Delitos informáticos y prevención del cibercrimen

El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional. Sin embargo, debe destacarse que el desarrollo de las técnicas informáticas ha generado nuevas posibilidades de uso indebido de los sistemas, impulsando lo que se conoce como cibercrimen y creando la necesidad de regulación y análisis de los riesgos técnicos.

Objetivos generales

Este curso está orientado a conocer a los cibercriminales y sus actividades, cómo se organizan los grupos delictivos a los que pertenecen y de que manera desarrollan los distintos tipos de herramientas de ataque que luego utilizan contra los usuarios de internet para generar ganancias económicas.

Se analiza además, cómo hacer frente a estos criminales y cómo combatirlos a través de la utilización de métodos manuales y automáticos.

Requisitos previos

Conocimiento básico sobre Seguridad de la Información.

Público Objetivo

El curso está orientado a administradores de IT, responsables de seguridad, área de legales y cualquier persona comprometida con el análisis interno o externo de seguridad en una organización. También está orientado a personas interesadas en la investigación del cibercrimen.

Finalizado el curso, el asistente será capaz de:

- Conocer cómo funciona el cibercrimen organizado internacional
- Conocer los distintos tipos de malware y las metodologías de análisis
- Conocer las herramientas de ataque más utilizadas por ciberterroristas
- Identificar los posibles escenarios de desarrollo de una ciberguerra
- Detectar y eliminar cualquier rastro de actividades criminales en un sistema

Este curso complementa los cursos **"Aspectos Legales de las Tecnologías de la Información en el marco de la Seguridad de la información"** y **"Investigación y protección contra el malware y el cibercrimen"** dictados por **Segu-Info.**

Material a entregar

Presentaciones utilizadas durante el curso y certificado de asistencia y aprobación, ambos en formato digital.

Duración y Modalidad

Este curso teórico/práctico tiene una duración de **20 horas** y la modalidad de cursada es presencial. También puede ser desarrollado ***in-company***.

Instructor

Cristian Borghello es Licenciado en Sistemas (UTN), desarrollador, Certified Information Systems Security Professional (CISSP), Certificate of Cloud Security Knowledge (CCSK), Microsoft MVP (Most Valuable Professional) Security.
Actualmente es Director de **Segu-Info** y **Segu-Kids** y se desempeña como consultor independiente en Seguridad de la Información.
Ha trabajado en la investigación de malware durante más de 15 años y escribe para diversos medios especializados e investiga en forma independiente sobre Seguridad Informática y de la Información.
Ha brindado cursos y dictado congresos y seminarios nacionales e internacionales sobre la temática.

Temario

Cibercrimen

- Cibercrimen, ciberactivismo y ciberguerra
- Ingeniería social
- Spam, Scam y Phishing
- Botnets
- Metodologías de infección
- Uso del malware como herramienta del cibercrimen
- Tipos de malware
- Objetivos del cibercrimen, ciberterrorimo y ciberguerra

Herramientas de seguridad

- Tipos de herramientas y funcionalidades
- Diferencias entre antispam, antivirus, antispyware, anti-X
- Funcionamiento y metodologías de detección
- Análisis pasivo vs activo
- Análisis Black-box vs White-box

Herramientas avanzadas del cibercrimen

- Funcionamiento de zombies y botnets
- Amenazas persistentes y avanzadas (APT)
- Scripting
- Empaquetamiento
- Ofuscamiento
- Drive-by-download
- Criptovirología
- Ataques automático
- Explotación de vulnerabilidades
- Generación de exploits
- Generación de archivos HTML, PDF, Flash y Java dañinos

Análisis de técnicas avanzadas - Práctica

- Análisis práctico de troyanos, gusanos, virus, rogue y otros tipos de malware
- Utilización de herramientas de análisis pasivo y activo
- Descompilación y Desofuscamiento
- Desempaquetado y análisis de archivos dañinos
- Análisis y técnicas de detección para evitar Drive-by-download
- Utilización de herramientas de detección y bloqueos