Ciberataques: el peor enemigo es el más silencioso

En un mundo totalmente interconectado y donde la dependencia de la informática es casi completa, cualquier falla o intrusión en un sistema informático puede causar daños irreparables. En ese sentido, la creciente importancia de los sistemas informáticos y la posibilidad de causarles daños, no ha pasado desapercibida para los grupos que operan al margen de la ley.

Actualmente, toda la sociedad se encuentra atravesada por una **guerra cibernética**, silenciosa y global a la vez, que involucra a los estados, compañías multinacionales, escuadrones terroristas y todo tipo de organizaciones. Si bien se invierten trillones de dólares anuales para mejorar los sistemas de ataques y defensa apoyados en la tecnología, la guerra cibernética **se multiplica al infinito alrededor del planeta**.

Por definición, un "**delito informático**" o "**ciberdelincuencia**" es toda aquella **acción ilegal que tiene lugar por vías informáticas** o cuyo objetivo es **destruir y dañar ordenadores, medios electrónicos y redes de Internet**. Estos actos, ya sea que se clasifiquen en criminalidad informática, terrorismo electrónico o guerra informática, se denominan **ciberataques** en su conjunto.

En cuanto a los países mejor preparados para enfrentar esa guerra cibernética, **Israel** es una potencia en el diseño de programas para enfrentar los ataques cibernéticos y comparte ese rango con **Estados Unidos, China, Rusia y Alemania**. Israel y Estados Unidos trabajan juntos, mientras que Rusia e Irán hacen lo mismo.

Si bien existe planificación de inteligencia y soporte técnico y logístico, principalmente en los países mencionados, se tratan de operaciones muy complejas, donde las estadísticas indican que **sólo se tiene éxito en un 18% en lo referido a prevención de ataques**.

Para la región de **América Latina**, los expertos en ciberseguridad dan a conocer algunos **pronósticos** nada alentadores, de los cuales se mencionan los tópicos más relevantes:

1. Adopción y uso de **técnicas de ataques dirigidos** (ATPs) en ciberataques contra **usuarios finales**.
2. **Múltiples ataques** hacia la banca que podrían ser complementados con *outsiders*, tecnologías maliciosas para los cajeros automáticos, así como los servidores internos y otras estaciones dentro de las propias **redes de las instituciones bancarias**.
3. **Ciberoperaciones militares secretas** en la región con el fin de sustraer información confidencial de los estados vecinos.
4. **Ciberataques a infraestructuras críticas** -instalaciones, redes, servicios y equipos físicos y de tecnología de la información- cuya interrupción o destrucción tendría un impacto directo en la salud, la seguridad o el bienestar económico de los ciudadanos o en el funcionamiento de las instituciones del Estado y de las Administraciones Públicas.
5. Los desarrolladores de **malware internacionales para dispositivos móviles** prepararían plantillas regionales en español. Esta táctica permitiría a los cibercriminales tener ventaja sobre infecciones móviles por medio de la instalación de diferentes tipos de malware para la plataforma Android desde *Bankers* hasta Ransomware/Lockers, los cuales **exigirían dinero** a través de los **sistemas de pago**, ya sea convencional o electrónico, con gran apoyo de la ingeniería social.
6. Mayor cantidad de **ataques a pequeñas y medianas empresas**. Los principales riesgos se encuentran asociados a **operaciones con tarjetas de crédito y débito**.
7. **Ataques a los sistemas y usuarios de criptomonedas**. El incremento en el valor de las criptomonedas ha captado la atención de los cibercriminales y esto, a su vez, ha provocado un aumento en el número de malware diseñado para su robo. Además, se ha descubierto cierto tipo de páginas Web, utilizadas para abusar de los recursos de hardware de los equipos de usuarios, visitantes de estos sitios para la generación o minado de criptomonedas. Esta amenaza se ha descubierto también en algunas aplicaciones de Android.
8. **El acortamiento de las brechas entre seguridad y privacidad por medio de dispositivos conectados**. Esta reducción se produce porque las vulnerabilidades de los dispositivos inteligentes de uso masivo en los hogares, ofrecen un problema de seguridad.

En cuanto a nuestro país, la preocupación por este tema, en la actualidad, se manifiesta **relacionado con los grandes riesgos en cuestión de ciberseguridad y vinculados a la realización de la cumbre del G20**, liderada esta vez por el actual presidente de Argentina. El recelo se dirige a grupos terroristas, movimientos antiglobalización y células independientes que reciben entrenamiento tecnológico constante.

El abordaje de esta problemática exige un **trabajo coordinado** y el **compromiso de las Autoridades Nacionales** y la participación de las Fuerzas Armadas, con el asesoramiento de los mayores expertos en la materia de **prevención tecnológica**.

El **ciberespacio** está sometido a múltiples **amenazas**, el desarrollo de una **política de ciberdefensa** significaría también **proteger nuestra soberanía**.