Curso Ciberseguridad y Cibercriminalidad CEF
Ponencia #1. El Ciberespacio y las TIC
Ponencia #2. Ciberseguridad y Seguridad en las Comunicaciones

Cesáreo García Rodicio
Asesor Técnico Grupo Forciberlac

El Problema. **Personas y Ciberespacio**

1. La persona en el mundo físico: derechos y deberes
    a. Privacidad: Derecho a la intimidad
    b. Responsabilidad: Deber sobre qué hago (a mí y al resto)
2. El ciberespacio
    a. ¿Ciber?
    b. Sistemas Informáticos conectados
    c. La tensión entre el mundo real y el (aparente) virtual
3. Nuevas Herramientas en (casi) el mismo mundo
4. Sistemas Informáticos
    a. Hardware, Sistema Operativo y Aplicaciones
    b. Conectados (Por ejemplo Internet)
5. Sistemas Complejos (Video Robots Spot de Boston Dynamics)
6. Paradigma Internet (un caso particular de Ciberespacio):
    a. Desde cualquier lugar
    b. A cualquier hora
    c. Desde cualquier dispositivo
7. Emociones y Ciberespacio
    a. Siempre conectados: Afectan al Miedo - Seguridad (Ansiedad)
    b. Mundo Virtual: Afecta a la Desconexión del otro - Empatía (Más ansiedad)
8. Privacidad: Datos, Datos, Datos (el nuevo negocio)
9. ¿Cual es el valor de mis datos? (Video Marta Peirano)
10. El dilema de las personas en el ciberespacio (El Dilema de las Redes)

El Sistema. **Seguridad informática**

1. Seguridad Informática.
    a. Confidencialidad
    b. Integridad
    c. Disponibilidad
2. Criterios de Diseño
    a. Usabilidad vs Seguridad

    b. Coste vs Beneficio
3. Tipos de Activos
    a. Infraestructura
    b. Información
    c. Usuarios
4. Seguridad 360: integral (y compleja
    a. Física, Lógica y de Comunicaciones
    b. Activa y Pasiva
5. El eslabón más débil del sistema (depende)
6. Ingeniería Social
    a. Táctica: Contexto (perfil) → CTA (Click To Action)
    b. Muchos tipos de ataque: Phising (Vishing, Smishing, Whaling ...), Baiting, etc
    c. Principios de Uso (cracking humans):
        i. Todos queremos ayudar
        ii. No nos gusta decir que no
        iii. A todos nos gusta que nos adulen
        iv. Tenemos tendencia a confiar
7. Sistemas AAA:
    a. Autenticación
    b. Autorización
    c. Auditoría
8. Seguridad: el gato y el ratón (no hay sistema 100% seguro)
    a. Educación (usuarios)
    b. Confianza (sistema y organizaciones)
9. Video con 8 Recomendaciones para Usuarios (sirven para el debate)

El día a día. **Prevención, Detección y Respuesta**

1. Entender el proceso (desde el punto de vista jurídico)
2. Vulnerabilidad → Ataque → Brecha → (posible) Problema
    a. Mejor Prevenir que curar
    b. Mejor Detectar de forma activa
    c. Responder de forma
        i. Pasiva (estar preparado)
        ii. Activa (combatir)
    d. Negociar con Secuestradores (Dilemma)
3. Pensando en los Activos. Lo que hay que proteger:
    a. Amenazas (causas, tipos, efectos, medios, …)
    b. Análisis de Riesgos: probabilidad x impacto

    c. Técnicas de Protección
    d. El coste (y el beneficio)
4. Datos Reales
    a. Brechas (Incidentes) de Seguridad (Ejemplo AEDP Ene 2024 2019)
        i. Afecta a mucha gente
        ii. Cantidad, Ámbito y Frecuencia
    b. Spam
    c. Vulnerabilidades (CVE)
        i. Importancia, Recursos Afectados. Nivel de Severidad (CVSS)
        ii. Solución (en general: tener los sistemas actualizados)
        iii. Cantidad (CVEdetails)
    d. ¿Está mi email comprometido? ¿Have I been pawned?
5. Glosario de Ciberseguridad Incibe. Hay muchos y bien explicados. Por citar algunos:
    a. 0-day
    b. APT
    c. Ataque Fuerza Bruta
    d. Exploit
    e. BackDoor
    f. Bulo
    g. DDOS
    h. Cadena de Custodia
    i. Carta Nigeriana
    j. CSIRT