

LA PROTECCIÓN DE LA INFORMACIÓN EN LA ÉPOCA DEL PHISHING II

NOTI 340 – Septiembre de 2023

Medidas básicas para implementar:

- Actualización de infraestructura informática.
- Copias de seguridad almacenadas en ubicaciones diferentes a las del origen.
- Realizar “Ethical Hacking”.
- Contar con una red protegida.



Imagen tomada de:

<https://cvnoticias.com.co/ifx-networks-avanza-en-recuperacion-tras-ciberataque/>

Como continuación de nuestro Noti N° 339 del presente mes de septiembre y ante los recientes acontecimientos en materia de ciberseguridad que han amenazado varias instituciones gubernamentales de alto nivel, tales como la rama judicial y el ministerio de salud, nos vemos en la necesidad de compartir con ustedes algunas recomendaciones que podrían minimizar la ocurrencia de este tipo de casos en sus ámbitos organizacionales.

En esta oportunidad, encontramos en el ojo del huracán a la empresa IFX Networks, que ofrece soluciones de internet dedicado, servicios en la nube, seguridad, servicios profesionales y de respaldo para aplicativos empresariales para entidades tanto públicas como privadas a nivel latinoamericano, quienes vieron comprometida la información y las aplicaciones de sus clientes ante un ataque de Ransomware a su infraestructura de servidores virtuales. Se estima que más de 70 instituciones en el país se vieron afectadas por estos ataques, dejándolos por fuera de línea, generando caos en sus procesos internos y poniendo en riesgo la información sensible de todos los usuarios de salud del país.

Si bien este es uno de los miles de casos que encontramos a diario en las noticias, es uno de gran relevancia por la importancia gubernamental y la sensibilidad de la información manejada por estas entidades. Con el fin de minimizar la posibilidad de ocurrencia en nuestras organizaciones, proponemos poner en práctica algunas medidas de protección que, si bien son técnicas o tecnológicas, no son de difícil implementación:

No importa el tamaño de la organización ni el sector al que pertenece, todos somos vulnerables a los ataques cibernéticos; acciones que van desde la protección de la infraestructura y la precaución de los usuarios, hacen más difícil el acceso a los delincuentes a nuestros sistemas de información.



Imagen tomada de:

<https://d3t4nwcgmfrp9x.cloudfront.net/uploads/buenas-practicas-seguridad-informatica-643x342.jpg>

Por: Santiago Duque Giraldo, Coordinador
Área de Conocimiento y Desarrollo
ASR S.A.S.

Medellín, Colombia
+573103923352 - 3233453366
asr@asr.com.co
<http://www.asr.com.co/>

- **Tener siempre actualizados todos los elementos de nuestra infraestructura tecnológica**, bien sea hardware como software a sus últimas versiones. Las actualizaciones tienen como propósito mejorar el desempeño de los sistemas y adicionalmente, cerrar brechas de seguridad descubiertas por los fabricantes y desarrolladores.

- **Realizar las copias de seguridad de nuestra información con regularidad y su guardado debe estar en ubicaciones diferentes** de la infraestructura en la cual se producen (diferentes servidores físicos, enviarlos a la nube). Una buena práctica será realizar pruebas frente a virus y malware sobre la copia que se realiza antes de enviarla a su nuevo repositorio.

- **Realizar periódicamente pruebas de "Ethical Hacking" sobre la infraestructura** que le permitan a la empresa conocer el estado de protección, la integridad de sus sistemas y poder contar con un plan de mejora frente a los riesgos identificados.

- **Contar con una red protegida** mediante buenos antivirus, firewall, VPN y demás elementos que permitan tener barreras perimetrales de seguridad de la información, y no dejar elementos por fuera de dichas protecciones.

Todas estas recomendaciones pueden ser sencillas de implementar pero su aplicación y su alcance es muy poderoso para enfrentar los riesgos que las organizaciones delictivas del mundo informático nos plantean en el día a día.

Esperamos que ya estén implementando las mejores prácticas en materia de seguridad informática y en caso de tener inquietudes sobre el estado de su propia infraestructura, en el equipo de ASR Consultores estaremos a su disposición para asesorarlos y alcanzar esos niveles que los protejan de estas amenazas.

Esperamos que ya estén implementando las mejores prácticas en materia de seguridad informática y en caso de tener inquietudes sobre el estado de su propia infraestructura, en el equipo de ASR Consultores estaremos a su disposición para asesorarlos y alcanzar esos niveles que los protejan de estas amenazas.

asr@asr.com.co