Práctica 1

PRIMER CONTACTO CON EL SECTOR DE LA CIBERSEGURIDAD

José Ángel Dorado González

Seguridad Informática

ÍNDICE

1º) Buscar al menos 5 foros técnicos (pueden ser listas de correo, boletines de noticias, webs, comunidades de noticias o de un producto o software, etc.) que traten temas de ciberseguridad. Describe brevemente el foro, quien lo mantiene (empresa, colectivo, usuarios, etc.), número de usuarios aproximados, valora su peso en la comunidad y en el sector, qué tipos de temas trata o si está especializado en algún tema concreto, etc.

Wilders Security Forums - https://www.wilderssecurity.com/

Es uno de los foros sobre ciberseguridad más populares, el cual sirve de recurso para aprender e investigar sobre casi cualquier tema de seguridad, por lo que el peso que tiene en el sector es enorme.
Está diseñado mediante una interfaz sencilla e intuitiva y su contenido está basado en multitud de temas relacionados con la seguridad informática, cuenta con más de 2.7 millones de posts y más de 250.000 hilos. Dentro de él, podrás encontrar sub-foros dedicados a casi todo, como problemas de seguridad, de cifrados móviles..
Dentro de la cabecera podemos acceder a las siguientes páginas:

- Foros: Página donde encontraremos todos los posts que han sido publicados de cualquier categoría.
- Miembros: Información sobre los miembros del foro.
- Productos de seguridad: Página donde encontraremos todos los posts que han sido publicados sobre los productos basados en seguridad.
- Privacidad: Página donde encontraremos todos los posts que han sido publicados sobre privacidad.

Actualmente está formado por más de 129.000 miembros, situándose como uno de los foros más grandes relacionados con la ciberseguridad.
Este foro se encuentra mantenido por los usuarios de la comunidad.

AntiOnline - https://www.antionline.com/

Es un foro sencillo, que se presenta como una larga lista de temas, donde dentro de cada uno encontraremos una gran variedad de posts relacionados con la temática seleccionada. Se utiliza un lenguaje técnico para la mayoría de posts, por lo que estaría dedicado a aquellas personas que tienen un buen conocimiento de ciberseguridad pero sin ser expertos.
La temática del foro es variada, tratando temas como firewalls, ciber-estafas o antivirus, aunque también tiene un espacio que está dedicado a temas como el cumplimiento de normativas, conferencias o aspectos éticos y morales de privacidad.
Actualmente cuenta con más de 100.000 miembros, más de 826.000 posts y más de 235.000 hilos.
El foro lo mantiene la empresa TechnologyAdvice, cuyo objetivo es crear oportunidades para los compradores y proveedores de tecnología.

Hack Forums - https://hackforums.net

Foro popularmente conocido con más de 3.5 millones de usuarios y más de 50 millones de post, siendo uno de los más activos. Está situado como uno de los más importantes

internacionalmente, no solo por los temas dedicados a la ciberseguridad, sino por las diferentes temáticas tecnológicas que posee, convirtiéndose en uno de los mejores sitios para discutir sobre cualquier tema relacionado con la informática.
Su contenido es muy variado y se puede encontrar casi cualquier tema relacionado con la seguridad, como malware o virus. Además, existen subforos que están dedicados a la protección de equipos y alertas de seguridad, por lo que se puede encontrar información muy valiosa. Un aspecto llamativo es que también existe un espacio dedicado a la programación, juegos, etc.
Este sitio es mantenido por Hack Forums, apoyado por la comunidad del foro y los patrocinadores que posee.

/r/NetSec - https://www.reddit.com/r/netsec/

Creado en 2007.

Alojado en el foro de Reddit, /r/NetSec es un subreddit donde se publican noticias, análisis y opiniones sobre todo lo relacionado con la seguridad informática. La comunidad de este sitio es bastante grande, ya que cuenta con más de 457.000 suscriptores.
El foro está especialmente dedicado a personas expertas, ya que se discuten temas en los que el contenido es complejo, por lo que puede que no sea correctamente entendido o que sea de poco interés para los usuarios principiantes. Por este motivo la importancia de este foro es relativa, debido a que no es inclusivo para todos los tipos de usuarios que quieren aprender más sobre la seguridad informática.
El sitio es mantenido principalmente por los usuarios, ya que se encuentra alojado en Reddit.

MalwareTips - https://malwaretips.com/

Creado en 2010.

Foro con un diseño más llamativo, formado por más de 60.000 miembros, más de 890.000 mensajes y más de 88.000 hilos.

Contiene diferentes secciones como son:

- Foros: Aquí es donde se encuentran todos los posts divididos en categorías, donde las mejores son las de “Software” y el “War Room”.
    - La sección de software se divide en aplicaciones generales y aplicaciones de seguridad. Las aplicaciones generales cubren la seguridad de los sistemas operativos o reproductores multimedia, mientras que la sección de aplicaciones de seguridad se centra en los software anti-virus y en las herramientas de eliminación de software malicioso.
    - La sección War Room se utiliza para que los usuarios comparen y discutan sobre dos aplicaciones.
- Noticias: En este apartado se exponen las noticias sobre la ciberseguridad actualizadas regularmente.
- Regalos: En este apartado se muestran diferentes regalos y promociones.
- Reseñas: Apartado en el que los usuarios pueden comentar diferentes aspectos que observen en la web.

- Apoyo: En este apartado se ofrece ayuda en la web.
- Blog: En este apartado aparecen tutoriales sobre diferentes temas, tales como “Ajustar y asegurar Windows” o “Cómo evitar el malware”.

Este sitio es mantenido por MalwareTips y por los usuarios de la comunidad.

2º)Idem para 5 páginas web de medios generalistas de noticias de ciberseguridad, es decir, páginas web de noticias de ciberseguridad o bien medios de comunicación especializados. O de medios generalistas que tengan buenas secciones de tecnología con temas de seguridad.

Wired - https://www.wired.com/

Wired es una revista mensual estadounidense que existe desde 1993 y un sitio web de noticias tecnológicas conocido internacionalmente, que cuenta con una sección dedicada a la seguridad. En la actualidad, posee bastante peso en este sector, debido a que aunque no es un portal únicamente centrado en la ciberseguridad, posee una gran cantidad de seguidores. La web de Wired, además de contener información de noticias actuales muy completa, cuenta con un diseño brillante. Por todo esto, se convierte en una de las páginas líderes en noticias tanto tecnológicas como de seguridad informática.

Se desconoce el número exacto de usuarios que frecuentan el sitio web, pero una noticia publicada a mediados de mayo de 2019, publicó que el número de suscriptores aumentó en un 300% con respecto al año anterior. Además, hay que tener en cuenta que su cuenta de Twitter cuenta con más de 10.2 millones de seguidores.

La revista es mantenida por Condé Nast Publications, qué es la editorial propietaria de la revista.

ThreatPost - https://threatpost.com/

Es una de las publicaciones más completas y actualizadas sobre ciberseguridad, cuenta con un diseño sencillo pero atractivo, lo que la convierte en una web de noticias muy accesible.

Este portal de noticias cuenta con el respaldo de Kaspersky Labs, que es una compañía internacional dedicada a la seguridad informática, con sede en Moscú. Por lo que ThreatPost está dirigido por expertos en comunicación centrados en el área de la ciberseguridad. Por la importancia de Kapersky Labs mundialmente y su objetivo de tener las noticias actualizadas frecuentemente, se puede considerar esta web de noticias una de las más influyentes en el sector.

No se conoce a ciencia cierta el número de usuarios que siguen este periódico digital, aunque se puede realizar una estimación teniendo en cuenta que en Twitter cuenta con más

de 231.000 seguidores, además posee un canal de YouTube en el que se discuten temas sobre ciberseguridad con diferentes invitados.

Revista Byte TI - https://revistabyte.es/

Byte fue una revista de informática estadounidense surgida en 1975, actualmente sus publicaciones solo son visibles vía internet. Dicho espacio online fue fundado en el año 2000 y adoptó el nombre de Revista Byte TI.

Esta revista cubre las noticias relacionadas con ordenadores y software, aunque existe un espacio dedicado especialmente a la ciberseguridad. Dicha revista fue muy influyente a finales de 1970 y en la década de 1980, aunque en la actualidad no es tan visitada como otras de esta lista, esto se ve reflejado en los poco más de 9.000 seguidores en Twitter y 3.000 en Facebook.

En general, posee un buen diseño con diferentes secciones de noticias tecnológicas divididas en categorías. De este espacio web hay que destacar su apartado de entrevistas donde se tratan diferentes temáticas actuales, otro aspecto llamativo del sitio es que se encuentra escrito en español, siendo uno de los pocos de esta lista.

Actualmente se encuentra mantenida por la editorial MKM Publicaciones, especializada en informática.

WeLiveSecurity - https://www.welivesecurity.com/la-es/

WeLiveSecurity es un portal web que reúne las noticias más actuales de seguridad y de tecnología, para que empresas y usuarios estén al día de las noticias de este campo. Cabe recalcar que este sitio web se encuentra más centrado en la temática de ciberseguridad.

Posee un diseño bastante sencillo y limpio pero contiene todo tipo de información actual, se encuentra dividido en secciones donde podemos encontrar algunas como vulnerabilidades, investigaciones, cibercrimen o informes. Además, podemos encontrar una sección de resumen donde están publicadas las noticias más importantes de cada mes. Un aspecto llamativo es que se encuentra disponible en los siguientes lenguajes: español, portugués, inglés y alemán.

Este periódico digital se encuentra mantenido por la firma de seguridad ESET junto con Frontech, donde sus objetivos son servir materiales educativos e informativos a la comunidad en el sector de la seguridad informática.

La importancia de este portal es enorme, ya que se encuentra respaldada por una gran compañía como es ESET, la cual posee más de 35.700 seguidores en Twitter y un canal en YouTube con más de 13.000 suscriptores, donde cuelgan vídeos de concienciación, de ciberseguridad o tutoriales.

MuySeguridad - https://www.muyseguridad.net/

MuySeguridad es una publicación online de referencia para los profesionales de seguridad informática, es un espacio dedicado únicamente al ámbito de la ciberseguridad.

Posee un diseño claro, limpio y muy visible donde se encuentra la información muy bien estructurada. En este medio se puede encontrar las noticias más actuales sobre nuevas amenazas, estrategias o gestión de los datos de la empresa. Además, en esta plataforma puedes encontrar la opinión de los mejores expertos en ciberseguridad, entrevistas, reportajes, contenidos prácticos o eventos, donde se publican las noticias más relevantes de los eventos de ciberseguridad realizados. Un aspecto llamativo y curioso es que existe un espacio únicamente dedicado a ataques de ransomware.

En la actualidad, no es un sitio que se frecuente mucho por los internautas de la red, esto se puede ver reflejado en los 341 seguidores que tienen en Twitter y en los más de 5000 en Facebook. Aún así, en un sitio muy interesante, con buenas secciones y con información completa sobre seguridad informática.

Este periódico digital se encuentra mantenido por MuyComputerPRO, web dedicada por y para los profesionales de la tecnología.

3º)Recopila al menos 5 noticias más o menos actuales que te interesen sobre ciberseguridad en los medios anteriormente encontrados en el apartado 1 y 2. Esto te ayudará a considerar diversos temas de interés y de actualidad y tomar un poco el pulso del sector.

Un desarrollador filtra el generador de ransomware de LockBit a la Red - https://revistabyte.es/actualidad-it/generador-de-ransomware-lockbit/

Esta noticia relata cómo un desarrollador que estaba descontento con el liderazgo de LockBit, publicó en Github el generador de ransomware de LockBit. Según los expertos, esto va a provocar una oleada de ciberataques utilizando dicha herramienta, debido a que la herramienta está disponible públicamente para todos, incluidos los atacantes.

Así roban los ciberdelincuentes tu cuenta de Steam ¡Cuidado! - https://www.muyseguridad.net/2022/09/16/asi-roban-tu-cuenta-de-steam/

En esta noticia se explica cómo los ciberdelincuentes roban las cuentas de Steam, utilizando una técnica de phishing conocida como Browser-in-the-Browser. Esta técnica involucra la creación de ventanas de navegador falsas dentro de una ventana activa, haciéndose pasar como una página web legítima. Dichos enlaces llevan a una supuesta página que patrocina y organiza competiciones de deportes electrónicos, donde los usuarios deben utilizar sus credenciales para iniciar sesión, una vez introducidas son cambiadas.

Cabe destacar que la campaña de Steam a la que se refiere esta noticia busca preferentemente cuentas de jugadores profesionales, las cuales pueden valer hasta 100.000 dólares.

Campaña de Lazarus dirigida a Bélgica y Países Bajos utiliza falsa oferta de trabajo de Amazon - https://www.welivesecurity.com/la-es/2022/09/30/ataque-grupo-lazarus-belgica-paises-bajos-falsa-oferta-trabajo-amazon/

Esta noticia explica las dos últimas vulnerabilidades que sufre Microsoft, llamadas zero-day. Estas están siendo utilizadas de forma conjunta en campañas para conseguir acceso a los servidores de Microsoft Exchange y así poder ejecutar código de manera remota en los sistemas comprometidos. Afectan a las versiones 2013, 2016 y 2019 de Microsoft Exchange Server.

Cybercriminals Are Selling Access to Chinese Surveillance Cameras - https://threatpost.com/cybercriminals-are-selling-access-to-chinese-surveillance-cameras/180478/

En esta noticia se explica como miles de cámaras de vigilancia, de la marca Hikvision, no han parcheado una CVE crítica, dejando expuestas a miles de organizaciones. Se trata de un fallo de inyección de comandos que fue descubierto hace 11 meses. Los ciberdelincuentes acceden a dichas cámaras para posteriormente poner a la venta las credenciales en la web oscura.

The Uber Hack's Devastation Is Just Starting to Reveal Itself - https://www.wired.com/story/uber-hack-mfa-phishing/

Esta publicación detalla la noticia del hackeo de Uber, en el que un joven de 18 años pudo acceder a toda la información y datos de la empresa, obligando a Uber a desconectar varias herramientas como Slack. El ciberdelincuente habría utilizado una técnica de ingeniería social, en la que habría vulnerado la seguridad mediante un mensaje de texto enviado a un empleado de la compañía, haciéndose pasar por una persona del equipo técnico de Uber. Al final, el joven persuadió al trabajador y este último le envió una contraseña, la cual le permitió acceder a los servicios de la empresa.

4º)Recopila al menos 5 noticias sobre ciberseguridad en medios de comunicación tradicionales no especializados en ciberseguridad, es decir, en la prensa nacional y/o internacional.

OCU insta a Google a actuar ante el fallo de seguridad detectado en el lector de huellas de Pixel 6a - https://www.cope.es/actualidad/tecnologia/noticias/ciberseguridad-ocu-insta-google-actuar-ante-fallo-seguridad-detectado-lector-huellas-pixel-20221006_2328943

En esta noticia del periódico digital COPE, se detalla como la OCU (Organización de Consumidores) insta a Google a resolver un problema de seguridad encontrado en el teléfono Pixel 6a. Este fallo implica un mal funcionamiento del sistema de huellas dactilares, el cual permite desbloquear el smartphone a usuarios que no han registrado su huella, o con huellas no registradas en el dispositivo.

Descubren casi 200 apps Android infectadas con Harly, un malware más dañino que Joker -
https://as.com/meristation/2022/10/06/betech/1665054460_293914.html

Esta noticia del diario As, explica cómo se ha colado en más de 190 aplicaciones de Google Store un malware llamado Harly. Su funcionamiento es simple, los usuarios se descargan una aplicación aparentemente normal, una vez instalada se inyecta en el dispositivo un código malicioso, el cual permite a los ciberdelincuentes obtener información del afectado, para posteriormente adquirir sin su consentimiento una suscripción. Hay que destacar que el número de descargas de estas aplicaciones con código malicioso asciende a 4.8 millones, aunque actualmente este malware solo se encuentra en Tailandia.

Cuidado, este malware espía podría grabarte para hacerte chantaje -
https://www.elespanol.com/elandroidelibre/aplicaciones/20221006/cuidado-malware-espia-podria-grabarte-hacerte-chantaje/708679179_0.html

Esta noticia publicada por el diario El Español, explica el descubrimiento de un malware muy peligroso llamado RatMilad. Este malware espía permite extraer datos almacenados de un dispositivo, realizar grabaciones de audio o vídeo y permite acceder a sistemas corporativos privados. Se distribuye a través de un generador de números virtuales llamado NumRent, al instalarlo en el móvil solicita los permisos para la instalación de RatMilad. El objetivo de infectar a los dispositivos con este malware es realizar chantajes con la información obtenida.

Wintermute, un nuevo atraco de criptodivisas por USD 160 millones -
https://www.france24.com/es/programas/econom%C3%ADa/20220920-wintermute-un-nuevo-atraco-de-criptodivisas-por-usd-160-millones-y-otros-grandes-robos

Esta noticia proporcionada por el diario digital France 24, relata cómo la firma de comercio de criptomonedas Wintermute sufrió un ataque informático, provocando el robo de 90 activos digitales por valor de unos 160 millones de dólares.

El FBI está investigando al hacker que filtró GTA VI -
https://www.marca.com/claro-mx/esports/2022/09/20/6329dc5522601d353d8b4587.html

La noticia publicada por el diario Marca, explica uno de los casos más llamativos dentro de los ataques informáticos a videojuegos. Un joven habría atacado a los servidores de la compañía Rockstar Games, permitiéndole el acceso a toda la información del juego GTA VI, incluyendo código fuente y varios vídeos de este. Posteriormente, el atacante habría solicitado dinero a la empresa para no divulgar toda la información obtenida. Al parecer el ciberdelincuente pertenece al grupo de piratas informáticos Lapsus, responsables entre otras cosas, del hackeo a Uber.

5º)¿Cuáles son los sistemas operativos (SO) más usados en el mundo? Busca información sobre ello y haz una lista con al menos 5, ordenada de más uso a menos uso. Haz al menos dos categorías, una para SO servidores y otra para SO de escritorio. Cita las fuentes que utilices.

Sistemas operativos para escritorio
Es un conjunto de programas que permiten manejar tanto los recursos físicos (hardware) como los programas (software) en una computadora.

El sistema operativo es el programa principal que debe tener una computadora y sirve de base para que se puedan ejecutar los programas llamados de aplicación, sin este los ordenadores no podrían funcionar. Esta información ha sido extraída de la siguiente página: https://www.uv.mx/apps/afbgcursos/Cursos%20anteriores/CBApoyoModalidadPresencial/internet/leccion1.html

Para la clasificación de los sistemas operativos más utilizados en escritorio, tendremos en cuenta un análisis desarrollado en 2021. La información ha sido extraída de la siguiente página: https://itsoftware.com.co/content/sistemas-operativos-mas-usados/

1. Windows
2. OSX
3. Linux
4. Chrome OS
5. FreeBSD

Sistemas operativos para servidores
Un sistema operativo para servidor es una plataforma que permite ejecutar programas y aplicaciones multiusuario. Además, estos sistemas operativos ofrecen la posibilidad de comunicarse con otros servidores para atender las solicitudes específicas de sus clientes. Por eso las grandes empresas los utilizan para gestionar de forma rápida y eficaz los recursos de una red. Esta información ha sido extraída de la siguiente página: https://fp.uoc.fje.edu/blog/que-es-un-sistema-operativo-para-servidor/

Para la clasificación de los sistemas operativos más utilizados en servidores nos basaremos en la información encontrada en la siguiente página: https://sites.google.com/site/aimbsor/introduccion-a-los-sor/1-6-sistemas-operativos-mas-frecuentes-en-una-infraestructura-cliente-servidor

1. Microsoft Windows Server (Principalmente las versiones 2003 y 2006)
2. GNU/Linux Server (Frecuentes las distribuciones RedHat, Ubuntu Server o CentOS)
3. UNIX (IBM AIX, HP-UX)
4. Solaris/OpenSolaris
5. Apple OS X Server

6º)Busca noticias sobre problemas de ciberseguridad relacionadas con los tres primeros de la categoría de escritorio. Recopila al menos 3 enlaces de noticias de alguno de ellos.

Se ha descubierto un malware que se esconde en el logo de inicio en Windows - https://as.com/meristation/2022/10/03/betech/1664798124_621905.html

En esta noticia se explica el descubrimiento de una nueva campaña de ciberespionaje a dispositivos Windows, dirigida a los gobiernos de Oriente Medio y África. El grupo de piratas informáticos que lo realizaron se llama “Witchetty”, empleando un malware usando el logotipo de Windows en un tipo de ataque llamado esteganografía. Este ataque consiste en ocultar información dentro de una información pública, evitando su detección. Cuando se consigue acceso se puede abrir archivos y directorios, iniciar o cerrar procesos, modificar el registro de Windows, descargar archivos y mucho más.

Así es Chaos: el malware que ha infectado millones de ordenadores Windows, Linux y dispositivos - https://computerhoy.com/noticias/chaos-malware-ha-infectado-millones-ordenadores-windows-linux-dispositivos-1134261

En esta noticia se detalla el descubrimiento de un malware nunca antes visto, denominado Chaos, este malware está diseñado para atacar a sistemas Windows y Linux, una vez infectados se utilizan para la minería de criptomonedas y lanzar ataques DDoS. Además, Chaos es capaz de atacar a routers de pequeñas oficinas, cajas FreeBSD y servidores de grandes empresas. Las infecciones de este malware se concentran principalmente en Europa y una manera de sortearlo es la revisión constante de los dispositivos.

Publican detalles sobre la nueva vulnerabilidad de macOS, Archive Utility, parcheada recientemente - https://blogs.masterhacks.net/noticias/hacking-y-ciberdelitos/publican-detalles-sobre-la-nueva-vulnerabilidad-de-macos-archive-utility-parcheada-recientemente/

En esta noticia se explican los detalles sobre una vulnerabilidad encontrada en el sistema operativo macOS de Apple, la cual se puede explotar para ejecutar aplicaciones maliciosas. Se describe como un problema lógico que podría permitir que un archivo eluda las comprobaciones de Gatekeeper, diseñado para que solo se ejecute software confiable en el sistema operativo.

7º)Repite el punto 5 para dispositivos smartphones. Y el 6 con los tres primeros.

La información extraída para la clasificación de los sistemas operativos en dispositivos smartphones viene recogida en el siguiente enlace: https://gs.statcounter.com/os-market-share/mobile/worldwide/2021

1. Android
2. iOS
3. Samsung
4. KaiOS

5. Windows

Este peligroso malware puede controlar un Android a distancia para robarle todas las claves - https://www.xatakandroid.com/seguridad/este-peligroso-malware-puede-controlar-android-a-distancia-para-robarle-todas-claves

En esta noticia se describe un nuevo malware que afecta a la seguridad de Android, llamado Octo. Este bot permite desactivar el Google Play Protect, después se superpone a las aplicaciones para capturar los toques, abre una ventana al teléfono y permite la interacción a distancia, todo esto sin que el usuario sea capaz de percibirlo. Puede observar a distancia cómo tecleas las claves de aplicaciones bancarias, puede espiar los códigos SMS de la autenticación en dos pasos y el resto de información privada.

Descubren que hasta 75 apps de iOS y Android están infectadas con adware - https://www.eleconomista.es/tecnologia/noticias/11965344/09/22/Descubren-que-hasta-75-apps-de-iOS-y-Android-estan-infectadas-con-adware-es-mejor-que-las-desinstales-.html

En esta noticia se explica el descubrimiento de 75 apps en iOS y Android infectadas con adware, este es un tipo de malware que no accede a tu información pero que muestra constantemente anuncios y publicidad. Además, esto puede ser la puerta de entrada de otros malware mucho más agresivos. Actualmente todas estas aplicaciones han sido eliminadas de la tienda de iOS y Android.

Una vulnerabilidad en los móviles Samsung permitía a una app sin permisos hacer todo tipo de maldades - https://www.xatakandroid.com/seguridad/vulnerabilidad-moviles-samsung-permitia-a-app-permisos-hacer-todo-tipo-maldades

En esta noticia se detalla una vulnerabilidad que afecta prácticamente a todos los móviles Samsung, con ella una aplicación maliciosa podría formatear un móvil, instalar o desinstalar apps y tareas similares con permisos de sistema. Actualmente, esta brecha de seguridad ya ha sido parcheada por Samsung en una actualización de seguridad.

9º)¿Has encontrado alguna información que relacione ciberseguridad con la seguridad física de las personas? ¿Crees que la ciberseguridad afecta a la seguridad física y privacidad de las personas?

Si he encontrado noticias que relacionan la ciberseguridad con la seguridad física de las personas, debido a que por ejemplo los ataques utilizados para el robo de información personal al fin o al cabo se relaciona con daños físicos, ya que este contenido sustraído puede contener información comprometida que genera daño a la víctima. Además, otras noticias encontradas como por ejemplo la de los malware capaces de acceder a la cámara del dispositivo y ver a la víctima en tiempo real, produce que la persona no tenga intimidad. Todas estas acciones atentan claramente contra la privacidad de las personas.

Como conclusión podemos decir que en un mundo tan informatizado la mayoría de estas acciones ilegales que se producen atentan claramente con la seguridad física y la privacidad de las personas, ya que los que realizan estos ataques comprometen la información personal, provocando un daño severo a la víctima y quitándole su privacidad.

10º)Como trabajo opcional adicional revisa las siguientes referencias. Busca información y haz una pequeña investigación (muy breve, sólo unos pequeños apuntes de varios párrafos para que te queden claros estos conceptos) sobre los siguientes temas tratados o que trataremos en clase:

1.Cloud. Principales empresas del sector. CSA – Cloud Security Alliance

2.Internet of Things (IoT) y sus implicaciones en seguridad.

3.NIST

4.Serie de normas 27k

5.INCIBE (Antes INTECO)

1. Cloud. Principales empresas del sector. CSA – Cloud Security Alliance

Lo primero que tenemos que saber es que el cloud computing, popularmente llamado cloud, es un suministro de archivos o recursos a petición del usuario mediante una conexión a internet. En el que el usuario puede almacenar y trabajar con dichos archivos sin tener que tenerlos descargados en su dispositivo, además, se pueden compartir con cualquier persona de una manera muy sencilla. El cloud computing se divide en:

- SaaS (Software as a service)
    - Entrega aplicaciones de software a través de internet, como un servicio. Se puede acceder a los datos desde cualquier lado, mientras haya conexión a internet.
    - Principales proveedores:
        - AppDirect
        - Concur
        - Ingram Micro
        - Jamcracker
- PaaS (Platform as a service)
    - Es un conjunto de servicios basados en la nube que permite a los desarrolladores y usuarios crear aplicaciones a una velocidad sorprendente. No se tienen que preocupar de la configuración o el mantenimiento, por lo que los usuarios se pueden centrar en crear la mejor experiencia de usuario posible.
    - Principales proveedores:

        - Heroku
        - Engine Yard
        - Red Hat Open Shift
        - Google App Engine
- IaaS (Infrastructure as a service)
    - Este sistema dota de una infraestructura a las empresas para sus recursos, servidores, redes, etc. Es un servicio muy usado por las empresas que quieren tener una especie de intranet en la que subir aplicaciones o datos. No hace falta invertir en hardware y los servicios se adaptan a las empresas.
    - Principales proveedores:
        - AWS
        - Google Cloud
        - Microsoft Azure
        - Alibaba Cloud

A continuación se enumeran algunos de los mejores proveedores de cloud computing en 2020:

1. Microsoft
2. Amazon
3. IBM
4. Salesforce
5. SAP
6. Google
7. Oracle

CSA (Cloud Security Alliance) es una empresa sin ánimo de lucro que avanza en el examen de las mejores prácticas para obtener computación en la nube y la utilización de tecnologías en la nube para obtener diferentes tipos de computación. CSA utiliza la habilidad de expertos de la industria, gobiernos y asociaciones, para ofrecer eventos, certificación, educación, investigación y elementos explícitos sobre la seguridad en la nube. CSA fue creado con el objetivo de ayudar a saber utilizar la nube de forma segura, con el fin de poder utilizar mejor las herramientas cloud que se tienen a disposición.
Las áreas de investigación de Cloud Security Alliance son las siguientes:

- Grupo de trabajo de gobernanza de datos en la nube
- Grupo de trabajo de IoT de Cloud Security Alliance
- Grupo de trabajo de microservicios y contenedores de aplicaciones de CSA
- Grupo de Trabajo de Gobernanza de SaaS

2. Internet of Things (IoT) y sus implicaciones en seguridad.

IoT se define como agrupación e interconexión de dispositivos y objetos a través de una red, dónde todos ellos podrían ser visibles e interaccionar. El tipo de objeto puede ser cualquiera, desde sensores y dispositivos mecánicos hasta objetos cotidianos como pueden ser el frigorífico, el calzado o la ropa. Cualquier cosa que se pueda imaginar podría ser conectada a internet e interaccionar sin necesidad de la intervención humana, el objetivo por tanto es una interacción de máquina a máquina, o lo que se conoce como una interacción M2M.

El internet de las cosas es una tecnología que se está aplicando, por lo que tiene riesgos de seguridad que pueden dar lugar a ataques exitosos en los sistemas y dispositivos. Según la práctica cibernética de Deloitte Risk & Financial Advisory y Dragos, los 10 principales riesgos de seguridad asociados con el entorno actual de IoT:

- No tener un programa de seguridad y privacidad.
- Falta de propiedad o dirección para impulsar la seguridad y la privacidad.
- La seguridad no se incorpora al diseño de productos y ecosistemas.
- Capacitación y concienciación sobre seguridad insuficientes para ingenieros y arquitectos.
- Falta de recursos de privacidad y seguridad de productos y de IoT / IIoT.
- Monitoreo insuficiente de dispositivos y sistemas para detectar eventos de seguridad.
- Falta de seguridad post-comercialización / implementación y gestión de riesgos de privacidad
- Falta de visibilidad de los productos o no tener un inventario completo de productos.
- Identificación y tratamiento de los riesgos de los productos existentes y heredados.
- Procesos de respuesta a incidentes sin experiencia / inmaduros

Todos los componentes principales de los sistemas de IoT pueden explotarse, por lo que la seguridad debe ser una prioridad en la construcción y el mantenimiento de dichos sistemas. A continuación se exponen algunas pautas a considerar cuando se trata de seguridad IoT:

- Se deben tener en cuenta todos los datos que se recopilan y la información que se almacena. Cada dato e información que circula dentro de un sistema de IoT debe mapearse en consecuencia.
- Cada dispositivo que se conecte a la red debe configurarse teniendo en cuenta la seguridad. Debe garantizarse una configuración segura antes de conectar un dispositivo a la red.
- La estrategia de seguridad de la organización debe basarse en el supuesto de un ataque. Reconocer que no existe una defensa perfecta contra las amenazas puede ayudar a crear protocolos de mitigación que puedan contener y reducir significativamente los efectos de un ataque exitoso.
- Cada dispositivo debe estar protegido físicamente. También es importante tener en cuenta la accesibilidad física de los dispositivos IoT.

3. NIST

El NIST (National Institute of Standards and Technology) ayuda a los negocios de todos los tamaños a comprender mejor sus riesgos de ciberseguridad, administrar y reducir sus riesgos, y proteger sus redes y datos. Este marco de ciberseguridad voluntario, le brinda a los negocios una reseña de las mejores prácticas, para ayudarlos a decidir donde tienen que concentrar su tiempo y su dinero en cuestiones de protección de ciberseguridad.

El marco de ciberseguridad está organizado en cinco funciones clave:

- Identificar
    - Desarrollar una comprensión organizacional para la gestión del riesgo de ciberseguridad de sistemas, activos, datos y capacidades.

    - Lista de todos los equipos, programas software y datos que use, incluyendo computadoras portátiles, teléfonos inteligentes, tablets y dispositivos utilizados en puntos de venta.
- Proteger
    - Desarrollar e implementar las protecciones apropiadas para garantizar la entrega de servicios.
- Detectar
    - Desarrollar e implementar las actividades apropiadas para identificar cuando ocurra un evento de ciberseguridad.
- Responder
    - Desarrollar e implementar las actividades apropiadas para tomar acción en relación con un evento de ciberseguridad detectado.
- Recuperar
    - Desarrollar e implementar las actividades apropiadas para mantener planes para la resiliencia y para reestablecer cualesquiera capacidades o servicios que hayan sido afectados durante un evento de ciberseguridad.l

4. Serie de normas 27k

ISO 27000 es un conjunto de estándares internacionales sobre la seguridad de la información. La familia ISO 27000 contiene un conjunto de buenas prácticas para el establecimiento, implementación, mantenimiento y mejora de sistemas de gestión de la seguridad de la información.

Los pilares principales de la familia 27000 son las normas 27001 y 27002. La principal diferencia entre estas dos normas, es que 27001 se basa en una gestión de la seguridad de forma continuada apoyada en la identificación de los riesgos de forma continuada en el tiempo, mientras que 27002, es una guía de buenas prácticas que describe una serie de objetivos de control y gestión que deberían ser perseguidos por las organizaciones.

Un sistema de gestión de la seguridad de la información es un conjunto de políticas y procedimientos que sirven para estandarizar la gestión de la seguridad de la información. Los estándares de la familia ISO 27000 son los siguientes:

- ISO 27000
    - Contiene el vocabulario en el que se apoyan el resto de normas.
- ISO 27001
    - Conjunto de requisitos para implementar un SGSI.
- ISO 27002
    - Recopilación de buenas prácticas para la seguridad de la información que describe los controles y objetivos de control.
- ISO 27003
    - Es una guía de ayuda en la implementación de un SGSI.
- ISO 27004
    - Describe una serie de recomendaciones sobre cómo realizar mediciones para la gestión de la seguridad de la información.
- ISO 27005

    - Es una guía de recomendaciones sobre cómo abordar la gestión de riesgos de seguridad de la información que puedan comprometer a las organizaciones.
- ISO 27006
    - Es un conjunto de requisitos de acreditación para las organizaciones certificadoras.
- ISO 27007
    - Es una guía para auditar SGSIs.

5. INCIBE (Antes INTECO)

El Instituto Nacional de Ciberseguridad de España (INCIBE) es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos. INCIBE contribuye a construir ciberseguridad a nivel nacional e internacional.

La misión de INCIBE es:

- Mejorar la ciberseguridad y la confianza digital de ciudadanos, menores y empresas privadas de España.
- Proteger y defender a los ciudadanos, menores y empresas privadas de España.
- Potenciar la industria española de ciberseguridad.
- Impulsar la I+D+i española en ciberseguridad.
- Identificar, generar, atraer y desarrollar profesionales del sector de ciberseguridad.

Con esto INCIBE pretende ser el motor para la transformación digital de la sociedad, protegiendo a los ciudadanos, menores y empresas privadas en España y fomentando la industria de la ciberseguridad, la I+D+I y el talento.

Dentro de las principales herramientas diseñadas por el INCIBE, destacamos las siguientes:

- Empleo
    - Una de las finalidades del INCIBE es fomentar la formación y el empleo de calidad en el sector de la ciberseguridad. Para ello ha creado un programa llamado Ciberemprende, dirigido a personas con vocación emprendedora.
    - Su objetivo principal es promover a atraer talento innovador en ciberseguridad, mediante un concurso de ideas y proyectos que consiga desarrollar sus proyectos de negocio.
- Formación
    - INCIBE dispone de dos catálogos donde se recopila la oferta académica en ciberseguridad existente en España:
        - Catálogo de másteres en ciberseguridad en España que incluye un total de 72 programas de Máster y 4 Grados.
        - Catálogo de entidades que proporcionan formación en ciberseguridad en España, se recogen 129 centros donde poder efectuar estudios en ciberseguridad.
- Cert

    - INCIBE-CERT es el centro de respuesta a incidentes de seguridad al que pueden acudir los ciudadanos y las empresas privadas en España operado por el Instituto Nacional de Ciberseguridad.
- Alertas
    - En el Incibe se establece un sistema de alertas para avisar a particulares y empresas de las amenazas de seguridad existentes. Esas alertas se actualizarán constantemente.
- Antivirus
    - Incibe dispone también de un catálogo de empresas que ofrecen soluciones antivirus.
    - Otras herramientas proporcionadas por la entidad son:
        - Antibotnet
        - AntiRamsomware
        - Análisis de riesgo
        - Políticas de seguridad para pymes
        - Catálogos de ciberseguridad

BIBLIOGRAFÍA

https://blogs.imf-formacion.com/blog/tecnologia/top-10-de-webs-y-blogs-sobre-ciberseguridad-201901/

https://ayudaleyprotecciondatos.es/cloud-computing/proveedores/

https://www.profesionalreview.com/2019/12/29/que-es-cloud-y-para-que-sirve/

https://ciberseguridad.com/guias/nuevas-tecnologias/cloud-computing/cloud-security-alliance-csa/#Programas_y_asociaciones

https://www2.deloitte.com/es/es/pages/technology/articles/IoT-internet-of-things.html

https://kippeo.com/los-riesgos-de-ciberseguridad-en-dispositivos-iot/

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1271es.pdf

https://www.intedya.com/internacional/757/noticia-iso-27000-y-el-conjuntode-estandares-de-seguridad-de-la-informacion.html

https://ayudaleyprotecciondatos.es/2020/05/26/incibe-instituto-nacional-ciberseguridad/

https://www.incibe.es/que-es-incibe