INDUSTRY 4.0 for VET

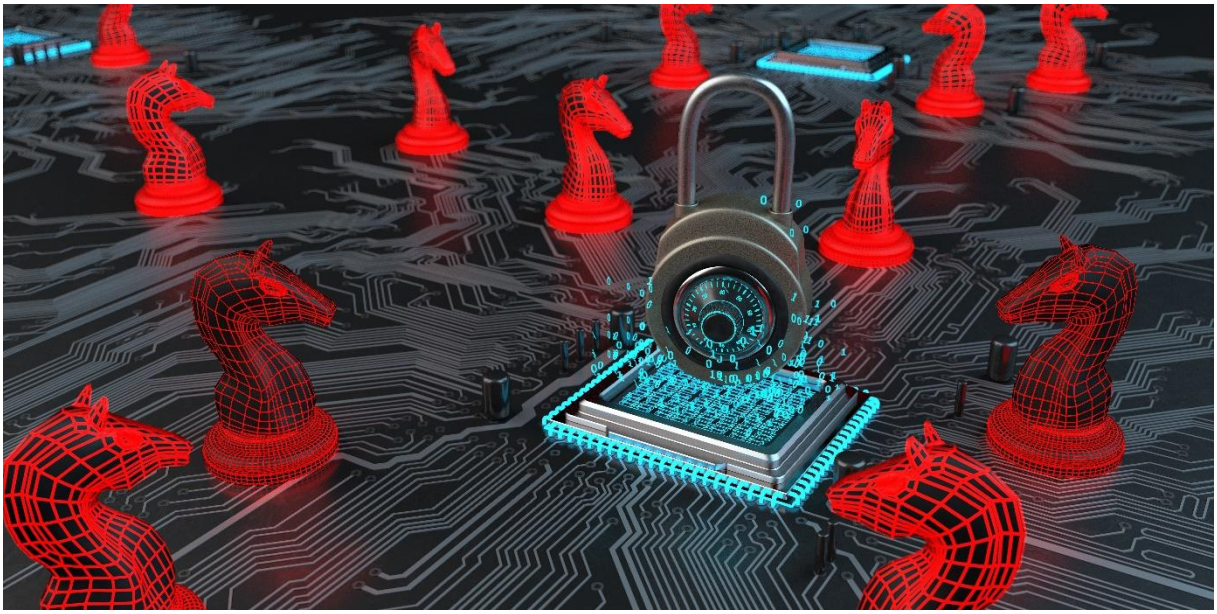
5. SEGURIDAD INFORMÁTICA

5.1 Concepto

Introducción

Hacer copias de seguridad de los datos era más fácil antes. En el pasado, los documentos importantes como los contratos o las libretas de ahorro solían guardarse bajo llave en cajas fuertes o simplemente se ocultaban. Esto aseguraba que las personas no autorizadas no pudieran acceder a ellos en absoluto o sólo con gran dificultad.

Hoy en día, ya no es tan simple. Los documentos y los datos están ahora digitalizados y a menudo ya no están físicamente disponibles. Piensa, por ejemplo, en tu banca en línea, en los contratos importantes que se firman electrónicamente y se envían por correo electrónico, o en los datos privados como las fotos. Al igual que los documentos analógicos solían estar "guardados bajo llave", hoy en día los datos también deben de almacenarse digitalmente. El robo de datos o el procesamiento o la manipulación ilegal de los mismos puede conllevar altos riesgos y graves consecuencias, tanto para los particulares como para empresas y organizaciones enteras.



La seguridad informática, también "seguridad de la información", no es un tema nuevo, pero está adquiriendo cada vez más importancia debido a los rápidos avances digitales de los últimos años. Deberíamos estar familiarizados con ella, porque la información digital, seamos conscientes de ello o no, es simplemente la base de la vida moderna.

Relevancia práctica: competencias y habilidades necesarias.

Desde la vida privada hasta el trabajo, desde las empresas individuales hasta las corporaciones globales, los datos y la información están presentes en todas las áreas de la vida y son un activo valioso. Ya sea un crimen cibernético, pérdida de datos o falsificación de datos - la seguridad informática debería preocupar a todo el mundo. Esta unidad de aprendizaje le ayudará a garantizar la seguridad de sus datos privados y a realizar una valiosa contribución a la seguridad de los datos en su empresa. Se le sensibilizará para que la seguridad informática actúe con confianza en este sentido.

Objetivos de aprendizaje y competencias

En este capítulo aprenderás sobre el término seguridad informática en sus facetas más importantes. Aprenderás más sobre su significado y objetivos, pero también qué amenazas y medidas existen actualmente en el área de la seguridad informática. Aprenderás cómo puedes contribuir personalmente a un entorno de información más seguro, tanto en el ámbito privado como en el profesional.

Co-funded by the Erasmus+ Programme of the European Union

Este proyecto ha sido financiado gracias al apoyo de la Comisión Europea. Esta publicación refleja únicamente el punto de vista del autor y la Comisión no se hace responsable de cualquier uso indebido que pueda hacerse de la información aquí presente.

Objetivos de aprendizaje
Conocer y comprender las definiciones generales y las áreas de aplicación de la seguridad informática.
Ser capaz de nombrar y explicar los objetivos y tareas de la seguridad informática.
Conocer las amenazas informáticas actuales y poder asignarlas a la seguridad informática en las áreas de aplicación.
Conocer las medidas y mecanismos de defensa de la seguridad informática en la aplicación

5.2 Definiciones y áreas de aplicación

La **seguridad informática no es sólo seguridad de la información** - aunque a menudo ambos términos se utilizan de la misma manera (especialmente si no se traducen exactamente del inglés a otro idioma), hay una sutil diferencia que le ayudará a definir el término.

En principio, seguridad informática significa "Seguridad de la Tecnología de la Información". Pero eso suena bastante largo - por eso preferimos quedarnos con "Seguridad informática".

Definición

Seguridad de la información vs. seguridad de la tecnología de la información

El término **seguridad de la información** significa medidas de protección para TODOS los sistemas que procesan o almacenan información de cualquier manera. No importa si son digitales o "analógicos". Así que el ordenador se entiende como un montón de documentos escritos a mano y confidenciales.

La seguridad informática es una subárea de la seguridad de la información. De hecho, aquí sólo se habla de las medidas de protección de los llamados sistemas "socio-técnicos". Los sistemas socio-técnicos no son más que sistemas en los que los humanos utilizan la tecnología de la información para almacenar y procesar datos.

Por cierto, según el diccionario, la **tecnología de la información** se define como "la tecnología para la recolección, transmisión, procesamiento y almacenamiento de información por medio de computadoras y equipo de telecomunicaciones".

Hasta ahora todo bien. Sin embargo, hoy en día se utiliza prácticamente en todos los ámbitos, por lo que la seguridad informática cubre una gran parte de la seguridad de la información.
Un ejemplo de una aplicación de seguridad de la información sin las TIC podría ser la receta secreta escrita a mano en la caja fuerte de su restaurante favorito. Pero en esta unidad nos centraremos en la seguridad informática...
También hay otros subconceptos en la seguridad informática cuya visión general inicial vale la pena, especialmente la forma en que están conectados:

- **Seguridad informática:** Se refiere específicamente a las medidas de seguridad de los propios sistemas informáticos locales y en red. ¿Cómo de seguro es un ordenador ante la amenaza de un acceso o manipulación no autorizados? ¿Qué sucede si un ordenador "se bloquea"?

- **Protección de datos:** El término está de moda y con razón, porque "la protección de datos es también protección personal". Este aspecto es el más importante para las persona privadas, porque se trata de la protección de los propios datos personales contra el mal uso. La privacidad y el anonimato son un tema delicado en un mundo digitalizado.

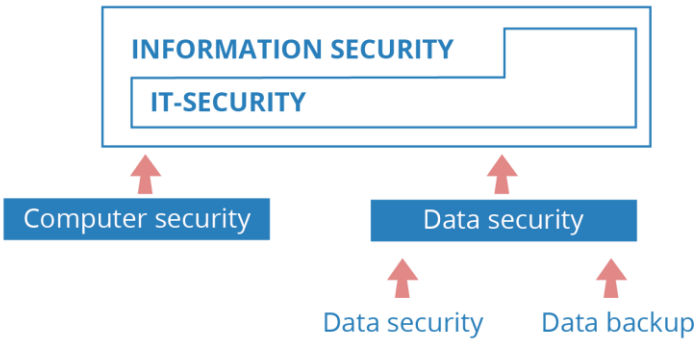
Co-funded by the Erasmus+ Programme of the European Union

Este proyecto ha sido financiado gracias al apoyo de la Comisión Europea. Esta publicación refleja únicamente el punto de vista del autor y la Comisión no se hace responsable de cualquier uso indebido que pueda hacerse de la información aquí presente.

- **Seguridad de datos:** Esto es de nuevo, de naturaleza más técnica. No se trata tanto de cuestiones legales, sino simplemente de cómo proteger los datos de la manipulación o la pérdida. La seguridad de los datos puede entenderse como la etapa técnica preliminar para una protección de datos exitosa.

- **Copia de seguridad de los datos:** Se trata específicamente de (múltiples) copias de seguridad de los datos - lo más probable es que estés familiarizado con el término "copia de seguridad. Se trata de la correcta duplicación de datos para prevenir su pérdida.

El siguiente diagrama aclara el contexto de todos los términos:
La seguridad informática constituye una gran parte de la seguridad de la información y consiste principalmente en seguridad informática y en seguridad de los datos.



La seguridad de los datos es la base del éxito de la protección de los datos y de las copias de seguridad de los mismos.

Importante

Datos e información

Ahora que ha leído los términos "datos" e "información" tan a menudo, seguramente querrá saber la diferencia:

- Los datos son en realidad signos y símbolos inútiles - sin contexto, estos datos permanecen vacíos y no hay nada que hacer con ellos. Tomemos la secuencia de números de 1908 a 1974, por ejemplo.
- La información es un dato que se coloca en un contexto. Estos datos se vuelven significativos y transportan información, por ejemplo, la fecha de nacimiento 08-19-1974 - ya está claro lo que se quería decir con la secuencia de números.

Por cierto, esta es también la idea básica detrás de la encriptación, no importa si se hace en el ordenador o a mano. Dejas los datos sin contexto, tal vez incluso los mezclas. Sólo alguien que también entienda el contexto puede entender el significado de la secuencia de números.

¿Para quién es importante implementar la seguridad informática?
En realidad, sirve para todos los que tienen un ordenador, ya sea un individuo o una organización. Sin embargo, ayuda a clasificar las áreas de aplicación de la seguridad informática con un poco más de precisión, también para poder asignar más tarde las amenazas y las medidas correspondientes al área de aplicación correcta.
La principal distinción es si los dispositivos y los datos se utilizan en privado o dentro de una organización.

El sector privado: Se trata de personas y dispositivos que se utilizan en el ámbito privado. Esto incluye un ordenador portátil o teléfono inteligente, por ejemplo. El hecho de que lo uses públicamente, por ejemplo,

Co-funded by the Erasmus+ Programme of the European Union

Este proyecto ha sido financiado gracias al apoyo de la Comisión Europea. Esta publicación refleja únicamente el punto de vista del autor y la Comisión no se hace responsable de cualquier uso indebido que pueda hacerse de la información aquí presente.

en la WLAN de una universidad, tiene una importancia secundaria: lo importante es que utilices el dispositivo para gestionar tus datos privados.

Empresas y organizaciones: Se trata de dispositivos que pueden utilizarse para acceder a los datos de empresas u organizaciones, por ejemplo, ordenadores portátiles o teléfonos de empresa. Esto se refiere tanto a las empresas comerciales como a las empresas y organizaciones estatales, se trata de *datos compartidos*, que pertenecen a una organización.

¿Cuáles son exactamente las diferencias entre estas dos áreas de aplicación?

- **Área privada**

Casi todos los programas contienen errores de programación que se aprecian de una forma u otra. Esto se debe a la inexactitud, pero también al desconocimiento - porque nadie puede saber por qué "puerta trasera" o por qué característica especial del código del software se puede obtener acceso no deseado.

Esto resulta bastante problemático porque la mayoría de los dispositivos están constantemente conectados a Internet. El ordenador privado, el smartphone, el smartwatch, la televisión o el asistente de voz pueden conectarse a internet. En la mayoría de los casos, el "allanamiento" o el acceso no autorizado a los datos personales se realiza a través de Internet. El robo de datos también puede tener lugar físicamente, por ejemplo, mediante el allanamiento y el robo del ordenador.
Puede suceder tan rápidamente que consigan robar las contraseñas del banco, los documentos importantes y hacer públicas las fotos privadas.

La seguridad de la tecnología de la información es un tema importante en el sector privado, aunque los medios de seguridad de la tecnología de la información se utilizan menos en esta esfera, ya sea por la falta de conocimiento por parte de las personas que utilizan el sistema o también por las menores posibilidades técnicas.

- **Empresas y organizaciones**

Cuando se trata de la seguridad informática en las empresas, el foco principal es el interés económico. Aunque la implementación técnica de la seguridad informática suele ser mejor que en el sector privado, la energía delictiva detrás de los posibles ataques informáticos es mucho mayor.

Uno piensa en los bancos y las compañías de seguros que manejan mucho dinero. O compañías de alta tecnología que quieren asegurar sus prototipos e ideas de la competencia.
Los sistemas informáticos están ahora conectados a través de Internet también en este caso. Un ejemplo de ello sería el uso de un servicio en la nube desde varios lugares de una empresa: un servidor en la nube

Co-funded by the Erasmus+ Programme of the European Union

Este proyecto ha sido financiado gracias al apoyo de la Comisión Europea. Esta publicación refleja únicamente el punto de vista del autor y la Comisión no se hace responsable de cualquier uso indebido que pueda hacerse de la información aquí presente.

proporciona espacio de almacenamiento para documentos que pueden leerse y editarse a través de Internet desde todos los lugares. En este caso, se debe garantizar que sólo las personas autorizadas puedan acceder a estos documentos.

Las grandes empresas tienen ahora sus propios departamentos, que sólo se ocupan de la seguridad informática e invierten mucho dinero en mantenerse al día. Aquí también se aplica lo siguiente: No se sabe de antemano cómo ocurrirá un ataque informático, así que lo principal es poder reaccionar rápidamente si se produce un ataque.

Por cierto, hay documentos estandarizados para la seguridad informática, los llamados catálogos de protección básica, que presentan modelos detallados de seguridad informática. Sin embargo, las TIC se están desarrollando tan rápidamente que no basta con seguir estos catálogos y algunos de ellos se vuelven rápidamente obsoletos.

Recuerda
La seguridad informática es un sub-ámbito de la seguridad de la información y hace referencia a todas las medidas de protección en el procesamiento y almacenamiento de datos con la ayuda de los sistemas de tecnología de la información. Esto incluye los ordenadores, así como todos los demás medios de telecomunicación en entornos privados y comerciales. La seguridad informática también puede definirse en subáreas que están vinculadas entre sí: Seguridad informática Protección de datos Copia de seguridad de los datos Seguridad de los datos Las áreas de aplicación de la seguridad informática pueden asignarse tanto al sector privado como al empresarial y al público. Dado que la mayoría de los dispositivos están conectados a Internet, los peligros de los ataques informáticos y las medidas de seguridad de la tecnología de la información son bastante similares en todas las áreas; las diferencias se encuentran en la conciencia personal y en los factores tecnológicos.

5.3 Objetivos y ámbito de aplicación de la seguridad informática

La tarea más importante en la seguridad informática es seguir los avances **técnicos.** El mundo de la digitalización y las redes está progresando muy rápidamente en términos de tecnología. Las nuevas tecnologías requieren nuevos programas informáticos, las nuevas áreas de aplicación requieren nuevas medidas de seguridad.

Mientras que en el pasado unos pocos ordenadores grandes simplemente asumían tareas para empresas enteras y eran operados por unas pocas personas, hoy en día hay muchísimos pequeños dispositivos que están todos interconectados.

Puede ser bastante complicado incluso explicar qué es exactamente lo que hay que proteger de qué, qué amenazas hay y qué lagunas en los sistemas de seguridad podrían ser peligrosas.

Sin embargo, los **objetivos de protección, se** consideran los "principales objetivos" para la seguridad informática. Estos son:

confidencialidad - integridad - disponibilidad

Co-funded by the Erasmus+ Programme of the European Union

Este proyecto ha sido financiado gracias al apoyo de la Comisión Europea. Esta publicación refleja únicamente el punto de vista del autor y la Comisión no se hace responsable de cualquier uso indebido que pueda hacerse de la información aquí presente.

Si conscientemente se toman en serio estos tres objetivos de protección, ya se habrían implementado la mitad de la seguridad informática.

- **Confidencialidad**
  Los datos, la información y el conocimiento resultante deben ocultarse a las personas que no tienen derecho a verlos.

- **Integridad**
  Los datos, la información y el conocimiento resultante deben protegerse contra cambios y manipulaciones no autorizados.

- **Disponibilidad**
  Los datos, la información y los conocimientos resultantes deberían ser accesibles a quienes han permitido el acceso, cuando sea necesario.
  Estos tres objetivos son tan importantes y centrales porque son igualmente importantes en el contexto privado y empresarial. Echa un vistazo a los siguientes ejemplos:

Ejemplos
Los tres objetivos de protección en un contexto privado utilizando el ejemplo de la "banca en línea". Imagina que utilizas el acceso online para entrar en tu cuenta bancaria. Este es un tema delicado, porque tu dinero está en juego. ¿Cómo se cumplen los objetivos de protección aquí? **Confidencialidad**: Solo tú tienes acceso a los datos de acceso y de la cuenta y a las contraseñas. **Integridad**: Las personas no autorizadas no pueden hacer transferencias online. **Disponibilidad**: La cuenta tiene acceso ilimitado en cualquier momento y desde cualquier lugar. Los tres objetivos de protección en el contexto empresarial. Ejemplo del "desarrollo de productos". Una compañía desarrolla un producto completamente nuevo que va a revolucionar el mercado. Por supuesto, no queremos que la competencia saque beneficios. ¿Cómo podrían cumplirse los objetivos de protección en este caso? **Confidencialidad**: Solo las personas autorizadas tienen acceso a toda la información sobre el desarrollo del nuevo producto. **Integridad**: Protección de los datos obtenidos del desarrollo del producto contra el sabotaje y la manipulación del exterior. **Disponibilidad:** Todas las personas involucradas y autorizadas tienen acceso seguro al desarrollo del nuevo producto y a los datos resultantes.

Además, también hay objetivos de protección ampliada que deben considerarse según los requisitos. Éstos no tienen que estar necesariamente anclados en la seguridad de la tecnología de la información y pueden variar enormemente en el contexto privado y empresarial.

- **Rendición de cuentas o anonimato**

Co-funded by the Erasmus+ Programme of the European Union

Este proyecto ha sido financiado gracias al apoyo de la Comisión Europea. Esta publicación refleja únicamente el punto de vista del autor y la Comisión no se hace responsable de cualquier uso indebido que pueda hacerse de la información aquí presente.

Una acción en el entorno informático puede asignarse claramente a una persona - o no. En el contexto empresarial, se puede identificar a la persona responsable del sabotaje interno. En la vida privada, sin embargo, es más probable que ocurra lo contrario, es decir, que la persona goce del mayor anonimato posible en relación con sus datos - por ejemplo, al investigar temas relacionados con la salud en Internet.

- **Autenticidad**

Los datos, la información y los conocimientos deben verificarse en cuanto a su autenticidad, por ejemplo, si los resultados de la investigación son originales o han sido manipulados por un tercero.

- **No Repudio**

Las acciones en un entorno de las TIC no deben negarse sin más, lo cual es particularmente importante para los contratos procesados electrónicamente. En este caso, por ejemplo, se utilizan firmas electrónicas.

¿Cómo se lograrán estos objetivos en la práctica?

Esta pregunta se refiere a los **puntos débiles**. Se trata de encontrar y eliminar las vulnerabilidades. Como ya has aprendido, todo el software tiene puntos débiles. Estos no se identifican facilmente. A menudo se debe a una mala programación del software o al diseño del sistema informático. Esto no significa necesariamente que se haya hecho una programación "errónea", sino simplemente que no se han tenido en cuenta en la programación todas las amenazas conocidas de las herramientas TIC. Sin embargo, el ser humano o el mal manejo de los sistemas de herramientas TIC también pueden ser puntos débiles.

Importante
Por supuesto, la seguridad informática **también** se puede evitar a **través del hardware,** no sólo a través del software. Pero esto es menos práctico, porque para manipular datos a través del hardware, tienes que estar físicamente presente, por ejemplo, con un USB en la mano o llevándote todo el ordenador. Por lo tanto, acceder al software a través de Internet es más conveniente, y sobre todo más difícil de rastrear si te quedas a mitad.

Por lo tanto, para alcanzar los objetivos de protección de la seguridad de la tecnología de la información, es de enorme importancia identificar estos puntos débiles y los posibles escenarios de amenaza. Y aquí es donde

Co-funded by the Erasmus+ Programme of the European Union

Este proyecto ha sido financiado gracias al apoyo de la Comisión Europea. Esta publicación refleja únicamente el punto de vista del autor y la Comisión no se hace responsable de cualquier uso indebido que pueda hacerse de la información aquí presente.

la tarea se vuelve más difícil, porque no es posible obtener una representación del 100% de todos los puntos débiles debido al constante desarrollo de los sistemas y a la incapacidad general de mirar hacia el futuro - sólo se puede aproximar lo más posible.

Recuerda
La seguridad de la tecnología de la información depende en gran medida de los avances **tecnológicos actuales**; los nuevos ámbitos de aplicación de la tecnología de la información también entrañan nuevos peligros. Aquí se requiere una reacción rápida para poder ofrecer las contramedidas adecuadas. Hay **tres objetivos de protección** que deben cumplirse en todas las áreas de aplicación: • Confidencialidad • Integridad • Disponibilidad Hay tres objetivos de protección adicionales, que varían según la zona de aplicación y deben considerarse en consecuencia: • Atribuibilidad o anonimato • Autenticidad • Compromiso Para lograr estos objetivos de protección, la tarea principal **de la seguridad informática es identificar los puntos débiles de los sistemas** y eliminarlos en consecuencia. Esto también puede afectar al hardware, pero actualmente más bien al software - esto se refiere principalmente a errores de programación o a debilidades en la programación. Se intenta pero la seguridad informática perfecta pero no se cumple al 100%. Por ello, la seguridad informática debe tratarse como un todo.

5.4 Amenazas para las TIC

Las amenazas en las TIC son múltiples y no necesariamente tienen que ser de naturaleza intencional o criminal. También puede verse amenazada por "fuerza mayor" y/o fallos técnicos, por ejemplo, un terremoto podría causar un corte de energía que resultara en la pérdida de datos.

Pero por supuesto, el error humano también es concebible. Un ejemplo clásico de esto es: un olvido de la contraseña del banco en línea, por lo que la información ya no estaría disponible.

Ahora aprenderás sobre las posibles amenazas informáticas, teniendo siempre en cuenta los objetivos de protección del capítulo anterior.

Importante
Por cierto, una posible amenaza no significa automáticamente que las TIC estén en peligro. Sólo se considera que una amenaza es real si el punto débil (por ejemplo, un error de programación o una red WLAN de fácil acceso) también se encuentra amenazado (por ejemplo, mediante el ataque de un hacker).

Ataques dirigidos por personas u organizaciones

En primer lugar, por supuesto, son los ataques que se llevan a cabo deliberadamente los que deben evitarse mediante una seguridad informática apropiada. El normalmente denominado "hacking", consiste en que un individuo o incluso una organización entera obtiene acceso no autorizado a datos extranjeros y trata de eludir

Co-funded by the Erasmus+ Programme of the European Union

Este proyecto ha sido financiado gracias al apoyo de la Comisión Europea. Esta publicación refleja únicamente el punto de vista del autor y la Comisión no se hace responsable de cualquier uso indebido que pueda hacerse de la información aquí presente.

la protección y seguridad informática. Esto se hace por diferentes razones: por el robo de fondos, sabotaje de empresas competidoras, motivación política, a veces simplemente por "diversión", pero siempre se trata de obtener, manipular o destruir información a través de la red a la que están conectados los dispositivos de destino.

Las herramientas más importantes de esos ataques de piratería informática son conocidas por las películas de Hollywood del cambio de milenio y suelen tener nombres graciosos: "virus", "troyanos", "gusanos", "spoofing", "phishing" y otros. Echemos un vistazo a algunos de estos ejemplos:

- **Virus**

Los virus informáticos son simplemente programas que realizan automáticamente su tarea programada en los sistemas de destino: por ejemplo, rastrear una contraseña. Los virus necesitan un llamado anfitrión para

propagarse. Este puede ser un correo electrónico masivo o un llamado "pop-up" - un sitio web de auto-apertura, por ejemplo, que apunta a una actualización supuestamente necesaria.

- **Gusanos**

Se trata de virus que pueden propagarse activamente por sí mismos, lo que significa que detectan activamente puntos débiles en los sistemas y redes y se reenvían a sí mismos en consecuencia sin que esté presente el llamado "anfitrión".

- **Troyanos**

También conocidos como "caballos de Troya", son programas aparentemente útiles que la víctima instala por sí misma, pero en el fondo, los troyanos abren independientemente puertas traseras en el sistema, reenvían datos e información y pueden, por ejemplo, registrar las contraseñas que se introducen.

- **Ataques de denegación de servicio**

En este caso, es más probable que se manipule la disponibilidad de los datos: al sobrecargar deliberadamente el sistema desde el exterior (esto puede hacerse, por ejemplo, llamando automáticamente y de forma repetida a un sitio web), el sistema se paraliza. A veces esto sucede hasta que la organización afectada paga un rescate, por ejemplo. Por cierto, el software para los métodos de chantaje se denomina también "programa de rescate".

- **Spoofing/Phishing**

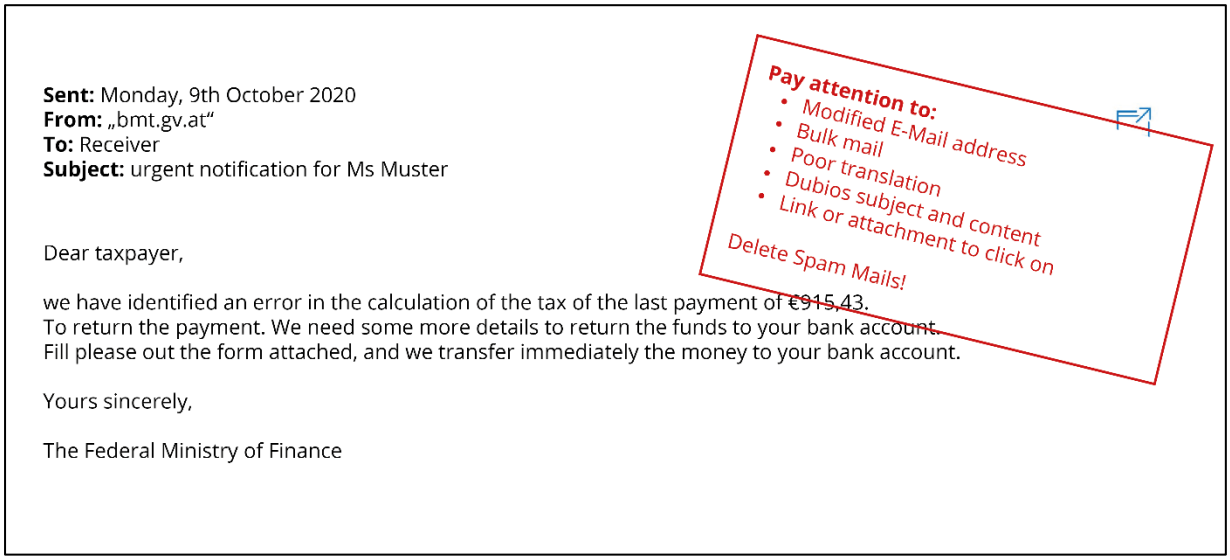
Co-funded by the Erasmus+ Programme of the European Union

Este proyecto ha sido financiado gracias al apoyo de la Comisión Europea. Esta publicación refleja únicamente el punto de vista del autor y la Comisión no se hace responsable de cualquier uso indebido que pueda hacerse de la información aquí presente.

Se trata principalmente del robo de identidad. Los sitios web falsos en Internet y los correos electrónicos que se vinculan a ellos, atraen a la víctima a compartir activamente contraseñas o información de cuentas. Estos se encuentran principalmente en el sector privado de la seguridad informática.

- **Spam**

Por cierto, el término probablemente más conocido en el ámbito de la seguridad informática no describe nada más que los correos electrónicos no solicitados, que pueden ser molestos boletines informativos, pero por supuesto también anfitriones de virus o intentos de phishing.



El malware mencionado también puede, por supuesto, "inyectarse" personalmente en el sistema informático: la información puede robarse o manipularse irrumpiendo físicamente en el edificio o la casa de la empresa. Sin embargo, debido a la conexión en red de los sistemas informáticos, esto ya no suele ser necesario.

Pero a veces tal manipulación física ocurre simplemente de forma interna. Por ejemplo, cuando el personal de su propia empresa roba datos de clientes o secretos de productos sin autorización para venderlos externamente.

Amenaza involuntaria de error humano

Pero las amenazas a la seguridad informática no siempre tienen que ser altamente criminales y deliberadas. A veces es simplemente la ignorancia en el manejo de las TIC lo que representa una amenaza:

- **Contraseñas**

Una buena contraseña es, en el mejor de los casos, difícil de recordar, esto es, por supuesto, poco práctico. Mucha gente todavía usa contraseñas que son demasiado débiles. 12345 por ejemplo es una contraseña débil. UfNS3-?ßsDa-hUdk& - es bastante diferente - cuantos más símbolos diferentes, caracteres especiales, números y letras, mejor.
Como ves, encontrar una contraseña adecuada y segura que la persona en cuestión pueda recordar no es tan fácil. Sobre todo, porque muchos sistemas le piden regularmente que cambie de contraseña y no se recomienda usar la misma contraseña más de una vez.

Excursus
Existen los llamados **gestores de contraseñas** que pueden ser utilizados tanto en el ámbito privado como en el empresarial. Son programas que pueden generar y almacenar contraseñas seguras para

Co-funded by the Erasmus+ Programme of the European Union

Este proyecto ha sido financiado gracias al apoyo de la Comisión Europea. Esta publicación refleja únicamente el punto de vista del autor y la Comisión no se hace responsable de cualquier uso indebido que pueda hacerse de la información aquí presente.

sitios web o programas. El programa en sí mismo está asegurado con una llamada llave **maestra**, es decir, UNA contraseña principal.

Las ventajas y desventajas son obvias: Puedes usar una variedad de contraseñas diferentes y seguras y no tienes que recordarlas individualmente. Pero si la contraseña principal es descifrada, se puede acceder a todas las contraseñas almacenadas. Un administrador de contraseñas sólo es seguro si la contraseña principal es fuerte y preferiblemente se cambia regularmente.

Sin embargo, la transmisión de contraseñas también es un problema. Esto no tiene que ser intencionalmente de mala fe. Imagina que quieres ayudar a un colega y darle rápidamente tu propio acceso al sistema. O el administrador del sistema solicita la contraseña para una comprobación. Esto puede llevar a situaciones críticas, especialmente cuando hay gente involucrada que roba deliberadamente las contraseñas de esta manera.

- **Trae tu propio dispositivo**

"Trae tu propio dispositivo" - esto no significa que lleves algo a una fiesta, sino que lleves tus propios dispositivos, como discos duros externos, memorias USB, smartphones y similares. Si la información interna de la empresa se almacena o edita en estos dispositivos, entonces la seguridad informática interna no puede ayudar realmente. Esto es especialmente crítico cuando la práctica se lleva a cabo en la llamada "oficina en casa", es decir, trabajar para una organización desde casa.

A veces, los medios de almacenamiento están "preparados" con programas informáticos maliciosos por terceros y luego se distribuyen deliberadamente a personas que trabajan para determinadas empresas, por ejemplo. Esto sucede, por ejemplo, en las ferias profesionales, donde a menudo se regalan memorias USB.

- **Instalación de aplicaciones no autorizadas**

Puede que te suceda lo siguiente. El portátil de la empresa es demasiado lento, así que "te ocupas tú mismo" instalando programas antivirus y otras cosas. Quizá te gusta jugar en tu tiempo libre en el trabajo y descargas sin querer un malware en ordenador de la empresa. Esto también puede provocar amenazas a la seguridad informática debido a la falta de conciencia.

Estas son esencialmente las principales amenazas a la seguridad de la tecnología de la información. Como ya se ha explicado, hay acontecimientos completamente imprevisibles que también pueden suponer una amenaza a las TIC: los desastres naturales como el fuego, los rayos o las inundaciones pueden paralizar o destruir completamente los sistemas informáticos.

Recuerda

Una amenaza real en términos de seguridad informática es un punto débil interno que se encuentra con una amenaza externa.

Tal amenaza puede ser un ataque deliberado, no intencional por parte de los humanos o por "fuerza mayor" como los desastres naturales.

Ataques deliberados:

3. Malware como virus, gusanos y troyanos

4. La intrusión física y el robo o la manipulación de información o sistemas informáticos

5. Robo de identidad o extorsión a través de phishing, rescates y ataques de negación de acción

Co-funded by the Erasmus+ Programme of the European Union

Este proyecto ha sido financiado gracias al apoyo de la Comisión Europea. Esta publicación refleja únicamente el punto de vista del autor y la Comisión no se hace responsable de cualquier uso indebido que pueda hacerse de la información aquí presente.

Peligro involuntario

6. Seguridad débil o compartir contraseñas.

7. El uso de dispositivos privados en entornos corporativos.

8. Instalación de aplicaciones no autorizadas

Fuerza mayor

9. Desastres naturales que posteriormente conducen a la destrucción o parálisis de los sistemas informáticos.

5.5 Medidas de seguridad en las TIC

La seguridad informática ofrece varias medidas, y no sólo en el aspecto técnico. **Hacer que la gente sea consciente de los programas maliciosos o del comportamiento dañino e inconsciente en la empresa o en su vida privada ya suele ayudar** mucho.

A tal efecto, a menudo se ofrecen cursos y talleres de formación, que pueden evitar uno u otro problema informático en la vida privada. Dentro de las empresas, a veces se diseñan estrategias para integrar la seguridad informática de forma holística y lo más completa posible en los procesos. Sin embargo, esto no puede funcionar si no se conciencia al personal de la empresa previamente.

Sin embargo, las inversiones en información y sensibilización no son suficientes, así que ¿qué más forma parte de la seguridad informática?

Software

Lo primero es obvio: existe el llamado **software antivirus** que analiza automáticamente su sistema informático y comprueba si hay malware. Esto ocurre en intervalos cortos y regulares y es útil tanto en ambientes privados como de negocios. De este modo, se pueden detectar y prohibir las lagunas de seguridad y los programas maliciosos que se quieran descargar de Internet.

Ya lo sabes, pero aún así no puedes confiar en él al 100%. A veces, el malware simplemente no se detecta como tal, o el software seguro se identifica como malware, se elimina automáticamente y luego el ordenador deja de funcionar. Por lo tanto, no es aconsejable confiar ciegamente en un programa antivirus.

Los llamados cortafuegos o **"firewalls"** también son medios populares tanto en el ámbito privado como en el empresarial. Se encargan de las conexiones de red de las TIC, por ejemplo, con la WLAN. Aquí, el acceso no autorizado desde el exterior a través de la red puede detectarse y prevenirse. En la mayoría de los casos, estos cortafuegos ya están integrados en los productos de software antivirus.

Las cajas de arena o **"sandbox"** son algo interesante, no sólo para los niños. En la seguridad informática, una caja de arena es un programa que bloquea el malware. Este concepto relativamente nuevo es particularmente efectivo para tipos de datos especiales. Por ejemplo, los documentos PDF se abren en un "cajón de arena" separado de otros programas. Si el PDF se daña, en el peor de los casos sólo se ataca al programa de la caja de arena, el resto del sistema se salva.

El uso de diferentes programas informáticos y, a veces, confiar en proveedores más pequeños puede resultar rentable, por cierto - **cuanto más "diversa" sean las TIC, más difícil será descifrar el sistema en su conjunto.** A veces las empresas de software antivirus más conocidas se ven especialmente afectadas por los ataques de los hackers, simplemente porque son los más comunes.

Co-funded by the Erasmus+ Programme of the European Union

Este proyecto ha sido financiado gracias al apoyo de la Comisión Europea. Esta publicación refleja únicamente el punto de vista del autor y la Comisión no se hace responsable de cualquier uso indebido que pueda hacerse de la información aquí presente.

Control de acceso

El control de acceso no significa simplemente una contraseña demasiado larga. Las empresas se ayudan entre sí con diferentes derechos de usuario. **Sólo muy pocas personas en la empresa tienen acceso a todos los datos, por lo general estos están limitados y divididos de acuerdo con la función en la empresa.**

También se puede aplicar el **acceso restringido a las páginas de Internet** o la prevención de programas informáticos externos en los ordenadores de las empresas. La red WLAN de la empresa también puede diseñarse para que sólo una selección muy limitada de aplicaciones y programas puedan ser descargados y utilizados.

Además, también existe la posibilidad de evitar el "contenido activo": el software autoejecutable (a menudo se trata de programas de utilidad) se desactiva de esta manera. Esto también puede ser efectivo contra el potencial malware. Por supuesto, las medidas mencionadas aquí tienen más probabilidades de aplicarse en un contexto comercial.

Sin embargo, **la criptografía** puede utilizarse con fines comerciales y privados. Se trata de una encriptación de datos. No sólo se asegura el acceso a los datos con una contraseña, sino que los datos en sí mismos están "encriptados".

Excursus
Criptografía de datos e información - de extremo a extremo La encriptación de extremo a extremo es un estándar común en la encriptación de datos. Aquí, el emisor y el receptor tienen un código traductor. El remitente envía mensajes o imágenes. Sin embargo, el código traductor cambia automáticamente los datos del mensaje en secuencias incomprensibles de números y símbolos. El receptor recibe estos y puede a su vez visualizar y comprender el mensaje o la imagen en su forma original gracias al traductor. Esto simplemente sirve para **que los datos posiblemente interceptados en el proceso de envío no puedan ponerse en un contexto** y, por lo tanto, sigan siendo incomprensibles.

Copias de seguridad y actualizaciones

Las actualizaciones regulares del software para mantenerlo al día también ayudan, por supuesto. Cuanto más antiguo es un software, más pronto se conocen sus errores. Especialmente los sistemas operativos y los programas antivirus deben actualizarse rápidamente, ya que las mayores amenazas son las que plantea el acceso externo.

Por supuesto, sólo hay una cosa que puede ayudar contra la pérdida de datos (si, por ejemplo, el ordenador se rompe o lo roban): las copias de seguridad regulares, es decir, copiar los datos y la información por sí mismo - preferiblemente separadas del sistema informático en un disco duro externo o en la llamada "nube". Los sistemas en la nube son servidores externos y lugares de almacenamiento que están disponibles a través de Internet. Aquí también se puede automatizar una copia de seguridad, pero por supuesto también existe el riesgo de que el propio proveedor de la nube se convierta en víctima de un ataque informático.

Recuerda
Concienciar a la gente sobre la correcta utilización de la seguridad informática, tanto en el ámbito privado como en el empresarial, es muy importante. También hay una serie de medidas de seguridad informática: **Software**

Co-funded by the Erasmus+ Programme of the European Union

Este proyecto ha sido financiado gracias al apoyo de la Comisión Europea. Esta publicación refleja únicamente el punto de vista del autor y la Comisión no se hace responsable de cualquier uso indebido que pueda hacerse de la información aquí presente.

Programas antivirus
Cortafuegos
Cajas de arena
Despliegue diverso del sistema informático
Control de acceso
Diferentes derechos de usuario
Acceso restringido a sitios web y programas en Internet
Criptografía
Medidas adicionales
Copias de seguridad regulares
Últimas actualizaciones

5.6 Resumen

La seguridad informática es un ámbito dentro de la seguridad de la información y hace referencia a todas las medidas de protección en el procesamiento y almacenamiento de datos en un sistema informático, tanto en el ámbito privado como en el empresarial. Esto incluye **la seguridad informática, la protección de datos y la copia de seguridad de los datos.**

La seguridad de la tecnología de la información depende en gran medida de los avances **tecnológicos actuales**. Sobre todo, es necesario reaccionar rápidamente para poder ofrecer contramedidas adecuadas. Hay **tres objetivos básicos de protección** que deben cumplirse en todas las áreas de operación:

confidencialidad - integridad - disponibilidad

Para lograr estos objetivos de protección**, la tarea fundamental de la seguridad informática es identificar las debilidades de los sistemas y eliminarlas en consecuencia**. Una amenaza real en el sentido de la seguridad informática es cuando un punto débil interno se encuentra con una amenaza externa.

Esa amenaza puede ser un ataque **deliberado** para robar o manipular datos (por ejemplo, con programas informáticos malignos a través de Internet o irrumpiendo físicamente en el departamento de informática de una empresa).

Pero un sistema informático también puede verse amenazado involuntariamente**,** por ejemplo, por una contraseña débil o por desastres naturales que dañen los sistemas informáticos.

Concienciar a la gente sobre la correcta utilización de la seguridad informática, tanto en el ámbito privado como en el empresarial es de gran ayuda. Además, hay **software de protección, controles de acceso restrictivo** y otras medidas de seguridad informática para minimizar las posibles amenazas.

Co-funded by the Erasmus+ Programme of the European Union

Este proyecto ha sido financiado gracias al apoyo de la Comisión Europea. Esta publicación refleja únicamente el punto de vista del autor y la Comisión no se hace responsable de cualquier uso indebido que pueda hacerse de la información aquí presente.