GUÍA DE TERMINOLOGÍA DE CIBERSEGURIDAD

Grupo de Trabajo de Ciberriesgos de AGERS - ISMS FORUM

agers
Asociación Española de Gerencia de Riesgos y Seguros

GUÍA DE TERMINOLOGÍA DE CIBERSEGURIDAD

AGERS- Asociación Española De Gerencia de Riesgos y Seguros

c/Príncipe de Vergara 86, 1ªesc. 2ºizq. 28006 Madrid

Depósito legal: M-15642-2017

ISBN: 978-84-697-3492-6

Agradecimientos

Esta publicación no hubiera sido posible sin el apoyo y la colaboración de grandes profesionales que colaboran y forman parte de AGERS. Gracias a D. Juan Gayá de EL CORTE INGLÉS, Dña. Elena Gil de INECO, D. Ignacio Martínez de Baroja de HISPASAT, D. Pedro Rodríguez de DEOLEO, D. José Molina de RED ELÉCTRICA ESPAÑOLA, D. Javier Bastarreche de INDRA, D. Pedro Morato y Dña. Eva Pérez de TRANSFESA, D. Alfredo Zorzo Losada de ONE ESECURITY, Álvaro González La Calle de AENA y D. Fernando Vegas de la UIVERSIDAD POLITÉCNICA DE MADRID, que forman el Grupo de Trabajo de Gerentes de Riesgos de Ciberriesgos de AGERS.

Agradecer también la colaboración de ISMS FORUM por su esfuerzo y dedicación.

Prólogo

Cuando no los sufrimos directamente, somos testigos de ciberataques masivos a nivel mundial o ciberatentados puntuales contra empresas, profesionales y particulares. La preocupación por gestionar adecuadamente la seguridad de los sistemas que, ante las vulnerabilidades aprovechadas por los piratas informáticos, justifica la implantación de medidas de prevención, control y mitigación de daños cuando se altera, modifica, destruye datos, ficheros o información confidencial.

La gestión de riesgos se enfrenta con el desafío de entender qué está pasando cuando se produce una situación crítica, como el ciberataque 'ransomware' que el 12 de mayo de 2017 produjo, según la Policía europea, más de 200.000 equipos infectados y 150 países afectados. La utilización de la terminología adecuada ayuda al discernimiento de cuanto acontece en los momentos críticos, cuando a la frustración del ciberataque se une la necesidad de emplear una misma terminología de ciberseguridad que permita saber cómo reaccionar.

La importancia del lenguaje es vital, ya que nos permite interactuar con el entorno y la sociedad de manera sistematizada y comprensible mediante un lenguaje que posibilita y potencia la comunicación en la prevención, control y tratamiento de los ciberriesgos.

La Guía de terminología de Ciberseguridad elaborada por el Grupo de Trabajo de Ciberriesgos de AGERS y ISMS FORUM, es una aportación para la mejora del empleo de los términos de este nuevo lenguaje, para fomentar un estilo comprensible sencillo, claro, conciso y directo de comunicación, que permita optimizar la política y procedimientos de gestión de estos riesgos.

Gonzalo Iturmendi Morales

Secretario General de AGERS.

Guía de terminología de Ciberseguridad

En los diferentes barómetros que miden los principales riesgos que preocupan a las empresas van ganando posiciones los riesgos relacionados con los incidentes cibernéticos.

Otros riesgos que preocupan de forma importante a las empresas, como puede ser la interrupción del negocio o la pérdida de reputación, están en ocasiones provocados por incidentes cibernéticos.

Esta preocupación parece lógica, ya que por un lado las empresas dependen cada vez más de las tecnologías de la información y de las comunicaciones y por otro la información es un activo cada vez más estratégico y de mayor valor.

Hay que ser conscientes, como sucede en muchos otros riesgos, que es posible minimizar de forma importante tanto el impacto como la frecuencia. Pero en la práctica suele ser imposible eliminar completamente el riesgo. Y a diferencia de riesgos más tradicionales, como el incendio, el riesgo cibernético está en constante evolución: continuamente aparecen nuevas fuentes de riesgo.

Uno de los principales problemas para conocer a que nos enfrentamos dentro de este ámbito es el lenguaje. La tecnología puede ser fácil de usar, pero muy compleja de comprender. Existe una barrera de comunicación - no exclusiva del mundo informático – entre el experto y el no experto. No es necesario ni eficiente que todos debamos tener el conocimiento de expertos para tomar decisiones relacionadas con el mundo de las tecnologías de la información y de las comunicaciones, pero si debemos compartir un lenguaje básico que nos permita entendernos de forma eficaz.

Este es el objetivo de este documento. Disponer de una guía/diccionario básico que permita conocer a personas no expertas a que riesgos nos enfrentamos y que medidas contamos para prevenirlos.

Somos conscientes de que un diccionario no es un documento que se lea. Es un documento que se consulta cuando se tienen una duda concreta. Por eso no hemos dado a este documento un formato estricto de diccionario. Porque nuestra intención es que este documento se lea, como se puede leer un libro.

Para esto hemos preferido no utilizar demasiados términos y agruparlos por conceptos. Tras una pequeña introducción se procede a la descripción de algunos términos.

Estructura de la Guía

¿Cuáles son los riesgos a que nos enfrentamos? Este es el primer asunto a tratar. Existen diferentes maneras de clasificarlos y por tanto se podrían desarrollar muchos capítulos tratando este tema. Se ha optado por dos: la primera atendiendo a la esencia del riesgo (CAPITULO 1) y la segunda al impacto en la empresa (CAPÍTULO 2).

A continuación, abordamos que tipos de incidentes podemos tener. Estos podrán ser intencionados (CAPÍTULO 3), para los que se utiliza diferentes herramientas (CAPÍTULO 4) y no intencionados (CAPÍTULO 5).

¿Y cómo podemos mitigar estos riesgos? Por un lado, con medidas tecnológicas (CAPÍTULO 6), pero también con medidas humanas (CAPÍTULO 7), entre las que se incluyen estructuras organizativas (CAPÍTULO 8).

Al final existe un índice para los casos en los que se quiera consultar un término concreto.

Índice

CAPÍTULO 1 – Clasificación de riesgos I

Una posible definición de seguridad de la Información es la siguiente: conjunto de controles cuyo propósito final es preservar la **confidencialidad, integridad y disponibilidad** de la información, colaborando a asegurar la competitividad, rentabilidad, el cumplimiento de la legalidad vigente y la buena imagen de la empresa.

De aquí podemos sacar una primera clasificación de riesgos en función de la característica de la información que se pretende preservar:

- **ACCESIBILIDAD O DISPONIBILIDAD.** Impide que los usuarios del sistema tengan a su disposición la información a la que están autorizados cuando la solicitan. Se puede atacar la accesibilidad destruyendo algún dispositivo, saturando la capacidad del procesador, encriptando la información para que no sea legible, etc.
- **CONFIDENCIALIDAD.** Una parte accede información a la que no está autorizada. Por ejemplo, visualizando información sin contar con los permisos, realizando copias no autorizadas de ficheros, escuchando en las redes de comunicación de datos, etc.
- **INTEGRIDAD.** Una parte no autorizada modifica el sistema de información, llegando incluso a incorporar nuevos componentes. Por ejemplo, cambiando contenidos de las bases de datos, añadiendo campos nuevos, modificando los programas, incorporando programas nuevos, alterando los datos de un pedido, etc.

CAPÍTULO 2 – Clasificación de riesgos II

Otra alternativa para clasificar los riesgos es la de utilizar el criterio del impacto que puede tener en la empresa.

- **RIESGO CIBERNÉTICO.** Aquel que puede producir un daño en los sistemas de información de una organización. El riesgo puede tener su origen en cualquier componente del sistema: equipos, aplicaciones, comunicaciones... Se puede producir como consecuencia de ataques de piratas informáticos o hackers y por fallos o errores no intencionados. Los daños pueden ser la alteración, modificación, destrucción o pérdida de información, el acceso indebido a la información y la falta de disponibilidad de servicio.

Este riesgo puede provocar riesgos de diferente índole:

- **FINANCIEROS.** Aquellos que se relacionan con la capacidad económica del asegurado, en relación con el capital asegurado.
- **LEGALES.** Es la incertidumbre relacionada con los riesgos legales, regulatorios y contractuales que inciden sobre los objetivos de la Organización y que pueden surgir en su entorno jurídico por los actos u omisiones de la misma, de sus accionistas y de otros terceros. Riesgo de recibir sanciones como consecuencia del incumplimiento o infracción de la normativa legal o requerimientos de órganos reguladores y/o supervisores, a consecuencia del desconocimiento, la inobservancia dolosa o culposa de la misma. Riesgos por incumplimiento contractual, extracontractual, estructural y litigioso.
- **PATRIMONIAL.** Aquel que implica una disminución o pérdida, total o parcial, del patrimonio del asegurado como consecuencia de un evento que puede afectarle.
- **REPUTACIONAL.** Posibilidad de que se produzcan daños en la imagen o reputación de la Organización o en la percepción de la misma por parte de la sociedad o cualquier otro grupo de interés.
- **PERSONALES.** Aquellos que afectan a circunstancias de la persona, tales como su salud, integridad física o mental, capacidad para el trabajo, vejez o supervivencia. La pérdida de control de un equipo controlado por un ordenador podría provocar este tipo de riesgos.
- **RESPONSABILIDAD CIVIL.** Posibilidad de ser reclamado por los daños causados a terceros, por culpa o negligencia del autor del daño, o sin necesidad de culpa cuando se realiza una actividad de riesgo, para reparar o indemnizar dicho daño.

CAPÍTULO 3 – Incidentes – Métodos de ataque

Existen una multitud de métodos de ataque, tanto tecnológicos como no tecnológicos, que atentan contra la confidencialidad, integridad o disponibilidad de la información.

Los métodos de ataque van aumentando tanto por el incremento de la superficie de ataque como por la posibilidad de contar con medios de ataque más potentes y sofisticados. Están en constante evolución, afectan a uno o varios tipos a la vez y suelen usarse en combinación en el caso de objetivos fuertemente protegidos.

- **ATAQUE DE FUERZA BRUTA.** Es un procedimiento para averiguar una contraseña consistente en probar todas las combinaciones posibles hasta encontrar la correcta. Dado que utilizar el método de prueba y error puede requerir mucho tiempo, se suele combinar utilizando todas las palabras de un diccionario.
- **CARDING.** Consiste en la obtención de los números secretos asociados a tarjetas de crédito con el objetivo de realizar compras a través de internet.
- **DEFACEMENT.** Es una palabra inglesa que significa desfiguración. Consiste en la deformación o cambio producido de manera intencionada en una página web. Se suelen realizar para ridiculizar al propietario de la página web o para mostrar mensajes reivindicativos.
- **DENEGACIÓN DE SERVICIO.** Es un ataque en el que el delincuente intenta dejar inoperativos los recursos de un ordenador o red. Saturan el sistema lanzando miles de peticiones de servicio de forma simultánea provocando el desbordamiento de este.
- **DENEGACIÓN DISTRIBUIDA DE SERVICIO (DOS.)** Es una variante, donde el ataque se realiza desde muchos origines, por ejemplo, desde cientos de equipos pertenecientes a una red de equipos infectados y controlados por terceros.
- **DESBORDAMIENTO DE BÚFER.** Provoca algo similar a lo que ocurre cuando llenamos un vaso más allá de su capacidad: el vaso se desborda y el contenido de derrama. Cuando el programador no incluye las medidas necesarias para comprobar que el tamaño del búfer en relación con el volumen de datos que tiene que alojar, se produce un derramamiento de datos que se sobrescriben en otros puntos de la memoria. El atacante calcula que cantidad de datos necesita enviar y donde se reescribirán los datos para enviar comandos que se ejecutarán en el sistema.

- **INGENIERIA SOCIAL.** Método utilizado por los atacantes para engañar a los usuarios para que realicen una acción que producirá consecuencias negativas, como la descarga de malware o la divulgación de información. Suelen valerse de la buena voluntad y falta de precaución de la víctima.

- **PHARMING.** Manipulación de nombres de dominio y que permite que cuando el usuario introduce la dirección de una página web le conduzca a otra falsa, que simula ser la deseada. Con esta técnica se intenta obtener información confidencial de los usuarios, desde números de tarjetas de crédito hasta contraseñas.

- **PHISHING.** Corresponde con la contracción en inglés de 'cosecha y pesca de contraseñas'. Esta técnica consiste en suplantar a través de medios telemáticos la personalidad de una persona o empresa de confianza. El usuario cree que recibe una comunicación de una entidad reconocida y seria que le solicita que debe actualizar o verificar sus datos. Una vez que el usuario entrega sus datos, los estafadores proceden a utilizarlos. Existen diferentes modalidades de phishing: cuando se realiza mediante SMS su nombre es smishing, cuando se realiza utilizando voz sobre IP se denomina vishing y si es a través de correos electrónicos spear phising.

- **RANSOMWARE.** El delincuente toma el control del equipo infectado y 'secuestra' la información del usuario cifrándola, de forma que resulta ilegible si no se dispone de una clave para descifrarla. El delincuente extorsiona a la víctima solicitando al usuario un rescate a cambio de las claves que permitan descifrar la información.

- **SPOOFING.** Técnicas de suplantación de identidad, llevada a cabo generalmente gracias a un proceso de investigación o con el uso de malware. Ponen en riesgo la privacidad de usuarios, así como la integridad de sus datos. La suplantación puede ser de la dirección de IP, de la tabla ARP (Advanced Resolution Protocol), el nombre del dominio (DNS), de la web o del correo electrónico.

- **SUPLANTACIÓN DE IDENTIDAD.** Es una actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude, acoso, etc. Un ejemplo sería la creación en redes sociales de un perfil de otra persona e interactuar con otros haciéndose pasar por ella.

CAPÍTULO 4 – Incidentes – Herramientas para realizar ataques

Para aplicar los métodos de ataque se utilizan diferentes herramientas.

- **0 DAY (ZERO DAY) (ATAQUES DE DÍA CERO):** Ataques contra aplicaciones o sistemas que aprovechan nuevas vulnerabilidades, desconocidas por los fabricantes del producto y/o software, y para los que no se han desarrollado aún "parches" o soluciones que las corrijan.

- **ADWARE.** Son programas que muestran, ejecutan o bajan anuncios de forma automática, sin que el usuario pueda interferir. No dañan el ordenador, pero pueden resultar irritantes. Una variante, es la contratación por terceros de "espacios de publicidad· que, en realidad, en lugar de publicidad, redirigen a webs de descarga de malware.

- **APLICACIONES ENGAÑOSAS.** Son programas que intentan engañar a los usuarios informáticos para que emprendan acciones encaminadas a descargar malware o para que los usuarios divulguen información adicional.

- **APT (ADVANCED PERSISTENT THREAT) (AMENAZA PERSISTENTE AVANZADA).** Ataques especialmente diseñados y dirigidos contra una organización o entidad concreta. Por lo general requieren de un elevado tiempo de preparación y combinan diferentes técnicas y vulnerabilidades de entre las ya comentadas anteriormente.

- **BOMBA LÓGICA.** Es un trozo de código insertado intencionalmente en un programa informático que permanece oculto hasta que se cumple una condición preprogramada (por ejemplo, después de encender el ordenador una serie de veces, en una fecha, etc.), momento en el que se ejecuta la acción maliciosa.

- **BOT (DE ROBOT).** Es un ordenador individual infectado con malware, lo cual da al atacante control y acceso remoto de la máquina (RAT).

- **BOTNET.** Red de bots. Conjunto de equipos bajo el control de un bot maestro, a través de un canal de mando y control. Se utilizan en actividades malintencionadas, como el envío de spam y ataques distribuidos de denegación de servicio. Los propietarios de los ordenadores infectados generalmente ignoran que su equipo forma parte de una botnet.

- **CABALLO DE TROYA.** Es un tipo de código malicioso que parece ser algo que no es; aparenta dar una funcionalidad deseada por el usuario cuando en realidad las facilidades se las proporciona al atacante No infectan archivos ni se propagan automáticamente. Su código malicioso, cuando se activa, causa pérdida o robo de datos. Pueden tener también un componente de puerta trasera que permite al atacante descargar amenazas adicionales en el equipo infectado. Se suele propagar a través de descargas inadvertidas, archivos adjuntos a correos electrónicos o al descargar algún archivo de internet. Es habitual la presencia de aplicaciones maliciosas con troyanos en los stores de apps móviles. Un ejemplo, paradigmático es una app linterna que pide al usuario permisos para controlar el micrófono, las llamadas, los sms y la agenda. En este ejemplo real, el usuario instala un troyano (la linterna).

- **CIFRADO.** Proceso mediante el cual se toman datos claros, se les aplica una función matemática y se obtienen datos codificados, incomprensibles para el que no disponga de un código para descodificarlo.

- **COOKIE.** Es un fichero que se envía al usuario en ocasiones cuando visita una página web. Su objetivo es registrar la visita del usuario y guardar cierta información al respecto. No suelen tener un objetivo malicioso.

- **ENMASCARAMIENTO.** Modificación de la identidad de origen real de una comunicación.

- **GUSANOS (WORM).** Son programas maliciosos que se reproducen de un sistema a otro.

- **HIJACKER.** Se corresponde con la palabra 'secuestrador' en inglés. Es un programa que cambia la configuración del navegador para hacer que la página de inicio, búsqueda, etc. apunte a otra distinta a la indicada por el usuario.

- **INYECCIÓN SQL.** Es un tipo de ataque que se aprovecha de una vulnerabilidad en la validación de los contenidos introducidos en una aplicación, típicamente en un formulario web, permitiendo la ejecución de una instrucción SQL diferente a la esperada. SQL (por sus siglas en inglés Structured Query Language; en español lenguaje de consulta estructurada), es un lenguaje para efectuar consultas que permiten recuperar de forma sencilla información de bases de datos, así como hacer cambios en ellas.

- **MALWARE.** Es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Se corresponde con la combinación de dos palabras inglesas: malicious y software. Entran en acción sin que el usuario del equipo se dé cuenta. A menudo utiliza para difundirse el correo

electrónico, la mensajería instantánea, descargas inadvertidas, medios extraíbles (como dispositivos USB) y ataques a la vulnerabilidad de seguridad en el software. Este término agrupa virus, gusanos, troyanos, etc.

- **PROGRAMA DE CAPTURA DE TECLADO (KEYLOGGER).** Es un tipo de malware diseñado para capturar las pulsaciones, movimientos y clics del teclado y ratón de forma encubierta para intentar robar información personal.

- **PUERTA TRASERA.** Cualquier punto débil de un programa o sistema mediante el cual una persona no autorizada puede acceder a un sistema. Pueden existir por fallos, errores o ser creadas a propósito de forma legítima para facilitar la administración. Pero también pueden ser instaladas por un atacante, dando el control del ordenador de forma remota a este.

- **ROOTKITS.** Se trata de un tipo de malware que tiene como fin el control del sistema operativo. Tiene una gran capacidad de esconderse de casi todos los programas antivirus a través de un avanzado código de programación. No infectan las máquinas por sí mismos, sino que tratan de proporcionar un entorno indetectable para ejecutar códigos maliciosos. Una vez instalados, el atacante puede realizar prácticamente cualquier función en el sistema. Aunque pueda ser encontrado, en algunos casos impiden que sea borrado.

- **SNIFFER.** Es un programa que monitoriza la información que circula por la red con el objeto de capturar información.

- **SOFTWARE DE SEGURIDAD FRAUDULENTO (ROGUE).** Es un tipo de aplicación engañosa que finge ser software de seguridad legítimo, aunque realmente no proporciona protección y puede incluso facilitar la instalación de códigos maliciosos contra los que el usuario busca protegerse.

- **SPAM.** Se conoce también como correo basura. Es un correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. Normalmente tiene contenido publicitario. Los mensajes de spam se utilizan en ocasiones como un método para propagar ataques de phising.

- **SPYWARE.** Son programas espías. Inicialmente se desarrollaron para monitorear las páginas visitadas y otros hábitos de navegación para llegar al usuario con anuncios de forma más eficiente. Pero con el tiempo se han desarrollado para robar información personal (p.ej. inicios de sesión y contraseñas) y para modificar la configuración del ordenador.

- **TOOLKIT.** Paquete de software diseñado para ayudar a los hackers a crear y propagar códigos maliciosos. Frecuentemente automatizan la creación y propagación del malware hasta el punto de permitir a principiantes utilizar amenazas complejas.

- **TROYANO (TROJAN).** Ver caballo de Troya.

- **VIRUS.** Programa informático escrito para alterar el funcionamiento del sistema de información, sin permiso ni conocimiento del usuario. Debe cumplir dos criterios:

I) Debe ejecutarse por sí mismo (generalmente coloca su propio código en la ruta de ejecución de otro programa)

II) Debe reproducirse (por ejemplo, reemplazando otros archivos ejecutables con una copia del archivo infectado por el virus).

- **WEB BUGGS (MICRO ESPÍAS O PULGAS).** Son imágenes transparentes dentro de una página web o dentro de un correo electrónico. Al igual que ocurre con las cookies, se utilizan para obtener información acerca de los lectores de esas páginas o los usuarios de los correos, tales como la dirección IP de su ordenador, el tipo y versión de navegador del internauta, el sistema operativo, idioma, cuanta gente ha leído el correo, etc.

CAPÍTULO 5 – Incidentes – No maliciosos

Los riesgos cibernéticos no siempre tienen un origen malicioso. En ocasiones se puede comprometer la confidencialidad, integridad o disponibilidad por incidencias de la más variada índole.

A continuación, se relacionan posibles orígenes de distintos incidentes. En esta ocasión, en vez de definiciones se relacionan componentes afectados y los eventos posibles.

- **COMUNICACIÓN.** Puede afectar a voz, datos, IP, cables, proveedores, internet, etc. Son susceptibles de caídas, degradación del servicio, cortes de línea, etc. pudiendo provocar la paralización o ralentización del servicio.

- **CONFIGURACIÓN.** Actúa sobre servidores, electrónica, LAN, WAN, back up, comunicaciones, aplicaciones, gestión de identidades, segregación de funciones, etc. Pueden generar incidencias como consecuencia de errores humanos o fallos en el software, pudiendo provocar pérdidas de funcionalidad, enlentecimiento, bloqueos, accesos indebidos, facilitar la intrusión, etc.

- **INFRAESTRUCTURA.** Se compone de servidores, electrónica, discos, cableado, Centros de Procesos de Datos, sistemas de back up, etc. Son susceptibles de cortes eléctricos, averías, calentamientos, falta de capacidad, etc. pudiendo provocar una paralización del servicio o su ralentización.

- **IOT (INTERNET DE LAS COSAS).** Puede afectar a instalaciones, vehículos, salud, hogar, infraestructuras críticas… Son susceptibles de incidentes por falta de seguridad y privacidad en las diferentes fases de su ciclo de vida; empezando por la fase de diseño. Las afectaciones a sus vulnerabilidades pueden llevar al fallo operacional, a servir de vector de entrada a las redes a las que se conecta o formar parte de redes boots que ataquen a terceros.

- **MANTENIMIENTO.** Puede afectar a infraestructuras, bases de datos, copias de seguridad, revisión de logs, planes de contingencia, planes de recuperación, planes de continuidad... Pueden provocar enlentecimiento, corrupción de datos, pérdida de datos, paradas, pérdida de control y facilitar la intrusión.

- **MOVILIDAD.** Puede afectar a smart phones, tablets, laptops, wearables, trabajo en casa, accesos remotos, videoconferencias, conectividad, trabajo compartidos, escritorios virtuales… Son susceptibles de utilización de aplicaciones no homologadas, hacer complejos los perímetros de seguridad, las políticas de seguridad, etc. pudiendo provocar la ralentización del servicio, deficiencias en el servicio, pérdida de datos, pérdida de control y facilitar la intrusión.

- **PROGRAMAS.** Puede afectar a aplicaciones, sistemas, bases de datos, etc. Son susceptibles de errores de diseño, errores de programación, de interfases inseguras, etc. pudiendo provocar pérdidas de funcionalidad, falta de seguridad, enlentecimiento, bloqueos, accesos indebidos y facilitar la intrusión.

- **SUBCONTRATACIÓN.** Puede afectar a la programación, sistemas, soporte, mantenimiento, seguridad, servicios, etc. Aunque aportan puntos fuertes en aquellos aspectos en los que la empresa no cuente con especialistas, hacen más complejo el control.

CAPÍTULO 6 – Medidas de mitigación tecnológicas

Para defendernos de los riesgos de ataques contamos con diferentes herramientas.

- **ANTISPAM.** Es una herramienta que detiene el spam o correo no deseado antes de que se convierta en una molestia para los usuarios. Cada vez más, forman parte del arsenal antispam listas que permiten filtrar el correo recibido.

- **ANTIVIRUS.** Es un software de seguridad que protege a los equipos de virus, a través de la detección en tiempo real y mediante el análisis del sistema, poniendo a los ficheros sospechosos en cuarentena y eliminándolos. La tendencia actual es a la sustitución (o cuanto menos a la complementariedad) de los antivirus tradicionales basados en firmas de malware conocido o en mecanismos heurísticos (comportamiento) por programas antimalware de defensa en profundidad basado en firmas de goodware (programas legítimos).

- **CERTIFICADO DIGITAL.** Es un fichero informático generado por una entidad (Autoridad Certificadora) que asocia unos datos de identidad a una persona física o de un organismo o empresa, confirmando su identidad en internet. Hay certificados digitales de servidores web, de código (aplicaciones), de persona física, de empleado público o de representación, entre otros.

- **CIFRADO.** Es un método de encriptado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Solo los individuos con acceso a una contraseña o clave pueden descifrar los datos.

- **CORTAFUEGOS (FIREWALL).** Es un sistema de seguridad, compuesto por programas y/o hardware, diseñado para bloquear o permitir las conexiones en determinados puertos TCPIP del sistema. Típicamente, los puertos están asociados a servicios.

- **FIRMA ANTIVIRUS / DEFINICIONES DE VIRUS.** Es un archivo que proporciona información al software antivirus para encontrar y reparar los riesgos. Sirve de protección contra el malware conocido.

- **HACKING ÉTICO Y PEN-TESTING:** La necesidad de contar con servicios y pruebas periódicas de hacking e intrusión en los sistemas, realizados bien sea a través de recursos internos o subcontratados con terceros.

- **HONEYPOT:** Sistema trampa o señuelo, es una herramienta de la seguridad informática dispuesta en una red o sistema informático para ser el objetivo de un posible ataque informático y así poder detectarlo y obtener información del mismo y del atacante.

- **IOC (INDICADOR DE COMPROMISO).** Datos estructurados que conforme a una convención contiene los elementos necesarios para identificar un compromiso en un sistema. Hay elementos generadores de IOCs y elementos consumidores de IOCs.
- **LISTAS BLANCAS (WHITELISTING).** Es un método utilizado por programas de bloqueo de spam, que solo permite a determinadas direcciones de correos electrónicos o nombres de dominio autorizados pasar por el software de seguridad.
- **LISTAS DINÁMICAS ANTISPAM.** Fuentes internas o externas, generalmente bases de datos, que contienen información sobre IPs que están catalogadas como spam.
- **LISTAS DINÁMICAS DE REPUTACIÓN.** Fuentes internas o externas, generalmente bases de datos, que contienen información sobre IPs que están catalogadas como maliciosas (spam, malware,..)
- **LISTA GRIS (GREYLIST).** Es un método de defensa contra el spam. Los correos electrónicos no reconocidos son rechazados temporalmente. Si posteriormente el correo se considera legítimo se aceptará.
- **LISTAS NEGRAS (BLACKLISTING).** Es el proceso de identificación y bloqueo de programas, correos electrónicos, direcciones o dominios IP maliciosos o malévolos.
- **SEGURIDAD BASADA EN LA REPUTACIÓN.** Es una estrategia de identificación de amenazas que clasifica las aplicaciones con base a ciertos criterios para determinar si probablemente son malignas o benignas. Estos atributos suelen incluir aspectos como la edad de los archivos, la fuente de descarga y la prevalencia de firmas digitales.
- **SISTEMA DE DETECCIÓN DE INTRUSOS.** Es un servicio que monitorea y analiza los eventos del sistema para encontrar y proporcionar en tiempo real advertencias de intentos de acceso a los recursos del sistema de manera no autorizada.
- **SISTEMA DE PREVENCIÓN DE INTRUSOS.** Es un dispositivo (hardware o software) que supervisa las actividades de un sistema en busca de comportamiento no deseado o malicioso y permite reaccionar para bloquear las actividades.
- **SONDA.** Equipo que analiza el tráfico y que típicamente tiene implementada reglas/fuentes de inteligencia para identificar ataques.

CAPÍTULO 7 – Medidas de mitigación humanas

El análisis del riesgo y su gestión es el primer paso que es necesario dar para mitigar el riesgo. De estas tareas surgirán los planes para minimizar el daño que se puede generar en los sistemas de información de las organizaciones.

En tanto que la inversión de las empresas en sistemas de protección va aumentando, es previsible que aumenten los ataques de ingeniería social, por lo que cada vez es más importante formar a los usuarios e involucrarlos en la prevención. Debe educarse a cada persona o grupos sobre aquellas amenazas que tienen más probabilidad de encontrar. Es importante que la información esté actualizada. Una explicación obsoleta puede ser contraproducente, al poder ofrecer una falsa sensación de seguridad.

ANÁLISIS Y GESTIÓN DE RIESGOS. Ver análisis y gestión del riesgo

- **ANÁLISIS.** Es la utilización sistemática de la información disponible para determinar el valor de los activos, la identificación de las vulnerabilidades y las amenazas, la probabilidad e impacto caso de materializarse y en consecuencia evaluar el riesgo.
- **GESTIÓN DEL RIESGO.** Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo (ISO 31000: 2009). El riesgo se puede tratar asumiéndolo, reduciéndolo, eliminándolo y/o transfiriéndolo.
- **CAMPAÑAS DE CONCIENCIACIÓN CONTINUA EN SEGURIDAD DE LA INFORMACIÓN.** Campañas orientadas a incidir y recordar los asuntos tratados en la formación en seguridad de la información.
- **FORMACIÓN EN SEGURIDAD DE LA INFORMACIÓN.** Cursos desarrollados con el objetivo de dar a conocer entre los usuarios y técnicos de los sistemas de información los riesgos de seguridad y las buenas prácticas para evitarlos. Estos cursos deben actualizarse para adaptarse a los cambios en los riesgos y prácticas. La formación debe ser continua.

CAPÍTULO 8 – Organización para la seguridad de la información

Para comenzar al hablar de organización para la seguridad de la información tenemos que dejar claro que no se está exento en ningún caso de sufrir una pérdida o daño derivado de un ataque sino lo que se establecen son las estructuras, procesos y procedimientos que permitan una rápida reacción minimizando esa perdida y en ocasiones evitándola. Para su evitación los sistemas de organización de la información deben ser flexibles y en continua adaptación pues el entorno y las amenazas a las que nos enfrentamos a diario son más que cambiantes.

Un elemento clave dentro de la organización de la seguridad de la información es la **política de seguridad de la información** con el fin de proteger el core de nuestro negocio y fuente de la ventaja competitiva de cada organización. Su objeto principal será la garantía de preservar nuestra información bajo los principios de confidencialidad, integridad y disponibilidad.

Las siguientes figuras son habituales en empresas que tienen desarrollada la gestión de la seguridad de la información.

- **CISO (CHIEF INFORMATION SECURITY OFFICER).** Es el responsable máximo en planificar, desarrollar, controlar y gestionar las políticas, procedimientos y acciones con el fin de mejorar la seguridad de la información dentro de sus pilares fundamentales de confidencialidad, integridad y disponibilidad.
- **CIO (CHIEF INFORMATION OFFICER).** Es el ejecutivo responsable de los sistemas de información de la empresa.
- **COS (SOC) (CENTRO DE OPERACIONES DE SEGURIDAD).** Es una central de seguridad informática que previene, monitorea y controla la seguridad en las redes y en Internet. Dotado de servidores, firewalls, sistemas de detección de intrusos, software antivirus y otros sistemas especializados, un COS monitorea la actividad en las redes e Internet en tiempo real, las 24 horas del día, los 7 días de la semana. Los datos eventos son analizados y rastreados por expertos certificados en estándares de seguridad.
- **CSI (COMITÉ DE SEGURIDAD DE LA INFORMACIÓN).** Es el órgano responsable del gobierno de la seguridad de la información. Sus funciones habituales son las siguientes: Revisión y aprobación de la política de seguridad, supervisión y control de la exposición al riesgo de los activos de información, revisión y seguimiento de las incidencias significativas y aprobación y seguimiento de las iniciativas de mejora. Está integrado por representantes de todas las áreas sustantivas de la organización.

- **CSIRT (GRUPO DE RESPUESTA ANTE INCIDENTES).** Iniciales en inglés de Computer Security Incident Response Team. Equipo multidisciplinar de personas involucradas en el proceso de respuesta ante un incidente de seguridad. Deben reaccionar frente a una violación de seguridad de forma rápida y coordinada, minimizando el impacto en el negocio, consiguiendo una rápida reparación de los daños y acumular experiencia para evitar que se vuelva a repetir.
- **CERT.** Ver CSIRT

Relación de términos nombrados

Lecturas recomendadas

- INCIBE. Glosario de términos de ciberseguridad
- Symantec. Glosario de seguridad
- Safemode. Glosario de términos de seguridad informática
- Auditores Internos. Ciberseguridad: Una guía de supervisión
- FERMA y ECIIA. Cyber Risk Governance Report

Patrocinadores 2017

Platino

Golden

Silver

Realizado por:

AGERS - Asociación Española de Gerencia de Riesgos e ISMS FORUM

agers | Asociación Española de Gerencia de Riesgos y Seguros

isms forum spain