemente un enfoque (política) prudente en relación con las copias de seguridad de los datos tras categorizar los diferentes tipos de datos que posee.

- Tenga en cuenta los datos importantes y confidenciales: ¿con qué regularidad deben realizarse copias de seguridad y cómo o dónde deben almacenarse?

Utilice las herramientas de «Copias de seguridad y recuperación» para configurar copias de seguridad en todos los sistemas. Utilice una unidad o dispositivo externo para realizar copias de seguridad sin conexión.

https://gcatoolkit.org/es/pequenas-empresas/copias-de-seguridad-y-recuperacion/