Se estima que la delincuencia cibernética genera en el mundo casi la misma cantidad de dinero que el narcotráfico. Un estudio de Rasmussen College, una institución privada estadounidense de investigación, indica que el año pasado la información personal robada por los hackers les generó ganancias por unos US$388.000 millones, mientras el tráfico ilegal de drogas alcanzó unos US$411.000 millones.

Los métodos que estos criminales utilizan están en constante evolución y hoy más que nunca las empresas deben prepararse para los desafíos y retos que sugiere la protección de sus sistemas de información y datos.

Según Alonso Ramírez, Gerente de Ciberseguridad de Deloitte, en su experiencia en Centroamérica han podido observar casos donde un criminal cibernético contrata por ejemplo, a la misma funcionaria de limpieza que tienen instituciones financieras con el fin de que ingrese al departamento de cómputo.

“El delincuente le indica a la funcionaria que cuando vea un documento que contiene tres números un punto, tres números un punto, le tome una fotografía. Esa información captada en la fotografía, es vendida por la funcionaria al delincuente cibernético y a partir de ese momento se genera una fuga de información que es confidencial de la institución”, agregó Ramírez.

Dicha información solo le sirve a un criminal cibernético (hacker) para crear un perfil personalizado de la empresa y poder violentar los sistemas de seguridad y así robar datos. Aunque muchas empresas creen que esto no sucede en la región, lo cierto es que ya se están observando los primeros grupos criminales que se apoyan en la tecnología para lucrar.

Precisamente con el fin de ofrecer a las empresas opciones para proteger sus datos y analizar las vulnerabilidades, Deloitte Costa Rica, en conjunto con el EC Council ofrecerán el Curso de Certificación Ethical Hacker v7 que se impartirá del 22 al 26 de octubre en la ULACIT.

El CEH (Certified Ethical Hacker por sus siglas en inglés) es la certificación oficial de hacking

ético desde una perspectiva independiente de fabricantes de tecnologías de información. El "Hacker Ético" es la persona que lleva a cabo intentos de intrusión en redes y/o sistemas utilizando los mismos métodos que un criminal. La diferencia más importante es que el Hacker Ético tiene autorización para realizar las pruebas sobre los sistemas que ataca.

Este tipo de profesional usualmente es un empleado o persona perteneciente a una organización, quien intenta introducirse a una red informática o un sistema informático, utilizando métodos y técnicas "hacker", pero su propósito principal es la búsqueda y resolución de vulnerabilidades de seguridad que permitieron la intrusión.

Este curso de "Certificación Ethical Hacker V7" está dirigido a oficiales de seguridad, auditores, profesionales en seguridad, administradores del sitio y cualquier persona involucrada en la integridad de la infraestructura de la red.

El curso tiene un costo de US$1.800 y se impartirá de 8:30 a 5:30 de la tarde durante la semana del 22 al 26 de octubre. La inversión incluye los materiales didácticos, DVDs y el examen para certificación.

Durante el curso, los asistentes participarán de intensivas prácticas de laboratorio que le ayudarán a entender cómo trabajan las defensas perimetrales, exploración y ataques a redes propias sin dañar una real, así como la forma en que los intrusos escalan privilegios y que medidas deben ejecutar para proteger sus sistemas.