Desconfiar cuando se navega en Internet y actualizar el software de defensa son elementos claves para evitar virus y “ataques”, según expertos que participaron en Buenos Aires en Ekoparty, la mayor cita sobre seguridad informática de Latinoamérica, organizada por “hackers”.

Ekoparty Security Conference reunió esta semana en la capital argentina a cientos de “hackers”, consultores oficiales de seguridad, investigadores, técnicos y amantes de las tecnologías para debatir sobre las últimas novedades en seguridad informática.

Para evitar confusiones, Francisco Amato, uno de los organizadores de la convocatoria, despeja, en una entrevista con Efe, las dudas sobre la convocatoria de los “hacker”.

“La palabra hacker siempre estuvo asociada a la delincuencia, quizás por como se los solía presentar en las películas, pero lo cierto es que un hacker no es un delincuente, sino una persona que se dedica a buscar soluciones distintas y que no sigue los manuales tradicionales, un hacker es una persona que piensa de una manera distinta”, asegura.

“La palabra hacker siempre estuvo asociada a la delincuencia”
Amato explica que la seguridad informática es la que más está creciendo en los últimos tiempos, debido al interés de las empresas por proteger sus servidores y sus bases de datos de posibles ataques.

“Los bancos son los que más están preocupados por la seguridad informática porque manejan dinero, y siempre donde hay dinero hay una posibilidad de ataque”, añade Juan Urbano, técnico informático de la empresa Infobyte.

Los expertos alertan sobre las nuevas estrategias, conocidas como “crimen services”, para atacar a este tipo de empresas y que consisten en que organizaciones criminalesbrindan su método a terceros que les pagan por su servicios para robar información a empresas.

“El blanco preferido que tienen es el canal económico, pero por suerte en Argentina las

empresas relacionadas con ello están tomando muchas precauciones para prevenirlos", apunta Gonzalo García, de la empresa Fortinet.

En el sector empresarial además se maneja información que puede llegar a resultar muy valiosa para terceros y ese tipo de datos también suelen ser blanco de robos informáticos.

"Hoy la información vale mucho dinero y está guardada en los servidores de las empresas; lo que nos proponemos, además de brindar software de protección para los sistemas, es otorgar una seguridad a nivel hardware, porque las empresas invierten mucho en proteger sus bases de datos, pero no resguardan la seguridad física dónde están los servidores", explica Juan Urbano.

"Lo primordial es desconfiar de las cosas que uno recibe en Internet"
Más allá de la seguridad que puedan llegar a adquirir las empresas, un usuario doméstico también está en riesgo a la hora de navegar en Internet y tiene que tomar sus precauciones.

"Lo primordial es desconfiar de las cosas que uno recibe en Internet, sí algo nos parece demasiado bueno de entrada, entonces tenemos que desconfiar; además es muy importante mantener los antivirus actualizados y todas las aplicaciones que nos puedan llegar a prevenir de un ataque", afirma Francisco Amato.

Para Juan Urbano la clave pasa por poder lograr adquirir una "defensa en capas" con distintos tipos de dispositivos que puedan actuar en caso de fallos.

Se puede tener el software actualizado, pero si se pone en el ordenador un lápiz de memoria infectado con un virus puede traspasarlo al sistema, por eso, "la clave está en tener distintos tipos de softwares efectivos de defensa", concluye Urbano.

Fuente: EFE