educación IT
CODE YOUR FUTURE

Introducción a la Ciberseguridad

Módulo 1

Conceptos clave de la Seguridad

Conceptos clave de la Seguridad

"Habitualmente sucede que la Seguridad está vista como un gasto y no como una inversión". Es una típica frase que se escucha decir a los profesionales del área, al tener que enfrentarse con los dueños o responsables de organizaciones que no quieren invertir en sistemas o medidas de seguridad que permitan proteger los activos de su organización. Inconscientemente, como estas personas tienen su preocupación puesta en las tareas que desarrollan sus empresas, ven a los sistemas y la información que manejan como simples herramientas que permiten llevar adelante su negocio. Esto es un error grave, que lamentablemente suele ponerse en evidencia, cuando por alguna razón, sus sistemas o la información allí almacenada es comprometida, e imposibilita que su actividad se desarrolle con normalidad. Solo en ese momento pueden notar que efectivamente, la protección de los activos informáticos es de suma importancia y es motor para poder desarrollar su actividad.

Por eso, al trabajar en seguridad de la información, debe conocer obligadamente cuáles son las amenazas que pueden afectar o comprometer la información de la organización, sistemas, red, etc.

Entonces, empecemos por definir conceptos:

- **Amenaza:** peligro potencial asociado a la explotación de una vulnerabilidad para usarla contra la compañía o el individuo. La entidad que aprovecha una vulnerabilidad se denomina *agente de amenaza* (*threat agent*).
- **Vulnerabilidad:** debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información, al permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma. Puede tener distintos orígenes, como fallos de diseño, errores de configuración, o carencias de procedimientos.
- **Riesgo:** es la probabilidad e impacto de que una amenaza explote una vulnerabilidad. El riesgo vincula lo siguiente: la vulnerabilidad, la amenaza y la probabilidad de explotación con el impacto resultante.
- **Contramedida:** medida para eliminar una vulnerabilidad, o reducir la probabilidad de que un agente de amenaza explote una vulnerabilidad. Suelen utilizarse como sinónimos: *Control* (*control*), *salvaguarda* (*safeguard*).

Ejemplo:

Si una organización no actualiza su *antimalware*, esto es una **vulnerabilidad**. Es vulnerable a ataques de *malware*. La **amenaza** es que un *malware* se introduzca en el entorno y genere daños. El **riesgo** es la probabilidad de que un *malware* se introduzca en el entorno y los potenciales daños. Si el *malware* se introduce en la organización y genera daños, entonces, la vulnerabilidad ha sido explotada y la organización está expuesta a pérdidas.

La **contramedida**: mantener actualizado el *antimalware*.

Ataques más comunes en la actualidad

Ataques más comunes en la actualidad

Además de conocer cómo funciona una organización, qué sistemas utiliza y cómo tiene montada su infraestructura, también es importante considerar cuáles son los ataques que dicha organización podría sufrir.

Si bien existen ataques comunes tanto a personas como empresas que utilizan tecnología, internet y manejen datos, **cada industria tiene sus propios riesgos inherentes a las actividades que realiza**.

Este es el motivo por el que se hace tanto énfasis en conocer la operatoria de una organización y **no repetir estrategias que funcionaron en una empresa pero que aplicada a otra puede no funcionar**.

¿Qué tipos de ataques podríamos sufrir como particular o como empresa?

1. **Infecciones por programas maliciosos**, en especial el *Ransomware*. Este es un tipo de *malware* que encripta todos los archivos de un dispositivo y solicita un pago a cambio de devolverlos a su formato original.

   Últimamente ha tenido mucho auge debido a su facilidad de propagación y a que muchas veces tanto personas como organizaciones no tienen un buen *backup* para recuperar los archivos comprometidos, obligándose a pagar el rescate de los archivos, o perderlos.

2. **Ataques de Ingeniería Social**, en especial el *Phishing*. Este es un engaño que consiste en que el atacante envía un mensaje a la víctima en búsqueda de que ésta realice una acción determinada (por ejemplo, abra un archivo adjunto infectado) o que brinde información confidencial, como podrían ser un usuario y una clave de alguna plataforma.

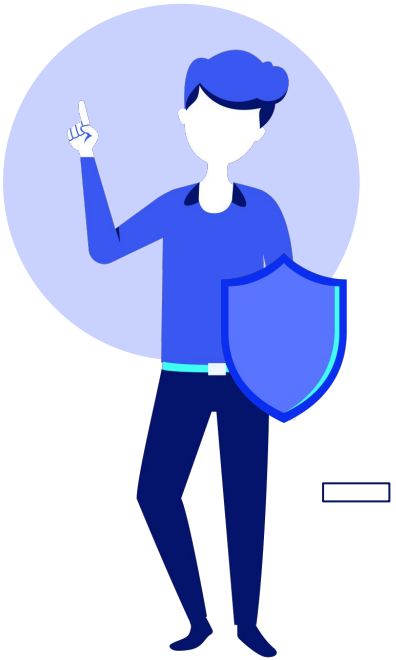
3. **Secuestro de cuentas de usuario**: con la explosión de las redes sociales y de las plataformas online, todas las personas y empresas tienen cuentas en la nube, gestionadas a veces, de forma incorrecta. Si se roban las credenciales, se perderá el acceso a estos servicios y el atacante podría solicitar dinero, a cambio de devolverlo.

4. **Denegación de servicio**: un tipo de ataque en el que se genera un gran volumen de tráfico contra un equipo víctima con el objetivo de saturar su capacidad de trabajo y buscar que falle y así deje de responder. La versión común de este ataque es de un equipo contra otro; mientras que existe otra versión, cuyo nombre es *DDoS*: en ella, muchos equipos envían tráfico contra uno para poder derribarlo.

5. **Filtraciones de Datos**: es otro tipo de ataque muy en boga en estos momentos, que implica que se exponga en Internet información confidencial o sensible de una empresa, organismo o particular. Puede suceder por varios motivos, entre ellos, un empleado descontento, un sistema mal configurado el cual es vulnerable, un servidor expuesto en Internet sin ninguna medida de seguridad para protegerlo, etc.

Podríamos mencionar muchos más, pero lo importante es reconocer que por el simple hecho de estar conectados a Internet, aumenta exponencialmente la probabilidad de sufrir algún evento negativo. Considerar que por ser un desconocido o porque una empresa es chica y nadie la conoce no sufrirá ataques, es un error.

Las personas suelen minimizar el hecho de que pueden ser víctimas porque nunca han experimentado un ataque, pero la realidad indica que cada vez es más fácil llevarlos a cabo, contra cualquier blanco y en cualquier lugar. De ahí la necesidad de estar preparados para reducir el impacto que pueden llegar a generar los riesgos en caso de materializarse.



Ingeniería Social

Ingeniería Social

Quienes hayan visto la película *9 Reinas* recordarán que el personaje de Ricardo Darín tenía un trabajo muy especial: es un estafador que utiliza toda artimaña posible para chantajear a las personas. Con el advenimiento y uso masivo de Internet a principios de la década del 2000 en Argentina y el mundo, muchas de estas técnicas delictivas que se muestran en la película, se volcaron a la red, sobre todo cuando se empezaron a realizar transacciones con dinero, compra-venta de productos y servicios, etc. Fue allí cuando los ciberdelincuentes vieron una nueva y atractiva oportunidad para cometer ilícitos, que significaba no poner en riesgo su integridad física, al menos en un primer momento.

En el ámbito de la informática, denominamos ***Ingeniería Social*** al arte de **manipular o engañar a las personas, para que brinden información confidencial, o realicen una determinada acción.** Es el famoso y conocido *Cuento del tío,* pero en el mundo digital. Se vale de muchas y variadas técnicas de recopilación de datos, que después son utilizados para cometer estafas.

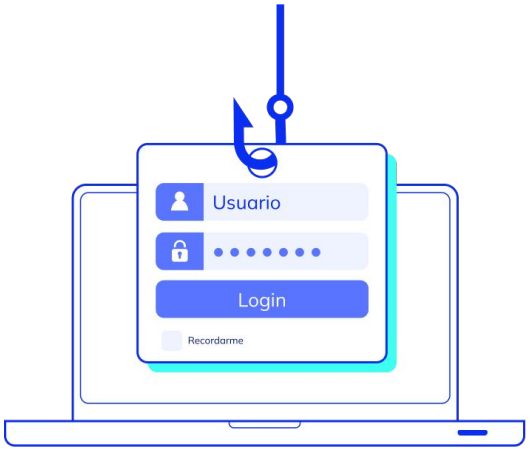
En la actualidad, muchas organizaciones son víctimas de ataques diseñados por bandas de ciberdelincuentes que buscan obtener un rédito económico por llevar a cabo este tipo de acciones. Para lograr ese objetivo, los delincuentes utilizan ingeniosas estrategias. **Una de las más usadas es atacar al eslabón más débil de toda organización: el usuario**.

Esto es así, porque las personas no conocen en profundidad las tecnologías que utilizan, desconocen los riesgos asociadas a estas, no disponen de herramientas para protegerse y, en la gran mayoría de los casos, porque no están capacitadas en materia de ciberseguridad.

Esta combinación de factores hace el escenario perfecto para que un atacante desee vulnerar a un usuario, hacerse de su información confidencial y luego perpetrar algún tipo de delito informático contra el mismo o contra la empresa.

Phishing

Sin lugar a dudas, la técnica más implementada por los ciberdelincuentes en la actualidad, es el ***Phishing***. En esta técnica, se crean **fraudulentos mensajes** que pueden enviarse por SMS, email o WhatsApp **con logos y formato idéntico a una empresa reconocida** (bancos, financieras, servicios tipo Netflix, Mercado Libre, etc.) en donde se busca manipular al usuario con alguna excusa, como las que enumeramos en la siguiente *slide*.



Algunas excusas para manipular al usuario:

- La cuenta fue bloqueada, o tiene movimientos extraños.
- Se requiere actualización de datos confidenciales: usuario, clave, código de seguridad, etc.
- Promociones llamativas o exclusivas.
- Mensajes de sextorsión, entre otros.
- Corroborar datos que figuran en archivos adjuntos.

Dentro de ese mensaje, existen links que llevan a una supuesta página verdadera, pero en realidad, es un sitio web clonado, creado por el delincuente; donde el cliente, basándose en la imagen similar que tiene la página, cae en la trampa e ingresa los datos requeridos o abre el archivo adjunto del correo.

educación IT
CODE YOUR FUTURE

¡Sigamos trabajando!