GERARDO MENOSCAL |EXPRESO

GUSTAVO BUITRON
Gerente general de AcroachCode, ha realizado proyectos en Desarrollo de Software de Enrolamiento y fue reconocido como webmaster award.

LUIS SAA GARZON
Ingeniero de Proyectos de Seguridad de AVP Sistemas, Ethical Hacker, además ha participado en proyectos con el sector público y privado

XAVIER ALMEIDA
Gerente de Relaciones Empresariales de GMS, empresa nacional que se dedica a la consultoría informática

KARINA ASTUDILLO
Gerente de IT de Elixircorp, empresa de Asesoría y Capacitación en Seguridad Informática. Magíster en Administración de Empresas.

OSWALDO BRAVO
Gerente del área de Enterprise Risk Services de Deloitte. Ingeniero Comercial con especialización en Productividad.

VICENTE LINGAN
Ethical Hacking de Kernel Panic, experto en Network Attack y System Attack como métodos para detectar fallas en redes.

50.000 NUEVAS AMENAZAS SE CREAN POR DIA

Delitos informáticos crecieron 360%

El foro sobre Seguridad Informática desarrollado ayer en Diario EXPRESO confirmó que Ecuador es un país vulnerable a los ataques a través de la red
Según las estadísticas presentadas en el evento, de 2009 a 2010 las pérdidas económicas a causa de esta fragilidad llegaron a 1'000.000 de dólares.

Giannella Espinoza Cobos
Redacción Guayaquil

DEMOSTRACIÓN. Karina Astudillo, gerente de Elixircorp y docente de la maestría de Seguridad Informática de la Espol, expuso un ejemplo de Phishing y un ataque a Facebook.

PRESENCIA. Al foro asistieron representantes de las empresas de seguridad informática, responsables de redes públicas, estudiantes universitarios y de colegios de la ciudad.

Incesantes y peligrosas, así son las amenazas informáticas que rodean a la información sensible que contienen los portales web de empresas públicas y privadas.

Y es que con los últimos eventos de ataques virtuales en el país (en donde quedaron al descubierto redes internas, bases de datos, claves de acceso, direcciones, teléfonos y hasta números de cuentas de funcionarios públicos, miembros de las Fuerzas Armadas y usuarios comunes) se evidenciaron las debilidades de la seguridad en las redes nacionales.

Por este motivo, Diario EXPRESO realizó ayer, a las 10:00, el foro "Seguridad informática: ¿protegidos o vulnerables?", en el que participaron expertos en el área con sus versiones sobre el tema de seguridad interna, la importancia del ethical hacking y la necesidad de estar protegidos y bien capacitados. Entre el público estuvieron alumnos del Liceo Naval Altamar, representantes de la CTE, Telconet, GMS, Deloitte y estudiantes de la U. Católica, Estatal y Espol.

Pero, en realidad, ¿qué sabe de a nivel nacional? De acuerdo con un estudio realizado por GMS y Kaspersky, los delitos informáticos en Ecuador crecieron en un 360% en 2010, en comparación con 2009, dejando una pérdida aproximada de un millón de dólares.

Estas estadísticas guardan relación con los reportes de la Fiscalía General del Estado, que indican que solo en los tres primeros meses del año 2011 **se han denunciado 1.308 delitos informáticos.**

Oswaldo Bravo, de Deloitte, explicó en su intervención que entre las mayores y más comunes amenazas están los ciberataques, malware, SQL injection, DoS Distribuido, IPV6, ataques internos, dispositivos móviles, análisis Logs y otros.

Además señaló que según estudios de Deloitte y empresas afines más de 30.000 nuevas amenazas, 10.000 virus y **30'000.000 de spams se crean y envían por día. También afirmó que hasta ayer, en horas de la mañana, se habían detectado 6'297.950 familias de virus.**

Estas cifras evidencian los peligros a los que las redes están expuestas a diario y la importancia de estar totalmente protegidos para no ser víctimas de fraudes electrónicos, suspensión de servicios, robos de datos, entre otros.

Un estudio global realizado por Deloitte revela que los mayores problemas en la seguridad interna se deben al uso de parámetros débiles para contraseñas (34%), compartir claves entre 2 o más empleados (32%), falta de políticas de seguridad (26%), falta de suficiente segregación de funciones (25%) y falta de concientización (25%).

Por su parte, Xavier Almeida, de GMS, acotó que el 90% de los ecuatorianos son "insuficientes de cara a las amenazas informáticas más modernas".

Corroboró además que la "guerra está declarada" especialmente a través de los medios sociales Twitter, MSN, Hotmail, Facebook, y los medios de pago: tarjetas de crédito, paypal y mercado libre.

Por este motivo recomendó que no se publique información sensible en estas páginas sociales, no se abran enlaces desconocidos y se identifiquen correctamente las direcciones antes de acceder.

"El tema no es nuevo lo que sucede es que recién estamos tomando conciencia. Es justo y necesario una culturización de usuarios, que se establezcan políticas administrativas y se apueste por herramientas de seguridad posibles", finalizó.

Karina Astudillo, de Elixircorp y docente de la maestría en Seguridad Informática de la Espol, mostró en cambio cómo los portales que se manejan con JAVA (software que permite el uso de programas punteros, como herramientas, juegos y aplicaciones de negocios) son vulnerables a los ataques de hackers. Como parte de su exposición, hizo una demostración, que tardó menos de 15 minutos, de un "ataque de Phishing usando Metasploit en Backtrack Linux".

De AVP Sistemas, Luis Saa, resaltó la importancia de proteger la información por medio del cifrado y codificación de datos. Explicó que mientras se continúe dependiendo de antivirus, firewall y otros tipos de seguridades "medias", los datos importantes de las empresas seguirán corriendo peligro.

"Es necesario salvaguardar de manera más segura la información, no solo con controles a la red interna, sino con el cifrado de la data sensible. Para que en cada caso de ataque exitoso a nuestras infraestructuras ningún dato sea robado ni divulgado", anotó.

Gustavo Buitrón, de la empresa de marketing digital AcroachCode, expuso los tipos de ataques. Entre estos destacó el DoS (de las siglas en inglés Denial of Service), que se trata de una denegación de servicio, utilizada por la red de hacktivistas Anonymous para mantener suspendidos los portales del Gobierno.

Afirmó que este método se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios.

Para concluir, Vicente Lingan, de Kernel Panic, mostró cómo mediante el proceso de "ethical hacking" (simulación de ataques hostiles controlados para ver los huecos de vulnerabilidad de las redes) ha descubierto las fallas de muchos sitios webs públicos. Este método es utilizado y recomendado para los bancos para que detecten sus fallas de seguridad.

"Para atrapar a un ladrón debes pensar como un ladrón", afirmó Lingan, quien además advirtió que "el Gobierno tiene que tener claro que no se trata de una película de ficción, sino de una realidad. Por lo tanto hay que luchar y protegerse".

El foro, que fue transmitido en vivo, está colgado en la página www.expreso.ec.