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.

Más de 400 organizaciones y de 300 individuos de 150 países han firmado los principios y han motivado a las naciones a estudiarlos y adoptarlos para restringir las actividades de vigilancia electrónica y crear unos marcos de límites. Los principios se alimentan de las obligaciones de la libertad de expresión y de asociación que se encuentran en la Declaración Universal de Derechos Humanos, el Convenio Internacional de los Derechos Políticos y Civiles, y la Carta Europea de Derechos Fundamentales.

Para su elaboración, dijo, se definieron algunos conceptos. El primer problema es el de contenido versus metadatos. "La mayoría de las leyes que gobiernan las comunicaciones electrónicas distinguen entre el contenido y los metadatos y ofrecen protección para los primeros y mucho menos para los segundos. La idea viene del correo físico porque se pensaba que cuando se entregaba una carta lo que estaba adentro era la conversación privada con derecho a protección. En la era digital, con nuevas herramientas de software, las empresas o gobiernos pueden hacer mapas de asociaciones, pueden ver quién se comunica por celular y con quién. Estos metadatos pueden ser tan reveladores o incluso más que el contenido de la comunicación", explicó.

Para manejar este tema, recalcó, los principios definen las comunicaciones de manera amplia, no solo como el contenido de las mismas sino que contemplan los metadatos y cualquier tipo de información que pueda utilizarse, incluso el número de serie del dispositivo electrónico.

El segundo problema que buscan proteger es "recolección versus análisis". Algunos gobiernos, agregó, "sostienen que la recolección automatizada de información que no sea analizada por ojos humanos no es una intromisión en la privacidad. Los principios explican que la vigilancia de comunicaciones significa recoger información, monitorear, interceptar, recopilar uso y retener. Es decir, tener acceso a comunicaciones y datos".

En ocasiones los *hackers* roban la información financiera y en otras, el Estado es el que viola la intimidad de los ciudadanos, explicó el conferencista.

Foto: Door JustinLing (Flickr- V) [CC-BY-2.0 (http://creativecommons.org/licenses/by/2.0)], via Wikimedia Commons

¿Cuándo hacer interceptaciones?

Fakhoury destacó algunos principios como "la necesidad y salvaguardias contra accesos ilegítimos y proporcionalidad". Y explicó que un agente puede llevar a cabo vigilancia o interceptación, pero esta debe ser necesaria, adecuada y proporcional. Es decir, debe haber razón de peso para que el Estado requiera esa información y no haya otra manera de obtenerla, pero la puede utilizar solo hasta que la necesite y después debe destruirla.

Otro principio es "la integridad de los sistemas de comunicación". Se refiere a que la privacidad es un derecho humano e incluye el de construir sistemas de comunicación libres de intromisiones externas, no importa si es un *hacker*, un ladrón de tarjetas de crédito o el mismo Estado.

Otros dos principios dicen que los Estados no pueden llevar a cabo interceptaciones interterritoriales sin el consentimiento del otro Estado. Y que hay que establecer salvaguardas contra el acceso ilegítimo, pues la ley debe imponerles pena a las interceptaciones ilegales de actores públicos y privados y después de utilizarlas deben destruirlas. ■

Los principios establecidos en la reunión de Río de Janeiro son:

1. Legalidad
2. Fin legítimo
3. Necesidad
4. Adecuación
5. Proporcionalidad
6. Componentes de autoridad judicial
7. Debido proceso
8. Notificación al usuario
9. Transparencia
10. Supervisión pública
11. Integridad de comunicaciones y sistemas
12. Garantías para la cooperación internacional
13. Salvaguardias contra accesos ilegítimos

> "A medida que una nación empieza a redactar el marco legal de ciberseguridad tiene que no perder de vista lo fundamental: proteger los derechos personales".
>
> **Hanni Fakhoury**