Module4.1.mp4

[00:00:12] ¡Hola! Bienvenidos al módulo 4 del curso "Periodismo de intenernet y tecnología: cómo cubrir sus impactos más allá de los gadgets". En este módulo trataremos temas de seguridad, de ciberseguridad y de seguridad informática.

[00:00:27] Lo primero que es importante destacar es que para este módulo cuenta mucho lo que vimos en el módulo 1 en infraestructura, pero también es importante que recurran a sus conocimientos de cómo funciona una computadora, lo más básico posible. Si tuvieron clases en la secundaria o si saben desarmar una computadora todos esos conocimientos muy, muy básicos y algunos más, por supuesto, cuentan. La primera definición más básica de todas que es la diferenciación entre hardware y software es muy relevante. Y también porque hay que agregar una tercera parte de las computadoras que es el firmware, ¿por qué? Hay una definición que tomó de Iván Arce, un especialista argentino en seguridad informática - de quien también tomó otras definiciones para este curso y agradezco-, es muy importante para entender qué es una computadora y cómo procesa información y cómo eso tiene que ver con la seguridad.

[00:01:37] El hardware, como sabemos, es la parte física de una computadora, el procesador, la memoria, la memoria y los periféricos. Es la parte que como dice Iván se puede patear cuando algo no funciona.

[00:01:49] Después tenemos el software que son los programas, que es la parte que se puede modificar, que podemos escribir y reescribir y que si no funciona se puede maldecir. Y después tenemos el firmware, que es una tercera parte que no es el soft ni es hard, son programas residentes en la memoria no volátil, generalmente que son dispositivos con un propósito especial, por ejemplo, los módem. En el firmware hay mucha opacidad para los usuarios comunes, para las personas comunes, pero en el firmware hay cuestiones modificables y cuestiones que tienen que ver con la información, con la modificación de la información, que también inciden en la seguridad de la información y de los datos que tenemos que tener en cuenta.

[00:02:40] Aquí un gráfico que es donde está el firmware y que también tenemos que tener en cuenta cuando analizamos dónde está el problema o algún problema de seguridad en una computadora.

[00:02:53] ¿Por qué digo esto también? Porque hoy no solamente las computadoras son computadoras. Todo es una computadora: los teléfonos, los autos, las televisiones, los lavarropas, los aires acondicionados. Lo que se llama el internet de las cosas que nos rodea es en sí una computadora. ¿Qué quiero decir con esto? Estamos rodeados de aparatos que a su vez tienen distintos fabricantes. Esos aparatos, además de tener un hardware que los fabrica, una empresa, tienen firmware y tienen software que pueden estar provistos por un mismo fabricante, pero que en general están provistos por distintos fabricantes, y eso hace que tengamos una complejidad de capas que mirar y que pueden generar distintas o vulnerabilidades o amenazas en la información.

[00:03:59] Las impresoras son computadoras, las máquinas de votación son computadoras y eso hace que tengamos que tener un cuidado extremo.

[00:04:10] Si todo es una computadora, lo que tenemos que tener en cuenta, avanzando hacia los temas de ciberseguridad y hacia los problemas de ciberseguridad, es que el objetivo de todo esto es almacenar información.

[00:04:25] La información es un conjunto organizado de datos. Los datos más mínimos, ustedes saben, están organizadas en bits. Y muchas veces cuando hablamos de bits estamos hablando de abstracciones y por eso algunas historias de seguridad al principio son difíciles de seguirlas. Lo más ustedes saben, la información en general cuando la vemos más difícil, es más fácil de distinguir. Hay dispositivos para almacenar datos: las memorias flash, los discos rígidos, los discos de estado sólido, las tarjetas de memoria, los CDs, los DVDs - ya no están en uso, pero bueno, ahora la nube más en uso, [ininteligible], no decir los servidores que en donde compramos espacio para almacenar nuestros datos.

[00:05:18] Pero esto es muy importante. ¿Por qué? Porque hay información que, por ejemplo, estamos cediendo a alguien, pero está transitando un camino a través de esos bits, a través de protocolos y todo eso tiene distintos dueños - esto ya lo vimos - pasa por distintas infraestructuras y digamos, toda esta información tiene que cumplir con distintos atributos para ser segura.

[00:05:48] Acá llegamos a un punto importante en la seguridad y que va a definir a partir de la teoría cuáles son las amenazas o las vulnerabilidades de seguridad.

[00:06:01] Hay tres atributos que tiene que cumplir la información para ser segura. ¿Cuáles son esos tres atributos de la información para ser segura? La información debe tener punto uno: confidencialidad. Es decir, no debe tener acceso a personal no autorizado. Debemos tener definido quién está autorizado para acceder a la información. Punto dos: la información debe tener integridad, es decir, no debe poder ser modificada por personal que no esté autorizado para hacerlo. Y punto tres: la información de detener o disponibilidad, es decir, el personal autorizado de poder modificarle información. Esto va a ser importante después cuando nos adentremos en las amenazas y las vulnerabilidades. Cualquier violación del principio de confidencialidad, integridad o disponibilidad es una amenaza a la seguridad de la información. Si violando el principio de confidencialidad alguien no autorizado accede a la información, vamos a tener un problema. Si alguien modifica la información, es decir, viola el principio de la integridad, vamos a tener un problema. Y si alguien no autorizado me impide acceder a la información, o sea me denega - aunque puede ser un ataque de denegación de servicio- me impide acceder a la información estamos teniendo un problema.

[00:07:42] Pero vamos a esto. ¿Cómo puede suceder esto? Bueno, en general se habla, y muy en general, de cibercrímenes. Cibercrímenes pueden ser de distinto tipo, pueden ser la utilización de las distintas herramientas informáticas para cometer algún tipo de delito o pueden ser algún tipo de delito cometido contra una computadora o contra algún tipo de infraestructura informática o alguna infraestructura de telecomunicaciones.

[00:08:18] Aunque yo les recomiendo, como periodista, al primero enfrentarse a un tema de ciber, de ciberseguridad, en este caso, es distinguir primero tres cuestiones. Primero: acciones. Ante qué tipo de situación estamos. Estamos ante una interceptación de datos, ante un acceso ilícito, aunque un software espía, ante un sabotaje, una denegación de servicio, una usurpación de identidad. Primero definamos qué acción está sucediendo. Luego, ante un tema de ciberseguridad, tenemos que definir quién lo está cometiendo. A veces eso no es fácil, no lo tenemos claro desde el principio, pero si lo tenemos claro, es cuestión de ponerlo en frente. Lo están cometiendo cibercriminales o criminales que están utilizando algún método online o algún método informático. Son hacktivistas, es decir, personas que tienen alguna motivación política. Son servicios secretos, organismos oscuros del Estado u organismos de la inteligencia del Estado. Son unidades criminales, son unidades del gobierno, son compañías o son compañías robando a otras compañías. Y por último, tercer punto es contra quién. Son delitos que se cometen contra individuos, contra compañías, contra organismos no gubernamentales, hacktivistas, contra medios, contra periodistas, contra organismos públicos. Se hace contra infraestructuras que puedan ser operadoras de telecomunicaciones, centros de datos, infraestructuras críticas, ¿a qué me refiero con esto?, a infraestructuras de energía, de electricidad, de agua, de tránsito, controladores de tránsito, fábricas, recursos militares. Acciones, quién y contra quién. Esto puede ser muy útil cuando nos enfrentamos por primera vez a un problema de ciberseguridad.

[00:10:26] Luego les recomiendo hacer una diferenciación grande, porque muchas veces en los temas de ciberseguridad se suelen hacer muchas mezclas y se suele poner toda en la misma caja.

[00:10:38] Tres cosas importantes, tres paquetes grandes. Por un lado está la ciberdelincuencia, la ciberdelincuencia común, es decir, delitos que antes se cometían a través de otros métodos y se cometen a través de computadoras o por internet. Pueden ser desde fraude, fraudes bancarios, robos de identidad, hasta explotación sexual hasta explotación infantil. En general, estos son delitos que ya tienen tipificación en el Código Penal, que ya existían antes y que en todo caso, lo que tienen son unidades especializadas en cibercrimen, tal como la nota que

ustedes van a ver mía "¿Cómo atrapar al ciberladrón?", que da cuenta de esto y que lo que hacen es cambiar de escenario, [ininteligible]. Después tenemos otra otra área. Digamos que son ciberconflictos de tipo ciberguerra, espionaje, ciberespionaje político, ciberespionaje económico. Este tipo de conflictos que tienen que ver con Estados contra Estados o altos niveles corporativos y ese tipo de problemas. Y después tenemos una cuestión que es una tercera cuestión, que es la protección de infraestructuras críticas. Con esto me refiero a las medidas de protección en seguridad que se toman para proteger a las centrales eléctricas de agua, las comunicaciones, las finanzas, la salud; que tienen que ver con las políticas de ciberseguridad que tiene en general un país o que debería tener un país a largo plazo para que las infraestructuras estén protegidas.

[00:12:28] Otra cuestión que me parece importante diferenciar es entre amenazas, vulnerabilidades, incidentes que son, son cuestiones distintas y es importante que las tengan en cuenta también para el abordaje periodístico.

[00:12:46] Las amenazas son la posibilidad de una violación específica de seguridad, es una condición de posibilidad de que algo se viole y por eso hay que prepararse para evitarla o para mitigarla. Las amenazas, como bien les decía, pueden amenazar a alguno de los tres principios de la seguridad. Es decir, si se divulga una información, se está violando el principio de la confidencialidad. Si se manipula una información, se está violando el principio de la integridad o si se denega la posibilidad de acceder a algún tipo de información, se está violando la disponibilidad. Y entonces aquí tenemos una serie de o todo un abanico de herramientas con las que se puede amenazar la información. Algunas de ellas el malware que son softwares maliciosos, el spyware que es software espía, el phishing que es la suplantación de identidad con distintas técnicas. Los ataques DoS que son la inundación de una computadora o un sitio con muchos pedidos al mismo tiempo para que ese sitio funcione mal, deje de funcionar o directamente caiga para denegar el acceso a su información. Las estafas electrónicas son una combinación de distintos tipos de técnicas. Las amenazas también también, una diferenciación, se pueden hacer contra un objetivo específico o se pueden hacer al voleo, como se llama, buscando en una escala, una masividad con un daño mayor.

[00:14:26] Y después tenemos otro tipo de diferenciación, que son las vulnerabilidades. Las vulnerabilidades [son] otra cosa. La vulnerabilidad es una falla o una debilidad en algún tipo de sistema que hace a su vez posible la amenaza y en todo caso el ataque. La vulnerabilidad puede ser una falla en el diseño, puede ser, por ejemplo, transmitir los datos sin cifrar, sin un protocolo de transmisión de datos seguro por ejemplo, de una computadora a una computadora o un centro de datos a una computadora o una máquina de votación a un centro de datos, como ha pasado muchas veces; es decir, es una falla en el diseño de la seguridad. Puede ser también una falla en la implementación digamos tener una comunicación cifrada, pero hacerlo mal. Puede ser una falla en la operación, no actualizar el sistema operativo o no actualizar el antivirus, tener mal puesto una contraseña, el doble factor autenticación, es decir, hacer alguno de los pasos de la seguridad mal.

[00:15:28] Y entonces, ¿cómo se puede...? Hay una posibilidad de contrarrestarlo haciendo bien alguna de estas partes y recuperándolo en caso de amenaza para el incidente, para que el incidente, digamos, no ocurra. También ustedes pueden llegar a escuchar o pueden haber escuchado o leído sobre los exploits. Los exploits son son programas que explotan una vulnerabilidad existente con un propósito específico. Esto también es parte de las definiciones, digamos, de vulnerabilidad.

[00:16:11] Y aquí me detengo también porque yo les hablé de amenazas, les hablé de ataques, pero también cuando ustedes estén haciendo la cobertura de este tipo de historias además de detectar ante qué situación estamos, cómo ocurrió esa situación - esto lo hablamos mucho en la entrevista que tenemos con Sebastián Davidovsky, a partir de su historia del robo al banco en una localidad bonaerense - cuando nosotros detectamos ante qué tipo de historia estábamos, como ocurrió o cuáles fueron los pasos, una cosa muy importante que debe aparecer en las historias de seguridad es preguntar y establecer qué políticas y qué mecanismos de seguridad tenía esa organización, tenía ese individuo, tenía ese país, tenía ese Estado, tenía ese banco, tenía esa compañía o lo que fuere.

[00:17:10] Una política de seguridad es qué está permitido y qué no está permitido, y cuáles son las reglas que va a tener esta organización para evitar que ocurran las amenazas, las vulnerabilidades para mitigarlas, etcétera. Por ejemplo, tales personas pueden acceder a esta información y tales no, las contraseñas tienen que cambiarse cada tanto, vamos a tener tal protección de seguridad, vamos a actualizarla, es decir, cuáles son las políticas que se deben dar para que no haya una falta de seguridad de la información. Y después tenemos mecanismos de seguridad, que son los métodos, las herramientas que van a ser parte de esa política.

[00:17:57] Nosotros, los periodistas que también trabajamos con información y con información muchas veces sensible, tenemos que tener también nuestras políticas de seguridad. Las repasamos con Denise Giusto en la otra entrevista que tenemos en este módulo cuando Denise Giusto del Laboratorio ESET de Seguridad Informática, pero es importante que tengamos algunas en cuenta, tengamos algunos mecanismos y prácticas de seguridad en cuenta.

[00:18:26] Por supuesto, si podemos hacerlo el cifrado de nuestras comunicaciones con PGP, con Pretty Good Privacy, una herramienta, algo vieja entre comillas, pero muy efectiva; la codificación de documentos. Nuestros documentos también, sean o no sean, entre comillas, importantes, cada uno considerará su escenario, pero tener un backup físico y un backup doble físico es muy relevante. Nuestras herramientas de trabajo; sean computadoras, sean celulares o cualquier herramienta de trabajo; tenerla, obviamente, con contraseñas y después, además de nuestras herramientas de trabajo con contraseñas, nuestras cuentas de todo tipo sea de comunicaciones o redes sociales o lo que usemos, tienen que tener contraseña segura. La regla de las contraseñas seguras las pueden encontrar en cualquier buen tutorial, los de We Live Security el blog de ESET son muy buenos, pero la regla es: fácil de recordar para nosotros, pero difícil de adivinar para otros. Gestor de contraseñas, tener un gestor de contraseñas y un cambio periódico que nosotros tengamos con alguna alerta es muy importante, el cambio de la contraseña también. No tener siempre, obviamente las mismas para todas las cuentas que tenemos. La privacidad de las cuentas también es importante, pero la configuración de las cuentas con doble factor de autenticación es relevante y con formas de probar la identidad, con las tres formas de probar la identidad, con algo que uno sabe, con algo que uno tiene que puede ser token, DNI o una tarjeta, y con algo que uno es, con una huella digital, algo que tenga en el cuerpo. Otra cosa importante es el cuidado de las descargas, de las descargas desconocidas o de descargas que no sean relevantes. La desactivación de las cámaras, de los WiFi, de las cuestiones que no sean seguras. Y hay otra cuestión importante, que es obviamente el cuidado de la información contextual, de lo que pueda dar cuenta de quiénes somos.

[00:20:40] Yendo a los temas, a los temas que se cubren más y los que se cubren menos. Ya vimos que los temas que se cubren más son los que tienen que ver con robos de identidad, bancarios, con fraudes, estos son los temas más cubiertos. Después hay otros temas que son los del eje seguridad y derechos humanos. ¿A qué me refiero con esto? Que tienen que ver con hasta dónde vigilar para proteger a las personas y hasta dónde se espía las personas. El caso más emblemático, ustedes saben, fue el caso Snowden con el programa PRISM, pero todo lo que tiene que ver con hasta dónde la seguridad tiene que garantizar los derechos a las personas y hasta dónde esto se utiliza como un espionaje es relevante. Hoy también se habla de temas de, entre comillas, ciberpatrullaje, pero esto tiene que ver con inteligencia de fuentes abiertas. Ahí hay también utilización de programas de espionaje contra las personas, contra civiles en muchos lugares que tienen que ver con cuestiones de seguridad que puedan ser parte de estos temas periodísticamente. Los temas de voto electrónico o utilización de herramientas con problemas de seguridad ya probados tienen una parte también en las historias de seguridad que hay que incluir y que es necesario entender estas cuestiones para abordar estas historias y también son parte. Y después, en el otro caso, en el otro tipo de historias, por ejemplo las que tienen que ver con cibercrimen, con las cuestiones de crímenes comunes trasladados a internet, es muy importante tener, tener en cuenta que son crímenes que ya existían y que hoy son abordados de otra manera, pero que siempre deben respetar - como lo dijimos también en el módulo y lo repasamos en el módulo 3 - tienen que respetar las garantías de derechos humanos también en internet.

[00:22:55] Hasta aquí llegamos en este módulo. Muchas gracias.