1. Ciberseguridad en las Organizaciones

1.1. Introducción y objetivos

Con este tema introducimos el concepto de la seguridad en la información como un proceso para eliminar los riesgos asociados a la confidencialidad, integridad, autenticación, autorización, trazabilidad y disponibilidad de los recursos empresariales más valiosos: la información y los sistemas que la procesan.

Para comenzar el tema, se debe leer el caso de estudio y consultar las fuentes mencionadas en él para comprender la perspectiva de la seguridad de la información desde el punto de vista de la empresa. Es particularmente interesante buscar información de estimaciones de coste de incidentes o brechas de seguridad que han sido notorias en los medios.

Finalmente, la pregunta fundamental en la gestión es si el coste de la «no-seguridad» es mayor que el de la seguridad. Dicho de otra forma, la gestión de la seguridad tiene que fundamentarse en un análisis coste-beneficio. El problema es que la cuantificación del coste, en este caso, depende del análisis de riesgos.

Además de lo anterior, es importante conocer la protección de las amenazas físicas. En este material solo se repasan sucintamente, pero esa formación debe completarse con recursos externos.

También como aspecto general de gran relevancia, debes comprender la importancia del factor humano y entender que las técnicas de ingeniería social hacen inútiles a los medios técnicos más sofisticados. Es interesante buscar y leer casos de brechas de seguridad en las que el «eslabón más débil» fue un empleado y no un sistema pobremente configurado.

El objetivo fundamental de este tema es el de comprender la seguridad de la información como una actividad orientada a garantizar la confidencialidad, integridad, autorización, autenticación, trazabilidad y disponibilidad de los recursos valiosos de un sistema de información.

Concretamente, se espera que al finalizar el tema seas capaz de:

* Comprender cuáles son las principales dimensiones de la ciberseguridad.
* Explicar por qué la seguridad de la información debe considerarse como un proceso y no como un producto.
* Enunciar y explicar los aspectos económicos fundamentales de la seguridad de la información.
* Describir y dar ejemplo de los diferentes tipos de amenazas y controles para la seguridad física.
* Describir la importancia y el papel de la gestión de riesgos en la seguridad de la información.
* Diferenciar y dar ejemplos de las diferentes herramientas de gestión para la seguridad de la información.
* Describir la importancia del factor humano en la seguridad de la información.

1.2. Justificación y motivación de la ciberseguridad

En muchas empresas no se toma suficientemente en cuenta la seguridad de la información hasta que experimentan un ataque o una brecha de seguridad. Una vez que el evento indeseado sucede, comienza la consideración económica.

Dado que la seguridad cuesta dinero, el problema fundamental es buscar un equilibrio entre el coste de la seguridad y el impacto económico de los riesgos probables. Es importante entender la vertiente económica de la seguridad, dado que, aparentemente, los avances técnicos en seguridad (como lo fue la criptografía en su día) no mejoran la seguridad de las empresas si estas no la ponen en práctica. La criptografía, siguiendo el ejemplo, se convierte en un «arma matemática» inútil si los empleados no cumplen con la política de elección y custodia de sus claves.

En general, la seguridad implica costes incluso más allá del coste de los sistemas, *softwares* o tiempo de expertos en la configuración y diseño de estos. También tiene un coste en la forma de la resistencia de los empleados o su frustración, que en ocasiones ven las medidas de seguridad como impedimentos para realizar su trabajo más ágilmente.

En el caso del desarrollo de aplicaciones, un *software* bien protegido es más caro y requiere más tiempo de desarrollo que uno que no lo esté. Por otro lado, solo las intrusiones con un efecto importante tienen un impacto económico considerable, y rara vez han llegado históricamente a llevar al cierre de operaciones de la empresa. Esto hace que, racionalmente, muchas empresas no dediquen grandes esfuerzos a la seguridad.

Por eso, muchas tecnologías de seguridad comienzan a utilizarse cuando se dan los dos siguientes elementos:

* Son fáciles de implantar.
* Los auditores de seguridad comienzan a demandarlas.

Este es el caso, por ejemplo, de los *firewalls.* El coste de implantarlos se ha reducido considerablemente porque cada vez son más fáciles de implantar y hay más gente preparada para hacerlo. Por otro lado, el coste de no tenerlos, en el caso de una auditoría, es grande (la empresa no pasará la auditoría).

El aspecto económico de la seguridad es tan importante que es un campo de estudio en sí mismo, denominado *information security economics*. Tyler Moore y Roose Anderson han elaborado informes técnicos con los avances en esta área que merece la pena conocer.

Marco económico para la seguridad de la información

Adrian Mizzi (2011) ha elaborado un marco conceptual para responder a la pregunta que se hacen tantas empresas sobre si están invirtiendo mucho o poco en seguridad de la información. Básicamente, este marco permite estimar el retorno de la inversión, si bien la estimación de las variables es compleja por lo elusiva de la medición de las amenazas y las vulnerabilidades.

La Figura 1 resume el marco conceptual:

A diagram of a construction process

Description automatically generated

Figura 1. Viabilidad de la inversión en seguridad de la información. Fuente: adaptado de Mizzi, 2011.

La idea es que hay unos costes, tanto desde el punto de vista del ataque como del de la defensa y posterior mitigación del daño. Los atacantes se enfrentan a medidas de defensa explícitas y a la identificación de vulnerabilidades. En general, para que un atacante incurra en este coste de ruptura o CTB, los beneficios de su acción tienen que ser superiores.

El problema en este lado es doble. Por un lado, los beneficios de los ataques son difíciles de estimar *a priori,* pero, en general, si se pretende vender información confidencial, por ejemplo, para el fraude de tarjetas de crédito, el coste de explorar las vulnerabilidades es bajo en relación con el beneficio posible. Solo cuando los mecanismos de protección sean más complejos de burlar, un atacante no lo seguirá intentando.

Por otro lado, los motivos de los atacantes son subjetivos e incluyen motivaciones no económicas que los pueden llevar a incurrir en CTB mayores que los beneficios económicos esperados (que, en ocasiones, es ninguno, simplemente). La estimación del CTB puede hacerse mediante la contratación de consultoría de *penetration testing,* por la cual se contratan servicios de profesionales que intentan realizar un ataque en condiciones realistas.

Del lado de la organización, los dos costes básicos son:

* Coste de construcción de las medidas defensivas, incluyendo la configuración de *firewalls,* sistemas redundantes, sistemas de detección de intrusos, etc.
* Coste de reparación de vulnerabilidades. En una configuración simple, esto puede consistir en mantener el *software* actualizado con los últimos parches, pero, en ocasiones, esto no es suficiente y hace falta un esfuerzo proactivo en buscar vulnerabilidades potenciales según aparecen.

Cómo parchear vulnerabilidades

Una política de reparación de vulnerabilidades proactiva puede incluir la búsqueda de este tipo de herramientas para comprobar vulnerabilidades en los sistemas a medida que aparecen.

Por ejemplo, si tenemos una pyme que ha decidido utilizar el sistema de CRM de código abierto SugarCRM, podemos encontrar la vulnerabilidad que se detalla en la siguiente captura de pantalla.

A screenshot of a computer

Description automatically generated

Figura 2. Vulnerabilidad según Metasploit. Fuente: elaboración propia.

Metasploit ofrece código, muestras de ejecución y documentación completa para la reparación de la vulnerabilidad. Esta empresa mantiene una [base de datos de *exploits* en línea](http://www.metasploit.com/modules/)(descripciones de secuencias de acciones o módulos *software* que permiten aprovechar una vulnerabilidad para conseguir un comportamiento no deseado de un sistema).

Además de los anteriores, hay costes, posteriores al incidente, que incluyen el cálculo de las pérdidas derivadas y de la reconstrucción de los sistemas. Esta reconstrucción, dependiendo del efecto del incidente, puede ser tan simple como una reinstalación o reparación de un *software*. Sin embargo, en ocasiones, puede ser tan costosa como el requerir servicios profesionales para recuperar datos dañados. En otras ocasiones, y de manera discutible, la reparación se complementa con un contraataque o persecución de los intrusos.

1.3. Amenazas y riesgos de la ciberseguridad

Para investigar las amenazas y riesgos de la ciberseguridad actuales hay que abordar dos aspectos fundamentales:

* Principales agentes o actores de la amenaza.
* Principales métodos y vectores de ataque.

Se recomienda la visualización de la clase magistral *Principales riesgos de ciberseguridad,*donde se hace un resumen de los principales riesgos de ciberseguridad y las tendencias.

Principales agentes o actores de la amenaza

En el informe CCN-CERT IA-13/21, *Ciberamenazas y tendencias*, se pueden consultar los principales actores durante 2020 (Centro Criptológico Nacional, 2021):

* Actores estado (actividad de grupos).
* Ciberdelincuencia *(ransomware, phishing, malware).*
* *Hacktivismo*.
* Actores internos.

Actores estado

En los últimos años, los estados han sido actores importantes de amenazas y sus actividades han evolucionado para alinearse con los objetivos políticos de los países en los que operan. En efecto, lo que implica un cambio de tendencia en el último año, los principales objetivos fueron las instituciones públicas como ONG y entidades relacionadas con la política social o la problemática internacional. Por sectores, los objetivos prioritarios de los organismos públicos o grupos que patrocinan son los relacionados con conflictos actuales y problemas globales, como crisis de salud o desastres versión multipolar de la política internacional, entre otros. Estas son las principales áreas de interés:

* Gubernamental, defensa.
* Industria armamentística.
* Salud e industria farmacéutica.
* Centros de investigación, tecnologías de la información y las comunicaciones.
* Energía.
* Telecomunicaciones.
* Inversión financiera.
* Comercio internacional.

A screenshot of a web page

Description automatically generated

Figura 3. Campaña contra organizaciones sanitarias 2020. Fuente: Centro Criptológico Nacional, 2021.

En la Figura 3 se pueden observar cuáles han sido las principales amenazas detectadas contra organizaciones sanitarias. Además de los objetivos relacionados con las instituciones de gobierno o defensa, la pandemia ha favorecido la proliferación de campañas de grupos APT (*advanced persistent threat*o amenaza persistente avanzada) contra organizaciones involucradas en la investigación científica o la gestión sanitaria. Estas acciones tienen como objetivo sustraer propiedad intelectual, información corporativa y datos sensibles.

Ciberdelincuencia

Los ciberdelincuentes se dirigen a agencias gubernamentales, industrias e infraestructuras críticas utilizando diferentes tipos de *ransomware,* como RobbinHood, Avaddon, NetWalker, Maze, Snake Locker y Vscript.re, para extorsionar a las víctimas y obtener excelentes retornos financieros. También recurren al envío de campañas de *phishing* masivas y de correo electrónico empresarial (*business email compromise*, BEC) o al uso de *malware* personalizado. El BEC sigue siendo un mecanismo cada vez más utilizado por los ciberdelincuentes y se ha aprovechado especialmente de la situación de trabajo remoto provocada por la pandemia, lo que ha facilitado la credibilidad de las medidas de engaño utilizadas (simular problemas para manejar los requisitos del mecanismo formal, necesidad urgente para transferir o imposibilidad de identificar los contactos habituales).

Junto al *ransomware* y al BEC, además, los ciberdelincuentes han aprovechado la crisis sanitaria para lanzar campañas masivas usando *malware* en general, convirtiendo troyanos conocidos en módulos maliciosos para cubrir una mayor superficie de ataque. Actualmente, estos mecanismos se han comercializado directamente en la *dark web* como un servicio de contrato, conocido como Malware-as-a-Service (MaaS), y son explotados directamente por el crimen organizado. Esta oferta de *malware* «hecha a medida» permite a los no expertos utilizar funciones avanzadas de *malware* para todo tipo de delincuencias.

Los factores más comunes que se dan en los ataques son los siguientes:

* Falta de conocimiento de amenazas de seguridad (especialmente debido a la reutilización de credenciales o el *phishing*).
* Actualizaciones de *software* insuficientes.
* Fallos en la gestión de las copias de seguridad.

*Hacktivismo*

Los grupos *hacktivistas* siguen utilizando las mismas técnicas, tácticas y procedimientos (TTP) que se basan en el uso de herramientas *open source* para:

* Ejecutar ataques de denegación de servicio (DoS y DDoS), lo que provoca que los activos web no estén disponibles (principalmente, se dirigen a sitios web de gobiernos).
* Realizar desconfiguraciones web*(defacements),*por las que se modifica la apariencia del sitio web y se publica contenido relacionado con la operación, en ocasiones, indicando su *hashtag*.
* Realizar inyecciones SQL (SQLi) para exfiltrar información de las bases de datos y publicarla.
* *Doxxing*, que consiste en obtener la máxima información privada relacionada con un objetivo para después publicarla en fuentes públicas.

Entre los medios utilizados para difundir propaganda o información sobre movimientos *hacktivistas*, destaca el uso de Twitter. Esta plataforma permite llegar a una gran audiencia en todo el mundo, algo que es ideal tanto para mostrar movimiento como para interactuar con los seguidores. Por lo general, estos movimientos usan *hashtags* creados agregando la cadena «#Op» antes de un elemento que identifica su causa. En particular, debido a los términos de servicio de Twitter, las cuentas asociadas con movimientos *hacktivistas* a menudo se suspenden.

Actores internos

Gran parte los incidentes de ciberseguridad se comenten directa o indirectamente por empleadosrelacionados con negligencias de seguridad. Este dato revela que los actores internos involuntarios son la amenaza interna más frecuente dentro de las organizaciones. Un porcentaje menor de incidentes está relacionado con los actores internos intencionados, que representarían un 14 %. En el primer caso (*insiders*involuntarios), expertos en ciberseguridad declaran que el *phishing* representa el vector de ataque más utilizado contra los actores internos más vulnerables de una organización; últimamente, hasta un 38 % de los incidentes involuntarios provocados por actores internos se han originado a través de este vector de ataque. Todo ello sitúa al personal interno como uno de los agentes de amenaza en un futuro próximo.

Asimismo, los actores vinculados relacionados con los estados adaptan cada vez más sus TTP a los escenarios y organizaciones a los que se dirigen. Estos actores buscan constantemente a los usuarios más vulnerables de la organización para desarrollar sus campañas, muchas veces haciéndolos parte del vector de entrada a través de ataques de *phishing.* Últimamente, más del 35 % de las infracciones de datos cibernéticos totales son el resultado directo de amenazas internas.

Los actores internos pueden tener un impacto negativo grave en la organización en términos de espionaje económico, sabotaje, fraude y pérdida de recursos de la empresa. Los principales atacantes interesados en realizar este tipo de acciones serían agencias de inteligencia extranjeras o delincuentes con intereses económicos.

Es importante tener en cuenta que la negligencia o el descuido de los empleados también pueden aumentar los casos de amenazas internas dentro de la organización.

Métodos de ataque

Los principales métodos de ataque que se utilizan actualmente y que se usarán a corto y medio plazo son:

* *Ransomware*.
* *Botnets* (*Internet of things*, IoT).
* Código dañino avanzado.
* Ataques a sistemas de acceso remoto.
* Ataques web.
* Ingeniería social.
* Ataques contra la cadena de suministro.
* Ataques a sistemas ciberfísicos.

*Ransomware*

Recientemente, se ha observado cómo los grupos de ciberdelincuencia han comenzado a configurar su propio cartel independiente de operaciones de *ransomware*, es decir, coaliciones de diferentes grupos de actores específicos de *ransomware* que deciden compartir sus infraestructuras de fuga de datos con fines de extorsión. Este sistema agrega credibilidad, sofisticación e interés al compartir plataformas, conocimientos y tácticas de violación de datos. Un ejemplo de cartel es la fusión de los grupos detrás de la amenaza Maze con LockBit y RagnarLocker. Además, existe competencia entre diferentes grupos de *ransomware* por la que se compite entre sí para ver quién genera más ganancias y tiene mayor éxito en sus ataques.

Los ataques de *spear phishing* continúan usándose como un vector de intrusión inicial, así como para explotar servidores RDP *(remote desktop protocol)* expuestos y mal configurados. Sin embargo, en muchos casos, el *ransomware* es el último paso en una infección en la que los atacantes han estado dentro de la red durante días a través de otras amenazas. En este tipo de casos, el *ransomware* es el artefacto final desplegado por los actores y, a menudo, aparece en los activos que pueden ser más importantes para la organización comprometida (controladores de dominio, servidores de respaldo, etc.), que intentan causar una colisión. Este modo de operación se conoce como *human operated ransomware*, un modelo de acción según el cual los actores irrumpen en redes manipulando un código malicioso con herramientas de ataque para establecer persistencia, realizar movimientos de partes, robar información y, finalmente, encriptar la información obtenida.

Entre los *ransomwares* más usados se encuentran Maze, LockBit y RagnarLocker, Ragnarok, NetWalker, Nemty, Tycoon, SNAKE, Avaddon, Thanos, Phobos, Black Kingdom, DoppelPaymer, REvil, TinyCryptor, Ryuk, RansomExx, Conti, Egregor, Pay2Key o Zeppelin.

*Botnets* (*Internet of things*, IoT)

El IoT está cada vez más presente en nuestra vida diaria. Con la llegada del 5G, se utilizan cada vez más dispositivos interconectados como altavoces, asistentes de voz, enchufes o bombillas. Actualmente, se estima que el 33 % de los dispositivos de esta categoría han experimentado un incidente de seguridad, frente al 19 % del año 2020. Este crecimiento sin precedentes se debe, principalmente, a los siguientes factores:

* Crecimiento exponencial de los dispositivos IoT.
* Implementación insegura de dispositivos IoT a los que se puede acceder fácilmente directamente desde Internet.
* Falta de actualizaciones de seguridad para estos dispositivos, lo que los hace vulnerables.
* Falta de un enfoque seguro de estos dispositivos por parte de los propietarios.
* Los dispositivos tienen una contraseña predeterminada, conocida por el público, que en la mayoría de los casos no se reemplaza.

Frente al crecimiento en la cantidad de dispositivos, las amenazas de *botnets* de IoT nuevas y modificadas se encontraban entre las categorías de amenazas de más rápido crecimiento en la primera mitad de 2020. Entre las *botnets* más destacadas se encuentra Dark Nexus, descubierta en abril de 2020. Sus elaborados mecanismos para recopilar información sobre procesos en ejecución en contenido corrupto son sobresalientes. Asimismo, otras redes de *bots*, como Mukashi, LeetHozer, Hoaxcalls y Mozi.m, han sido un problema últimamente. Se estima que en 2025 habrá más de 30 000 millones de conexiones IoT, con una media de cuatro dispositivos de este tipo por persona. Esto presenta una superficie de ataque muy grande y asegurarla con tantos estándares diferentes hoy en día no es tarea fácil, además de convertirse en un auténtico campo minado para muchos ciberdelincuentes.

Otro tipo de *botnet* que tiene más impacto que relevancia son las que tienen como objetivo campañas para infectar con distintos tipos de *malware*, generalmente troyanos y *stealers*. Durante el primer trimestre de 2020, Spamhaus *Malware* Labs identificó un total de 2738 nuevos servidores de comando y control de *botnet*. Una media de 671 personas al mes está bajo el control directo de los ciberdelincuentes.

Código dañino avanzado

En el caso del *malware* avanzado, la sofisticación y el desarrollo de nuevas técnicas y amenazas sigue siendo una tendencia de los últimos años, la cual los atacantes pueden ver casi como un proceso de investigación, desarrollo e innovación (I+D+I). Los grupos más avanzados se benefician de cualquier evento que se realice en un país, región o continente, y más para realizar campañas dirigidas.

Estas son las tendencias en técnicas de código dañino observadas últimamente:

* En particular, los actores avanzados utilizan vulnerabilidades críticas en dispositivos revelados por organizaciones, como Citrix NetScaler y Gateway (CVE 2019-19781), Microsoft SharePoint (CVE 2020-0931) o Microsoft Exchange (CVE 2020-16875). Estas brechas sirven como punto de entrada a la organización de diferentes grupos con diferentes motivaciones. Se ha observado que estos actores prestan especial atención a este tipo de vulnerabilidad, ya que intentan aprovecharlas horas después de la publicación o existencia de un *exploit*. Los implantes que usan DNS sobre HTTPS también se han visto en 2020, como el PowerPepper, utilizado por el equipo DeathStalker. Esta tecnología está diseñada para evitar que el navegador de un usuario sepa en qué dominio se encuentra, al encapsular el tráfico DNS de solicitudes HTTPS.
* En cuanto a las amenazas persistentes avanzadas (*advanced persistent threats*, APT), algunas muestras de *malware* especialmente interesantes analizadas en 2020 corresponden a grupos como Turla o APT27. En mayo de 2020, se lanzó una muestra del *malware* Penquin del equipo de Turla en su versión de 64 bits. Este *malware*, desarrollado para sistemas GNU/Linux, permite a los atacantes tomar el control de los servidores Linux en los que se ha implementado la muestra. A pesar de que dicho *malware* fue descubierto en 2014, lo que muestra este descubrimiento de 2020 es una versión de 64 bits, por lo que el equipo detrás de su desarrollo continúa trabajando en él. Además, este informe abre la puerta a la realización de análisis para detectar posibles víctimas del *malware*. Kaspersky (2019) señala en su informe de tendencias del segundo trimestre de 2020 que hay muchos sitios web comprometidos por Penquin en su versión de 64 bits.
* Los grupos APT27 continúan desarrollando y modificando sus capacidades. Destacan los avances de ZxShell RootKit, según los cuales los atacantes introdujeron una ofuscación mínima y cambiaron la firma del controlador para que funcione a nivel del *kernel*.
* En enero de 2020 se descubrió una campaña en la que se utilizaba el *malware* LightSpy, utilizando un *exploit* para el sistema operativo iOS. Esta campaña contra los usuarios de Hong Kong muestra cuán sofisticados son algunos jugadores, ya que los *exploits* de ejecución remota para iOS son complejos y costosos. Asimismo, a principios de 2020, el equipo de Sofacy implementó una variante .NET del *malware* XTunnel y varios cargadores en el lenguaje, hecho que muestra la tendencia y crecimiento hacia .NET.
* En diciembre de 2020 se descubrió el *malware* SunBurst, lanzado a través de un ataque a la cadena de suministro a un *software* desarrollado por la empresa SolarWinds y usado por empresas como FireEye, Cisco, etc.
* Una de las otras amenazas de *malware* utilizadas por los actores avanzados es PlugX, que, a pesar de estar presente hace muchos años, sigue siendo una de las amenazas más utilizadas por muchos actores, lo que difiere entre los delincuentes es cómo se implementa PlugX para evitar la detección por parte del *software* de seguridad. Mustang Panda es uno de los actores más activos en la implementación de PlugX y Cobalt Strike, ya que utiliza técnicas de *dynamic-link library* (DLL) *side-loading.*
* Finalmente, en la parte más baja del sistema, MosaicRegressor es uno de los *frameworks* descubiertos que tenía como objetivo la interfaz de *firmware* extensible unificada o UEFI *(unified extensible firmware interface).* Los ataques identificados con este código se dirigieron a diplomáticos y miembros de ONG de África, Asia y Europa.

Ataques a sistemas de acceso remoto

Como señalamos, situaciones como la pandemia han contribuido a un aumento en el uso de varios servicios de conexión remota. En poco tiempo, un número importante de organizaciones se han visto obligadas a pasar a entornos más descentralizados que permiten el acceso remoto a infraestructuras que no están debidamente auditadas o evaluadas. Este factor, junto con la gran cantidad de informes de vulnerabilidades y exposiciones comunes (Common Vulnerabilities and Exposures*,* CVE) publicados en 2020 relacionados con vulnerabilidades en este tipo de entornos, ha resultado en un aumento significativo de la superficie de ataque expuesta a Internet.

Una simple búsqueda en portales como Shodan o ZoomEye arroja datos muy interesantes al respecto. Si comparamos el número de dispositivos involucrados en el teletrabajo a finales de 2020 frente al número de dispositivos expuestos antes de que se anunciara la pandemia, se observa que el número se ha multiplicado significativamente y ha llegado a más del 100 % para determinados productos específicos.

Por otra parte, algunas de las aplicaciones cuyo uso se ha extendido exponencialmente durante la pandemia, como Zoom, han demostrado que los actores maliciosos se centran en investigar las vulnerabilidades de los productos cuyo uso ha aumentado drásticamente en un corto período de tiempo. Como resultado, se han anunciado varias vulnerabilidades de seguridad (CVE 2020-6109, CVE 2020-6110, entre otras) que, por ejemplo, permiten comprometer la seguridad de la aplicación al enviar un mensaje especialmente diseñado, específicamente aprovechando la anomalía en la gestión de rutas de archivos que utiliza Zoom.

Debemos tener en cuenta que la mayoría de estas vulnerabilidades se solucionan aplicando laactualización anunciada por el fabricante. Esto sugiere que los ciclos de actualización y parche ocurren a un ritmo significativamente más lento a medida que los actores malintencionados desarrollan vulnerabilidades funcionales y aprovechan estas debilidades.

Ataques web

En general, las aplicaciones y tecnologías web se han convertido en una parte fundamental de Internet, adoptando diferentes usos y funciones. La situación atípica provocada por situaciones como la pandemia y la crisis económica pareja en todos los sectores y actividades se ha traducido en una mayor exposición de activos en Internet, en algunos casos, de forma precipitada y sin las medidas de seguridad adecuadas. La creciente complejidad de las aplicaciones web y sus servicios crea desafíos para protegerlas contra amenazas por una variedad de razones, desde daños financieros o de reputación hasta fraude o robo de información personal. Los servicios y aplicaciones web dependen, principalmente, de bases de datos para almacenar o atender la información que solicitan.

Los ataques de inyección SQL son un ejemplo bien conocido y están incluidos en el Top Ten de OWASP. Otro ejemplo son los ataques *cross-site scripting* (XSS), donde un actor hostil abusa de una debilidad en un formulario u otras funciones de entrada de una aplicación web, lo que lleva a acciones maliciosas, como ser redirigido a un sitio web malicioso o a una sesión de vuelo de una aplicación web.

Para mejorar la funcionalidad y productividad, el desarrollo y uso de interfaces de programación de aplicaciones (*application programming interfaces*, API) está más extendido que nunca. La llegada de estos entornos complejos impulsa la adopción de nuevos servicios de seguridad y pruebas para aplicaciones web. Se estima que alrededor del 80 % de los usuarios de API han implementado controles de seguridad sobre su tráfico entrante. En 2020 y principios de 2021 se reportaron vulnerabilidades críticas en los principales gestores de contenidos (*content management system*, CMS) utilizados en España, tal y como se muestra en la Figura 4.

A graph of a number of different colored columns

Description automatically generated with medium confidence

Figura 4. Vulnerabilidades CMS. Fuente: Centro Criptológico Nacional, 2021.

Ingeniería social

Las técnicas de ingeniería social también están cobrando especial relevancia en las campañas de *fake news*a escala global. En un momento de alarma, crisis, pandemia, novedad e incertidumbre, se han multiplicado los informes falsos, de emergencia y teorías conspirativas. Esta información y teoría no comprobada ha creado, en muchos casos, caos entre la población, y sigue siendo un problema de seguridad. Este panorama caótico puede fomentar descargas de *malware*, transmitir enlaces maliciosos e incluso facilitar ciberataques.

Otros ejemplos relevantes son las estafas que, aprovechándose de la situación de demanda de muchos usuarios por la crisis económica derivada de la crisis sanitaria, enviaban mensajes con ofertas falsas relacionadas con descuentos, beneficios en supermercados, alimentos y otros bienes. Por otro lado, la necesidad de uso de Internet de muchas empresas, incluidas las pequeñas y medianas, ha provocado que algunas marcas tengan novedades en el uso de la tecnología, que también ha sido utilizada para crear confusión y promover el fraude en línea.

Ataques contra la cadena de suministro

La ciberseguridad de la cadena de suministro es uno de los aspectos de la seguridad de la información que nos ha rodeado durante varios años. Su importancia ha sido reconocida por la industria (y, lamentablemente, lo demostramos con incidentes de la vida real con un gran impacto), pero, en la práctica, aún tiene que crecer.

La verdad es que, hoy en día, muy pocas organizaciones cuentan con procesos de seguridad de la cadena de suministro completos y efectivos. Varios factores explican esta situación: la asimetría entre clientes y proveedores en determinados procesos contractuales, una concepción débil de la seguridad de la información como un proceso transversal a la organización o que la complejidad y el volumen de recursos necesarios para asegurar un entorno empresarial se subcontrata y distribuye cada vez más.

Como si esta falta de desarrollo eficiente no fuera un problema lo suficientemente grave, el crecimiento de *shadow IT*, junto con la abundancia de herramientas en la nube en los últimos años, ha empeorado las perspectivas: ahora ya no tenemos que administrar solo la cadena de suministro, sino, además, todo lo que está fuera del alcance de los equipos de tecnología de la información y ciberseguridad.

Ataques a sistemas ciberfísicos

En relación con sistemas ciberfísicos e infraestructuras críticas, se han confirmado las tendencias observadas en 2019 y principios de 2020 que se recogieron en la edición de 2020 de este informe, sobre todo en lo relacionado con tres líneas principales:

* El abuso de vulnerabilidades asociadas al acceso remoto a través del perímetro a sistemas de control industrial, en un contexto de pandemia que ha restringido, en muchos casos, el acceso físico a los sistemas.
* La selección como objetivo de infraestructuras sanitarias y centros de investigación relacionados con la lucha contra el SARS-COV-2.
* Los ataques de *ransomware* contra infraestructuras industriales con impacto en las pocas organizaciones que tienen operaciones de producción.

1.4. Dimensiones de la ciberseguridad

Para impedir que se materialice cualquier tipo de las amenazas expuestas en los apartados anteriores, los sistemas de tecnología de la información y la comunicación (TIC) deben observar determinadas dimensiones de la ciberseguridad:

* Identificar a las personas que acceden a la información manejada por un sistema o a los recursos de este mediante un identificador y su información asociada.
* Autenticar a las personas que acceden a la información manejada por un sistema o a los recursos de este mediante credenciales.
* Autorizar controlando el acceso de los usuarios a la información manejada por un sistema o a los recursos de este.
* Proporcionar confidencialidad a la información manejada por un sistema en almacenamiento o en tránsito mediante el uso de la criptografía.
* Proporcionar integridad a la información manejada por un sistema o a los recursos de este, usando las propiedades de la firma digital avanzada.
* Mantener la disponibilidad de la información manejada por un sistema o de los recursos de este. El uso de sistemas redundantes y la gestión de activos de *backup* son fundamentales.
* Proporcionar la prueba de que una determinada transmisión o recepción ha sido realizada, sin que su receptor/transmisor pueda negar que se haya producido, usando las propiedades de la firma digital avanzada.
* Proporcionar los controles que determinen que en todo momento se podrá demostrar quién hizo qué y en qué momento. Es necesario un correcto diseño de *logging* o registro que permita una trazabilidad eficaz y eficiente.

1.5. La ciberseguridad es un proceso

La seguridad no es un producto, algo que se puede conseguir y, una vez terminado, se tiene. Por el contrario, son actividades continuas, realizadas dentro de un plan sistemático que debe evaluarse continuamente. Es decir, la seguridad de la información es un proceso. Los elementos fundamentales de ese proceso son los activos de información, por eso, la base de todo el proceso es su identificación, para después aplicar una serie de herramientas de gestión.

La gestión de la seguridad implica la identificación de activos de información y el desarrollo, documentación e implementación de políticas, normas, procedimientos y directrices que garanticen su disponibilidad, integridad y confidencialidad.

Las herramientas de gestión (como la clasificación de datos, la formación de concienciación sobre seguridad, la evaluación de riesgos y el análisis de riesgos) se utilizan para identificar las amenazas y clasificar los activos y su vulnerabilidad para establecer controles de seguridad eficaces.

Es importante diferenciar las diversas herramientas de gestión. En muchas ocasiones, se habla de «políticas» para hacer referencia a diferentes herramientas que se utilizan en diversos niveles de la gestión. Por ello, es importante hacer una clarificación terminológica.

La Figura 5 muestra una jerarquía de herramientas y sus relaciones.

A diagram of a company

Description automatically generated

Figura 5. Clasificación de las políticas por implantar. Fuente: elaboración propia.

A continuación, se describe cada una de ellas.

Política general de seguridad

Esta es una política general de alto nivel y de carácter estratégico; de ella derivan las demás. Típicamente, contiene lo siguiente:

* Una declaración de la importancia de los recursos de información en la empresa.
* Una declaración de compromiso de la dirección clara con la seguridad de la información.
* Un compromiso de delegación a las políticas derivadas de la mencionada política general.

Políticas funcionales

Estas políticas también son de alto nivel, por lo que indican qué debe hacerse, pero no detallan el cómo(esto vendrá detallado concretamente en los procedimientos). Típicamente, estas políticas afectan a un área funcional o a un determinado tipo de aplicación, como puede ser la política de uso del correo electrónico.

Estándares, directrices y procedimientos

Los estándares, directrices y procedimientos son medios para implementar las políticas. Los estándaresespecifican el uso de ciertas tecnologías o métodos de un modo uniforme. Son obligatorios y, en ocasiones, implican determinados compromisos con ciertos sistemas operativos o fabricantes de *software*.

Las directrices son similares a los estándares, pero son solo recomendaciones, no son de obligado cumplimiento. Son un mecanismo más flexible que los estándares y pueden utilizarse para determinarlos.

Los procedimientos (a veces denominados «prácticas») son descripciones detalladas de los pasos para llevar a cabo una determinada tarea por los usuarios sin dudas.

También mencionamos las líneas base *(baselines),*que son descripciones sobre cómo configurar determinados elementos de seguridad para que sean aplicados de manera uniforme en toda la organización.

Para comprender las diferencias, la Tabla 1 recoge un ejemplo concreto:

A screenshot of a computer

Description automatically generated

Tabla 1. Ejemplo de aplicación de política, estándar, procedimiento, directriz y línea base.Fuente: elaboración propia.

En el ejemplo anterior, la política es aún de un nivel general. Es frecuente tener políticas más específicas para cada tipo de aplicación que se utiliza en la organización.

La ciberseguridad implica la gestión de riesgos

Todo el mundo tiene una noción intuitiva de qué es un riesgo. Asumir un riesgo es equivalente a hacer una elección, dado que, siempre que actuamos, elegimos hacer algo en lugar de dedicar nuestro tiempo y recursos a otras cosas.

En el dominio de la seguridad de la información, los riesgos están asociados a eventos no deseados. Por ejemplo, el riesgo de tener un ataque de un cierto tipo y, como consecuencia, sufrir un robo de datos personales.

No obstante, para poder medir con una cierta fiabilidad el impacto y la posibilidad de que un evento no deseado suceda, primero hay que analizar los elementos que componen el riesgo y sus relaciones. Una vez que un riesgo ha sido analizado y evaluado, básicamente, hay dos opciones: o bien aceptarlo tal cual o bien tratar de tomar alguna medida para mitigarlo en su impacto o en su probabilidad de ocurrencia.

Hay una tercera vía para la gestión del riesgo que realmente no actúa sobre este en sí. Esta es la opción de externalizar el riesgo, es decir, de recurrir a algún tipo de seguro para que, en caso de ocurrencia del evento no deseado, haya una compensación económica.

Al conjunto de procesos de análisis, evaluación y planificación del riesgo se lo denomina «gestión de riesgos».

La ciberseguridad se articula en controles

Toda la gestión de la seguridad de la información gira en torno a la identificación de amenazas potenciales, es decir, de riesgos. Dado que el riesgo, por su naturaleza, no puede eliminarse completamente, de lo que se trata es de establecer mecanismos para reducir su probabilidad de ocurrencia (en el sentido de posibilidad) o bien para disminuir su impacto en caso de que, finalmente, la amenaza se materialice.

Se recomienda la visualización de la clase magistral *Controles de ciberseguridad*, en la que mencionamos los tipos de controles de ciberseguridad.

El control de seguridad tiene como objetivo reducir los efectos de una amenaza o vulnerabilidad de la seguridad.

El establecimiento de un control de seguridad es consecuencia de un estudio previo del impacto de determinadas vulnerabilidades o amenazas. El proceso estructurado que produce estimaciones de las pérdidas por esas vulnerabilidades es el análisis de riesgos *(risk assessment).*

Los conceptos de riesgo son la vara de medir para determinar si un control está bien implementado o no. Por ejemplo, consideremos el siguiente control mencionado en la norma ISO 27001 (s. f.):

* Objetivo de control: responsabilidades del usuario.
* Control o medida de ejemplo: uso de clave de control; se debe requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves.

El riesgo, en este caso, redundaría en la pérdida de confidencialidad (y también de integridad o disponibilidad, ya que la obtención de claves de usuarios puede permitir a un intruso entrar en los sistemas y modificarlos).

La organización debe implementar este control en la forma de políticas (filosofía general sobre las claves) y en procedimientos concretos (por ejemplo, cambios de contraseña cada seis meses y uso de un comprobador de fortaleza de las contraseñas).

Esas medidas concretas, en este caso, permiten reducir la probabilidad de que un intruso sea capaz de adivinar una clave y, en el caso de que lo consiga, que su efecto (impacto) sea temporal. No obstante, no permitirán eliminar el riesgo completamente, dado que un ataque de ingeniería social puede engañar a un usuario para dar la clave a un *software* malicioso (este sería el caso del *phishing*).

La seguridad es tanto física como lógica

El dominio de la seguridad abarca todo aquello en el entorno de los sistemas de información que puede tener un impacto en la disponibilidad, integridad y confidencialidad de la información: instalaciones, personas y documentación. Un desastre natural es un ejemplo de una amenaza física. Las medidas también son de una variedad muy diversa, como los circuitos cerrados de televigilancia. A pesar de que este dominio de la seguridad de la información puede parecer el más alejado de la profesión en sí, es importante entenderlo, ya que el *firewall* mejor configurado no podrá aguantar si alguien es capaz de acceder físicamente a la máquina que lo ejecuta.

Como ejemplo de la importancia de la seguridad, es interesante conocer algún ejemplo de instalación con medidas bien diseñadas de seguridad física. Un ejemplo es un búnker de la empresa Bahnhof, que cuenta con WikiLeaks como uno de sus clientes más famosos. Aunque el construir un centro de datos en un búnker les parece a muchos analistas más una operación de *marketing* que una necesidad física, sus características son interesantes para ilustrar el diseño conjunto físico-lógico de sistemas seguros. Entre los aspectos que sus creadores tuvieron en cuenta se encuentran la estabilidad geológica y el aislamiento frente a ataques físicos externos. No obstante, dado que uno de los mayores riesgos físicos es el acceso no autorizado, en ese aspecto, la ubicación del centro no aporta ningún beneficio adicional.

La seguridad implica a las personas

Una percepción falsa relativamente extendida es la de que el mantenimiento de los sistemas en cuanto al sistema operativo, *software* de red y aplicaciones, junto con sistemas defensivos y políticas de seguridad escritas, proporcionan un nivel adecuado de seguridad. La realidad es que el elemento más débil del sistema de seguridad es, en muchos casos, el factor humano.

La ingeniería social hace referencia a la práctica y los métodos de obtener información confidencial a través de la manipulación de usuarios legítimos.

Es importante entender que el factor humano es un elemento más del sistema de información y, como tal, las políticas y las herramientas que se implementan deben tenerlos en cuenta.