Ciberseguridad de redes/Internet, resumen
protección del SI y de las comunicaciones de empresa

Seminario de 3 días - 21h
Ref.: SRI - Precio 2024: 2 020€ sin IVA

Este seminario le muestra cómo cumplir los requisitos de seguridad de las empresas e integrar la seguridad en la arquitectura de un sistema de información. Incluye un análisis detallado de las amenazas y los medios de intrusión, así como una visión general de las principales medidas de seguridad disponibles en el mercado. Dispondrá de los elementos técnicos y jurídicos para garantizar y supervisar la seguridad de su SI.

OBJETIVOS PEDAGÓGICOS

Al término de la formación, el alumno podrá:

Conocer la evolución de la ciberdelincuencia y sus retos

Dominar la seguridad de la nube, de las aplicaciones y de los equipos cliente

Entender los principios de la criptografía

Gestionar los procesos de supervisión de la seguridad del SI

PROGRAMA

última actualización: 01/2023

1) Seguridad de la información y ciberdelincuencia

- Principios de seguridad: defensa en profundidad, modelización del riesgo cibernético.
- Métodos de gestión de riesgos (ISO 27005, EBIOS RM).
- Visión general de las normas ISO 2700x.
- Evolución de la ciberdelincuencia.
- Nuevas amenazas (APT, spear phishing, watering hole, Crypto-jacking...).
- Fallos de seguridad en el software.
- El desarrollo de un ciberataque (kill chain).
- 0day, 0day Exploit y kit de explotación.

2) Cortafuegos, virtualización y computación en la nube

- Protección perimetral basada en cortafuegos y zonas desmilitarizadas (DMZ).
- Diferencias entre cortafuegos UTM, de empresa, NG y NG-v2.
- Productos IPS (sistema de prevención de intrusiones) e IPS NG.
- Vulnerabilidades en la virtualización.
- Riesgos asociados a la computación en la nube según CESIN, ENISA y CSA.
- Soluciones CASB para proteger los datos y aplicaciones en la nube.
- El marco de control de ciberseguridad Cloud Controls Matrix y su uso para evaluar a los proveedores de la nube.

3) Seguridad de los equipos cliente

- Comprender las amenazas orientadas a los equipos cliente.
- Software antivirus/antispyware.
- ¿Cómo gestionar los parches de seguridad en los equipos cliente?
- Ransomware: medidas preventivas y correctivas.
- ¿Cómo proteger los dispositivos extraíbles?
- Vulnerabilidades de navegadores y plug-ins.

PARTICIPANTES

Directores de seguridad de la información, departamentos de TI, arquitectos, desarrolladores, jefes de proyectos, comerciales de preventa, administradores de sistemas y redes.

REQUISITOS PREVIOS

Se requieren conocimientos generales de informática y de la red Internet.

COMPETENCIAS DEL FORMADOR

Los expertos que imparten la formación son especialistas en las materias tratadas. Han sido validados por nuestros equipos pedagógicos, tanto en el plano de los conocimientos profesionales como en el de la pedagogía, para cada curso que imparten. Cuentan al menos con entre cinco y diez años de experiencia en su área y ocupan o han ocupado puestos de responsabilidad en empresas.

MODALIDADES DE EVALUACIÓN

El formador evalúa los progresos pedagógicos del participante a lo largo de toda la formación mediante preguntas de opción múltiple, escenificaciones de situaciones, trabajos prácticos, etc.
El participante también completará una prueba de posicionamiento previo y posterior para validar las competencias adquiridas.

MEDIOS PEDAGÓGICOS Y TÉCNICOS

• Los medios pedagógicos y los métodos de enseñanza utilizados son principalmente: ayudas audiovisuales, documentación y soporte de cursos, ejercicios prácticos de aplicación y ejercicios corregidos para los cursillos prácticos, estudios de casos o presentación de casos reales para los seminarios de formación.
• Al final de cada cursillo o seminario, ORSYS facilita a los participantes un cuestionario de evaluación del curso que analizarán luego nuestros equipos pedagógicos.
• Al final de la formación se entrega una hoja de presencia por cada media jornada de presencia, así como un certificado de fin de formación si el alumno ha asistido a la totalidad de la sesión.

MODALIDADES Y PLAZOS DE ACCESO

La inscripción debe estar finalizada 24 horas antes del inicio de la formación.

ACCESIBILIDAD DE LAS PERSONAS CON DISCAPACIDAD

¿Tiene alguna necesidad específica de accesibilidad? Póngase en contacto con la Sra. FOSSE, interlocutora sobre discapacidad, en la siguiente dirección psh-accueil@orsys.fr para estudiar de la mejor forma posible su solicitud y su viabilidad.

- El ataque Drive-by download.
- Amenazas a través de dispositivos USB (BadUSB, rubber ducky, etc.).

4) Fundamentos de la criptografía
- Técnicas criptográficas.
- Algoritmos de clave pública y simétricos.
- Funciones de resumen simples, con sal y con clave (HMAC).
- Arquitecturas de clave pública (PKI).
- Certificación CC y cualificación ANSSI de productos criptográficos.

5) Autenticación y habilitación del usuario
- Autenticación biométrica y aspectos legales.
- Autenticación por desafío/respuesta.
- Diferentes técnicas de ataque (fuerza bruta, captura del teclado, recuperación de credenciales robadas, etc.).
- Autenticación multifactorial fuerte (MFA).
- Autenticación con tarjeta inteligente y certificado de cliente X509.
- Estándares HOTP y TOTP de la OATH.
- Estándares UAF y U2F de la alianza FIDO (Fast ID Online).

6) Seguridad de los flujos de la red
- API de criptografía SSL y evolución de SSL v2 a TLS v1.3.
- Ataques a los protocolos SSL/TLS.
- Ataques a los flujos HTTPS.
- Contención de claves por hardware, certificaciones FIPS-140-2.
- Estándar IPsec, modos AH y ESP, IKE y gestión de claves.
- Superación de los problemas entre IPSec y NAT.
- Las VPN SSL. ¿Cuál es la ventaja sobre IPSec?
- Uso de SSH y OpenSSH para una administración remota segura.
- Desencriptación de los flujos sobre la marcha: aspectos legales.
- Evaluar fácilmente la seguridad de un servidor HTTPS.

7) Seguridad Wi-Fi
- Ataques específicos al Wi-Fi.
- ¿Cómo se detectan los Rogue AP?
- Mecanismos de seguridad de los terminales.
- Ataque KRACK a WPA y WPA2.
- Descripción de los riesgos.
- El estándar de seguridad IEEE 802.11i.
- Las aportaciones de WPA3 y las vulnerabilidades de DragonBlood.
- Autenticación de usuarios y terminales.
- Autenticación Wi-Fi en la empresa.
- Herramientas de auditoría, software libre, aircrack-ng, Netstumbler, WiFiScanner...

8) Seguridad de los smartphones
- Amenazas y ataques a la movilidad.
- iOS y Android: puntos fuertes y débiles.
- Virus y códigos maliciosos en dispositivos móviles.
- Soluciones MDM y EMM para la gestión de flotas.

9) Seguridad de las aplicaciones
- Aplicación del principio de defensa en profundidad.
- Aplicaciones web y móviles: ¿cuáles son las diferencias en materia de seguridad?
- Los principales riesgos según el OWASP.
- Centrarse en los ataques XSS, CSRF, inyección SQL y secuestro de sesión.
- Los principales métodos de desarrollo seguro.

- ¿Qué cláusula de seguridad es la más adecuada en los contratos de desarrollo?
- El cortafuegos de aplicaciones o WAF.
- Evaluar el nivel de seguridad de una aplicación.

10) Gestión y supervisión activa de la seguridad

- Auditorías de seguridad (alcance y normas: ISO 27001, RGPD, etc.).
- Pruebas de intrusión (caja negra, caja gris y caja blanca).
- ¿Cómo responder eficazmente a los ataques?
- Implantación de una solución SIEM.
- ¿Implementar o externalizar su Centro de Operaciones de Seguridad (SOC)?
- Tecnologías SOC 2.0 (CASB, UEBA, seguridad engañosa, EDR, SOAR, aprendizaje automático, etc.).
- Certificaciones de la Agencia Nacional de Seguridad de los Sistemas de Información de Francia (PASSI, PDIS y PRIS) para la subcontratación.
- Procedimientos de respuesta a incidentes (ISO 27035 y NIST SP 800-61 R2).
- Plataformas «Bug Bounty».

FECHAS

Contacto