"No se puede defender todo. Hay que priorizar"

En la conferencia "El dilema de la ciberseguridad y la seguridad nacional", Néstor Camilo, de Oracle, trató sobre cómo enfrentar, prevenir y detectar ataques. El ponente aconsejó: "Hay que identificar qué quieren proteger, hagan un plan y ejecútenlo".

Traitoware, un virus malicioso.

Una joven, Robyn, empezó a contactar a personal de seguridad militar de Estados Unidos diciéndoles algo así:

—¿Te acuerdas de mí? Fuimos al colegios juntos. ¡Qué gran época!

Poco a poco la recibieron en las redes sociales y el grupito fue aumentando. Al finalizar el año les mandó una tarjeta de Navidad. ¿Adivinen qué había adentro? un *malware*, diseñado específicamente para entrar en ese lugar. Era muy difícil de detectar porque estaba armado a medida, por lo cual no había mecanismos de defensa.

Los dispositivos de ingeniería social son sofisticados y cada vez lo serán más, explicó Néstor Camilo, responsable del equipo de arquitectura de Oracle, que trabaja en el sector público, especialmente con organismos de seguridad en Latinoamérica.

Dijo que en las redes hay montones de ataques nuevos que no son detectados por los mecanismos tradicionales. "Y tenemos dos o tres de larga duración donde pasan meses desde el momento que siembran algo hasta que empiezan a sacar provecho. Además, cambian continuamente parte del rector de ataque para que sea difícil de hallar".

La información es un activo crítico y hay muchas formas de llegar a ella, anotó, y los riesgos de ser robada están por fuera y por dentro de las organizaciones; los atacantes son cada vez más calificados. "Por ello hay situaciones complejas que desconocemos, hay que aprender a reaccionar rápido y se requieren muchas técnicas, en particular de *big data*".

Los malhechores, por ejemplo, se agrupan y arman aplicaciones a la medida para identificar dónde están los policías y alejarse del sector. Hace poco en la oficina de crédito de Corea, robaron más del 40 % de la información de crédito. "Son el tipo de problemas que encontramos en la calle y hay muchos más", agregó el conferencista.

También hay pérdidas accidentales porque el desarrollador almacenó la información en el lugar incorrecto, o casos de personas que abusan de los privilegios que tienen sobre la información confidencial. Por otro lado, el Gobierno es el *target*

"La información es un activo crítico y hay muchas formas de llegar a ella, los riesgos de ser robada están por fuera y por dentro de las organizaciones; los atacantes son cada vez más calificados".

Néstor Camilo

de esos ataques muy bien definidos, en algunos casos por *hackers* o activistas, pero en otros es espionaje de nacionales que quieren extraer secretos industriales.

El problema grave, recordó Néstor Camilo, es que actualmente todo el contenido no está dentro de nuestra instalación porque hay dispositivos móviles sueltos donde la protección es muchísimo más difícil que en una red privada. "Cuando hablamos de *cloud* es más grave porque la mayoría de sus usuarios no evalúan su seguridad".

Elementos para proteger la arquitectura

Camilo expuso un caso con agencias de ciberseguridad donde armaron una arquitectura especializada para la detección y la reacción temprana. Lo primero, dijo, es poner seguridad en distintas capas dentro de un sistema y la tarea no es simple. "Estamos acostumbrados a comprar carros por piezas, y después queremos que las especificaciones coincidan perfectamente. Eso deja un montón de espacios que no se toman en cuenta y queda un peligro de seguridad".

Generalmente —añadió—, el objetivo de los ataques es el lugar donde se guarda la información. Por ello hay que proteger las bases de datos con varios elementos: Lo primero es encriptar, luego tener modelos duros de autenticación y que las personas que se conecten tengan acceso a la menor cantidad de datos que necesitan. Después, hay que generar un tren de auditorías y monitorear y bloquear el acceso de esa base de datos con un *firewall* especializado.

"Finalmente —dijo—, hay que monitorear el nivel de configuración y verificar que se tienen los últimos *patches* de seguridad. Normalmente el 50 % de los hardwares no tiene la última versión de esos parches del sistema operativo y la base de datos. La mayoría de las veces, los ataques entran por donde no hay protección en red". ■

Recomendaciones:

No se puede defender todo. Hay que priorizar. Mirar cuáles son las áreas clave del organismo, cuál es la información atípica, hay que dejar señuelos, elementos que puedan ser atacables y si alguien accede a esta tabla, la auditoría puede encontrarlos.

Los dispositivos son un problema. Hoy la mayoría de los accesos a las redes se hacen con teléfonos inteligentes, tabletas y computadores portátiles. El mundo real es por donde pasan redes y los teléfonos son una amenaza muchísimo más grande que el resto de cosas.

El Estado no puede olvidar los derechos personales

Hanni Fakhoury, de Electronic Frontier Foundation (EFF), habló sobre los derechos humanos y, específicamente, el derecho a la privacidad, un componente fundamental de la ciberseguridad. Expuso los principales puntos del marco legal suscrito en Río de Janeiro por varias ONG de la sociedad civil.

La ciberseguridad busca proteger la privacidad de los ciudadanos. Esta no solo pretende que los *hackers* no roben la información financiera, sino que el Estado respete su intimidad.

Hanni Fakhoury reveló abusos cometidos por las autoridades de Estados Unidos en nombre de la ciberseguridad, y expuso casos en los que el FBI "desplegaba herramientas de *hackeo* y las accionaba remotamente para activar micrófonos en un teléfono inteligente. En otros, con un software sofisticado, malicioso, podía reportar digitaciones, leer correos y tomar fotos de una cámara adjunta durante varios meses". En estas acciones no solo eran espiados los malhechores sino personas inocentes.

"Cuando algunos países comienzan a manejar los procesos de la ciberseguridad y la ciberdefensa y a pensar en cómo defender la infraestructura crítica o enjuiciar el ciberdelito, los aliento a que tengan en cuenta los derechos humanos. Es importante que aprendan de los errores cometidos por Estados Unidos", señaló Fakhoury.

A medida que una nación empieza a redactar el marco legal de ciberseguridad, dijo, tiene que limitar lo que puede hacer el Gobierno, cómo puede tener acceso, enjuiciar y castigar para no perder de vista lo fundamental del Estado que es proteger las libertades y los derechos personales.

En el 2012, un grupo de ONG y organizaciones de la sociedad civil se reunió en Río de Janeiro para crear un marco legal que llamaron "necesario y proporcional" encaminado a que los países pudieran mantener a los ciudadanos seguros frente al delito y el terrorismo con una vigilancia acorde con los derechos humanos. Como resultado publicaron 13 principios que dicen cómo el Estado puede vigilar las comunicaciones, en el contexto de la seguridad nacional o afuera de las fronteras.