LA CIBERSEGURIDAD

AUTOR: JAVIER CHINCHILLA MORALES

MARZO: 2021

San Marcos

Tabla de contenido

Introducción

- La Ciberseguridad es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore y signifique un riesgo.

La ciberseguridad

Contexto de seguridad de la infraestructuras de comunicación

El desarrollo explosivo de las tecnologías de la información y la comunicación ha modificado radicalmente el quehacer humano y transformado los patrones de comportamiento y las relaciones sociales. Todo esto ha dado diversos beneficios, pero también nos ofrece un aspecto negativo y es que se ha abierto la puerta a conductas antisociales y delictivas que se manifiestan de formas que hasta la actualidad no era posible imaginar. Han surgido nuevas maneras de atentar contra la privacidad y el patrimonio de las personas y las empresas, y transformar el delito tradicional en no tradicional, estos delitos informáticos han aumentado los riesgos en el ciberespacio y ponen en entredicho la seguridad informática digital, y cada día se multiplican exponencialmente.

Hasta hoy se reconocen cuatro grandes categorías de delitos como son fraudes cometidos mediante la manipulación de computadoras, las falsificaciones informáticas, las modificaciones de programas o datos computarizados, y el acceso no autorizado a servicios y sistemas informáticos. Dentro de estos podemos citar algunos delitos como violación de la privacidad, divulgación de material ilegal, sustracción de datos, virus, fraudes bancarios, espionaje informático.

Retos de ciberseguridad

Desde el punto de vista tecnológico, la aparición de aplicaciones cada vez más complejas y costosas para la protección de equipos y redes disminuye el riesgo, pero no garantiza inmunidad total. El sistema jurídico casi siempre va un paso atrás en cuanto a la creación de un marco normativo que permita sancionar a los hackers y a los piratas informáticos. Y la identificación y captura de las personas y organizaciones criminales que han hecho un negocio del robo de identidades, los fraudes virtuales y las agresiones infecciosas, conllevan dificultades inherentes y demandan especialización y gran cantidad de recursos represivos. A estas dificultades debe agregarse el hecho de que los ciberdelitos son por lo general de naturaleza “global”, es decir, ocurren en ámbitos que transcienden las competencias nacionales. También se enfatiza “la necesidad de concebir instrumentos eficaces y mecanismos eficientes, a nivel nacional e internacional, para promover la cooperación internacional entre los organismos encargados de aplicar la ley en materia de ciberdelito.” Este conjunto de elementos y circunstancias ponen en evidencia que enfrentar las amenazas informáticas no es una tarea fácil. En verdad se requiere de una cultura de la ciberseguridad, cuyos rasgos principales deben incluir: la sensibilización sobre el problema la responsabilidad, la respuesta oportuna, el respeto a los intereses legítimos, la adhesión a los valores democráticos, la estimación de los riesgos, la implementación de los instrumentos de protección, la gestión de la seguridad, y la evaluación continua.

La Ciberseguridad se produce sin duda en un momento en que el mundo vive, más que nunca, dramáticos cambios en materia de tecnología que impactan drásticamente todos los aspectos de las relaciones humanas. Esto nos presenta como una sociedad de enormes oportunidades, pero también de grandes retos. La nueva era tecnológica muestra un mundo virtual absolutamente interdependiente con el mundo real, del cual dependemos cada vez más. El ciberespacio es real y reales son también los riesgos que vienen con él. Dependemos de la Internet cada vez más, para hacer nuestras transacciones bancarias, pagar recibos, hacer compras, trabajar y gozar de ratos de ocio y eso es aprovechado por algunos para sacar ventajas ilegítimas. Unos para espiar, otros para robar. Así surge el spoofing, phishing y otros términos nuevos a los que los

ciudadanos apenas nos acostumbramos. Dineros robados, identidades robadas, violación a la privacidad, espionaje corporativo, son sólo algunos de los retos que nos presenta esta nueva era de la interconectividad.

Usualmente se acepta que el objetivo de la ciberseguridad o seguridad informática es descubrir y aclarar la naturaleza de las amenazas y proveer metodologías para mitigarlas. Por lo tanto, al hablar de su conceptualización, es indispensable definir las clases de amenazas, y las vulnerabilidades y ataques asociados a ellas. No hay que perder de vista, sin embargo que el alcance de cada uno de estos conceptos va a variar de acuerdo al contexto y a la aplicación en particular que se esté analizando.

Una amenaza es cualquier ocurrencia potencial, maliciosa o no, que pueda tener un efecto indeseable en los recursos de una organización. Una vulnerabilidad está siempre asociada a una amenaza y es básicamente cualquier característica de un sistema que permita (potencialmente) que una amenaza ocurra.

Claramente, al identificar y bloquear vulnerabilidades se logran mitigar las amenazas respectivas. Finalmente, un ataque involucra un ente malicioso que explota alguna vulnerabilidad para ejecutar la amenaza. Se puede ver un ataque como una instanciaciòn de una o varias amenazas.

Manifestación de la inseguridad digital

En este ambiente informativo, con intensidades directamente proporcionales al grado de penetración tecnológica que haya tenido el país, tenemos a un ser humano indefenso. No se trata sólo de ser objeto de observaciones no deseadas de nuestro intercambio epistolar o de nuestros contactos, apetencias y pecados, sino también por la posibilidad de ser víctimas de nuevas formas de delito y de violencia. Nuestra generación ha visto cambios descomunales en las costumbres comunicativas, pero sin duda serán las generaciones futuras las que tendrán una cuota mayor de asombro. Ya viven nuestros jóvenes inmersos en comunidades virtuales donde se intercambian todo tipo de datos e informaciones, se invitan y se alejan, se conocen y se expresan. Estas nuevas formas de comunicación, la exhibición tan evidente de ámbitos de intimidad que nuestras generaciones cuidaban tan celosamente, son el ámbito en el que ahora debemos poner a prueba nuestros esquemas de valores. Hasta ahora hemos dado una mirada a lo que tenemos a nuestro alrededor, con lo que convivimos y que apenas estamos empezando a comprender en toda su dimensión, sin embargo, el ciberespacio también se ha convertido en un objeto de regulación y de estudio científico.

Es evidente que las infovías que han sido construidas a partir del acceso al Internet ofrecen diversos problemas de seguridad, donde sin duda el más importante es su crecimiento exponencial y sin control, donde nuevos sitios y ofertas de servicios, crecen por doquier en cualquier momento.

Conclusiones de orden práctico

Existen tres tipos básicos de amenazas: revelación de información, denegación de servicio, o repudio y corrupción de la integridad de los recursos. Otras amenazas que se van a tocar explícitamente, aunque sean instancias de la última clase son el secuestro del control y la suplantación. La relativa importancia de cada uno de ellos va a depender del sistema estudiado. Por ejemplo, en un sistema de telemedicina en tiempo real, una denegación de servicios representa una amenaza mucho más grande que la revelación de información. La revelación de información se refiere a la amenaza de que un ente que no cuenta con

autorización para el acceso a ciertos recursos, logra accederlos de forma indebida. Un ejemplo es el acceso de un ladrón al número de una tarjeta de crédito ajena, pero también al acceso no autorizado de una compañía de datos personales de ciudadanos con los que no posee ninguna relación legal.

La denegación de servicio, o repudio corresponde a la amenaza "inversa": que los entes que sì cuentan con autorización de acceso a los recursos no consigan entrar (esto es, sean repudiados a la entrada). Por ejemplo, la amenaza de que los usuarios no logren navegar en el sitio web de una empresa debido a que el servicio de nombres (DNS) esté atascado por solicitudes mal formadas.

La corrupción de la integridad es intuitivamente la más "agresiva", ya que se trata del acceso directo a los recursos, y como individuos con mayor o menor grado de territorialidad, es la que despierta mayor grado de rechazo. Sin embargo, se debe recordar que las amenazas no viven en el vacío. Si el recurso indebidamente modificado es de poco valor para la organización, quizás una preparación demasiado reactiva ante esa amenaza sea contraproducente.

La amenaza de corrupción de integridad comprende muchos aspectos, más allá de la definición de daño, pérdida o inserción de información falsa. En particular se quiere resaltar dos de ellos: el secuestro de control y la supantación de identidad, ambas amenazas muy reales actualmente. Es fácil imaginarse las consecuencias de que un atacante esté controlando su máquina, que puede ser el servidor corporativo o su laptop, y que además esté utilizando sus datos para realizar transacciones.

El punto de vista de la gestión

Uno de los aspectos de mucha importancia en la gestión es coincidir en la necesidad de la ciberseguridad: Que la dirección de la empresa tenga una clara conciencia sobre el tema y que entienda que es de vital importancia para la continuidad del negocio. Adicionalmente se debe contar con un responsable del tema que sepa transladar y ejecutar esa conciencia en acciones diarias y en prácticas adecuadas, teniendo en cuenta los protocolos que deben de tener los procesos, la formación y lso recursos adecuados para poder responder de una forma eicaz y eficiente en conjunto con los elementos de prevención, detección, reacción y recuperación de los sistemas ante un problema.

El punto de vista político

La ciberseguridad se ha convertido en uno de los retos más importantes para cualquier país y la política de un país debe lograr que el país gestione el riesgo cibernético sin sacrificar la oportunidad que trae consigo la era digital, siguiendo los pasos de países más avanzados en el tema.

El punto de vista económico

Este compromiso implica que para implantar una seguridad efectiva, se debe estar dispuesto a negociar con las comunidades involucradas dentro de la organización, dado que existe una tendencia general a subestimar los costos de no implementar medidas de seguridad, lo que redunda en resistencia a pagar los costos de implantación.

El punto de vista social

Desde el punto de vista social cada vez las personas se encuentran más expuestas a los ataques de cibernautas dado que todas mantienen su información digitalizada, lo que implica que siempre los datos personales y valiosos sean transmitidos muchas veces, y el acceso a más dispositivos en más lugares alternos los expone exponencialmente.

El punto de vista jurídico

Desde éste punto de vista se requiere un puno de vista jurídico flexible y actualizado que permita perseguir delitos que cambian ede método rápido, ya que a medida que los sistemas informáticos se han vuelto más rápidos y sofisticados, los cibercriminales también han sofisticado sus métodos y son más difíciles de detectar. Un enfoque legal fragmentado, en vez de una única ley global de ciberseguridad, permite a hace frente a la versatilidad de la delincuencia informática con mayor eficiencia.

Fundamento de ciberseguridad

Disponibilidad

Significa que la información debe estar disponible para los usuarios autorizados cuando sea necesaria, para ello se deben de tener controles de seguridad y canales de comunicación que funcionen correctamente. La disponibilidad debe examinarse durante todo el ciclo de vida de un servicio, desde el DNS hasta contenido web y base de datos, así como su transporte

Integridad

Significa que los datos deben estar integros y que no sufran alteraciones ni degradación durante o después de un envío, la certeza de que los datos no han sido sujeto sa modificaciones no autorizadas, ya sean intencionales o no. Hay dos puntos durante el proceso de transmisión en los cuales la integridad podría verse comprometida: durante la carga o transmisión de datos o durante el almacenamiento del documento en la base de datos o la recopilación.

Confidencialidad

Significa que los datos solo están disponibles para las partes autorizadas, cuando la información es de éste tipo, significa que no ha sido comprometida por otras partes, y los datos confidenciales no se divulgan a personas que no los requieran o que no deberían tener acceso a ellos.

Identificación y autenticación

El sistema de autenticación basado en usuario y contraseña sigue siendo el más extendido para acceder a los distintos servicios online. Sin embargo, existen otras formas de autenticarnos en los que interviene otro elemento. Pasamos del “algo que sé”, es decir, una contraseña, una clave o un PIN, al “algo que tengo”, como, por ejemplo, un token USB o una tarjeta de coordenadas.

La autenticación doble, o verificación en dos pasos, es una capa adicional de seguridad que complementa el uso de una contraseña. Su objetivo es el de asegurarse de que el usuario no solo conoce la contraseña para acceder al servicio, sino que además es quien dice ser aportando en el proceso de logueo información, un código, por ejemplo, sobre algo que solo él posee.

La utilización de las contraseñas sirve para autentificar al usuario frente al proceso de verificación de identidad de cualquier servicio que lo requiera. De este modo, se asegura que el usuario es realmente quien dice ser y no un impostor. No obstante, no es el único mecanismo que hay para identificar a un usuario.

Seguridad física

La seguridad física de nuestros dispositivos tiene el objetivo de mantener nuestra información a salvo mediante la incorporación de una serie de medidas de protección que van más allá de instalar un antivirus.

Soluciones de seguridad

Existen distintas y variadas soluciones de seguridad tales como:

- Firewall de siguiente generación.
- Filtro de contenido
- Firewall de aplicaciones WEB, base de datos, servidor de archivos, entre otros.
- Sistema de protección contra ataques de denegación de servicio (No servicio)
- Sistema de prevención de intrusos.
- Control de acceso a red.

Conclusiones y recomendaciones

La ciberseguridad es un tema que nos afecta a todos por igual, ya sea que tengamos solamente un correo o administremos un sitio web con información sensible, basta que un eslabón de la cadena falle para que nuestra seguridad se vea compromedida por ello es importante tener en cuenta las siguientes tres recomendaciones:

- Contemplar la nueva realidad: Entre más usuarios y dispositivos estén conectados, desde cualquier sitio y con diversos contextos, los riesgos asociados a fraudes electrónicos y ciberataques serán un dolor de cabeza después del Covid-19. La poca planificación, cultura cibernética y escasa inversión en ciberseguridad, traerá consecuencias tecnológicas devastadoras.
- Crear estrategias de monitoreo y reacción: El análisis de amenazas, que incluyan inteligencia, controles y que tengan en cuenta contextos y sobre todo la flexibilidad del negocio del cibercrimen y de las nuevas realidades, serán una necesidad mayúscula para el sector.
- La ciberseguridad es la prioridad: Más que nunca, las empresas tienen que incluir en el ADN de su organización la seguridad informática, sin importar el tamaño o el nicho del mercado al que pertenezcan.

Referencias bibliográficas

- Corletti, A. (2017). *Ciberseguridad (una estrategia informático (militar).* www.darFe.es. Recuperado de https://www.slideshare.net/acorletti/libro-ciberseguridad-una-estrategia-informtico-militar?from_action=save
- Salas, A. (2015). *Los hombres que susurran a las máquinas*. Espasa Libros, S. L. U. Recuperado de https://www.planetadelibros.com/libros_contenido_extra/32/31258_1_PREFACIO_Los_hombres_que_susurran_a_las_maquinas.pdf

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica