Transcripción: Módulo 4: Ciberseguridad (Entrevista a Denise Giusto)

[00:00:00] ¡Hola Denise! Bienvenida este curso. Gracias por estar con nosotros, con nuestros alumnos también.

[00:00:06] Por favor, muchas gracias por tenerme en consideración.

[00:00:10] Bueno, vos sos especialista en seguridad de ESET, una empresa de seguridad informática que además tiene un laboratorio que está investigando todo el tiempo distintas amenazas y distintos problemas de seguridad. Me gustaría preguntarte qué puedes enseñarnos o qué podrías enseñarnos sobre cómo abordar un problema de seguridad que podría servirle a un periodista. ¿Cuál es la lógica con la cual un investigador de seguridad aborda un problema? Cuando tenés, digamos, el problema ahí enfrente, ¿qué cuestiones mirás que podrían servirnos a nosotros los periodistas?

[00:00:50] Bueno, la verdad es que siempre, cuando tratamos cuestiones de ciberseguridad, tenemos que quizás no caer en la tendencia de ser amarillistas. Intentar centrarnos en ser lo más objetivos posibles y analizar las cuestiones que son propias del problema en sí. ¿Cómo se originó esto? ¿Cómo se está propagando? ¿A qué usuarios está afectando? ¿Cuáles son las consecuencias? ¿Cómo, qué tienen que hacer los usuarios para estar protegidos ante este tipo de problemas? Sin caer en los amarillismo que solemos ver en las noticias de ciberseguridad que tienden más a ser clickbaits que realmente analizar lo que está ocurriendo con esa campaña de cibercrimen, supongamos, o con ese fallo en esa determinada aplicación. Y sí centrarnos en quizás intentar tomar ese problema técnico, si es que es un problema técnico, y traducirlo lo mejor posible hacia usuarios - que dependerá del público de la plataforma en la cual estemos escribiendo, redactando o quizás hagamos un video - pero ponernos en sus zapatos e intentar reducir o traducir estas cuestiones técnicas para que ellos lo entiendan lo más posible. Y por supuesto, en este proceso tenemos que hacernos de las referencias y de los especialistas de seguridad que nos van a acompañar para que nos podamos asegurar de que esa noticia realmente va a ser lo más clara posible y que no va a incluir ningún tipo de error. De hecho, recuerdo mucho un artículo que leía hace bastantes años sobre un chico que había sido entrevistado, que también trabajaba era un compañero mío en ESET, al cual el periodista había querido buscar sinónimos de virus informático y había puesto bacterias informáticas, cosas así que uno dice bueno quizás, en vez de modificar el texto original o intentar llevar a la historia para que sea grandilocuente desde el punto de vista de escritura, cerciorarnos de que técnicamente también es correcta haciendo un peer review con las personas especialistas en el tema.

[00:02:58] ¿Qué historias de seguridad informática o de ciberseguridad vos ves que están más relatadas en los medios y cuáles vos ves, tal vez en el laboratorio, que necesitarían más cobertura, como que están faltando, pero que se ven en el día a día?

[00:03:14] Bueno, las que son más relatas en los medios siempre tienen que ver con cuestiones de phishing o de ingeniería social en algunas campañas que se puedan estar propagando, por ejemplo, a través de WhatsApp. El típico esta campaña sobre instalar esta aplicación en tu teléfono para obtener videollamadas es falsa. Lo cual está bien. Está genial que ese tipo de coberturas se hagan, pero por detrás también existe un mundo de campañas de cibercrimen que tienen que ver con espionaje dentro de Latinoamérica, con espionaje corporativo, con diferentes troyanos y backdoors que se están instalando en las empresas. También, por supuesto, vale la pena hablar para que la gente entienda que cualquiera puede ser blanco de este tipo de campañas y que tenemos muchos motivos hoy en día para asegurar nuestra información, para preocuparnos por nuestra privacidad y por preocuparnos, para tener las buenas prácticas de privacidad y de seguridad al día con las herramientas necesarias para poder solucionar cualquier incidente en caso de que lo hubiese.

[00:04:22] ¿Podés hablarnos más de estos troyanos o backdoors y cómo afectan al mundo, tal vez corporativo?

[00:04:29] Sí, la verdad es que en Latinoamérica en el último tiempo estamos viendo un montón de campañas de cibercrimen que están dirigidas puntualmente a países de Latinoamérica, muchas veces los usuarios piensan que estas grandes campañas de cibercrimen en realidad se

dan sólo a nivel internacional, pero esto no es así, también lo estamos viendo a nivel regional. Y por cierto, nosotros tenemos un blog que se llama WeLiveSecurity.com, donde constantemente los investigadores de ESET estamos publicando cuáles son las amenazas y las campañas que estamos viendo, y hemos visto muchísimos troyanos bancarios que están apuntando a Chile, a Brasil, a México. También algunos criptomineros estaban apuntando puntualmente a Perú de manera muy enfocada, donde vemos que algunos países de Latinoamérica también son blancos de forma muy enfocada por los cibercriminales, y que también vale la pena hablar de este tipo de campañas que son tan dirigidas y que pueden tener un impacto muy grande para los usuarios de ese país.

[00:05:37] Sí, nosotros recomendamos mucho el blog We Live Security porque siempre hay información muy actualizada, es súper útil también como fuente para pensar notas que salgan más allá de lo común o como fuente para tener una punta para una nota y a partir de ahí profundizar o encontrar una historia. Y por otro lado, es interesante lo que decís respecto de que en esos temas que están muy hablados, como se llama muy hypeados, como las criptomonedas, también hay, y cuando algo está en la boca de muchas personas, también ahí los ciberdelincuentes apuntan, ¿no?, porque ahí tal vez es una oportunidad.

[00:06:29] Sí, el hecho de que se generen estas tendencias dentro del mundo de la informática es por un motivo. Donde haya una mayor cantidad de usuarios y una mayor cantidad de diversidad en el público y el tipo de usuarios, también ahí van a estar los cibercriminales porque tienen una mayor tasa de efectividad. Obviamente, si hay una mayor cantidad de computadores utilizando una determinada plataforma y hay una determinada, y hay una mayor cantidad de vulnerabilidades sobre esas plataformas, entonces es un combo ideal para poder explotar y poder acceder a la información de las víctimas o comprometer esos dispositivos. Entonces vemos una relación directa entre la cantidad de usuarios que tiene una determinada plataforma y también la cantidad de ataques que se ven contra esa plataforma. Y algo muy interesante que mencionabas es esto de la importancia de estar informado sobre el tema. Hoy en día hay muchísimos blogs de seguridad, muchísimas cuentas en Twitter sobre todo donde se maneja mucho el mundo de la ciberseguridad y donde se postean constantemente nuevos artículos, nuevos papers, nuevas investigaciones que se están realizando desde el punto de vista técnico, como también de las campañas de cibercrimen que se están dando de manera actual. Y es muy importante estar al tanto de cuáles son estas campañas, de cuáles son las noticias que se están publicando, ya sea por investigaciones de seguridad individuales de ciertos investigadores o bien por empresas de seguridad, para justamente poder saber qué está pasando y de qué tenemos que hablar.

[00:08:05] Además de las de las empresas de seguridad, ¿podés recomendarnos dos o tres que vos sigas que puedan ser en español y que estén bueno seguir?

[00:08:14] Bueno, de por sí tengo que recomendar a We Live Security porque nosotros siempre ponemos mucho esfuerzo en mantener esta plataforma y no solo van a encontrar noticias, sino que también pueden encontrar todos los papers, todas las guías de buenas prácticas de configuración de diferentes dispositivos, infografías, bueno tenemos muchísimo material todo libre e incluso también está la academia, que se llama Academia ESET, donde se pueden acceder a un montón de cursos que son gratuitos sobre cómo utilizar diferentes tecnologías y asegurar nuestras plataformas. Y después hay muchísimos contenidos en línea. Nosotros dentro de We Live Security tenemos una sección que es aprender seguridad. Si van al buscador pueden poner aprender seguridad y van a encontrar varios posts donde están enumerados todos los recursos a los cuales podemos acceder, ya sean blogs, podcast de seguridad, canales de YouTube, donde uno puede ir a enterarse de cuáles son las tendencias en el mundo de la ciberseguridad. Por ejemplo, está el InfoSec Institute, que tiene posts y artículos muy interesantes. Si vamos a hablar de vulnerabilidades de aplicaciones está OWASP por supuesto que tiene muchísimas guías al respecto, aunque son mayormente técnicas, pero también tienen muchísima información. Hay muchos canales que hoy en día se puede acceder a esta información que es libre y que es gratuita, y quizás ahí es lo que necesitamos más es un post donde tras esto se organice. Entonces justamente era la idea de los artículos que publicamos, ya en We Live Security así que si les interesa pueden acceder. Recuerden: "aprender seguridad" en el buscador y ahí aparecen inmediatamente tres artículos donde van a encontrar muchísimos recursos para mantenerse al tanto de las últimas novedades en seguridad.

[00:10:05] Genial. Como última pregunta, además, es muy importante que mientras estamos trabajando sobre estas cuestiones, los periodistas también estén al tanto del cuidado de su seguridad, de su propia seguridad. Y esto es un tema que se habla menos, pero también es muy importante. ¿Cuáles son las cuestiones más estructurales y más importantes que un periodista debería cuidar a la hora de hacer su trabajo como periodista en términos de seguridad, en este caso informática, de sus propios equipos y de sus propias comunicaciones?

[00:10:42] Bueno, totalmente. Los periodistas son personas públicas de las cuales muchas veces despiertan ciertos sentimientos muy fuertes en quienes leen sus notas y que pueden discrepar. Entonces tenemos que tener mucho cuidado con cómo nos manejamos dentro de las tecnologías y dentro de las redes en general. Así que lo primero que debemos hacer es ser conscientes en el uso de las herramientas de seguridad que nos brindan las plataformas que estamos utilizando. Por ejemplo, tenemos que tener mucho cuidado con nuestras cuentas en redes sociales u otras plataformas que utilicemos. Siempre saber cuáles son las buenas prácticas para esas determinadas redes. Tener contraseñas seguras que esto ya lo escuchamos un montón de veces, pero además tener habilitado el doble factor de autenticación que es este código que se nos envía a nuestro teléfono para que sea mucho más difícil para un atacante poder suplantar nuestra identidad y entrar a esas redes. Y en el caso de que logre robar el usuario y contraseña o que ocurra una fuga de información en las bases de datos. También tienen que tener mucho cuidado con que segurizar o asegurar, mejor dicho, los equipos desde los cuales estamos generando estas conexiones, nuestros teléfonos, nuestras laptops. Muchas personas creen que no existe el malware para teléfonos y esto no es así. Tanto los televisores, como las tabletas, como los dispositivos biotech también pueden ser susceptibles de tener malware, así que hay que intentar asegurarlos a través de herramientas de seguridad.

[00:12:15] Tener las últimas actualizaciones en todas las herramientas de los sistemas operativos y las aplicaciones que estemos corriendo para asegurarnos de tener esos parches de seguridad que van a impedir que alguien pueda sacar provecho de estas vulnerabilidades y explotarlas. Por ejemplo, instalar un spyware dentro de nuestros equipos, tener mucho cuidado con el tema del phishing, porque a veces pueden llegar correos malintencionados o dirigiéndonos a una determinada página o con un adjunto malicioso. Entonces tenemos que entrenarnos para saber identificar cuándo una cuenta es genuina y cuándo no. Más en el caso de los periodistas que están constantemente hablando y recibiendo mensajes de gente a las cuales no conocen. Y también, por supuesto, tenemos que asegurar las conexiones, sobre todo si estamos realizando una investigación que puede llegar a ser peligrosa de alguna manera para nuestra privacidad o que nos puede poner en una situación sensible si estamos investigando actores del Gobierno, cuestiones así tenemos que tener en cuenta nuestra seguridad. Para eso, por ejemplo, podemos navegar la internet a través de una máquina virtual dentro de nuestro equipo y utilizar redes como Tor, que son redes que van a ir cifrando el tráfico de nodo en nodo, entre nuestro origen nuestra computadora y el destino, que va a ser el servidor que queremos, al cual queremos llegar, de forma que sea mucho más difícil saber realmente quién está navegando. Existen un montón de herramientas de anonimización de los datos que nos pueden servir para investigar este tipo de cuestiones y por supuesto, los periodistas, como si se quiere intrínseco a su profesión, debiesen de alguna manera conocer estas herramientas que son tan útiles.

[00:14:02] Perfecto. Sí hablamos de alguna de estas cosas en el módulo, en la clase, pero es importante que también de tu lado recuerdes todas estas cuestiones, porque si no, estaremos haciendo una buena investigación, pero también nos estaremos exponiendo a nosotros que es la otra parte luego publicarlo. Y en el largo plazo de una trayectoria profesional eso puede jugar en contra.

[00:14:28] Así que bueno, muchísimas gracias Denise. Muy interesante y te agradecemos compartir toda tu experiencia con nosotros.

[00:14:37] Gracias a ustedes.

[00:14:39] Bueno, un beso. Chao, chao.