Índice

0. Conceptos básicos de ciberserguridad

Introducción

Podemos definir **qué es la seguridad informática o ciberseguridad** como el proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente. **La seguridad informática** es en realidad una rama de un término más genérico que es la seguridad de la información, aunque en la práctica se suelen utilizar de forma indistinta ambos términos.

Aunque ambas estrategias de seguridad, la seguridad informática y la seguridad de la información cubren diferentes objetivos y alcances con ciertos solapamientos. La seguridad de la información es un tipo de protección más amplio, que abarca la criptografía, la informática móvil y los aspectos sociales. Se utiliza para proteger la información contra amenazas no basadas en la persona, como los fallos de los servidores o los desastres naturales. En cambio, la ciberseguridad sólo abarca las amenazas basadas en Internet y los datos digitales.

En otras palabras, busca proteger el uso de nuestros recursos informáticos por parte de intrusos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente.

Objetivos de la seguridad informática

Los principios u objetivos básicos de la seguridad informática son:

1. **Confidencialidad**: Sólo los usuarios autorizados pueden acceder a nuestros recursos, datos e información. (Ej: Archivos con contraseña)
2. **Integridad**: Sólo los usuarios autorizados deben ser capaces de modificar los datos cuando sea necesario.
3. **Disponibilidad**: Los datos deben estar disponibles para los usuarios cuando sea necesario. (Ej: Redundancia de hardware)
4. **Autenticación**: Estás realmente comunicándote con los que piensas que te estás comunicando. (Ej: Firmar digitalmente un archivo)

5. **No repudio:** Mecanismo que permite que ninguna de las partes de la comunicación niegue su participación en la misma (Ej: Firma digital, acuse de recibo de un email).

¿Por qué es importante la seguridad informática?

Algunos casos famosos sólo en 2023:

- Brecha de seguridad de 37 millones de clientes de T-Mobile

- Fuga de datos de Activision
- Mailchimp confirma haber sufrido un ataque de ingeniería social que puso en riesgo las cuentas de 133 clientes
- Unos hackers han atacado la fábrica de Suzuki. Llevan 10 días parados y han perdido más de 20.000 motos
- Un ciberataque a un proveedor está detrás de la brecha de datos de Discord
- Reddit confirma haber sufrido un ataque de 'phishing', pero insiste en que los datos de los usuarios están seguros
- Ataque Cibernético a Toyota: Hackers habrían filtrado 3,1 millones de datos sensibles de clientes.

¿Qué protege la seguridad informática?

La ciberseguridad se centra en proteger los activos de una empresa u organización. Se entiendew como activos lo siguiente:

- Información: Son diferencia el principal y más importante activo de una empresa. Es almacenada en la infraestructura de la empresa y hace uso de ella.
- Equipamiento físico: Se debe proteger el hardware, tanto de ataques intencionados, como de posibles accidentes.
- Redes y comunicaciones/Infraestructura: La información circula por la red de una empresa, además de información de control.
- Usuarios: Sin lugar a duda, el eslabón más débil de la cadena en seguridad informática. Se necesitará por tanto establecer una serie de políticas de acceso y autorización.

Tipos de seguridad

Del anterior punto se deduce que la seguridad puede ser:

- *Seguridad lógica:* se encarga de proteger todo lo relacionado con la parte software y la información.

- *Seguridad física*: Intenta proteger la parte hardware de posibles desastres naturales (inundaciones, terremotos...) o accidentes (incendios, sobrecargas eléctricas, robos, cable cortado por error haciendo obras…).

  Parece imposible pero los accidentes ocurren: Un rayo parte la 'nube de computación' de Amazon y afecta a miles de sitios web en Europa

A la hora de poner en marcha las medidas adecuadas para cada uno de los dos tipos de seguridad mencionadas arriba, éstas se clasifican a su vez en:

- *Seguridad activa:* Su principal misión es la prevención de daños de cualquier tipo, tanto físicos como lógicos.

  Ejemplos: Firewall/WAF, IDS/IPS, antivirus, controles de acceso (radius, directorio activo…), 2FA, controles de acceso físicos (sistemas biométricos), redundancia de hardware, cifrado de la información.

- *Seguridad pasiva:* Es aquel tipo de seguridad que, una vez se produce el daño porque las medidas de seguridad activa no han resultado efectivas, intenta minimizar las consecuencias del mismo.

  Ejemplos: Copias de seguridad, SAI

Se deben implantar ambos tipos de mecanismos de seguridad, tanto activos como pasivos, no deben ser excluyentes entre sí.

Amenazas y vulnerabilidades en los sistemas de información[1]

La diferencia entre vulnerabilidad y amenaza es muy interesante, aunque son términos que se confunden a menudo. Veamos cómo se definen:

- Una **vulnerabilidad** (en términos de informática) es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros»

1 Nota: esta sección ha sido obtenida de aquí https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

pueden tener distintos orígenes por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos.

Algunos ejemplos de vulnerabilidades recientes:

- Heartbleed → Vulnerabilidad que afecta a las comunicaciones cifradas con openSSL
- Eternalblue → Vulnerabilidad que aprovechó el ransomware Wannacry
- KRACK → Vulnerabilidad que afectaba a la seguridad del cifrado WPA2 en comunicaciones WiFI

- Por su parte, una **amenaza** es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas.

El riesgo es la probabilidad de que se produzca un incidente de seguridad, materializándose una amenaza y causando pérdidas o daños. Se mide asumiendo que existe una cierta vulnerabilidad frente a una determinada amenaza, como puede ser un hacker, un ataque de denegación de servicios, un virus… El riesgo depende entonces de los siguientes factores: la probabilidad de que la amenaza se materialice aprovechando una vulnerabilidad y produciendo un daño o impacto. El producto de estos factores representa el riesgo.

Algunas de las fuentes de amenazas más comunes en el ámbito de sistemas de información son:

- Malware o código malicioso: permite realizar diferentes acciones a un atacante. Desde ataques genéricos mediante la utilización de troyanos, a ataques de precisión dirigidos, con objetivos específicos y diseñados para atacar a un dispositivos, configuración o componente específico de la red.
- Ingeniería social: Utilizan técnicas de persuasión que aprovechan la buena voluntad y falta de precaución de la víctima para obtener información sensible o confidencial. Los datos así obtenidos son utilizados posteriormente para realizar otro tipo de ataques, o para su venta.
- APT o Amenazas Persistentes Avanzadas (*Advanced Persistent Threats*): son ataques coordinados dirigidos contra una empresa u organización, que tratan de robar o filtrar información sin ser identificados. Se suelen ayudar de técnicas de ingeniería social y son difíciles de detectar.
- Botnets: conjunto de equipos infectados que ejecutan programas de manera automática y autónoma, que permite al creador del botnet controlar los equipos infectados y utilizarlos para ataques más sofisticados como ataques DDoS.
- Redes sociales: el uso no controlado de este tipo de redes puede poner en riesgo la reputación de la empresa.
- Servicios en la nube: una empresa que contrate este tipo de servicios tiene que tener en cuenta que ha de exigir los mismos criterios de seguridad que tiene en sus sistemas a su proveedor de servicios. Se ha de asegurar de contratarlos con empresas cuya seguridad este demostrada, y firmar SLA o ANS (Acuerdos de Nivel de Servicio) en los que quede definida la seguridad que necesita la empresa.

Algunos incidentes pueden implicar problemas legales que pueden suponer sanciones económicas y daños a la reputación e imagen de la empresa. Por eso, es importante conocer los riesgos, medirlos y evaluarlos para evitar en la medida de lo posible los incidentes, implantando las medidas de seguridad adecuadas.

Podemos identificar los activos críticos de los sistemas de información que pueden suponer un riesgo para la empresa, realizando un análisis de riesgos. Análisis que nos llevará a obtener una imagen rigurosa de los riesgos a los que se encuentra expuesta nuestra empresa. Estas fases son las siguientes:

Este análisis nos servirá para averiguar la magnitud y la gravedad de las consecuencias del riesgo a la que está expuesta nuestra empresa y, de esta forma, gestionarlos adecuadamente. Para ello tendremos que definir un umbral que determine los riesgos asumibles de los que no lo son. En función de la relevancia de los riegos podremos optar por:

- **Evitar el riesgo** eliminando su causa, por ejemplo, cuando sea viable optar por no implementar una actividad o proceso que pudiera implicar un riesgo.
- **Adoptar medidas que mitiguen el impacto o la probabilidad del riesgo** a través de la implementación y monitorización de controles.
- **Compartir o transferir el riesgo** con terceros a través de seguros, contratos etc.
- **Aceptar la existencia del riesgo** y monitorizarlo.

Política de seguridad

Una vez han sido identificado todos los activos de la empresa y se han evaluado los riesgos a los que se ven sometidos, se debe establecer una política de seguridad para protegerlos. Esta política se establece teniendo en cuenta los objetivos de la seguridad de la información vista en el punto .

Esta política de seguridad es un documento a alto nivel dónde la gerencia de una empresa muestra su compromiso con la seguridad de información de la misma.

En este documento se establecen una serie de buenas prácticas, instrucciones técnicas y procedimientos para implementar la seguridad en la organización. Algunos puntos que puede recoger este documento pueden ser, por ejemplo:

- Controles de acceso físico: tornos, cámaras, tarjetas de acceso, sistemas biométricos
- Controles de acceso lógico: implementación de distintos permisos y roles, autorización de acceso remoto por VPN para el teletrabajo
- Gestión de usuarios: altas y bajas de usuario en el sistema, concesión de permisos (Principio de mínimo privilegio)
- Clasificación de la información en función de su importancia
- Gestión de incidentes de seguridad
- Otros: backups, antimalware, actualizaciones de software

Es de vital importancia que esta política esté aprobada por la dirección de la empresa y que se comunique a todos los trabajadores para que tengan conocimiento de ella.

Protección de la información

Protege la información: un caso de éxito en una empresa de organización de congresos

¿Cuáles serían pues unos consejos básicos y mínimos para empezar con la protección de la información en nuestra empresa?

1. Control de accesos
    - Gestionar permisos de los usuarios razonablemente
2. Cifrado de la información
    - En sobremesas, portátiles y todo tipo de dispositivos móviles
3. Eliminación de la información,
    - Hacerlo de forma segura e impidiendo el acceso a los datos eliminados
4. Limitar uso de herramientas no autorizadas por la empresa
5. Cláusulas legales
    - Confidencialidad
6. Copias de seguridad

7. Contraseñas fuertes

8. Herramientas de protección adecuadas
    - Antivirus, antispam, sistemas avanzados
9. Sentido común

Ciberdelincuencia

A pesar de lo que el cine nos ha transmitido, la ciberdelincuencia queda lejos de un adolescente superdotado para la informática que, capucha negra mediante, se dispone a introducirse en los sistemas más avanzados del mundo desde la soledad de su habitación.

Se trata de grupos, normalmente de tamaño pequeño-mediano y bien estructurado, con unos roles muy definidos. Existen incluso grupos organizados de cibercriminales cuya infraestructura poco o nada tiene que envidiar a una gran empresa, incluyendo la división en departamentos.

De hecho, el modelo de *pago por servicio* (**as a service**) ha llegado a este ámbito, el de la ciberdelincuencia y permite contratar servicios delictivos a demanda. Profesionales de esta vertiente del crimen organizado desarrollan herramientas e infraestructuran que venden o alquilan a otros cibercriminales con menos recursos y del que obtienen beneficios a costa de unas comisiones por las ganancias que se deriven de su uso. Esto se conoce como afiliados.

Un estudio de la empresa de seguridad Trend Micro intenta hacer una clasificación aproximada de este tipo de "empresas" ilegítimas. Para hacernos una idea:

	Número de empleados y afiliados	Ganancias anuales	Capas de management
Pequeña	1-5	Menos de 500k $	1
Mediana	6-49	Hasta 50 millones de $	2
Grande	+50	+50 millones de $	3

A muy grandes rasgos a partir de este estudio, deducimos que:

1. Las **organizaciones pequeñas:**

- Tienen pocos miembros y poca jerarquía (no se reporta a nadie, simplemente se es socio)
- Los miembros suelen tener un trabajo legítimo común y lo combinan con su actividad delictiva
- Las ganancias son muy moderadas

2. Las **organizaciones medianas:**
   - Aquí ya existen grupos de *empleados* con funciones específicas y que además ya empiezan a deber reportar a alguien.
   - Las ganancias anuales ya permiten que los miembros tengan esta actividad como su único trabajo a tiempo completo
3. Las **organizaciones grandes:**
   - Están organizados en departamentos, de forma prácticamente similar a una empresa legítima
   - Existe una fuerte jerarquía en forma de pirámide.
   - Muestran unas ganancias anuales similares a las de una empresa legal

1. Principales amenazas en Internet

Introducción

Las ciberamenazas son especialmente notorias en las empresas de gran envergadura pero afectan a todas ellas. De hecho, las pequeñas y medianas empresas, las PYMES, suelen ser más vulnerables a estos ataques debido a la escasa atención, por unas u otras razones, puesta en sus medidas de seguridad. En un informe realizado por Hiscox en 2022, se concluye que el 44% de las pymes españolas sufrío al menos un ciberataque en 2021

Mientras que la mayoría de ataques suceden por la noche, la gran mayoría necesitan días, semanas e incluso meses en ser descubiertos. Así pues, los desafíos que afrontan todas las empresas y las PYMES en particular, es la concienciación y la disponibilidad de recursos para enfrentarse a este tipo de amenazas.

Este asunto se vuelve aún de mayor vital importancia, si es que cabe, en las PYMES industriales, tal y como podemos leer en este artículo de Incibe.

El coste por la pérdida de datos debida a un ataque para una PYME puede oscilar, según cifras ofrecidas por el Incibe, entre los 2000 y 50000€.

En definitiva, el mayor activo de una compañía es su información por encima de todo y, por tanto, toda precaución es poca para protegerla a ella y a los sistemas que la albergan, para así evitar las consecuencias de cualquier problema derivado de la ciberseguridad.

Estas consecuencias pueden ir desde la pérdida de confianza de los clientes, pérdidas económicas directas, legales

Malware

Dentro del malware se incluyen virus, gusanos, troyanos y/o software espía. Su intención es infectar, dañar e inhabilitar sistemas, redes, dispositivos u otros con el fin de impedir su correcto funcionamiento.

Su impacto se vio reducido en 2020, coincidiendo con la pandemia del Covid-19, aunque repuntó abruptamente en 2021 con la vuelta de los trabajadores a las oficinas.

Hace unos años el malware tuvo un auge especial debido a lo que se conoce como *crypto-jacking* así como el malware desarrolllado para IoT (Internet of Things). Según este informe de ENISA[2], en los 6 primeros meses de 2022 el volumen de ataques a estos dispositivos fue mayor que todo el registrado en los 4 años anteriores.

Puesto que los móviles ya son parte fundamental del día a día de cualquier persona y, por ende, de cualquier empresa, se han convertido en una nueva amenaza de seguridad. El malware para móvil debe ser también muy tenido en cuenta puesto que puede camuflarse en aplicaciones a priori legítimas e inocentes (lectores QR, linternas, juegos…). Las descargas desde app store no oficiales son el principal vector de entrada.

Ransomware

Quizás estemos hablando del tipo de malware más lucrativo del último lustro y una de las principales ciberamenazas en la actualidad. Cabe recordar la irrupción sonadísima de Wannacry en nuestras vidas en 2017

Este tipo de malware actúa infectado la red empresarial y cifrando todos los archivos (a veces incluso distingue si pueden ser archivos importantes o no) con una clave lo suficientemente fuerte como para dejarlos inoperativos si no se cuenta con ella. Tras ello, el atacante demanda un rescate a la víctima para facilitarle dicha clave o el proceso de descifrado.

Sólo en 2022, de acuerdo a las estadísticas, se produjeron 493 millones de ataques de ransomware en el mundo.

2 ENISA (Agencia de la Unión Europea para la Ciberseguridad) es la agencia de la Unión Europea a la que se le ha encomendado la misión **de velar por un alto nivel común de ciberseguridad en toda Europa**

Según la agencia de la UE para la ciberseguridad, la demanda de rescate más alta para un ataque de ransomware ha pasado de 13 millones de € en 2019 a 62 millones de € en 2021. De la misma forma, la media de rescate pagado ha pasado de los 71.000€ de 2019 a los 150.000€ de 2020. Se estima que el negcio del ransomware llegó a provocar unos daños de 18 miles de millones de forma global en 2021.

Además de la pérdida monetaria del rescate, se produce un impacto muy considerable en la pérdido de productividad y disponibilidad mientras los sistemas están inoperativos debido al cifrado.

Como todo en ciberseguridad, esta amenaza ha ido evolucionando. En un principio los ataques eran poco sofisticados y, en parte, indiscriminados. Hoy en día, todo el proceso se ha sofisticado y especializado. Para ciertos sectores críticos y estratégicos, se crean ataques de ransomware específicos que permiten obtener un beneficio mucho mayor de ellos por su necesidad o capacidad de hacer frente al pago de una fuerte suma.

También ocurre que el hecho de cifrar todo un sistema con datos es un proceso que consume una gran cantidad de tiempo, lo que hace posible que la víctima pueda salvar algunos datos del completo desastre si es capaz de detener el proceso en marcha. Además, las empresas más preparadas serán capaces de restaurar las copias del seguridad que tengan hechas de forma adecuada, a pesar de que muchos ransomware también ponen su foco en las copias de seguridad.

La situación descrita en el párrafo anterior hace que muchos grupos organizados hayan pasado de realizar la petición de rescate únicamente a sumar el robo de datos al cocktail, e incluso a centrarse únicamente en la segunda parte, la extorsión.

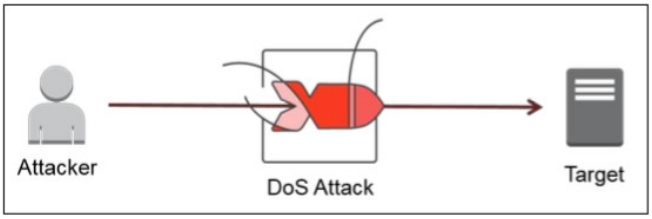
Es decir, muchos grupos directamente prescinden del cifrado de datos y demandan un rescate por una información robada. Este tipo de ataques son más rápidos de llevar a cabo, más difíciles de detectar y no se pueden solucionar con una copia de seguridad, haciendo de ellos una forma de negocio más efectiva para los cibercriminales y una gran amenaza para las empresas.

Por último, de una forma un tanto opuesta, también se da la situación de que el ransomware está ahora disponible para cibercriminales menos sofisticados en forma de kits listos para usar que se psueden comprar. Es lo que se conoce como **RaaS (Ransomware as a Service).**

Este tipo de kits son usados principalmente contra empresas pequeñas con pocas medidas de defensa en materia de ciberseguridad. Esto es porque un atacante, de forma individual, puede llevar a cabo múltiples campañas de bajo coste en materia de rescates pero que le reportan un monto lo suficientemente suculento como para llevarlo a cabo.

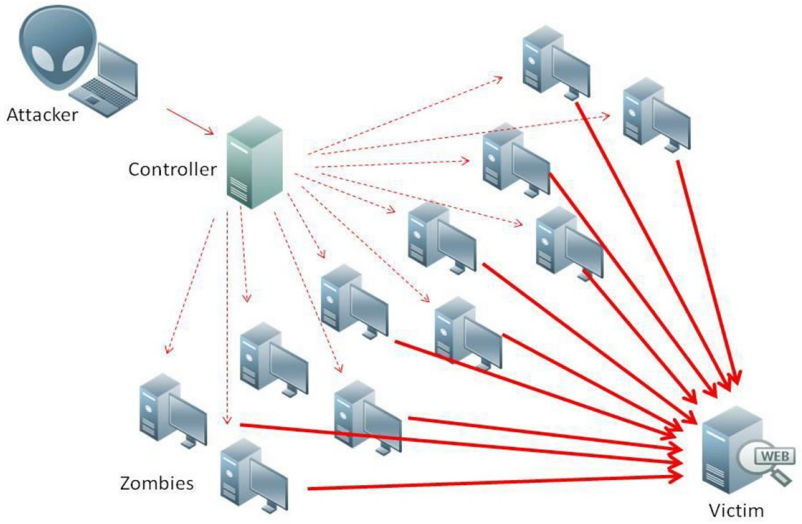
Riesgos contra la disponibilidad de servicios: DDoS (Ataques distribuidos de denegación de servicio)

Los ataques de tipo de denegación de servicio (DoS – Denial of Service, del inglés) tienen como objetivo fundamental de producir el colapso de un servicio ofrecido por un servidor o red. Esto se suele conseguir inundándolos de tráfico o peticiones mediante solicitudes hasta sobrepasar la capacidad de las máquinas pertinentes.



DDoS

La *D* inicial en este caso proviene de *Distributed*. Así pues, se trata de un ataque distribuido de denegación de servicio. El hecho de que sea distribuido es debido a que el tráfico del atacante proviene de muchos puntos distintos, potenciando así su efecto indeseado así como su mitigación.



Hay ataques DDoS que pueden implicar a cientos de miles de dispositivos atacantes. En estos casos se suele utilizar lo que se conoce como *botnet*. Una botnet es una red formada por ordenadores *zombies*.

Un ordenador *zombie* es aquel que ha sido víctima de una infección por malware y que permite al atacante controlarlo de forma remota. Todos estas máquinas infectadas forman parte de una red conjunta llamada *botnet* y que permanece latente a la espera de las órdenes del atacante sin que los usuarios infectados lo sepan.

En el momento oportuno el cibercriminal da la orden de atacar de forma conjunta, contando así con un gran poder de actuación.

Han sido muy sonados muchos ataques de esta clase e incluso el famoso grupo Anonymous facilita la participación de cualquier persona en sus ataques DDoS, a modo de colaboración.

Desinformación: fake news, astroturfing

La información manipulada se sirve tanto de lo emocional como de lo racional para llegar a intentar reescribir la realidad, mediante su difusión en plataformas multitudinarias.

El astroturfing "engloba cualquier acción online que tenga como fin manipular una tendencia social, una opinión pública o el apoyo o rechazo masivo a una idea, o producto, en definitiva, una conducta que altere el mercado y la libre competencia." Pretende dotar de una apariencia de naturalidad y espontaneidad a una actitud estratégica de apoyo colectivo a una idea.

Normalmente esta técnica es utilizada con fines políticos con el fin de influir en la opinión pública, aunque también pueden suponer un riesgo para las empresas precisamente por el mismo motivo.

Un ejemplo muy sonado fue el de cuando Meta (Facebook) utilizó *astroturfing* para desprestigiar a TikTok, aquí podéis consultar el enlace a la noticia. Básicamente Meta contrató a la empresa Targeted Victory, quienes intentaron difundir historias de adolescentes con coportamientos nocivos y que incluso amenazaban la seguridad nacional debido al uso que hacían de TikTok. Todo ello amparándose en supuestos estudios o encuestas de más que dudosa procedencia.

Ejemplos hay muchos y algunos de ellos son:

- Las reviews y opiniones pagadas, tanto positivas como negativas, en redes sociales o en la misma página de difusión (Amazon, TripAdvisor…)
- En el año 2013, la compañía **Samsung** fue multada en Taiwán por crear una campaña de desprestigio en contra de su rival HTC, pagando a aquellos que publicasen comentarios negativos sobre HTC.
- A principios de 2013, **Movistar España** sufrió una crisis en redes sociales por el despido de un empleado. Empleados de Telefónica denunciaban al despido como improcedente, y comenzaron una campaña online contra la empresa, que surtió efecto principalmente en Twitter, donde el hashtag alcanzó a ser trending topic. En respuesta, aparecieron en Twitter varias cuentas en defensa de la empresa y atacando al empleado. Varios indicios demostraban que esas cuentas eran falsas, como la incoherencia de los datos personales, las fechas de creación, el nombre de la aplicación desde la que se enviaban los tweets ("EnvioMensajes") y el hecho de que espontáneamente usaban los mismos hashtags sin que mediase relación entre ellas. Varios blogs señalaron esos indicadores y denunciaron la acción.
- En octubre de 2018, después de que el gigante de semiconductores **Broadcom anunciara su intención de adquirir CA Technologies** por 19.000 millones de dólares, un memorando hecho para que pareciera que provenía del Departamento de Defensa de Estados Unidos advertía que el gobierno de este país revisaría la transacción en busca de posibles amenazas a la seguridad nacional. Las acciones de Broadcom cayeron cuando el falso memorando fue publicado.
- Mayo de 2020. El problema no se limita a Estados Unidos. **Metro Bank**, en el Reino Unido, vio caer el precio de sus acciones un 11 por ciento después de que circularan falsos rumores en WhatsApp y Twitter que decían que el banco estaba al borde del colapso y que los clientes deberían vaciar sus cuentas lo antes posible.

- Muy comentada y debatida fue la campaña de desprestigio que desde España se orquestó contra el hotel de Cerdeña del exmarido de Juana Rivas tras saltar a los medios el caso de sustracción de menores, apareciendo en portales como TripAdvisor numerosos comentarios negativos sobre el hotel del exmarido en Cerdeña, unos comentarios que se produjeron en masa durante varios días, siendo publicados en su mayoría por perfiles españoles, en represalia al comportamiento del exmarido de Juana Rivas, al objeto de desprestigiar la calidad del citado establecimiento de hospedaje.

Es difícil combatir estas malas artes puesto que dependen en gran medida de la madurez digital de los usuarios. No obstante, como empresa, podemos construirnos una reputación lo más sólida posible con el fin de que esos falsos creadores de opinión no tengan una credibilidad suficiente como para que su difusión sea amplia.

También conviene tener una comunidad activa alrededor de nuestra organización, de tal forma que no sean los astroturfers los que dominen el discurso sin que nadie pueda rebatirles.

Ataques contra la cadena de suministro

También conocidos como ataques a la cadena de valor o ataque a terceros. Este tipo de acciones, cada vez más populares, no van dirigidas directamente contra la empresa objetivo o víctima principal, sino que que la infiltración se produce vulnerando a los proveedores o socios suministradores de la misma.

Esto se traduce en un descomunal aumento de la superficie de ataque y de los vectores de ataque.

¿Cómo funcionan?

Los atacantes se dedican a escanear su objetivo en busca de protocolos de red inseguro, infraestructuras desprotegids o código escrito de forma insegura. Tras encontrar una puerta de entrada, introducen el malware en algún punto del proceso de construcción del producto.

Puesto que el producto, el software, es vendido por proveedores reputados, las aplicaciones y sus actualizaciones están firmadas y certificadas por ellos. Es decir, estas empresas estarán vendiendo un software infectado y, en apariencia, completamente legítimo, sin darse cuenta y además validado por ellas mismas.

Si se trata de aplicaciones que gocen de gran popularidad en el mercado, el número de víctimas potenciales es significativo.

Según este estudio de la empresa de seguridad CrowdStrike:

- El 84% de las empresas cree que este tipo de ataques puede convertirse en una de las mayores ciberamenazas para organizaciones como las suyas en los próximos 3 años
- Sólo el 36% ha investigado a todos los proveedores nuevos y existentes por motivos de seguridad en los últimos 12 meses.
- El 59% de las organizaciones que han sufrido su primer ataque en la cadena de sumnistro carecía de una estrategia de respuesta

Ejemplos

Algunos ejemplos muy sonados de este tipo de ataques pueden ser:

- **SolarWinds.** Esta empresa comercializa un software denominado Orion cuyo objetivo es facilitar la monitorización y administración de la infraestructura IT de una empresa.

  En 2020 un actor malicioso consiguió introducir un backdoor en una de las actualizaciones de Orion lo que le permitió un posible acceso a los datos los clientes de SolarWinds que la hubiesen instalado. En ese momento SolarWinds tenía 33.000 clientes.

  Se sospecha que este ataque pudo ser perpetrado por algún grupo financiado por un estado nación.

- En 2017 otra brecha de seguridad sonada fue la de **Equifax**, la cual la compañía valoró en unos 2 billones (estadounidenses) de dólares. Los atacantes se aprovecharon de una vulnerabilidad descubierta en Apache Struts, un framework o herramienta para desarrollo web.

- En 2018 una aplicación que viene preinstalada en los ordenadores **ASUS** con el fin de actualizar controladores fue comprometida e infectada con un malware. Los atacantes consiguieron robar certificados dititales y manipularon el software a voluntad.

Ejercicio

En nuestra empresa estamos desarrollando una aplicación tipo Moodle (aula virtual) y la vamos a integrar con un proveedor de pago que nos suministra una serie de plugins para aumentar la funcionalidad.

Estos plugins, por su funcionamiento, necesitan realizar una serie de acciones en el servidor donde están instalados. Se ha decidido que estos plugins se ejecuten con privilegios de administrador en lugar de crearles un usuario raso, así nos aseguraremos de que su funcionamiento no nos dará problemas y además nos ahorramos crear usuarios nuevos.

El servidor donde estarán instalados los plugins trabaja en una red donde además tenemos el servidor de correo, el servidor web de la empresa, el servidor encargado de las nóminas, el directorio compartido entre todos los empleados de la empresa, etc.

Tras acabar el desarrollo de la aplicación e integrar los plugins, se pasarán varias pruebas al software como son funcionales, de rendimiento y también de seguridad.

Se ha decidido, por motivos de rendimiento de los equipos, poner soluciones antivirus en los servidores pero no en los ordenadores de los empleados de oficina.

¿Lo consideras seguro?¿Por qué?

Posibles defensas

- Implementar lo que se conoce como **la regla del mínimo privilegio**. Con este nombre tan descriptivo esta regla viene a decir que no se otorguen más que los permisos necesarios a los usuario que los necesitan para su trabajo y ninguno más.
- Realizar una **segmentación de red** adecuada. Esto quiere decir que los diferentes recursos estén en diferentes redes, de tal forma que gente que para nada los necesita, no puedan tener acceso a ellos de ninguna forma.
- Integrar la seguridad dentro del ciclo desarrollo del software y no al final del mismo.
- Monitorización de la red y los endpoints (equipos finales, de usuario).

Man in the Middle (MITM)

Este ataque se produce cuando el cibercriminal se interpone en una transacción entre dos partes. Tras interrumpir el tráfico, sin el conocimiento de las partes obviamente, el atacante puede filtrar y robar datos.

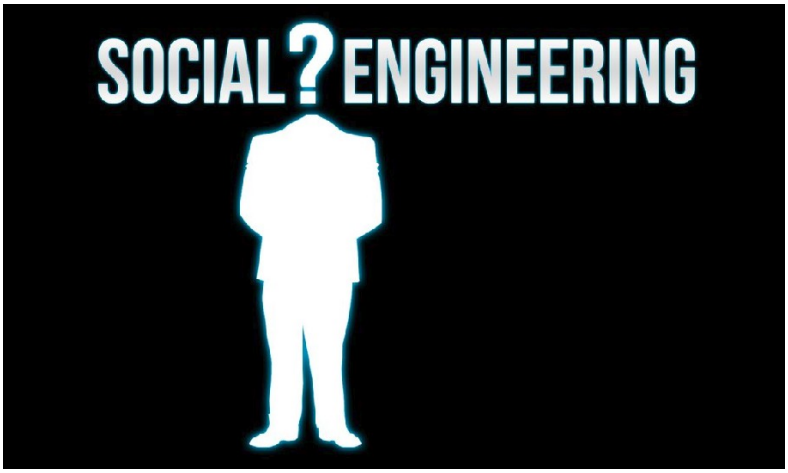
shutterstock.com · 2077888264

Este tipo de riesgo en las empresas se sufre cuando por ejemplo un visitante externo se conecta a nuestra WiFi pública si esta no está todo lo bien protegida que debería. El atacante se interpondrá entre la red y el visitante, pudiendo hacer uso de otras técnicas para realizar el daño deseado.

Estos ataques se pueden paliar cifrando todas las comunicaciones y utilizando autenticación multifactor.

Ingeniería social

La ingeniería social es la versión moderna de los estafadores o timadores. Son atacantes que mediante el arte de la sugestión intentan ganarse la confianza de usuarios autorizados para que les proporcionen sus credenciales.



Este tipo de criminales aprovechan en la naturaleza bondadosa de la gente a la hora de brindar ayuda, explotando gracias a ellos las debilidades que hayan detectado en la persona.

Los empleados deben estar bien formados para poder identificar y evitar este tipo de ataques.

Ejercicio

Visualiza las siguientes escenas de ingeniería social. Busca en Internet técnicas que utiliza la ingeniería social e identíficalas en cada escena. Siguiendo el mismo procedimiento, indica de qué forma podría haberse evitado en cada caso.

- Escena 1: https://acortar.link/qXcx3Z y https://acortar.link/wzAGSf
- Escena 2: https://www.youtube.com/watch?v=fHhNWAKw0bY
- Escena 3: https://www.youtube.com/watch?v=YmGwdoS706M

Phishing

Técnica que, haciendo uso de la ingeniería social, intenta engañar o manipular a la víctima para que le proporcione información sensible.

Se ha ido sofisticando con el tiempo pero suelen tratarse de mensajes, vía email o SMS que falsean la dirección de un remitente para simular ser una comunicación legítima. Dentro del mensaje se suele incluir un link donde introducir la información demandada pero que en realidad es una página falsa.

Spear phising

Son ataques dirigidos con el fin de aumentar la probabilidad de llegar a buen término. En lugar de realizar un envío de correo masivo confiando en que alguno de los receptores "pique", lo que se hace es una investigación del objetivo del ataque. De esta forma el mensaje parecerá mucho más convincente y la tasa de éxito aumenta.

Por ejemplo, pueden hacerse pasar por el departamento de informática para pedirte que confirmes algo haciendo click en algún sitio.

Smishing y vishing

El *vishing* es un fraude, similar al *phising,* pero de carácter telefónico. Se recibe una llamada de alguien que se hace pasar por una persona o entidad de confianza, como por ejemplo un banco o compañía de suministro de servicios (eléctrica, gas…) y que, utilizando ingeniería social, pretende hacerse con algún dato personal.

Las medidas preventivas que se pueden llevar a cabo son:

- Sospechar de llamadas de números desconocidos
- No facilitar información personal ni comprometedora por teléfono
- No dejarse llevar por ofertas atractivas o excesivamente buenas
- Si se tienen dudas de la veracidad, contactar directamente con la entidad que supuestamente nos contacta a nosotros

El *smishing* es otro tipo de fraude que entra dentro de esta misma categoría, conservando la herramienta del teléfono pero en este caso haciendo uso de los mensajes SMS. Un ejemplo

relativamente reciente fue una serie de mensajes que se enviaban en nombre de correos informando de un pago de aduanas pendiente para poder entregar un paquete. Al acceder a la página, la víctima pensaba que hacía un pago legítimo cuando en realidad le estaba proporcionando sus datos a un impostor:

Este tipo de mensajes en épocas propicas como Navidades o Black Friday pueden tener una tasa de éxito mucho más alta de la que debería.

Whaling

El Whaling es un tipo de *phising* muy específico, de hecho casi podríamos decir que es un *spear phising* hiperconcreto. Esta concreción se traduce en tener como objetivos a ejecutivos de muy alto nivel en la empresa víctima.

Tras una investigación previa y una minuciosa planificación, se envía un email a una persona de alto rango de la empresa o con algún rol clave (autorizado para pagos, por ejemplo), generalmente haciéndose pasar por alguien también de alto rango.

Estos emails intentan apoyarse en la confianza, haciendo uso de información personalizada, para realizar peticiones urgentes de pagos o transferencias, de credenciales, de acceso a alguna web fraudulenta o click a algún archivo adjunto.

En ocasiones incluso, para mayor credibiidad, seguidamente al email se produce una llamada telefónica también fraudulenta.

Las consecuencias de este tipo de ataques pueden ser desastrosas, desde una gran pérdida económica hasta una exfiltración de datos sensibles de la empresa.

Un ejemplo muy claro de este tipo de fraudes son las llamadas **“estafas del CEO”.**

Ejercicio

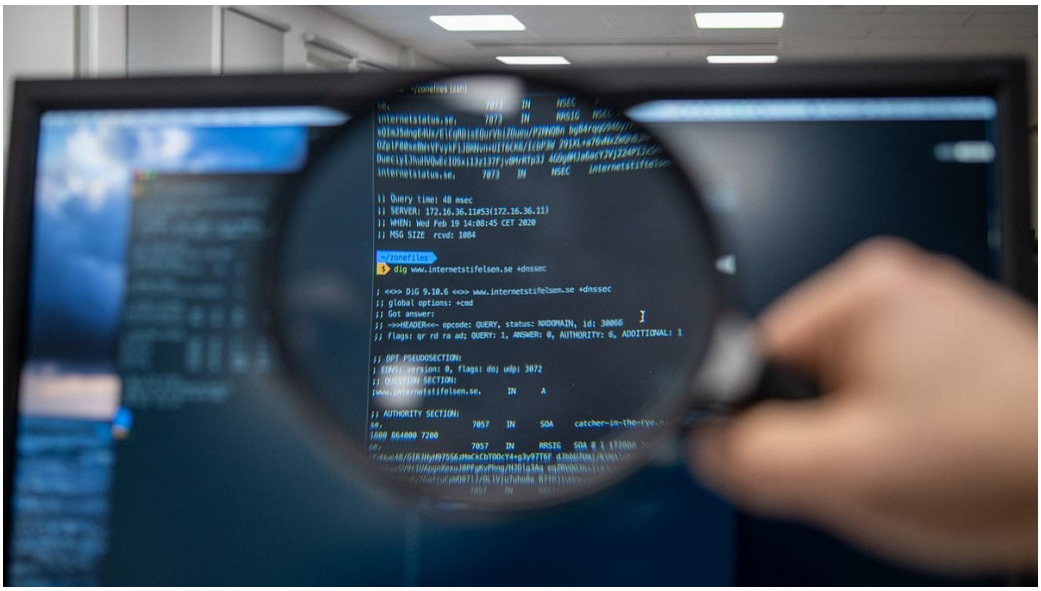
Busca en Internet en qué consiste la estafa del CEO y descríbela con tus palabras. Busca además algún ejemplo que haya ocurrido en los últimos 5 años en España.

Como todos los tipos de ataques de phising, algunas formas de hacer frente a esto son:

- Pecar de desconfiado ante emails mínimamente “raros”
- Intentar hacer uso de la racionalidad y no dejarse llevar por emociones como el miedo o la curiosidad, que son precisamente de las que el criminal intenta aprovecharse.
- Comprobar minuciosamente el remitente o URLs adjuntas en busca de pequeños cambios tipográficos en la dirección
- Evitar descargar imágenes y/o archivos adjuntos si se tiene el mínimo atisbo de duda

SQLi

SQL (Structured Query Language) es un lenguaje que permite interactuar con las bases de datos, realizando consultas de información, insertar/eliminar datos o actualizar los existentes entre otras cosas.



La inyección SQL hace referencia a un ataque muy popular desde hace muchos años y que consiste, normalmente, en atacar una aplicación web intentando introducir sentencias maliciosas para acceder de forma no autorizada al contenido de la base de datos.

A pesar de que, precisamente por ser tan popular y común, ya hay multitud de defensas contra este tipo de ataque, sigue siendo de los más utilizados con tasas de éxito relativamente altas. Algunos ejemplos:

- El 19 de mayo de 2016 un atacante logró acceder y difundir los datos de 5540 agentes de los Mossos d'Esquadra mediante una vulnerabilidad de tipo SQL injection en la página web de cursos su sindicato.
- En 2011, a partir de un SQLi, el grupo Lulzsec se atribuye el **robo de datos personales de un millón de usuarios de Sony Pictures Entertainment**, la división de cine de Sony.
- En 2020 la base de datos del sistema central de salud en Estonia fue atacada y compometida mediante una vulnerabilidad SQLi, exponiéndose datos personales de sus usuarios, por lo que hablamos de un profundo impacto en la privacidad.

Ataques de contraseñas

Es un vector de ataque típico usado para comprometer la autenticación de los usuarios y a partir de ahí escalar privilegios en el sistema si fuese necesario. Es una de las formas más comunes en las que los sistemas son comprometidos.

Un password comprometido puede tener grandes repercusiones como fraude financiero, un DDoS o el robo de información sensible.

Un caso muy sonado fue el de Twitter en 2020, cuando unos ciberatacantes adolescentes consiguieron las credenciales de trabajadores de Twitter. Tras ello, las utilizaron para comprometer cuentas de alto perfil y renombre, con las que twittear pidiendo bitcoins, a modo de estafa. Las acciones de Twitter bajaron un 4%.

Algunos tipos de ataques de contraseñas son:

- **Phishing**
- **Fuerza bruta.** Si un password es la llave que abre un candado, la fuerza bruta sería usar una radial. El atacante prueba millones de permutaciones de letras, números y símbolos para poder adivinar una contraseña de usuario.

A pesar de ser un método antiguo, la potencia de las tarjetas gráficas hacen que este proceso aún merezca la pena en algunos casos pues es muy fácil de automatizar.

Se puede combatir limitando el número de logins fallidos en un lapso de tiempo razonable o provenientes de la misma IP, además de utilizando contraseñas lo suficientemente complejas.

- **Ataques de diccionario.** En este caso la técnica incluye la preparación de una lista o diccionario que son susceptibles de ser usados como password.

  Esta lista se elabora analizando los patrones y comportamientos a la hora de establecer contraseñas en otros ataques que hayan tenido éxito. Con esta información, el diccionario se configura alterando sufijos y prefijos o añadiendo términos comunes.

  así como listas obtenidas a partir de la vulneración o compromiso de los sistemas de otras empresas y con las que se comercia en el mercado negro. Esta es la razón por la que cuando se conoce una brecha de seguridad, se recomienda cambiar el password. Por el mismo motivo se recomienda no compartir contraseñas entre distintos servicios en Internet.

  Para prevenirlos:

  - Nunca usar “palabras de diccionario” como contraseña. Mejor utilizar una combinación de letras, números y símbolos con una longitud decente.
  - Bloquear cuentas después de muchos intentos de login fallidos.
  - Utilizar un gestor de contraseñas que genere contraseñas aleatorias y complejas (los navegadores web por ejemplo suelen tenerlo por defecto).

- **Password spraying.** Se aprovecha de algo que ya se ha comentado más arriba; cuando unas credenciales son vulneradas en una brecha de seguridad, los atacantes se dedican a

probar esas mismas credenciales en multitud de sitios web antes de que las víctimas las cambien.

- **Keylogging.** Los keyloggers son un tipo de software que, usado maliciosamente por parte de un atacante, permite registrar todas las pulsaciones de teclas que se producen. De esta forma, si la víctima introduce sus credenciales en algún momento, éstas quedaran registradas y a disposición del cibercriminal.

  A modo de prevención:

  - Examinar físicamente nuestro ordenador puesto que el kelogger puede ser hardware también.
  - Hacer uso de protección antivirus/EDR.
  - Utilizar autenticación multifactor (SMS, código de seguridad, biometría…).

Ejercicio

Imagina que eres un consultor experto en ciberseguridad y acudes a una empresa cliente:

1. ¿Qué consejos darías en una empresa para tener una política de contraseñas fuertes y seguras?

2. ¿Es necesario cambiar la contraseña cada cierto tiempo? Busca razones que avalen que no haga falta.

Ayúdate de una búsqueda en Internet.

Internet of Things (IoT)

La llegada del 5G nos ha traído una serie de novedades y una de las más grandes es la eclosión del IoT o Internet de las Cosas. Este término hace refererencia a la capacidad de poder conectar prácticamente cualquier dispositivo a Internet: dispositivos domésticos de uso común (frigoríficos, lavadoras…), bombillas, dispositivos médicos, prendas de vestir y wearables, crear las denominadas *ciudades inteligentes*.

¿Por qué suponen una amenaza? El IoT, aunque cada vez más conocido, continúa siendo una tecnología relativamente nueva y poco madura en la industria. Este tipo de dispositivos abren una puerta gigante a la red a la que estén conectados, permitiendo múltiples puntos de entrada. Basta recordar el caso en 2018 de un casino en Las Vegas que sufrió un ataque a través **una pecera**.

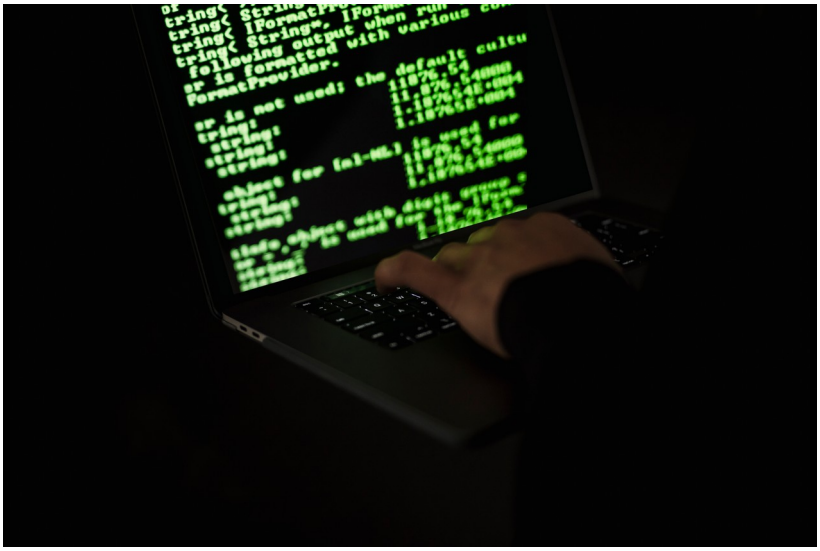
Esto quiere decir que aún no están suficientemente investigados sus riesgos en cuanto a seguridad y es que, además, los propios fabricantes aún no ponen el suficiente empeño en proteger sus dispositivos IoT. Como muestra algunos botones:

- En 2016 un malware conocido como Mirai infectó miles de cámaras de videovigilancia IP, conformando una gigantesca botnet que se utilizó más tarde para lanzar ataques de tipo DDoS.
- También en 2016 un cibercriminal logró comprometer y controlar la cámara-monitor que utilizan los padres para vigilar a los hijos.

Algunas de las precauciones que deberían tomarse son cambiar las contraseñas por defecto de estos dispositivos y considerarlos un activo más a proteger dentro de la red en la que estén ubicados.

Emotet

Se trata de un malware que fue identificado por primera vez en el año 2014 y clasificado como un troyano bancario. Es decir, este malware en sus orígenes infectaba los ordenadores para intentar extraer o robar información confidencial y privada de carácter financiero.



Mientras la *"fama y la gloria"* se la llevaban otros malwares como Wannacry o Lockbit, Emotet fue gestándose a fuego lento y con un perfil bajo a lo largo del tiempo y esto le permitió evolucionar y mutar a otros tipos de malwares más dañinos.

El principal medio de transmisión de Emotet fue el spam vía email. Correos que solían incluir archivos de Office infectados o links maliciosos.

Como decimos, Emotet ha pasado ya por varias versiones, cada vez más sofisticadas. La actual es de carácter modular, es decir, cuando este malware infecta a su víctima es capaz de contactar con un servidor externo para descargar e instalar módulos externos que aportan nuevas funcionalidades, tales como:

- Robar credenciales de cuentas de correo electrónico
- Obtener nombres de usuario y contraseñas almacenadas en el navegador web
- Realizar ataques DDoS (denegación de servicio distribuido).
- Instalar otros malwares

Tal es la sofisticación de este malware y, por tanto, tan grande su amenaza que es capaz de descubrir la mejor vía para monetizar la infección de la máquina donde acaba de alojarse, considerando diferentes escenarios:

- ¿El historial de navegación de este ordenador muestra visitas frecuentes al sitios bancarios? Despliega entonces los módulos dedicados a robar credenciales y transferir dinero.
- ¿Es el dispositivo que acabo de infectar un portátil de última tecnología tope gama? Posible indicativo de que la víctima tiene dinero, despliega módulos de ransomware y criptominado.
- ¿Es esta máquina un servidor en una red con gran ancho de banda? Instala los módulos para distribuir malware por la red via email.

2. Herramientas y soluciones de ciberseguridad

Introducción

Vivimos un contexto actual donde la información es el activo más importante de una empresa, por lo que el cibercrimen, tal y como veíamos en el bloque anterior, es un negocio lucrativo. El cibercrimen ya está lejos de ser considerado como una amenaza residual y un negocio de nicho. Se ha convertido, por méritos propios, en todo un mercado donde se mueven ingentes cantidades de dinero.

Todo lo mencionado ha hecho que la regulación haya ido evolucionando, las leyes y normativas cada vez más refuerzan la protección de los datos de todo tipo y poner mayor énfasis en las negligencias de su cumplimiento.

Por todo ello, una empresa debe ser consciente de todas las herramientas y soluciones de ciberseguridad que tiene a su alcance para poder hacer frente a ellas de una forma altamente satisfactoria.

Está claro que es literalmente imposible tener la certeza de estar 100% protegidos frente a cualquier tipo de amenaza pero debemos conocer todas las opciones a nuestra disposición para reducir al máximo nuestra superficie de ataque.

Herramientas y soluciones de ciberseguridad

Antivirus/EDR/XDR

Un antivirus es un software que está diseñado principalmente para detectar y eliminar varios tipos de malware. Una vez instalado en nuestro ordenador, suele ejecutarse en un segundo plano para proporcionar una protección en tiempo real.

Los antivirus suelen proporcionarse con una información actualizada de los virus conocidos en ese momento. No obstante, *"los malos"* no descansan nunca y siguen apareciendo nuevas amenazas día a día. Por este motivo, los antivirus van recibiendo actualizaciones periódicas de los nuevos descubrimientos de malware ya que, de otra forma, serían un producto inservible.

Así pues, ya hemos dicho que los antivirus contienen una base de datos con información concerniente a los malwares a detectar. Estos datos se conocen como **firmas** y no son más que una secuencia concreta de bytes que identifican a un virus/malware.

Cuando se escanean los archivos de un ordenador y se detecta una de estas secuencias en cualquier archivo, automáticamente se clasifica como malware y se pone en cuarentena o se elimina, dependiendo de la configuración del antivirus.

El método descrito arriba, basado en firmas, es un **enfoque reactivo** en cuanto a la lucha contra el malware, ya que intentan resolver el problema cuando éste ya se ha producido. Además, adolece de cierta obsolescencia si lo miramos desde 3 ángulos:

1. Si nos basamos en *firmas* de virus ya conocidos y detectados, nunca podremos detectar virus que sean de reciente aparición, únicamente aquellos que ya han infectado otras máquinas, han sido reportados y caracterizados para ser incluidos en la base de datos del antivirus.
2. Relacionado con el punto anterior, por pura lógica existe un lapso de tiempo entre que se identifica un nuevo malware y se genera la firma correspondiente para actualizar la base de datos del antivirus. Duranto la duración de esta ventana temporal el usuario del antivirus queda desprotegido ante la nueva amenaza.
3. Cada día se generan cantidades ingentes de malware nuevo y, además, este malware es mucho más moderno y sofisticado ya que emplea técnicas de ofuscación para evitar ser detectados por firmas.

El otro enfoque que se puede tomar y que, de alguna manera, suple las carencias del anterior, es el **enfoque proactivo,** también conocido como detección ***heuristica***. Este método se basa en buscar propiedades sospechosas en la ejecución de programas, es decir, busca comandos o instrucciones que no estarían presentes en una aplicación inocua.

Imagen comparativa

El análisis heurístico puede ser de dos tipos:

- Estático: Se examina el código de la aplicación o programa en busca de instrucciones maliciosas

- Dinámico: Utiliza una máquina virtual conocida como *sandbox,* esto es, se simula un sistema real en un entorno aislado y seguro, para que el malware no haga daño al sistema real.

Cabe decir que esta técnica no sustituye por completo a la basada en firmas, sino que la complementa. Y esto lo hace porque permite detectar un malware que aún no posea una firma o que haya sido descubierto pero cuya firma aún no haya sido introducida en la base de firmas del antivirus del usuario.

Este método además se basa en inteligencia artificiar y aprendizaje automático para detectar nuevas amenazas.

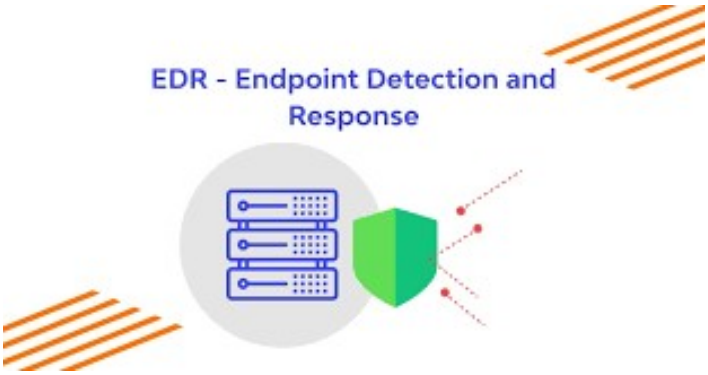
No obstante y como pasa con cualquier tipo de defensa, no todo es de color de rosas. La detección heurística viene marcada por los falsos positivos (programas inocuos que son clasificados como malware por error) y por los recursos que necesita utilizar de nuestro ordenador, pudiendo afectar a otras tareas que estemos realizando en ese momento.

EDR (Endpoint Detection and Response)

Estas siglas hacen referencia a un tipo de herramientas dedicadas a detectar e investigar amenazas en los endpoints. **Se denomina endpoint a cualquier dispositivo informático conectado a una red y que se comunica con ella.**

Un EDR proporciona una protección en distintas capas y para ello combina la monitorización en tiempo real con el análisis de datos del endpoint en base a unas reglas que permiten una respuesta automática.

¿Por qué utilizar un EDR? Los estudios estiman que un 90% de los ciberataques *exitosos y* un 79% de las fugas de datos se originan en los endpoints.



¿Cuál es la diferencia con un antivirus? Dependiendo del fabricante, los EDR pueden variar sus funcionalidades aunque combinan 5 capacidades principales:

1. Recolección continua de los datos del endpoint: Un EDR está continuamente analizando datos de todo tipo; datos de procesos, cambios en la configuración, conexiones de red, bajada o transferencia de ficheros, comportamiento del usuario y/o dispositivo…

   Para este cometido los EDR suelen instalar un pequeño software, conocido como agente, en el endpoint que se encarga de la recolección de datos.

2. Análisis en tiempo real y detección de amenazas: Los EDR utilizan análisis avanzados y algoritmos de **machine learning** para identificar patrones que puedan coincidir con actividades maliciosas.

Los EDR por lo general buscan dos indicios; los *indicadores de compromiso* (**IOC**), que son acciones o eventos que denotan un potencial ataque y los *indicadores de ataque* (**IOA**) que son eventos que se relacionan directamente con ciberamenazas o cibercriminales conocidos.

3. Respuesta automática frente a amenazas: Como ya hemos dicho, esta respuesta está automatizada en función de unas reglas que haya configurado el administrador o en comportamientos “aprendidos” en el tiempo. Por poner algún ejemplo de este tipo de respuestas automatizadas:

   - Priorizar alertas en función de su severidad
   - Desconectar el endpoint de la red o desconectar a un usuario
   - Lanzar el antivirus para escanear otros endpoints de la red en busca de un mismo riesgo

4. Investigación y remediación: Una vez se ha aislado la amenaza, un EDR proporciona herramientas para una investigación en profudidad. Estas herramientas van desde datos para un análisis forens o identificación delos archivos impactados hasta identificar las vulnreabilidades que han sido aprovechadas.

5. Apoyo al *threat hunting:* El threat hunting es una disciplina que consiste en peinar la red en búsqueda de amenazas aún desconocidas. Sabemos que cada nueva amenaza puede estar en activo durante meses hasta que es detectado, es por ello que este ejercicio es tan importante.

Los EDR proporcionan herramientas para ayudar a este cometido.

Ejercicio

Haz una búsqueda en Internet e intenta encontrar y definir:

- 5 indicadores de compromiso (IOC)

- 5 indicadores de ataque (IOA)

XDR (Extended Detection and Response)

Se trata de un tipo de arquitectura que unifica datos de varias herramientas y en distintas capas (usuarios, endpoints, email, cloud…). XDR elimina los vacíos de visibilidad entre distintas herramientas dedicadas a la protección en materia de ciberamenazas, ya que éstas serán capaces de compartir datos entre ellas.

Es común que una empresa tenga en funcionamiento varias herramientas de seguridad, cada una especializada en una telemetría diferente. El problema es que no interactúan entre ellas y deja a los equipos de seguridad la tarea de correlar toda esta información de forma manual, intentando separar falso positivos de potenciales incidentes.

Típicamente un XDR está basado en la nube, es decir, se trata de un **Saas (Software as a Service**).

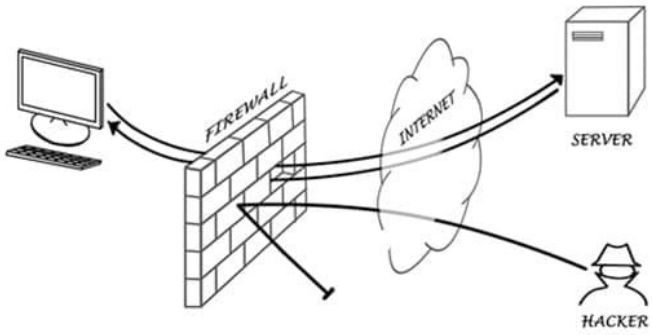
Algunos investigadores consideran los XDR como un *EDR vitaminado* puesto que sus funciones son similares, añadiéndole la capacidad de compartir su información.

Información extendida

Firewall

Un firewall es un dispositivo de seguridad de red. Su función es la de monitorizar las conexiones o el tráfico de red entrante y saliente y permitir o bloquear estas comunicaciones en función de unas reglas que le configuremos. Un firewall puede ser hardware, software o ambos.

Se basan en la sencilla idea de que el tráfico que proviene de un entorno menos seguro ha de ser inspeccionado antes de que pase a otro más seguro.



Los firewalls han sido la primera línea de defensa en seguridad de la red durante más de 25 años. Como hemos dicho, etablecen una barrera entre las redes internas seguras, controladas y fiables y las redes externas poco fiables como Internet.

A pesar de que un firewall por sí solo ya no es suficiente para proteger nuestra empresa, se considera la primera línea *de combate* que se ha de establecer.

Ejercicio

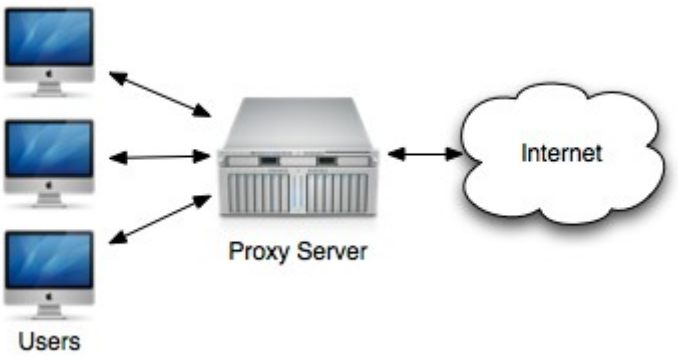
Haz una búsqueda en Internet y descubre que es el *"Proyecto escudo dorado"*.

Indica qué tipos de contenido se bloquean y algunas técnicas que puedan emplearse para saltarse esos bloqueos, a priori.

Proxy

Un servidor proxy es un sistema o un router que proporciona una pasarela de paso entre los usuarios e Internet. De esta forma, al contar con este servidor intermediario, se intenta impedir que los ciberatacantes tengan acceso a una red privada.

Podemos decir que, de alguna forma, cuando los usuarios acceden a Internet, lo hacen de tal manera que es el proxy el que *da la cara* por ellos.



Los proxys proporcionan una capa de seguridad bastante útil. Se pueden utilizar como firewalls o como filtros web, protegiendo a los usuarios del malware. Este filtro web puede configurarse de una forma muy versátil, no permitiendo el acceso a webs que entren dentro de diferentes categorías (malware, descargas, violencia, sexo…), impidiendo descargar según qué archivos u otras.

Cuando utiliza un proxy, el navegador se conecta primero al proxy y este redirige el tráfico al sitio web. Por eso los servidores proxy también se denominan “proxies de reenvío”. El proxy también recibe la respuesta del sitio web y se la envía de vuelta al navegador.

Otra utilidad de estos servidores es la de mejorar la disponibilidad. Si tenemos una aplicación web que recibe muchas visitas y necesitamos varios servidores para poder ofrecer el servicio, podremos utilizar un servidor proxy delante de ellos que se encargue de balancear o repartir a los usuarios de forma equitativa entre todos ellos.

Cifrado punto a punto – VPN (Virtual Private Network)

En 2020, debidos a unos hechos que todos recordamos a raíz de la pandemia, muchos trabajos pasaron a realizarse de forma remota desde casa. Esto provocó una eclosión del uso de las VPN para establecer conexiones seguras desde los hogares hasta las redes corporativas.

Hoy, a pesar de que todo ese trabajo remoto parece que en su gran mayoría ha ido volviendo a las oficinas, las VPN continúan siendo un punto muy importante ya no sólo para las grandes empresas, sino también para las PYME.

Una conexión VPN establece una especie de *túnel* entre el dispositivo del usuario y un servidor remoto. Dicho de otro modo y aplicado al caso que nos ocupa, desde el hogar del trabajador se

establece un túnel completamente seguro hasta la red interna de la empresa y todo ello a través de la red más insegura, Internet.

Cuando estamos conectados mediante VPN a la red corporativa al ordenador se le otorga una IP (dirección que identifica a un ordendor dentro de una red) de la red de la empresa por lo que, en principio y a todos los efectos, es como si estuviéramos sentados en un ordenador en nuestra oficina.

Si lo pensamos bien, ¿cómo podemos establecer una conexión segura entre dos puntos si lo vamos a hacer a través de la red más insegura de todas, Internet? La respuesta es, cifrando toda la información.

Cuando se cifra la información lo que se está haciendo es convertir datos legibles en ilegibles mediante el uso de un algoritmo matemático. Esta información sólo podrá descifrarse con la clave adecuada. Esto hace que si un posible atacante intentara interceptar nuestro tráfico, podría descubrir que estamos haciendo uso de una VPN pero sería incapaz de extraer los datos de ella al no poseer la clave de descifrado.

Autenticación multifactor

La autenticación multifactor (MFA) es un método, valga la redundancia, de autenticación en la que se necesitan dos o más verificaciones para quedar autorizado en una aplicación, en una VPN o en cualquier otro servicio.

En lugar de utilizar únicamente un nombre de usuario y una contraseña, se necesitan más factores para asegurarse de que el usuario es legítimo. Idealmente una autenticación multifactor para los usuarios debe quedar definida por:

- Algo que poseen: una llave o tarjeta de identificación p.ej.
- Algo que sabe: un PIN o un password.
- Algo que se es: huella dactilar, iris del ojos, voz, reconocimiento facial.

Un ejemplo muy claro de autenticación multifactor es cuando un banco nos pide que además de identificarnos con nuestro DNI y nuestro PIN, introduzcamos un código que nos envían al móvil y que es de un solo uso.

Ya vimos en el bloque anterior de amenazas que este método nos protege de riesgos tales como el Man-in-the-Middle, el Keylogging o la fuerza bruta.

Ya son numerosos los servicios en Internet que permiten configurar al menos un segundo factor de autenticación: Gmail, Facebook, GitHub, Linkedin…

El factor que, adicionalmente a nuestras credenciales, proporcionamos, se conoce como **OTP o One-Time Password**. Un OTP es un código generado de forma periódica y que se envía en cada solicitud de autenticación. Este valor se genera a partir de lo que se conoce como *semilla* original y de forma *aleatoria*.

Sistemas físicos (biométricos)

En la MFA, otro factor que puede entrar en juego es la autenticación biométrica. Es decir, factores inherentes a cada persona que permiten identificarla unívocamente; reconocimiento facial, huella dactilar, lectura del iris del ojo, reconocimiento de voz… No obstante, nada esta libre de inconvenientes, como vemos en la tabla a continuación.

	Ojo - Iris	Ojo - Retina	Huellas dactilares	Geometría de la mano	Escritura - Firma	Voz
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta
Prevención de ataques	Muy Alta	Muy alta	Alta	Alta	Media	Media
Aceptación	Media	Media	Media	Alta	Muy alta	Alta
Interferen-cias	Gafas	Irritaciones	Suciedad, heridas, asperezas ...	Artritis, reumatismo ...	Firmas fáciles o cambiantes	Ruido, resfriados ...

Ejercicio

Vamos a configurar un segundo factor de autenticación en algún servicio común (Linkedin, Facebook, Instagram…).

Cifrado de datos en los equipos (incluidos dispositivos móviles)

Con el fin de proteger la información sensible o confidencial corporativa, es necesario el uso del cifrado en la misma. Ya hemos comentado antes grosso modo que el cifrado de datos deja la información ilegible para todo aquel que no posea la clave correcta de descifrado.

La información es el activo más importante de una empresa y por tanto, cualquier empeño en protegerla es poco.

Así las cosas, deberemos realizar una clasificación de nuestra información y decidir cuál necesita estar cifrada.

Tanto las comunicaciones (email, web, VPN) deben estar cifradas pero también aquellos datos sensibles o con planes estratégicos de la empresa, además de los backups o copias de seguridad que vayamos realizando.

Debido a políticas empresariales de BYOD (Bring Your Own Device) o simplemente a dispositivos corporativos en trabajadores móviles (comerciales, técnicos que visitan clientes…), todos los dispositivos móviles suponen un riesgo. Para protegernos de robos, pérdidas, despistes o cualquier otro inconveniente, estos dispositivos también deberán incluirse en esta política de seguridad de cifrado de datos.

En el caso de dispositivos móviles además debería ir acompañado de otras precauciones como la geolocalización, el bloqueo remoto de dispositivo o el borrado remoto de datos.

Análisis de vulnerabilidades

Un análisis de vulnerabilidades es un proceso que nos permite buscar, detectar, clasificar y priorizar las deficiencias en nuestras aplicaciones y sistemas, con el fin de ponerles la mejor solución posible.

Para este cometido se puede hacer uso de un producto software conocido como escáner de vulnerabilidades. Suelen ser aplicaciones que permiten automatizar el análisis de vulnerabilidades. No son una solución perfecta en la que depositar el 100% de nuestra confianza sino que más bien deben ser concebida como una ayuda a la tarea de reforzar la ciberseguridad de la empresa junto con la acción humana.

Se pueden realizar de diferentes maneras; de forma externa, interna, con algún usuario autenticado o sin autenticar, más o menos intrusivos… En cualquier caso, es un proceso que

debiera realizarse de forma periódica, investigando las vulnerabilidades que se reporten en función de su importancia/severidad/gravedad para decartar falsos positivos y ponerle solución lo antes posible a los auténticos positivos.

Las mejores prácticas incluyen:

- Analizar todos los activos de la red
- Realizar el escaneo de forma regular ya que aunque se mantenga el número de activos, pueden aparecer nuevos riesgos.
- Asignar responsables para los activos críticos, que puedan tomar las decisiones oportunas.
- Establecer un proceso de parcheo y/o corrección que, en función de la importancia de la vulnerabilidad, vaya solucionando los problemas encontrados de forma eficiente.
- Generar informes a partir de estos análisis

Backups

Es **absolutamente imprescindible** realizar backups de la información importante de nuestra empresa.

Como hemos visto antes, cada empresa debe identificar qué datos quiere proteger mediante copia de seguridad. Hay tres tipos de copia:

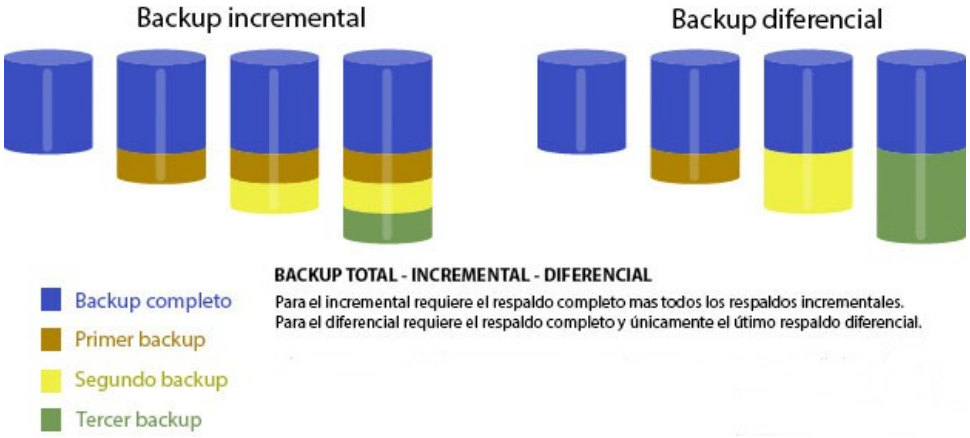
- **Completa**. Incluye toda la información identificada. Si era una unidad de disco, todos los archivos y carpetas que contiene; si era una base de datos, la exportación de todas sus tablas.
- **Diferencial.** Incluye toda la información que ha cambiado desde la última vez que se hizo una copia de seguridad completa. Por ejemplo, si el lunes se hizo una completa y el martes solo ha cambiado el fichero a.txt, en la cinta del martes solo se escribe ese fichero. Si el miércoles solo ha cambiado el fichero b.doc, en la cinta del miércoles se escribirán a.txt y b.doc.

  Para la restauración, se debería utilizar la última copia completa + la última diferencial, siendo así la restauración más rápida.

- **Incremental**. Incluye toda la información que ha cambiado desde la última copia de seguridad, sea esta del tipo que sea. En el ejemplo anterior, la cinta del martes llevará el fichero a.txt, pero la cinta del miércoles solo b.doc.

  La ventaja de este tipo de copia de seguridad es que se puede hacer tantas veces como se quiera dado que el aumento de almacenamiento no será muy significativo, así como tampoco la rapidez con la que se realiza esta copia.

  Para restaurar, se debería utilizar la última copia completa + las copias incrementales acumuladas hasta la fecha del fallo

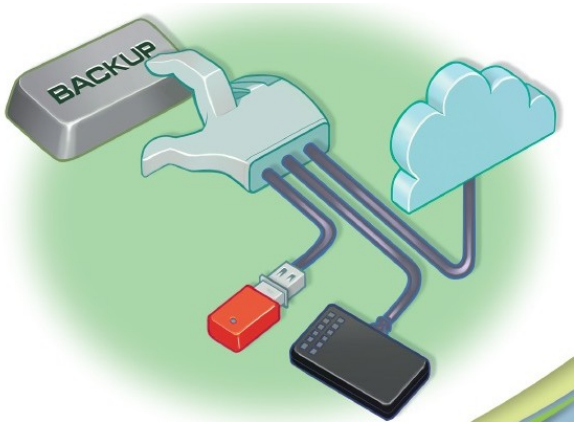


Una empresa podría decidir hacer todos los días copia completa. Pero, si hay muchos datos, es un proceso lento y algo arriesgado, porque hay que vigilar que se esté haciendo una copia consistente de la información (mientras se hace la copia, el sistema sigue funcionando y en cualquier momento alguien puede introducir cambios). Con la copia diferencial o incremental tenemos las mismas garantías, porque recuperamos la información aplicando la última cinta completa y la última diferencial (o la última completa y todas las incrementales).

En una empresa mediana es habitual el esquema de diez cintas:

- Una para un backup completo (los viernes).
- Cuatro para un backup parcial diario (diferencial o incremental) de lunes a jueves.
- Cinco para backups completos anteriores: quincenal, mensual, trimestral, semestral y anual.

Elegir entre diferencial o incremental para el backup diario depende de cada empresa. Si hay poca actividad diaria, se puede permitir el diferencial, porque aporta la ventaja de que cada cinta diaria tiene toda la información necesaria para recuperar ese día (en el incremental, si perdemos la cinta de un día, puede que tenga ficheros que no estén en las cintas siguientes). Pero si hay mucha actividad, estamos de nuevo ante el problema de mantener la consistencia de la copia.



También cabe destacar que una de las reglas más recomendadas para realizar backups es la conocida como la estrategia 3-2-1:

- Se deben tener 3 copias de los datos, el original y dos más.
- Se deben utilizar 2 formas de almacenamiento diferente: Cintas, discos duros externos, cloud, NAS, SAN…
- Al menos una de las copias debe estar ubicada, físicamente, fuera de la empresa para tener protección frente a desastres físicos.

Esta estrategia nos ofrece una protección más que suficiente frente a posibles desastres.

Como último, cabe destacar que igual de importante que realizar el esfuerzo de mantener las copias de seguridad, se deben realizar tests para comprobar que éstas pueden ser restauradas sin problemas, manteniendo la integridad. De poco sirve tener copias de seguridad de todos los datos si antes no se ha probado que la restauración funciona sin problemas.

Ciberseguros

No son más que el concepto de los seguros tradicionales pero aplicado al mundo de la ciberdelincuencia.

Si los riesgos de los que queremos defendernos necesitan una infraestructura que nosotros no podemos asumir, es posible estudiar la transferencia del riesgo a un tercero.

La empresa aseguradora evaluará el nivel de seguridad de nuestra empresa y exigirá las correcciones o mejoras necesarias para alcanzar un nivel óptimo de seguridad antes de poder contratar el ciberseguro. Este ciberseguro puede cubrir cosas como:

- Daños en los sistemas informáticos
- Robo de datos
- Ataques de denegación de servicio (DoS)
- Recuperación de cuentas o datos perdidos
- Restauración de backups
- Responsabilidad civil

Sin embargo, se debe tener en mente que el ciberseguro es un complemento, no una solución integral de ciberseguridad para nuestra empresa. Deberá ir acompañado de las medidas de seguridad propias de la empresa.

Formación a empleados

Si echamos un ojo a las mayores brechas de seguridad o a los más dañinos ataques de ransomware con infección via phishing, está claro que el eslabón más débil de la cadena siempre es el ser humano.

De nada sirve tener los más avanzados sistemas de ciberdefensa si no lo acompañamos del fortalecimiento de la mayor debilidad, los empleados. Esto se consigue con una formación continua y actualizada.

Es fundamental que los empleados reciban una formación que les permita identificar un posible riesgo de seguridad y con quién contactar en caso de sospecha. Además, esta formación debe ir desde el nivel más bajo de personas que trabajen con recursos TI hasta el nivel más algo de gerencia.

La formación de empleados puede parecer a priori un coste pero no es más que una inversión ya que a largo plazo reduce riesgos y costes. Algunos de los aspectos sobre los que se puede educar a los empleados son:

- Identificación y protección ante el phishing
- Navegación segura en Internet
- Uso seguro de contraseñas
- Uso seguro y responsable de dispositivos móviles
- Identificación y protección frente a la ingeniería social

Esta formación debe resultar atractiva de cara a los empleados para que sea lo más útil posible. Para ello se puede optar por la gamificación y/o adaptación al día a día real de los puestos de trabajo, entre otras.

Antispam/antiphising

Las soluciones antispam/antiphising pueden ser tanto software como hardware (Cisco ESA por ejemplo).

Estos sistemas están dedicados a inspeccionar los emails que se reciben, en busca de indicios de emails no deseados o dañinos. Es decir, el destinatario sólo recibirá los emails que han pasado por un proceso previo de filtrado con el fin de asegurar que son legítimos.

Algunas de las acciones que llevan a cabo estas soluciones pueden ser:

- Autenticar al remitente en base a unas políticas establecidas para el dominio del remitente
- Emular la apertura del email en un sandbox para observar sus acciones
- Protección contra la suplantación de identidad

- DLP (Data Loss Prevention) o, lo que es lo mismo, la protección frente a la exfiltración de datos confidenciales mediante el análsis de palabras clave o expresiones regulares.
- Utilizar Whitelists/Blacklists para correos recibidos desde un dominio concreto

Soluciones basadas en la nube

Cuando una empresa, normalmente una PYME, no posee el músculo financiero o la estructura suficiente como para tener un equipo de TI propio, puede subcontratar estos servicios y utilizar soluciones basadas en la nube. De esta forma, la gestión y administración de herramientas se delega sobre técnicos especializados que forman parte del servicio ofrecido en la nube.

Algunas de las soluciones que se pueden ofrecer ya las hemos visto:

- Firewall
- Antispam/Antiphishing
- Antivirus
- Backups
- Autenticación
- Gestión de dispositivos móviles
- Gobernanza (políticas de prevención, detección y mitigación de amenazas)

Pentesting

Un pentest o test de intrusión es una simulación de un ciberataque real a la infraestructura de nuestra empresa, en busca de vulnerabilidades, debilidades o deficiencias que puedan ser explotadas por un atacante real, de forma que podamos ponerle solución lo antes posible.

Es como si un banco contratara a alguien para que se vistiera de ladrón e intentara entrar en su edificio y acceder a la cámara acorazada. Si el "ladrón" tiene éxito, y entra en el banco o en la cámara acorazada, el banco obtendrá una valiosa información sobre cómo debe reforzar sus medidas de seguridad.

Las personas que auditan la seguridad de la empresa de esta forma suelen ser expertos en ciberseguridad y se denominan hackers éticos ya que deben contar con el permiso contractual de la empresa para llevar a cabo este ejercicio.

Tipos de pentesting

- Pentesting de caja blanca: se les proporciona a los hackers éticos toda la información sobre el sistema o arquitectura. Incluso es posible facilitarles las credenciales de algún usuario. Puede detectar las vulnerabilidades al detalle.
- Pentesting de caja gris: se cuenta únicamente con alguna información parcial del sistema.
- Pentesting de caja negra: no se tiene ningúna información previa del sistema. Se limita un poco el alcance de este test puesto que no se intenta comprometer la funcionalidad interna.

Fases de un pentesting

1. Recopilación y planificación: Aquí se definen los objetivos y se recolectan los datos necesarios mediante diferentes herramientas para abordar las fases siguientes.
2. Análisis de vulnerabilidades: Con los datos obtenidos en la fase anterior, se analiza la situación para detectar los puntos de entrada y los vectores de ataque más factibles.
3. Modelado de amenazas y explotación: Se intenta demostrar la viabilidad de los puntos establecidos en la fase del análisis de vulnerabilidades. Esto se hace simulando esos ataque al sistema y observando la respuesta del mismo.

   De esta forma se demuestra bajo que riesgos está el sistema y se pueden definir sus posibles soluciones.
4. Elaboración de los informes: Puesto que el fin último de este proceso es informar al cliente de sus debilidades es fundamental elaborar un informe lo más preciso y comprensible posible. Debe ir acompañado de las posibles soluciones propuestas, así como de dos partes, una más técnica para los especialistas y una ejecutiva para los directivos.

Consideraciones legales

Puesto que la empresa que realizará este tipo de auditoría va a intentar vulnerar la seguridad de la empresa contratante, debe quedar todo bien atado en un contrato para evitar repercusiones indeseadas.

En este contrato se autorizará a la empresa contratada a llevar a cabo el test de intrusión pero se debe específicar clara y unívocamente los términos:

- Sólo se autorizará el test sobre las máquinas y sistemas que sean propiedad de la empresa contratante
- Se establecerá claramente el **alcance**, es decir, qué maquinas y/o IPs serán objetos de la prueba y cuáles no.
- El horario exacto en el que pueden realizarse estas pruebas, puesto que en el peor de los casos, puede afectar al rendimiento normal de los sistemas.
- Las técnicas y herramientas que se utilizarán para llevar a cabo el pentesting
- Incluir una cláusula de confidencialidad para no difundir ni los problemas encontrados ni la información comprometida

Phising "ético"

Ya hemos dicho que el factor humano es el eslabón más débil de la cadena que establecen las diferentes soluciones de seguridad de una empresa. A esto le sumamos otro concepto que se viene repitiendo en estos apuntes, el hecho de que el phishing es la mayor puerta de entrada del malware en una empresa.

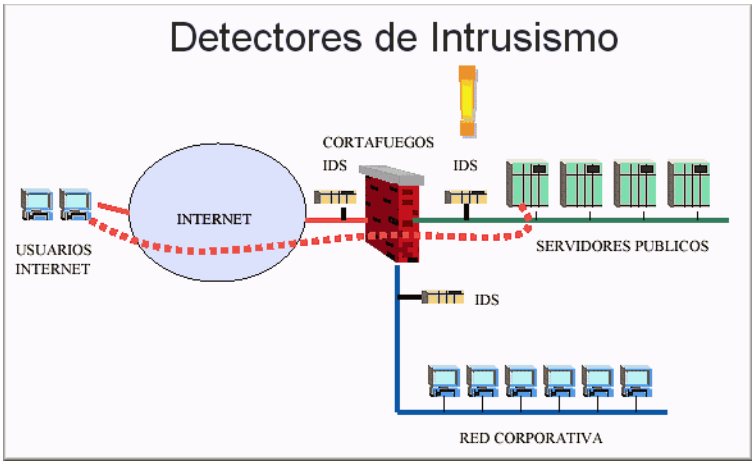
Como último ingrediente de la receta, podemos añadir otro concepto ya presentado: la más que necesaria formación de los empleados en materia de ciberseguridad.

Con todo esto, queda justificado lo que llamamos *phishing ético,* que no son más que campañas de phishing orquestadas por la misma empresa, simulando ser realmente cibercriminales, con el fin de detectar el nivel de concienciación de los empleados y/o como comprobar el nivel de madurez gracias de las campañas de formación previas.

Estas campañas se pueden repetir de forma periódica, con intervalos lo suficientemente grandes, para ir monitorizando el estado de nuestra seguridad.

IDS (Intrusion Detection System)

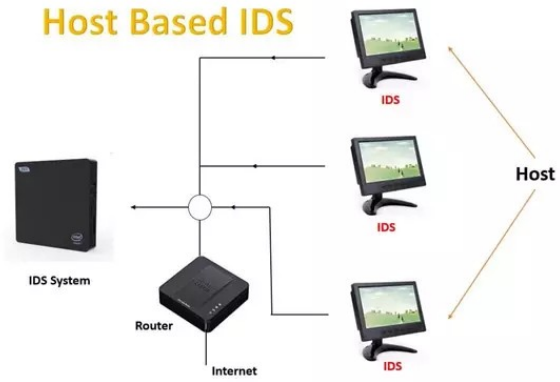
Son sistemas que monitorizan el tráfico entrante y lo cotejan con una base de datos actualizada de firmas de ataque conocidas. Ante cualquier actividad sospechosa, emiten una alerta a los administradores del sistema quienes han de tomar las medidas oportunas. Estos accesos pueden ser ataques esporádicos realizados por usuarios malintencionados o repetidos cada cierto tiempo, lanzados con herramientas automáticas. Estos sistemas sólo detectan los accesos sospechosos emitiendo alertas anticipatorias de posibles intrusiones, pero no tratan de mitigar la intrusión. Su actuación es reactiva.



¿Cómo funcionan los IDS?

Podemos distinguir dos tipos de IDS:

1. **NIDS (Network-based intrusion detections systems)**: Monitorizan el tráfico de dos formas; o bien configurándolo para que todo el tráfico de la red pase a través de él o haciendo un port mirroring (una copia del tráfico)



2. **HIDS (Host-based intrusion detections systems)**: Se configura un sistema para comprobar actividad sospechosa o anómala en un host concreto en lugar de en toda la red. Esto limita en gran medida los dipositivos que se monitorizan pero permite detectar con mayor detalle amenazas en ese host.

Típicamente se utilizan tres metodologías para detectar incidentes:

- Basada en firmas: compara las firmas con los eventos observados para identificar posibles incidentes. Se trata del método de detección más sencillo, ya que compara únicamente la unidad de actividad actual (como por ejemplo un paquete o una entrada de log) contra una lista de firmas mediante operaciones de comparación de cadenas. Estas firmas permiten al IDS distinguir entre el uso normal del PC y el uso fraudulento, y/o entre el tráfico normal de la red y el tráfico que puede ser resultado de un ataque o intento del mismo y son patrones de ataque preconfigurados y predeterminados.
- Detección basada en anomalías: compara las definiciones de lo que se considera una actividad normal con los eventos observados para identificar desviaciones significativas. Este método de detección puede ser muy eficaz para detectar amenazas desconocidas hasta ahora.
- Análisis de protocolos de estado: utiliza información sobre las conexiones entre hosts y la compara con las entradas de una tabla de estado. La tabla de estado mantiene un registro de la conexión entre las computadoras que incluye: dirección IP de origen y puerto, dirección IP de destino y puerto, y los protocolos que se utilizan. Este método busca cambios repentinos o bruscos en la actividad de la red. Otras funciones incluyen a veces el seguimiento del estado del protocolo, los análisis dinámicos del protocolo de aplicación y el reensamblaje de paquetes IP, lo que evita que fragmentos de paquetes IP lleguen a la red interna.

  Entre las **ventajas** del análisis de protocolo de estado están:

  - Identifica secuencias inesperadas de comandos.
  - Añade características de estado al análisis regular de protocolos.
  - Comprueba la racionalidad de los umbrales de los comandos individuales.

  Entre las **desventajas** están:

  - Uso intensivo de recursos, sobrecarga de recursos elevada.

- No puede detectar ataques que no violen las características de comportamiento del protocolo generalmente aceptado.
- Presenta conflictos entre el modelo de protocolo utilizado por el sistema y cómo se implementa realmente el protocolo.

IPS (Intrusion Prevention System)

IPS (Intrusion Prevention System) o sistema de prevención de intrusiones: es un software que se utiliza para proteger a los sistemas de ataques e intrusiones. Como su nombre indica, su actuación es de carácter preventivo.

Estos sistemas llevan a cabo un análisis en tiempo real de las conexiones y los protocolos para determinar si se está produciendo o se va a producir un incidente, identificando ataques según patrones, anomalías o comportamientos sospechosos y permitiendo el control de acceso a la red, implementando políticas que se basan en el contenido del tráfico monitorizado, es decir, el IPS además de lanzar alarmas, puede descartar paquetes y desconectar conexiones.

Muchos proveedores ofrecen productos mixtos, llamándolos IPS/IDS, integrándose frecuentemente con cortafuegos y UTM (en inglés Unified Threat Management o Gestión Unificada de Amenazas) que controlan el acceso en función de reglas sobre protocolos y sobre el destino u origen del tráfico.

Limitaciones de de los IDS/IPS

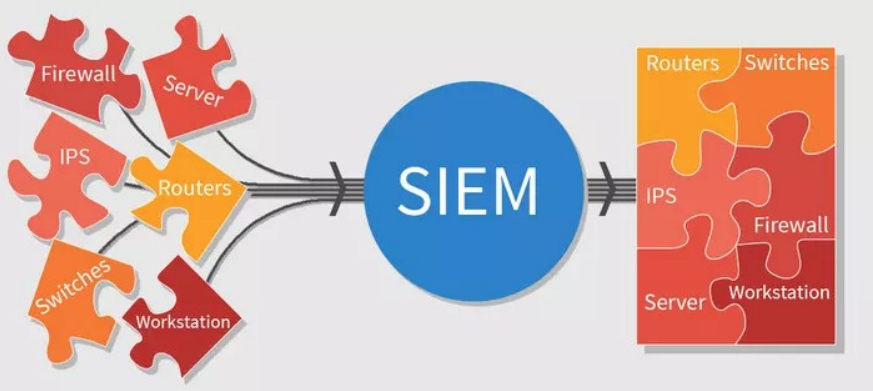
No todo es bonito con estos sistemas, algunos de sus handicaps más importantes son:

- Un IDS sólo detectará lo que esté configurado para detectar. Es decir, están limitados únicamente a detectar ataques ya conocidos.
- Son completamente dependientes de las reglas que escribamos o les carguemos y esto lleva inevitablemente a los **falsos positivos**. Una regla configurada para detectar un ataque también puede generar una alerta ante tráfico legítimo si ésta no ha sido configurada con sumo cuidado o si el ataque usa un patrón común de tráfico.
- Capacidades limitadas ante tráfico cifrado.
- Su visibilidad está limitada en función de dónde se coloquen en la red.

SIEM (Security Information and Event Management)

Un SIEM es un sistema dedicado a la cibersegridad, utilizado para monitorizar los ataques o peligros a los que nuestro sistema puede estar expuesto en ese momento.

Se trata de una plataforma dedicada a unificar logs (registros) de distintos puntos de una red empresarial en un mismo punto para tenerlos monitorizados. Pero no sólo eso, sino que además es capaz de correlar los eventos que aparecen en estos logs con el fin de detectar comportamientos anómalos o inusuales que puedan ser indicativo de estar sufriendo algún tipo de incidente de ciberseguridad.



Es decir, en esencia un SIEM centraliza toda la información que tenemos en nuestra red para poder detectar incidencias y nos permite gestionar estos eventos de la mejor manera posible, incluso integrándose con otras soluciones de ciberseguridad como las que hemos visto con anterioridad.

Algunas de las desventajas de estos sistemas es su alto coste de implantación, tanto monetario como en formación a los empleados para su manejo debido a su larga curva de aprendizaje.

Referencias

¿Qué es un EDR? ¿Por qué es diferente de un antivirus?

¿Qué hace un antivirus para detectar el malware?

Understanding Anti-Virus Software

What is EDR (endpoint detection and response)?

What is XDR?

¿Qué tipos de filtros antispam existen?

Dispositivo Cisco Ironport Email Security

Ciberseguridad de las pymes en 2022: mismos retos, mejores soluciones

¿Qué es el pentesting?

3. Marcos de gestión para la prevención, protección, respuesta y gobierno

Introducción

Hagamos un ejercicio de imaginación y supongamos que queremos convertirnos en un pintor de reputada fama internacional aunque, desafortunadamente, no conocemos nada del mundo del arte.

¿Qué necesitaremos para conseguirlo? Pues bueno, en primer lugar está claro que debemos conocer los colores que existen en el mercado o los sistemas de definición cromática como Pantone, que podemos utilizar para conseguir un buen cuadro.

Cada color se asemejaría a los diferentes controles que queremos incorporar a nuestros planes de seguridad. Pero es que además, debemos saber cómo combinarlos para que la producción sea profesional y esto se consigue a base de pruebas, ya sea de color, de formas o experimentos varios que quedan plasmados en libros de bocetos por ejemplo, donde dejamos plasmados las combinaciones que nos sirven y que funcionan. Estas fórmulas que nos indican qué mezclas son exitosas y se asemejan a los marcos programáticos que nos ayudan a organizar nuestras actividades.

Cualquier pintor tendrá como meta ser expuesto en los mejores museos, Hermitage, Louvre o Metropolitan, entre otros. Queremos hacer que la gente desee ir a ver nuestra obra una y otra vez. Esto es lo que intentaremos conseguir con los marcos de riesgo.

Marcos de control

Un marco de control se utiliza para:

- **Desarrollar una estrategia básica para el equipo de seguridad**. Es normal que en equipos jóvenes o poco maduros en materia de seguridad, se estén llevando a cabo actividades relacionadas con la ciberseguridad pero de manera ad-hoc, sin ninguna base que lo sustente detrás.
- **Proporcionar un conjunto de controles básicos**
- **Evaluar el estado técnico actual**

- **Priorizar la implementación de controles**

NIST SP 800-53

El Instituto Nacional de Normas y Tecnología de Estados Unidos (NIST), que forma parte del Departamento de Comercio del país, define estándares y directrices relacionados con la seguridad de la información. El NIST desarrolló la publicación especial 800-53 (NIST SP 800-53) como guía para el cumplimiento de las obligaciones que define la ley federal de protección de la información de Estados Unidos (Federal Information Security Management Act o FISMA). Cuenta con 20 familias distintas de controles.

Servicios en la nube tales como Azure, AWS o GCP, cumplen con este estándar.

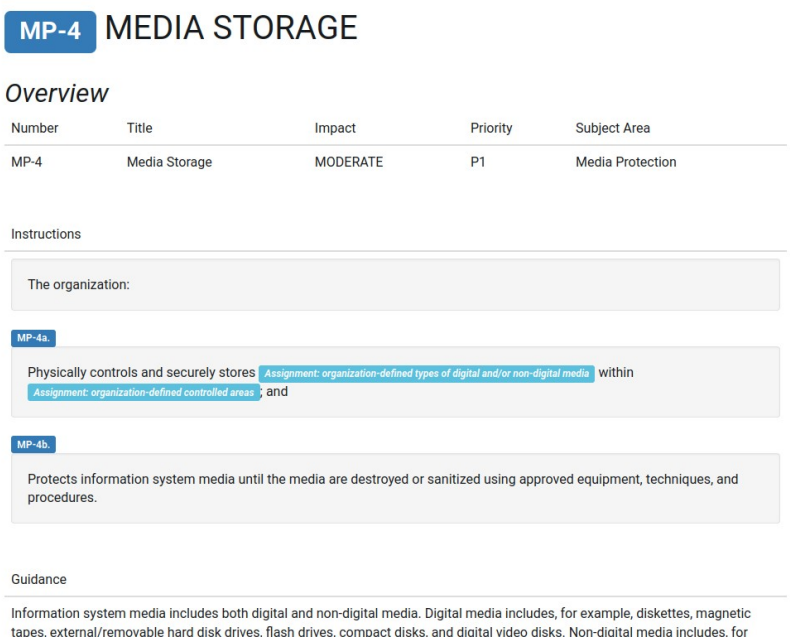
Aquí un ejemplo de la lista completa de controles del NIST 800-53.

Visión general del NIST 800-53

Se trata de un catálogo integral de controles de seguridad y privacidad. Este catálogo está, como hemos dicho, organizado por familias, con una serie de controles dentro de ellas, así como un refuerzo de esos controles.

Si seguimos con el símil de la introducción y consideramos que cada control es un color de nuestra paleta, ¿vamos a usar todos los colores disponibles para un mismo cuadro? Probablemente no. Por eso mismo, podemos decidir implementar los controles en función de su prioridad (P0, P1, P2, P3, P4) o de su impacto en el negocio (bajo, moderado, alto).

Cojamos cualquier control a modo de ejemplo:



MP-4 MEDIA STORAGE

Overview

Number	Title	Impact	Priority	Subject Area
MP-4	Media Storage	MODERATE	P1	Media Protection

Instructions

The organization:

MP-4a.

Physically controls and securely stores *Assignment: organization-defined types of digital and/or non-digital media* within *Assignment: organization-defined controlled areas*; and

MP-4b.

Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Guidance

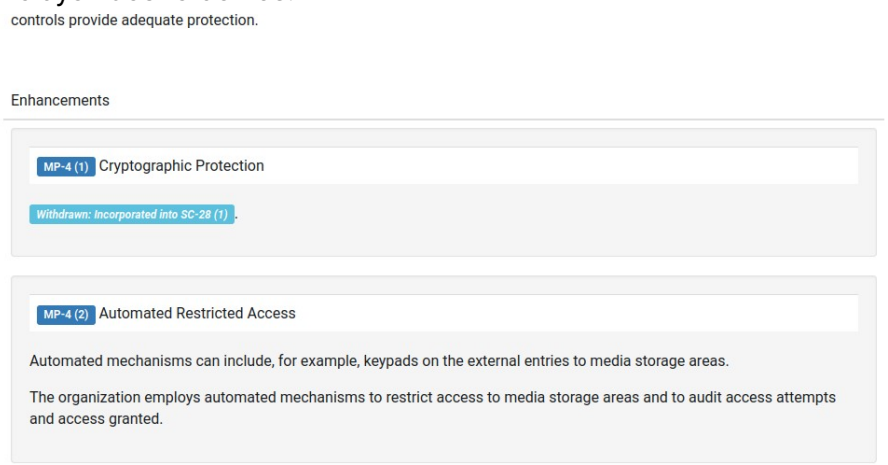
Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for

Vemos que se trata del cuarto control de la familia *Media Protection,* con impacto *Moderate* y prioridad *P1*.

Tiene dos subapartados a y b. En el primero se nos indica que se debe controlar el acceso físico y asegurar el almacenamiento en el dispositivo que se elija (digital o no digital) dentro de las areas que defina la empresa para ello.

El segundo hace referencia a que se ha de proteger los medios donde se almacen la información hasta que esta sea destruida o sanitiada siguiendo los debidos procedimientos.

Además, se incluyen dos refuerzos:



controls provide adequate protection.

Enhancements

MP-4 (1) Cryptographic Protection

Withdrawn: Incorporated into SC-28 (1).

MP-4 (2) Automated Restricted Access

Automated mechanisms can include, for example, keypads on the external entries to media storage areas.

The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.

Uno donde se habla de la protección criptográfica, aunque se indica que ha sido incorporado en otro control de refuerzo, el SC-28 (1) y eliminado de este.

Y el segundo refuerzo donde se habla de controlar el acceso a las ubicaciones donde se guardan los sistemas que almacenan la información, auditando los accesos tanto exitosos como erróneos.

Controles CIS

Puesto que raramente vamos a implementar absolutamente todos los controles que nos proporciona el marco anterior, es entonces cuando entran en juego los controles CIS (Center for Internet Security)

El CIS es una organización sin fines de lucro establecida en octubre de 2000. Está promovido por una comunidad global de TI con el objetivo común de identificar, desarrollar, validar, promover y mantener soluciones de prácticas recomendadas para la ciberdefensa. Desde su creación, el CIS ha producido y distribuido varias herramientas y soluciones gratuitas para empresas de todos los tamaños, diseñadas para reforzar su ciberseguridad.

Se trata de una colección de 20 controles prioritarios que se deben cumplir para defenderse de los riesgos más comunes en materia de ciberseguridad y reducir la superficie de ataque.

Este tipo de controles tienen un gran éxito ya que consiguieron reducir durante su primer año de implementación un 90% el riesgo en el departamento de defensa de EEUU y bloqueó el 85% de las instrusiones en los servicios de defensa australianos.

Pero, lo que es más importante para el caso que nos ocupa a nosotros, este tipo de controles asume que no todas las empresas poseen el presupuesto necesario para implementar un amplio marco de ciberseguridad, por lo que les da unas pautas básicas para protegerse de la forma más efectiva posible ante los riesgos más prioritarios.

Además, de alguna manera, se podrían mapear estos controles CIS a otros marcos de ciberseguridad. Y para muestra un botón, con el Síndic de Comptes de la Comunitat Valenciana donde se mapean algunos controles CIS a otros del ENS (Esquema Nacional de Ciberseguridad).

De hecho, sitios como AuditScripts nos ofrecen herramientas para llevar a cabo la implementación de estos controles e incluso para mapearlos a multitud de controles de otros marcos.

Marcos programáticos

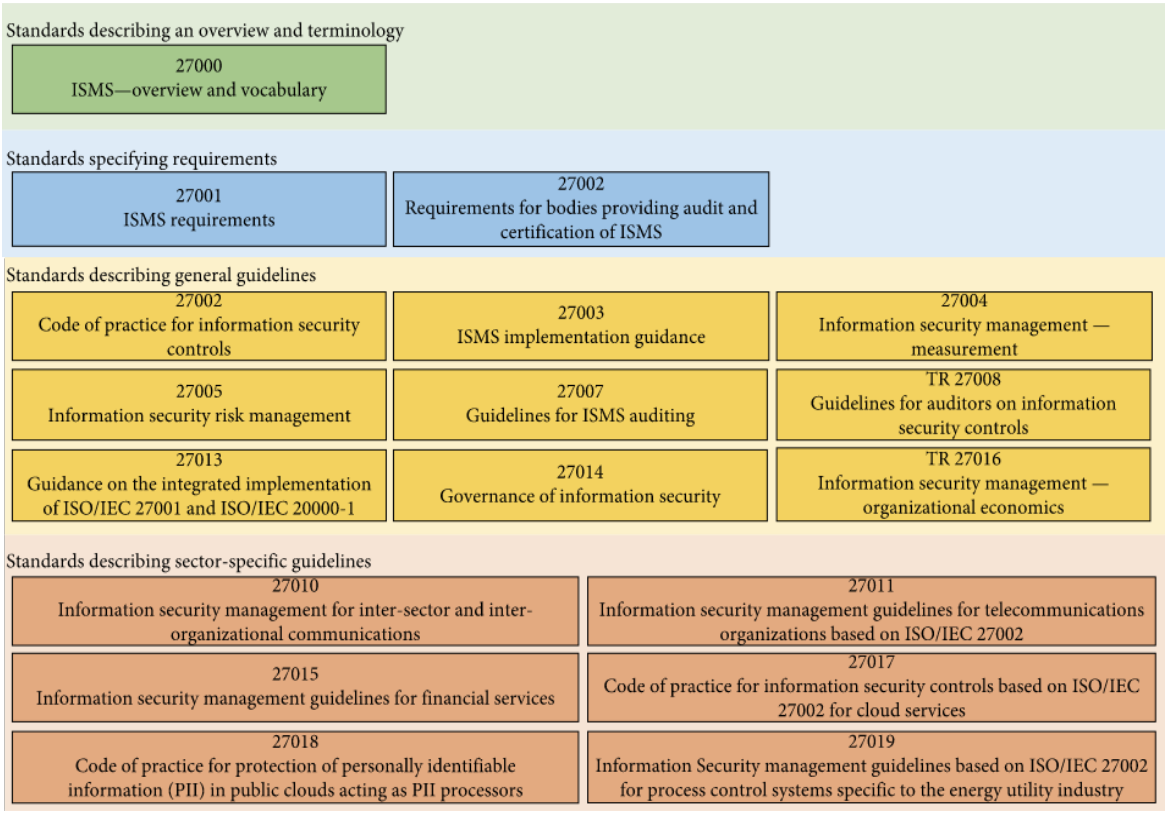
Estos marcos nos ayudan con la comunicación a alto nivel con los ejecutivos a cargo del negocio para que tengan una mejor perspectiva y conocimiento de qué se está haciendo desde la perspectiva de ciberseguridad.

Algunos de sus puntos claves son:

- Evaluar el estado del programa de seguridad
- Construir un programa integral de seguridad
- Medir la seguridad del programa/análisis competitivo
- Simplificar la comunicación entre el equipo de seguridad y los líderes de empresa

Visión general de la serie ISO 27000

ISO, como es obvio debido a su naturaleza, publica una gran cantidad de documentos. Es sin embargo la serie 27000 la dedicada a seguridad de la información.



El primero, el 27001 define nuestro plan de seguridad, los requerimientos que debe cumplir nuestro sistema de información o ISMS (Information Security Management System).

El 27002 es una guía para la implementación de los controles de seguridad en una organización, de tal forma que sirva de referencia para ello, vaya encaminado a cumplir la 27001 o no.

ISO 27001

Define diferentes áreas de actuación sobre las que construir un plan de seguridad y su estructura es la que vemos en la imagen a continuación:

Una explicación somera de cada área puede consultarse aquí.

La ISO 27001 no suele ser utilizada en norteamérica porque es muy exigente en términos de consumo de recursos a la hora de aplicarse, tanto de personal como de tiempo y, por tanto, económicos. Sin embargo, todos los proveedores cloud se aseguran de cumplirla, ¿por qué se da este fenómeno? Simplemente, por su enfoque global, quieren poder hacer negocio con clientes a todo lo largo y ancho del globo, por lo que quieren poder demostrar que cumplen los más altos requisitos de seguridad.

Así pues, podemos considerar la 27001 como un estándar de carácter más internacional.

Los controles de seguridad a implementar se pueden encontrar en el Anexo A de la ISO 27001. Estos controles se distribuyen dentro del Anexo A **en 14 secciones** de esta forma:

- Políticas de seguridad de la información: A. 5.

- Organización de la seguridad de la información: A.6.
- Seguridad de los recursos humanos: A. 7.
- Gestión de Activos: A.8.
- Controles de acceso: A.9.
- Criptografía – Cifrado y gestión de claves: A.10.
- Seguridad física y ambiental: A.11.
- Seguridad operacional: A.12.
- Seguridad de las comunicaciones: A.13.
- Adquisición, desarrollo y mantenimiento del sistema: A.14.
- Gestión de incidentes de seguridad de la información A.16.
- Cumplimiento: A.18.

NIST Cybersecurity Framework (CSF)

Es un marco publicado por el Instituto Nacional de Estándares y Tecnología (NIST, National Institute of Standards and Technology) de los Estados Unidos de América

Es un framework mucho más sencillo ya que permite comunicarse de forma más sencilla con personal no tecnico, ni relacionado con la ciberseguridad a propósito de las funciones y controles a implementar en el ciclo de vida de la seguridad.

Ayuda a las organizaciones a hacerse preguntas como:

- ¿Qué estamos haciendo a día de hoy?
- ¿Cómo lo estamos haciendo?
- ¿A dónde queremos llegar?
- ¿Cuándo queremos llegar?

En esencia, intenta guiar a empresas de cualquier tamaño a gestionar y reducir los riesgos asociados a la seguridad de su información. Recopila una serie de mejores prácticas.

Este marco de trabajo se encuentra compuesto de tres partes principales: **El marco básico** (Framework Core), **los niveles de implementación del marco** (Framework Implementation Tiers) y **los perfiles del marco** (Framework Profiles).

El núcleo o marco básico (Core), es un conjunto de actividades, resultados a obtener y referencias informativas, comunes en sectores donde las infraestructuras son críticas.

Este Core sirve a su vez como guía para desarrollar **perfiles** en la organización. Estos **perfiles** determinan el estado actual y el estado objetivo para identificar la brecha que debe subsanarse con el fin de cumplir con las metas sobre gestión de riesgos y establecer una hoja de ruta.

Por último, los **niveles de implementación (Tiers)** define la visión de una organización en cuánto a los riesgos de cibeseguridad y qué tan maduros son los procesos que se implementan para manejarlos, desde lo más informal hasta las más formales.

El Core del **CSF** consta de 5 funciones clave y de un alto nivel de abstracción:

1. **Identificar:** Consistente en inventariar todos los activos, tanto software como hardware de la empresa, así como los datos tratados. También deben quedar claros los roles y responsabilidades dentro de la organización y de cualquier proveedor que tenga acceso a esos activos.
2. **Proteger:** Describe las medidas de seguridad adecuadas para garantizar la entrega de servicios de las infraestructuras críticas. Se contemplan aspectos como los controles de acceso, el almacenamiento de datos o la capacitación de los empleados.
3. **Detectar:** En este nivel se abordan las acciones llevadas a cabo para poder monitorizar e identificar un evento o incidencia de seguridad.
4. **Responder:** Trata la capacidad de actuar frente a un incidente de ciberseguridad, limitando su pontencial daño. Se centra en cómo informar a clientes y empleados de ello, en mantener funcionando el negocio, la investigación y el análisis del incidente.
5. **Recuperar:** Íntimamente relacionado con la fase anterior de respuesta, identifica las acciones a llevar a cabo para recuperarse de un incidente previo, resturando las partes de la infraestructura afectadas así como informando a empleados y clientes de estas acciones.

Para más detalle a propósito de este framework y cómo se organiza, conviene consultar el siguiente enlace.

Si consultamos el archivo Excel que el propio NIST pone a nuestra disposición para la implementación del CSF, vemos que existe un mapeo de cada subcategoría a otros marcos como el NIST 800-53 visto anteriormente o a los controles CIS (CSC).

Si nos fijamos en esta imagen donde aparece resumido el mapeo del NIST CSF a los controles CIS, existe un vacío en la función de Identificación, concretamente en las funciones de Gobernanza y Evaluación de riesgos.

Esto no es que sea malo per se, sino que simplemente los controles CIS están fuertemente centrados en el aspecto técnico. Es por eso que necesitamos combinar los frameworks o marcos programáticos con los de control, para así cubrir todos los aspectos necesarios de nuestro plan de seguridad.

Marcos de riesgo

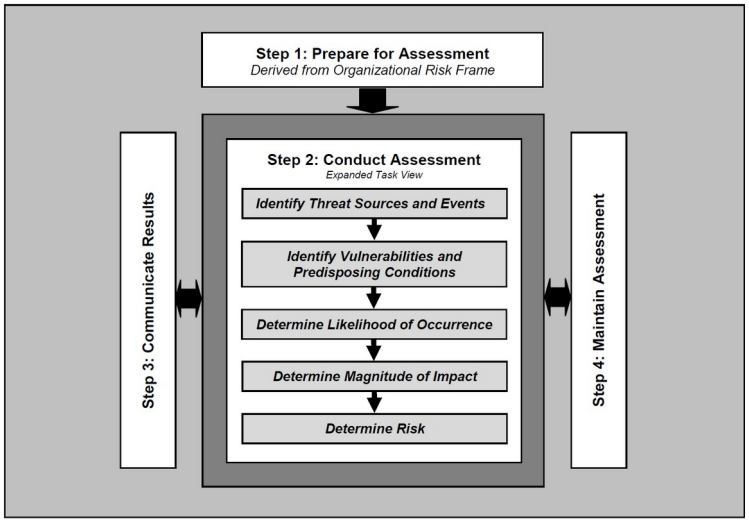
Cuando ya se tiene una organización madura en materia de ciberseguridad, se puede intentar dar un paso más y subir un escalón en nuestro sistema o plan de seguridad. En concreto podemos usar este tipo de marcos para:

- Definir pasos clave del proceso para evaluar y gestionar el riesgo
- Estructurar el programa para la gestión del riesgo
- Identificar, medir y cuantificar el riesgo
- Priorizar las actividades de seguridad

Como ejemplos de marcos de este tipo, como no podía ser de otra manera, podemos nombrar brevemente en primer lugar a NIST, dividiéndolos en dos tipos de estándares:

- Gestión de riesgos
  - NIST SP 800-39: Proceso de gestión de riesgos en general
  - NIST SP 800-37: Marco para la gestión de riesgos (RMF – Risk Management Framework) de los sistemas de información federales.
- Evaluación o valoración de riesgos:
  - NIST SP 800-30: Procesos de evaluacion de riesgos

Particularizando en el 800-30, aquí vemos cómo es el proceso de evaluación de riesgos, dividido en 4 pasos:



Fuente: https://www.nccoe.nist.gov/publication/1800-21/VolB/vol-b-appendix.html

RMF

En cuánto al RMF, a pesar de ser concebido originalmente para estamentos federales, puede resultar útil ya que al fin y al cabo se trata de la gestión de riesgos, algo a lo que toda organización deberá hacer frente.

Para seguir el RMF, podemos caracterizar 6 fases, como vemos aquí

ISO 27005

ISO también publica estánderes al respecto de la gestión de riesgos en su serie 27000 dedicada a la seguridad de la información. Concretamente, es ISO 27005 el encargado abordar el tema de la gestión del riesgo de los sistemas de información.

Este estándar define un enfoque sistemático para gestionar los riesgos en una organización.

Aquí podemos ver un diagrama donde se resume la metodología. Vemos que es bastante parecido al que hemos visto del NIST 800-30, solo que aquí además aparece en la parte de abajo dos *cajones* que hacen referencia al tratamiento del riesgo y a a la aceptación del riesgo.

Esto es así porque la ISO 27005 hace referencia a la **gestión integral** del riesgo, no únicamente a la valoración o evaluación del mismo.

Modelo FAIR

Examinando estos frameworks, siempre vemos que nos hablan de que podemos medir el riesgo o analizarlo pero siempre de forma cualitativa (por ejemplo con la típica escala LOW, MEDIUM, HIGH)

El modelo o estándar FAIR, por otra parte, permite medir los riesgos de forma cuantitativa y aporta una metodología para ello. Esto además es perfectamente compatible con los marcos de riesgo que hemos visto puesto que perfectamente permiten medir los riesgos tanto de una forma como de la otra, por lo que es un complemento para ellos.

Aquí podemos ver el modelo en cuestión.

Podemos definir o medir un riesgo de la siguiente forma a alto nivel:

Riesgo = Impacto x Probabilidad (de ocurrencia)

Pero podemos descomponer el término probabilidad de esta fórmula así:

Riesgo = Impacto x (Vulnerabilidad x Amenaza)

Tradicionalmente las empresas han puesto su foco de atención en las vulnerabilidades y en eliminarlas o solucionarlas. Sin embargo, conviene fijarse en cómo hacer frente al riesgo en su conjunto y, por lo tanto, pensar también en el impacto.

Mitre Framework

MITRE ATT&CK son las siglas de MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK). El marco MITRE ATT&CK es una base de conocimientos y un modelo seleccionados para el comportamiento del adversario cibernético, que refleja las diversas fases del ciclo de vida del ataque de un adversario y las plataformas a las que se sabe que se dirigen.

Es decir, este framework recoge en una matriz de conocimientos, todas las técnicas y procedimientos que se han visto utilizar a distintos atacantes, con el fin de conocer de qué maneras nos podemos proteger ante ellas.

Marcos de gobernanza de datos

De acuerdo con la archiconocida empresa alemana SAP, la gobernanza de datos “abarca las políticas y procedimientos que se implementan para garantizar que los datos de una organización

sean precisos –y que se manejen correctamente cuando se ingresan, almacenan, manejan, acceden y eliminan–. Las responsabilidades de gobernanza de datos incluyen establecer la infraestructura y tecnología, configurar y mantener procesos y políticas, e identificar a las personas (o cargos) de una organización que tienen la autoridad y responsabilidad de gestionar y salvaguardar tipos específicos de datos."

Dicho de otra forma, es un concepto que habla del correcto tratamiento y gestión de los datos empresariales. Y este concepto es clave para llevar a cabo la tan mencionada transformación digital en las empresas, por ello un marco de gobernanza de datos resulta esencial, máxime cuando el Big Data ha irrumpido con tanta fuerza de un tiempo a esta parte.

Son 4 los pilares básicos sobre los que se sustentaré un marco de gobernanza de datos:

1. Gobernanza
2. Gestión
3. Calidad
4. Seguridad y privacidad

La Asociación Española de Normalización (UNE) ha señalado las distintas pautas a considerar para un buen gobierno del dato. Estas normas las ha recogido el Ministerio de asuntos económicos y transformación digital para resumirlas en la siguiente infografía:

datos.gob.es

NORMAS UNE PARA UN CORRECTO GOBIERNO DEL DATO

1 GESTIÓN DE LA CALIDAD DE LOS DATOS

ISO 8000
Marcos para mejorar la calidad de los datos. **Incluye:**

Intercambio de datos maestros entre organizaciones

ISO 8000-100 a ISO 8000-150

ISO 8000-6

Guía para la aplicación de la calidad de los datos de la forma del producto

ISO 8000-311

ISO 8000-1 ISO 8000-2 y ISO 8000-8

Conceptos generales de la calidad de los datos

Procesos de gestión de la calidad de los datos

- **ISO 8000-60**: visión general.
- **ISO 8000-61**: modelo de referencia de los procesos de gestión.
- **ISO 8000-62**: aplicación y evaluación de madurez de procesos organizacionales.

ISO/IEC 25012
Modelo general de calidad aplicable a datos almacenados de forma estructurada en un sistema de información.

2 MEDICIÓN DE LA CALIDAD

ISO 25024:
requisitos y evaluación de la calidad de los sistemas y el software (SQuaRE).

3 GOBIERNO DEL DATO

- **ISO/IEC 38505-1**: marco de gobierno de datos y mapa de responsabilidad de datos que identifica las áreas de la organización en las que debe aplicarse el gobierno de datos.
- **ISO/IEC 38505-2**: implementación de la Norma ISO/IEC 38505-1 que proporciona orientación sobre el gobierno de datos.

4 NORMAS TRANSVERSALES PARA LA SEGURIDAD Y PRIVACIDAD DE DATOS

SEGURIDAD DE LA INFORMACIÓN

ISO/IEC 27001: requisitos del SGSI (Sistema de Gestión de Seguridad de la Información).

ISO/IEC 27002: código de prácticas del SGSI.

ISO/IEC 27018: PII (información personalmente identificable) en la nube pública.

PRIVACIDAD Y PROTECCIÓN DE DATOS

ISO/IEC 27701: requisitos del SGPI (Sistema de Gestión de la Privacidad de la Información).

ISO/IEC 29100: marco de privacidad.

ISO/IEC 29151: protección de la información personal. Código de prácticas.

ISO/IEC 29134: evaluación del impacto de la privacidad.

ISO/IEC 20889: técnicas de desidentificación de datos para la mejora de la privacidad.

SEGURIDAD Y PRIVACIDAD POR DISEÑO/DEFECTO

PNE-prEN 17529: protección de los datos y de la privacidad por diseño y por defecto.

ISO/DIS 31700: protección del consumidor. Privacidad por diseño para bienes y servicios de consumo.

red.es Iniciativa aporta

Conclusiones

A medida que vamos evolucionando y madurando el plan de seguridad de nuestra empresa, deberemos ir eligiendo implementar al menos uno de los marcos de cada uno de los tres tipos que hemos visto.

Recordemos que:

1. Los marcos de control permiten identificar los puntos de control objetivo a implementar
2. Los marcos programáticos nos ayudan tanto a constuir un plan integral de seguridad como a simplificar la comunicación con la capa ejecutiva, la de negocio
3. Los marcos de riesgo nos permiten prioridad las tareas de seguridad apropiadamente.

Referencias

Guía completa sobre controles de seguridad CIS

AuditScripts - Critical Security Controls

ISO 27002 de Tecnología de la información

¿Qué es el Cybersecurity Framework de NIST de los Estados Unidos?

How to Make Sense of Cybersecurity Frameworks – RSA Conference 2019

Qué es el Marco MITRE ATT&CK y cómo implementarlo