Ciberseguridad 1.2

Transcribed on July 4, 2025 at 5:15 PM by Minutes AI

Speaker 1 (00:12)

Bienvenidos a esta nueva sesión donde vamos a hablar del concepto de ciberseguridad.

En esta sesión vamos a explicar lo que es la ciberseguridad, vamos a hablar un poco sobre la motivación de los atacantes.

Esto va a ser importante ya que para poder defender cualquier organización, sea grande, pequeña, mediana, incluso como usuarios poder defendernos, tenemos que entender cuál es la motivación de los atacantes.

Y además contaremos algunas historias, algunos tales en los cuales vamos a ver cómo la historia ha ido teniendo diferentes tipos de incidentes, iremos viendo los diferentes tipos de riesgos que con los que nos encontramos en Internet.

Vamos a comenzar hablando de lo que es la ciberseguridad.

La ciberseguridad es el proceso por el cual vamos a proteger la confidencialidad, la disponibilidad y la integridad de la información siempre en un soporte digital.

A diferencia de lo que es la seguridad de información, que es la protección de la confidencialidad, disponibilidad e integridad de la información independientemente del soporte en el que se encuentre, la ciberseguridad pone el foco en la parte digital.

Cualquier información que tenga una organización en un entorno digital, en un soporte digital, es cuestión de la rama de ciberseguridad, su protección.

Dicho esto, tenemos que entender que la ciberseguridad es una rama dentro de la seguridad de información.

De esta forma ya vamos cogiendo el contexto de lo que es la seguridad de la información y la rama en este caso de la ciberseguridad.

En la ciberseguridad existen diferentes tipos de perfiles, esto se irá viendo durante el módulo también iremos viendo diferentes posibilidades.

No solamente es la parte ofensiva o seguridad ofensiva o no solamente es la parte de seguridad defensiva, sino que existen otro tipo de perfiles.

Bien, visto esto vamos a explicar cuál es la motivación de los atacantes.

Existen muchas motivaciones de un atacante para atacar ya sea a un usuario, a un estado o atacar a una empresa.

Principalmente una de las motivaciones inicial que tiene un atacante a atacar a otro usuario u otra entidad es la baja seguridad o la seguridad inexistente.

Si se analizasen diferentes tipos de informes sobre la motivación o los incidentes que han ido ocurriendo a lo largo de los años, iremos viendo que uno de los principales defectos que tenemos es la baja seguridad o seguridad inexistente.

Si aplicamos también los modelos de defensa en profundidad y otro tipo de modelos que nos proponen seguridad por capa, iremos viendo que claro, en el momento que ponemos más dificultad a la hora de atacar, ese porcentaje de atacantes que se aprovechan de la seguridad baja o de seguridad inexistente desaparecen.

De ahí no es poco el porcentaje de ataques que es por mala seguridad o por inseguridad inexistente, no es poco y hay que tenerlo en cuenta.

Otra motivación ligada a la anterior es la alta exposición.

Cuanto mayor la exposición de activos, cuantas más elementos exponemos a Internet, mayor será el riesgo, pero también pueden estar protegidos de forma adecuada y minimizar ese riesgo.

Pero esa exposición, la alta exposición va en contra de uno de los principios dentro de la ciberseguridad, que es la mínima exposición.

Entonces, tener mucha exposición también provoca que los atacantes se fijen y busquen ese ataque.

También tenemos el espionaje industrial o el ataque o incidente financiero, buscando un rédito económico, buscando dinero.

También temas de espionaje porque les vendan esa información a un tercero, la competencia de manera de competencia, etc.

También hay una motivación vacante para esto, pero ahí empezamos a ver que hay un tema económico detrás.

Tenemos también el tema del descontento de la persona, el empleado que está descontento, ya sea porque no está de acuerdo con las políticas que sigue la organización o la empresa, o ya sea porque está descontento por su trabajo o por cualquier cosa que le pueda suceder, o porque se pueda vender a un tercero.

Ese tipo de motivaciones está muy ligado al concepto de insider.

Un insider racional es una persona que está dentro de la empresa, que tiene acceso a información de la empresa y que puede hacer un mal uso de ella en un momento determinado.

Y también tenemos otra motivación que sería el hacktivismo.

El hacktivismo ya es una motivación diferente, donde no buscan un beneficio, donde el atacante no busca un beneficio, sino lo que está buscando es una reivindicación.

También se llama muchas veces activismo.

El hacktivismo al final busca una reivindicación, busca una protesta, es un tipo de protesta que se puede realizar y está bastante ligado a temas de negación de servicios principalmente.

Luego tenemos también la motivación de el ponerse a prueba, el famoso autodidacta que quiere ponerse a prueba y se pone a prueba con sistemas o servicios de la vida real.

Lógicamente, cuando uno está aprendiendo temas de ciberseguridad y luego en profundidad más ligado a temas de hacking, tiene que entender que la legalidad es importante, las leyes son importantes y hay que respetarlas, por lo que es muy importante no ponerse a prueba con sistemas reales.

Hay muchas maneras de ponerse a prueba, como puede ser, por ejemplo, utilizar entornos virtualizados, laboratorios propios o incluso distribuciones que ya vienen preparadas con vulnerabilidades para poder practicar.

Pero es verdad que es una motivación para los atacantes que no buscan hacer daño, pero sí están incumpliendo con la ley y eso no se puede hacer.

Bien, continuamos.

Vamos a contar ahora algunas historias relacionadas con la ciberseguridad en el sentido de visualizar sobre incidentes reales, amenazas, amenazas que existen.

Por ejemplo, el concepto del Insider, es verdad que en el incidente de Mossack Fonseca que ocurrió en el año 2016, se robó de la organización varios teras de información de diferentes tipos de clientes, se hizo un leak y esa información salía hacia el exterior.

Hay que tener en cuenta que siempre hubo dos hipótesis desde el ataque outside, ataque desde fuera, coordinado desde fuera, un gran ataque desde fuera con temas de pivoting, accediendo a diferentes servidores, pivotando la red interna, etc.

O la vía del insider, es decir, alguien que tenía acceso a la información, porque hablamos de varios teras información, alguien que tenía acceso a la información y pudo en un momento determinado ir extrayendo esa información de la empresa.

Bueno, al final, sea como sea, nos vale como ejemplo para identificar, para aplicar el concepto del insider.

Al final el insider es una persona que está dentro de una empresa, tiene acceso a la información, por eso es muy importante la trazabilidad para poder trazar qué acciones realiza un usuario, tiene acceso a la información y la va extrayendo.

Luego ya puede ser por temas de estar descontento, por temas de por temas de venderse a un tercero o por cualquier tipo de tema.

Los insiders al final son una amenaza que pueden estar dentro de las empresas y para ello hay que tener esos controles internos para intentar evitar este tipo de situaciones.

Segundo caso, vamos a hablar de Ashley Madison, es otro de los grandes incidentes conocidos, de los cientos que hay, pero pero es uno de los grandes incidentes.

Es un data breach, es una brecha de datos donde hay un gran robo de identidades digitales.

En este caso esos millones de usuarios que fueron liqueados, que fueron publicados en Internet.

Bueno, es verdad que inicialmente hubo una liberación de datos de 2500 usuarios, recordar, pero el problema estaba ahí, esa base de datos se filtró y las identidades de los usuarios se filtraron.

En este caso es un entorno sensible donde uno no tiene por qué salirse público.

Esto lógicamente, el concepto del data breach es un concepto que acompaña al mundo de la ciberseguridad desde hace más de una década, es decir, data breach han estado y están a la orden del día.

Al final cualquier empresa puede sufrir un data breach.

Existen leyes como la GDPR, por ejemplo, a nivel europeo, donde se debe notificar en el momento que esto ocurre, pues se debe notificar a los usuarios que esto sucede y definir el data breach.

Podemos decir que es la mejor publicidad en el sentido de que la necesidad de la ciberseguridad, en parte gracias a estos incidentes que han ido ocurriendo a lo largo de la última década, notifican o ponen en valor la necesidad de la ciberseguridad.

Y de valor que ésta aporta, la necesidad que tienen las empresas, la necesidad que tiene la sociedad, la necesidad que tienen los estados, los países de ser ciberseguros o de tener una ciberseguridad aceptable de forma que evitar este tipo de problemas.

Bien, ahí tenéis un recurso que es el de Jafi Imponet, un sitio donde podéis comprobar si vuestra dirección de correo electrónico se encuentra en algún data breach de los que ellos tienen registrados, alguna base de datos que ha sido filtrada tiempo atrás, o en algún paste de los de paste bin u otro tipo de servicios.

Está publicado vuestro email, alguna contraseña, aunque sea con un hash, si está en algún sitio en Internet.

Es una buena práctica de vez en cuando estos servicios utilizarlos para ver si uno mismo, mediación de correo, por ejemplo, está filtrada en alguna base de datos.

Más que nada porque al final tenemos que cambiar esa contraseña si esto ocurre, aplicar 1 s factor de autenticación si esto es necesario, lógicamente esto es necesario y bueno, pues ponerlo, intentar poner soluciones ante una brecha de seguridad en una organización que al final todas pueden tenerlo.

Vamos con otro ejemplo.

Aquí tenemos el del Selectgate.

Es un caso muy famoso que salpicó a icloud principalmente, aunque no era una vulnerabilidad de icloud ni mucho menos, al final lo que estaban apoyando los delincuentes era en el phishing.

Al final el phishing es la virtud, en este caso del atacante por presentar un mundo ficticio pero que parece a los ojos del usuario, parece un mundo real.

El usuario confía en ese mundo que es ficticio, es decir, no es el mundo real, es una página falsa, es un entorno falso.

El usuario concede esas credenciales o esa información que le están suscitando y en ese momento le roban la cuenta.

En este caso los afectados fueron algunas actrices de Hollywood y accedieron a su contenido en icloud y la historia está ahí.

El tema está que en la noticia aquí veis como sí que hubo una sentencia, se encontraron a las personas culpables de estos robos y fueron condenados.

Al final es un fotoleak, es un leak, una fuga de información, pero provocado porque había un phishing, una campaña de phishing donde decir pues correos electrónicos que nos llegan, nos presentan un entorno que nos puede parecer real, que no lo es, pero nos puede parecer real, confiamos en ese entorno, accedemos a una página web, nos parece que la página web es real y confiamos en ello.

En el momento que estamos confiando ya vamos a entregar cualquier tipo de dato a ese entorno que nos están robando, ya sean credenciales, ya sean tarjetas, ya sean información de otro tipo.

Bien, como conclusiones de esta sesión tenemos la ciberseguridad, es todo proceso y protecciones que vamos a aplicar para proteger la confidencialidad, la disponibilidad e integridad de la información en soporte digital.

Como activo digital.

Tenemos la motivación de los atacantes.

Hemos visto varios tipos de motivaciones.

Es importante conocer la motivación porque cuando uno tiene que proteger cualquier entorno necesita saber también por qué me van a atacar.

Y es importante una que hemos visto que es la mala seguridad o la seguridad inexistente.

¿Nos van a atacar más si no invertimos en seguridad?

¿Nos van a atacar menos si invertimos más en seguridad?

Bueno, la experiencia de muchos informes y de muchos años parece ser que nos dice que sí, en el momento que hacemos una inversión en seguridad.

Lógicamente la seguridad es algo cíclico, tenemos que ir midiéndolo y reinvirtiendo si necesitamos solventar problemas, pero estamos haciendo esa inversión y esa inversión nos va a quitar un porcentaje alto de posibles atacantes.

Además, hemos visto también algunos tipos de ataques.

Repasando algunos de los más clásicos, acordaros del phishing.

El phishing es un ataque que a día de hoy las empresas siguen teniendo y lo conocemos hace más de 20 años, pero todavía a día de hoy el phishing es algo que funciona mucho y las empresas lo saben, entonces, pues hay que poner esas contramedidas.

Hemos visto también las brechas de datos o los data leaks, donde hay un robo de bases de datos y se publican en Internet.

Pues eso es algo también, una amenaza importante y global a la que estamos expuestos.

Y hemos visto también el caso de los insiders, que son amenazas que tenemos que un empleado al final no es que sea una amenaza, pero en un momento determinado puede haber circunstancias que lo puedan convertir en amenaza.

Nos quedan muchas cosas, muchos tipos de ataques y muchas gracias por ver esto, lo iremos viendo y con esto finalizamos la sesión.

Nos vemos en la siguiente sesión.