12. CIBERSEGURIDAD

Autor: Ing. Fernando Martinez LLamosas

12.1 INTRODUCCIÓN

La **ciberseguridad** o **seguridad informática** es la disciplina que tiene como objeto el resguardo de **activos informáticos**, siendo entre estos la información sensible de una persona, institución, empresa (cuando esta información se genera, almacena o transmite mediante medios informáticos) como el activo más evidente, pero también son considerados activos a proteger en el ámbito de la ciberseguridad la infraestructura informática y los usuarios de esta.

Para esto se definen estándares, protocolos y políticas, a la vez que se diseñan y desarrollan metodologías, técnicas y herramientas para la protección de la información informatizada.

12.2 FACTOR HUMANO Y FACTOR TÉCNICO EN LA SEGURIDAD INFORMÁTICA

Existe una tendencia a abordar la ciberseguridad desde un aspecto netamente tecnológico, con énfasis en los recursos de hardware y software involucrados en los procesos de gestión de la información, es decir los componentes del **factor técnico** de la ciberseguridad, sin embargo, está estadísticamente verificado que el mayor porcentaje de vulneraciones informáticas tienen origen en aspectos relacionados con las personas involucradas en dichos procesos, es decir en el **factor humano.**

12.2.1 Seguridad física, control de acceso

Un primer aspecto para considerar es respecto al resguardo material de los componentes de hardware involucrados en los procesos informáticos ya que quien posea acceso físico al hardware tiene el camino allanado para el uso malintencionado de la información por este gestionada.

La utilización de data-centers o communication-centers que concentren físicamente los recursos de hardware más sensibles de una organización en relación a sus datos informatizados tiene un objetivo que trasciende las ventajas técnico-operativas aportando la posibilidad de tener un control riguroso de las personas que acceden al hardware físicamente.

12.2.2 Identificación de identidad de usuarios

Los sistemas informáticos deben poder determinar la identidad del usuario que pretende hacer uso de estos, y una vez hecha esta identificación aplicarse las

restricciones de acceso y manipulación que correspondan según las políticas de la organización.

Para que un usuario pueda validar su identidad ante un sistema informático existen un amplio abanico de soluciones técnicas con distintas fortalezas y debilidades, ventajas y desventajas en cada caso.

12.2.3 Métodos (token con clave pública, métodos biométricos, OTP, autenticación por doble factor)

12.2.3.1 Clave / contraseña / password / passphrase

Es el método más habitual para identificación, es un método basado en algo que el usuario ***conoce***.

Como principal **ventaja** nos encontramos con el hecho de que cualquier usuario informático ya está familiarizado con este método de identificación. Y que si se cuenta con políticas de elección de clave adecuadas estas brindan un alto grado de resistencia a ataques.

Como **desventaja** este método presenta el hecho de que esta información que el usuario conoce como método de identificación (la clave) es transferible, ya sea voluntaria o involuntariamente, con el grado de inseguridad que esto presenta.

12.2.3.2 Datos biométricos del usuario

Cuando un sistema informático utiliza alguna característica física o comportamiento/personalidad del usuario para identificarlo, algo que el usuario ***es*** (característica que debe ser universal, única y permanente) estaremos ante un sistema de identificación biométrico. Los ejemplos más habituales son la utilización de huella digital, patrón ocular de iris o retina, patrón de voz o reconocimiento facial, entre otros.

Poseen la **ventaja** que todo usuario, de por sí, cuenta con la característica que le es propia, única e intransferible para poder identificarse.

Por **la contra** las interfaces (en hardware y software) para la lectura de datos biométricos son mecanismos más complejos y costosos (lectores de huellas, de iris, retina, cámaras y software de reconocimiento facial, etc). Además, dependiendo de la complejidad del proceso de identificación, hay un historial de métodos que han sido usados para *engañar* a los sistemas de identificación, aunque estos dispositivos están en constante evolución y son cada vez más seguros y confiables. Otro punto a tener en cuenta es que en la mayoría de las legislaciones actuales los datos biométricos son considerados información sensible por lo que su almacenamiento y tratamiento

debe cumplir con regulaciones más rígidas que las requeridas por otros métodos de autenticación.

12.2.3.3 Token USB y tarjetas inteligentes

Estos mecanismos entran dentro de la categoría de aquellos basados en los que el usuario ***posee*** algo (externo a él) que lo identifica, como puede ser un dispositivo USB denominado token, o una tarjeta inteligente. Actualmente estos suelen funcionar en conjunto con una infraestructura de clave pública (PKI).

Poseen la **ventaja** de que la PKI es una solución sumamente robusta y escalable, y que los dispositivos para almacenamiento de certificados (token USB, tarjetas inteligentes) son fabricados bajo estándares técnicos que aseguran niveles de seguridad elevados.

También poseen las misma**s desventajas** que las claves según la cual el dispositivo utilizado como identificador puede ser transferido (o sustraído). Aunque la infraestructura de clave pública permite la revocación de los certificados autenticantes ante un compromiso de estos.

12.3 NOCIONES DE CRIPTOGRAFÍA

12.3.1 Ciber-amenazas

Las ciber-amenazas son aquellos eventos que involucran la infraestructura informática de una organización, a sus usuarios, a los servicios por que esta proporciona y a los datos que en ella circulan y se almacenan (ciber), que de alguna manera ponen en cierto grado de riesgo la integridad de cualquiera de estos componentes (amenaza).

Una primera clasificación posible de estas amenazas se basa en el tipo de activo que está siendo puesto en riesgo.

Por un lado, tenemos las amenazas sobre los datos privados de la organización, ya sea que estos sean sustraídos vulnerando la privacidad de datos sensibles o que sean destruídos perjudicando el activo que constituyen dichos datos para el funcionamiento de la organización o las personas que la componen.

Y por otro lado están las amenazas a la continuidad de negocio, (o funcionamiento de la organización cualquiera sea su objetivo como tal) cuando se interfiere maliciosamente sobre la infraestructura informática que posibilita dicho funcionamiento.

12.3.2 Ingeniería social

Se mencionó anteriormente que el factor humano es clave a la hora de determinar potenciales puntos vulnerables en los procesos informáticos de los datos de una organización. Esto es debido a que en mayor o menor medida los sistemas siempre tendrán interacción con personas, ya sean los usuarios o los administradores técnicos, y esto implica que aunque puede ponerse un fuerte énfasis en que el sistema informático posea un conjunto de características técnicas que estén en la vanguardia de los estándares y recomendaciones profesionales, siempre la efectividad de las mismas dependerá, en última instancia, de su correcta aplicación por parte de los factores humanos involucrados.

Por lo anterior puede deducirse que cabe la posibilidad de abordar un intento de vulneración de un sistema o infraestructura informática en este punto: el factor humano que lo utiliza o administra. Así, al explotar falencias de carácter personal / humano / psicosocial, se puede lograr hacer uso indebido, tener acceso no autorizado o comprometer servicios informáticos sin que haya habido una falencia de orden tecnológico.

Al conjunto de técnicas orientadas a vulnerar sistemas informáticos abordando el factor humano de estos se lo denomina **ingeniería social.**

Dentro de las técnicas de la ingeniería social encontraremos que se tratan de defraudación y engaños existentes en muchos otros ámbitos humanos pero orientados en este caso al fin de atentar contra activos informatizados. Ejemplos básicos de esto es el caso en que se engaña a un usuario haciéndose pasar por un soporte o servicio técnico para que proporcione sus credenciales de acceso, típicamente a través de correos electrónicos o llamadas telefónicas fraudulentas.

El abordaje organizacional respecto de la amenaza que constituye la ingeniería social es, también, más humano que técnico, implementando **estrictos y eficientes protocolos de conducta** de los usuarios y administradores de los sistemas informáticos en conjunto con una buena **educación informática** y advertencia de riesgos potenciales para con los usuarios finales de estos sistemas.

12.3.3 Suplantación o robo de identidad digital

Un activo informático muy importante, aunque no tan evidente como los datos almacenados o transmitidos por un sistema informático, es la identidad digital de los usuarios de este. Como puede observarse lo que se pone en juego aquí no es un valor fácilmente mensurable (como puede ser, por ejemplo, un número de tarjeta de crédito) sino las posibilidades de acción y daño que pueden surgir a partir de la apropiación por terceros de la identidad digital de una persona, es decir, de hacerse

con la posibilidad de presentarse a los demás con una identidad ajena y hacer uso ilegítimo de esa identidad, su reputación y significancia asociadas.

Los mecanismos para suplantar la identidad de alguien pueden ser técnicos (explotando fallas de hardware o software por el apropiador) o de ingeniería social (por ejemplo, algo tan común como apropiarse de un teléfono inteligente ajeno y hacer uso de sus redes sociales). En todo caso lo que se pone en juego aquí es un activo social subjetivo de la organización que además puede ser un factor desencadenante para comprometer otros activos a través del mecanismo asociado de ingeniería social al utilizar la identidad comprometida para acceder a información sensible.

12.3.4 Fishing

De las técnicas utilizadas en la ingeniería social cabe destacar el caso del *fishing* (del inglés: pescar) que se trata de la obtención mediante el pedido de información personal a los usuarios, particularmente información confidencial como nombres de usuario y contraseñas, datos bancarios o de tarjetas de crédito, o información personal que pueda ser utilizada para suplantar identidad, como números de documento, fechas de nacimiento, etc. A fin de concretar el engaño estos pedidos se hacen a través de cuentas de correo o de redes sociales fraudulentas que se hacen pasar por distintas entidades confiables como bancos u otras empresas e instituciones.

Estas diversas técnicas pueden utilizarse para comprometer información personal particular de los usuarios, pero también información de esos usuarios que potencialmente podría comprometer a la organización a la cual este pertenece. Es por esto que como parte de la política de seguridad informática una organización debe plantearse capacitar y educar respecto del correcto uso de los medios de comunicación informáticos, y de las potenciales amenazas.

12.4 SEGURIDAD DE DATOS ALMACENADOS

Respecto de la seguridad de los datos generados y almacenados por una organización hay dos aspectos centrales a considerar: Confidencialidad y Contingencia ante corrupción.

La confidencialidad hace referencia al hecho de que la información almacenada sólo pueda ser accedida por aquellas personas o sistemas autorizados. Esto implica una primera validación mediante mecanismos de autenticación del usuario o sistema que intenta leer los datos. El software implicado en esta autenticación de usuario puede ser el sistema operativo y/o el software de manipulación de la información, sin embargo, esta capa de autenticación no protege la información de ser leída si se logra un acceso físico a los medios de almacenamiento masivos que contienen los datos

crudos, o bien un acceso ya sea local o remoto al sistema de archivos que aloja la información evadiendo o comprometiendo el software destinado a la autenticación.

12.4.1 Cifrado de información almacenada

Para evitar el compromiso de la información en los últimos casos mencionados existen las técnicas de cifrado de la información la cual permite que mediante procedimientos algorítmicos-matemáticos la información sea indescifrable o carente de sentido semántico si no se posee un conjunto de datos adecuados (llaves criptográficas / claves / certificados, etc) que permitan el descifrado de los datos almacenados. Es así que, ante un eventual compromiso de los dispositivos de almacenamiento o los sistemas de archivos, los datos crudos podrán ser leídos pero esta no podrá ser traducida a la información sensible que representa.

12.4.2 Redundancia, versionado, (política de backup)

Sin embargo, puede comprenderse que, aunque los datos estén cifrados y no puedan ser leídos aún corren el riesgo de que se atente contra su integridad, al corromperlos o destruirlos lo cual puede no implicar un compromiso de la información sensible, pero sigue significando un potencial peligro al capital informático y un riesgo para el funcionamiento de la organización.

Para afrontar el riesgo de pérdida (intencional o no) de los datos almacenados han de establecerse técnicas mediante las cuales estos se encuentren replicados. Existe un gran abanico de posibilidades en el grado de replicación y las características y patrones de periodicidad de esta replicación. Una buena práctica será contar con una política de backup de información que deberá conjugar la probabilidad de fallas o atentados, el valor de los datos a respaldar y los costos implicados en las técnicas de respaldo.

12.4.3 Firma digital

El intercambio de documentos informáticos requiere en ciertos casos la posibilidad de asegurar la autenticidad del origen del documento (autor), la integridad del mismo (que el documento no ha sido alterado) y proveer lo que se denomina no-repudio el cual implica que quien está identificado como autor del documento no puede negar su autoría. La técnica informática que brinda estas características es la denominada firma digital.

Actualmente el sistema más ampliamente difundido de firma digital es el basado en infraestructuras de clave pública (PKI), donde existen entidades dedicadas

a proveer esta infraestructura de manera de contar con un sistema que permite la firma verificable de documentos digitales.

En Argentina existe un marco legal que regula el funcionamiento de la firma digital y los entes involucrados en proveer la infraestructura tecnológica necesaria para su implementación.

12.5 SEGURIDAD EN LAS COMUNICACIONES

Existe una linealidad entre las amenazas a la información almacenada por una organización y las amenazas a la información que se encuentra en circulación por medios de transmisión informáticos desde un punto a otro.

La información en tránsito corre riesgos análogos a aquella que se encuentra almacenada: ser accedida por personas o sistemas no autorizados, ser alterada o corrompida.

Una primera medida de protección de los datos circulantes es la restricción física de los medios de transmisión. Esta posibilidad dependerá de las características físicas propias del medio y de los puntos interconectados. Hay medios susceptibles de ser protegidos de intervención como los cables físicos (en sus distintos materiales) y otros que por su naturaleza utilizan medios que no pueden resguardarse del acceso externo (como es el caso de los radioenlaces).

Además, los puntos interconectados pueden permitir un control estricto cuando se encuentran dentro de un dominio técnico controlado por una misma organización (Redes propias) o bien pueden requerir hacer uso de redes de terceras organizaciones que permitan la interconexión y por lo tanto estar fuera del dominio de confianza técnico respecto de lo que sucede con los datos en tránsito (este es el caso de la red internet).

Es por esto que las técnicas de cifrado de la información también han de aplicarse a los datos sensibles que circulan por las redes informáticas entre sistemas distribuidos.

12.5.1 Seguridad en el acceso a servicios de red

Los datos almacenados o circulantes por las redes no son el único activo de una organización, cada vez más habitualmente estas prestan sus servicios a través de redes informáticas, los cuales también sos susceptibles de ser amenazados ya sea haciendo una explotación de fallas a nivel técnico del software o hardware que presta el servicio, o bien haciendo un uso inadecuado de los servicios que los lleven a puntos límites de sus capacidades provocando interrupciones en la provisión de atención a los requerimientos legítimos que deberían ser atendidos.

La circulación de datos en la red de una organización debe seguir los lineamientos de una política de seguridad de comunicaciones, estableciendo claramente dominios de confianza entre las distintas redes y en el acceso desde y hacia la red pública internet. El control del tráfico se hará mediante dispositivos técnicos más o menos complejos que permitirán evaluar el cumplimiento de diversas características y patrones en dicho tráfico y tomar acciones tendientes a mitigar los riesgos de seguridad anteriormente planteados.

En esta categoría de dispositivos es que encontramos los firewalls de red, los sistemas de proxy con control de contenido, IDS/IPS (*intrusion detection system / intrusion prevention system*), entre los más comunes.

12.6 POLÍTICA DE SEGURIDAD

Toda organización que haga uso de datos y servicios informatizados debe tender a formalizar en una **política de seguridad informática** los requerimientos técnicos y procedimentales para el almacenamiento, tratamiento y transmisión de los datos informatizados. Esta política dispondrá para todos los agentes involucrados en el tratamiento de los datos informáticos, tanto técnicos como usuarios, de las pautas requeridas para su protección en todo el proceso de generación y tratamiento.

Una política de seguridad debe derivar en **manuales de procedimientos** con protocolos de actuación en lo relativo a la infraestructura informática y gestión de información que los agentes deben implementar en sus tareas.

12.6.1 Auditorías

Al contar con una política de seguridad una institución puede arbitrar mecanismos de evaluación que determinen el grado de efectividad con que esta política está siendo implementada a la vez que medirá en qué grado esta política asegura los estándares de ciberseguridad requeridos por la institución y determinando eventuales brechas a cubrir en la política de ciberseguridad y sus procedimientos asociados.

Las auditorías pueden ser internas o externas, según el grado de relación del personal auditor con la institución auditada, y más o menos exhaustivas según el grado de intensidad con que se evalúen las posibles vulnerabilidades, así como ser de carácter general respecto de todo el proceso de generación, transmisión, tratamiento y almacenamiento de la información o estar enfocadas sólo a algunos de estos aspectos puntuales del subsistema informático.

La política de seguridad informática podrá incluir como parte de esta un plan de auditorías acorde.