EL ESPIONAJE Y LA FUGA DE INFORMACIÓN

UNA FUGA DE INFORMACIÓN SUELE OCURRIR EN VARIOS ESCENARIOS INTERNOS Y EXTERNOS, INTENCIONALES O NO, Y QUE PUEDEN SER CONSECUENCIA DE PROTOCOLOS DE SEGURIDAD DÉBILES, LA NEGLIGENCIA O SIMPLEMENTE LA MALA SUERTE. VEAMOS ALGUNOS

¿CUÁLES SON LAS CONSECUENCIAS DE UNA FUGA DE INFORMACIÓN?

- **Problemas legales:** cuando se produce una fuga de información, las empresas suelen enfrentarse a sanciones, multas o juicios por el incumplimiento de leyes y normativas que buscan proteger la privacidad de los clientes.
- **Pérdidas financieras:** las empresas pueden verse obligadas a indemnizar económicamente a clientes afectados, si se trata del caso de robo de información de sus clientes, o podrían perder su competitividad, si se fugó información asociada al core del negocio.
- **Suspensión de las operaciones:** este caso puede darse cuando información sensible sobre el funcionamiento del negocio se ve comprometida, y se produce un segundo ataque una vez que los cibercriminales saben cómo interrumpir procesos o dar de baja servicios que son clave para la operatividad de la empresa.
- **Pérdida de credibilidad:** esta es una de las consecuencias más difíciles de reparar, ya que cuando una empresa es víctima de este tipo de incidentes, queda ante sus clientes como una organización descuidada en la que no se puede confiar para brindar información sensible como datos médicos o financieros.

MÉTODOS DE FUGA DE INFORMACIÓN

- Un cibercriminal que ataca los sistemas de una organización y extrae la información.
- Una persona con acceso a las instalaciones de la organización
- Comportamiento negligente de los empleados.
- Uso inapropiado de la información.
- Empleados malintencionados o ex empleados.
- Uso de aplicaciones de comunicación y transferencia de archivos que no son controladas como: Whatsapp, Dropbox o Google Drive.
- Si se produce la infección del sistema por un malware diseñado para el robo de información, como el muy utilizado Ransomware, los troyanos, keyloggers y spyware.

CONSEJOS PARA EVITAR LA FUGA DE INFORMACIÓN

Conocer el valor de la propia información.
Realizar un análisis de riesgos y un estudio de evaluación de activos para poder determinar un plan de acción adecuado que permita evitar posibles filtraciones.

Concientizar y disuadir.
Diseñar una estrategia de concientización que incluya la responsabilidad en el manejo de la información.

Incluir herramientas tecnológicas.
En ámbitos corporativos, contar de ser posible con una solución técnica de protección, por medio de hardware, software, o combinación de ambos, tanto a nivel de redes como de equipos (servidores y estaciones de trabajo).

Seguir los estándares.
Alinearse con estándares internacionales de gestión de la seguridad permite disminuir el riesgo de que puedan ocurrir incidentes, así como también de que el negocio se vea afectado por un determinado evento de filtración.

Seguir procesos de eliminación segura de datos.
Es fundamental que los datos que se desean eliminar sean efectivamente eliminados, y los medios de almacenamiento adecuadamente tratados antes de ser reutilizados.

CSIRT
EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

E-Mail: info@cert.pa
Phone: +507 520-2378
Web: https://cert.pa
Twitter: @CSIRTPanama