En menos de 1000 palabras: Seguridad de la Información

Introducción
La seguridad de la información ya no es un requisito sólo para las grandes organizaciones como bancos, compañías de seguros, mineras, ministerios, etc.; hoy es una necesidad imperiosa para organizaciones de menor tamaño que pretenden subsistir en el tiempo.

Efectivamente, la transitividad en la cadena de suministro obliga a que cada eslabón de esta cadena cumpla, al menos, los mismos requisitos de seguridad que el eslabón precedente. De otra forma la cadena se rompe y la organización debe buscar un nuevo proveedor que si cumpla los requisitos y formar una nueva cadena.

Durante la pandemia por Covid-19 se ha materializado un aumento explosivo en la cantidad, calidad y profundidad de ciberataques en todo el mundo. Las barreras de entrada para convertirse en un ciber-delincuente son extremadamente bajas; un computador, una conexión a internet, aplicaciones libres que cualquiera puede descargar y algunos cursos online en youtube.

Hoy, la industria del cibercrimen mueve más dinero que la industria de armamentos: en 2015 el costo del cibercrimen a nivel mundial era de 3 trillones de dólares mientras que para el 2025 se estima que alcance los 10,5 trillones.

¿Qué debemos proteger?
La respuesta es simple: toda información confidencial, critica o activo de información de la organización, y cuando me refiero a organizaciones también incluyo a entidades unitarias: o sea, Ud. como persona natural.

Un activo de información puede ser una persona, un objeto, información en cualquier medio, los conocimientos que posee una persona, sistemas, suministros, etc.

Para obtener esta lista de activos a proteger es necesario construir un Inventario de Activos. Por ejemplo, en el caso de una persona natural, algunos de sus activos de información serían: las contraseñas, números de tarjetas de crédito, las llaves de la casa, del auto, de la oficina, los registros financieros y médicos, información de su entorno familiar, gustos, preferencias, etc. En resumen, todo lo que si fuera sustraído o conocido por terceros pudiera ocasionar perjuicios a la entidad.

Un ejemplo, si se tiene un sistema que se abre sólo con la huella dactilar de una persona, esa persona es en sí un activo de información, porque su ausencia imposibilita la continuidad de una actividad necesaria para la organización.

¿Cómo debemos proteger?
Lo siguiente es detallar las vulnerabilidades para cada activo, las amenazas a las que está expuesto (los eventos que aprovechan las vulnerabilidades), las consecuencias que podría tener y finalmente las medidas que podemos implementar para disminuir el riesgo de ocurrencia o mitigar el impacto si llegase a ocurrir.

La norma ISO 27.001, de seguridad de la información, identifica 3 conceptos primordiales para evaluar la seguridad de la información de un activo:

Confidencialidad, que la información sea conocida sólo por quienes están autorizados a conocerla;
Integridad, que la información esté completa, no corrupta y sin modificaciones no autorizadas; y
Disponibilidad, que la información esté disponible en el momento que sea requerida.

En el ejemplo de la huella dactilar, el concepto que no se está cumpliendo es el de Disponibilidad. El activo de información no estaba disponible cuando era requerido.

Bajo el concepto de la ISO, todos los activos de información deben ser evaluados en estos tres conceptos. Un mismo activo puede tener una combinación de vulnerabilidades.

¿De qué nos debemos proteger?
Primeramente, es necesario declarar dos tipos de amenazas:

Las intencionales, en las que deliberadamente se intenta producir un daño, y
Las no intencionales, en las que se producen acciones u omisiones que ponen en riesgo un activo de información.

Dentro de las intencionales se pueden destacar los siguientes:

Phishing	Es una técnica de ciberdelincuencia que utiliza el fraude, el engaño y el timo para manipular a sus víctimas y hacer que revelen información confidencial.
Ramsonware	Es la introducción de un malware que se ejecuta en el sistema de la víctima y que impide a esta acceder al sistema o a la información y exige un rescate en dinero para recuperar el control y el acceso.

Virus	El virus informático es un software que se instala en un dispositivo con el objetivo de ocasionar problemas en su funcionamiento. Para que un virus infecte un sistema es necesaria la intervención de un usuario (intencionada o inintencionadamente).
Troyanos	Los troyanos son programas que se instalan en un equipo y pasan desapercibidos para el usuario. Su objetivo es el de ir abriendo puertas para que otro tipo de software malicioso se instale.
Gusanos	Es uno de los malware más comunes que infectan los equipos y sistemas de una empresa, ya que no requieren de la intervención del usuario ni de la modificación de algún archivo para poder infectar un equipo. El objetivo de los gusanos es el de replicarse e infectar el mayor número de dispositivos posibles utilizando la red para ello. Son una amenaza para las redes empresariales, porque un solo equipo infectado puede hacer que la red entera se vea afectada en un espacio corto de tiempo.
Keyloggers	Se instalan a través de troyanos y se encargan de robar datos de acceso a plataformas web, sitios bancarios y similares.
Inteligencia Social	En tiempos de Facebook, Twitter, Linkedin, etc., la inteligencia social se está convirtiendo cada vez más en el centro de atención. Se refiere a la explotación selectiva de las vulnerabilidades humanas y a los ataques a nivel personal. Las empresas de todo el mundo gastan casi 75.000 millones de euros en la protección de sus infraestructuras de TI.

Para terminar, dentro de las amenazas no intencionales se incluyen todos los errores humanos posibles que inadvertidamente ponen en riesgos nuestros sistemas e información. Desde anotar nuestras credenciales en un papel, pinchar links desconocidos, hablar temas confidenciales en espacios públicos, conectar un pendrive desconocido, compartir información en redes sociales, etc.