Taller de Administración de Servidores Linux

CC5308

Clase 22: 29 de abril de 2011

Evaluación de Riesgos

Luis León Cárdenas Graide
l cardena [at] nic . cl

Cosas que pasan

- Utilidad = Ingresos - Costos
- Incidente: Afecta servicios
  - ΔUtilidad = mix de ΔCosto y ΔIngreso
  - Ataque, accidente, falla, error, imprevisto
- Probabilidad: Distribución Frecuencia
- Impacto: $$$ "Muy alto" .. "Muy bajo"
  - Fatalidad, quiebra, merma, demanda, parálisis, prestigio
  - Costos directos, indirectos y de oportunidad
- Riesgo = Impacto Esperado
  - (= suma(probabilidad_i x impacto_i))
  - "Promedio" (esperanza), ¿varianza?

Cosas que pueden pasar

- Utilidad Esperada = Utilidad +/- %Riesgo
- ¿Seguridad?
  - ΔCosto(ahora) > 0 a cambio de ΔRiesgo(después) < 0
  - Cuesta venderla
  - Cortoplacismo simplista
    - Al límite de solvencia/hambruna
    - ΔCosto > 0 (pequeño) => quiebra/muerte
    - Evolución + Selección Natural
    - Evitar ΔCosto > 0 a toda costa ¡en nuestros genes!
  - Preferencia innata
    - Utilidad(ahora) > 0 aunque Utilidad(después) << 0
  - ¿Cómo vender ΔCosto > 0?

Cosas que empeoran

- Sobrevivencia: Urgencia vs Importancia
  - Evitar hambruna/quiebra hoy
  - Evitar hambruna/quiebra mañana
  - Evitar hambruna/quiebra descendencia
- Recursos limitados => Administración ¿Racional?
- Evolución + Selección Natural: Paranoia
  - Falsos positivos, a lo mejor salvan
  - Falsos negativos, de seguro matan
- FUD: Miedo, Incerteza, Duda (desinformada)
  - Administración Irracional

Objetivo Seguridad

- ΔCosto(ahora) > 0 por ΔRiesgo(después) < 0
- Medidas de seguridad
  - ΔCosto(ahora) > 0 ¿cuánto?
  - ΔRiesgo(después) < 0 ¿cuánto?
- Eficacia = Cuánto consigo / Cuánto quiero
  - Seguridad quiere ΔRiesgo(después) << 0
- Eficiencia = Cuánto consigo / Cuánto gasto
  - Seguridad quiere ΔCosto(ahora) ≈ 0 factible
- Tradeoff: Eficacia vs Eficiencia
- Racionalidad
  - Maximizar ΔRiesgo(después) / ΔCosto(ahora)

Externalidades Seguridad

- Mala seguridad
  - Inefectiva: ¿Sirve para algo? ¿Sale a cuentas?
    - ¿A quién afecta (más)? ¿Usuarios legítimos o atacantes? ¿Uso de seguridad contra legítimos?
    - ¿Remedio peor que enfermedad? (Ojo: leyes)
  - Ineficiente: ¿Vale la pena?
    - Costos ocultos: ¿usabilidad?, ¿funcionalidad?
      - (Derechos civiles)
    - Costo oportunidad: Desvío de recursos no-ociosos que podrían usarse en alternativas más productivas
- Keywords FUD: "100% seguridad", "T-word"
- ¿FUD vs no-FUD?
  - Evaluación (racional) de Riesgo

Evaluación de Riesgos

- Administración racional del riesgo
- Sin seguridad
  - Proyección Utilidad: alta
    - ΔCosto(ahora) = 0
  - Riesgo: alto
    - ΔRiesgo(después) = 0 (con Riesgo(después) >> 0)
- Con seguridad
  - Proyección Utilidad: menos alta
    - ΔCosto(ahora) > 0
  - Riesgo: acotado
    - ΔRiesgo(después) < 0
- RoI: Return of Investment

Evaluación de Riesgos

- ¿Qué vende la Seguridad?
  - Vende ahorro de costos futuros
  - Vende utilidad futura menos baja
    - A cambio de mayor costo hoy
      - Contra cortoplacismo paranoico
- Evaluación de Proyectos
  - Proyectos "normales": RoI(futuro) > 0 (aparentemente)
    - ¿Costos y riesgos sinceros?
  - Proyecto seguridad: ¡También RoI(futuro) > 0!
    - Porque RoI(futuro inseguro) < RoI (futuro seguro)
    - ¡Sincerando costos y riesgos!
  - Proyecto Seguridad = Proyecto "Normal" + precaución

¿Seguridad? Engañosa

- Sensación de Seguridad vs Realidad de Seguridad
  - Realidad: Evaluación de Riesgos
  - Sensación: Información disponible + Publicidad FUD
  - Sensación > Realidad
    - Decisiones temerarias: Alto riesgo
      - Alta probabilidad o Alto impacto
  - Sensación < Realidad
    - Desperdicio de recursos: Sobreaseguramiento
      - Pagar varias veces por lo mismo
- Problema: Seguridad requiere ser estructural
  - Reestructuración organizacional, tiempo, costo, cultura
- Solución perversa: Publicidad FUD

Gestión del Riesgo

- Identificar Activos de Información
- Valorizarlos
- Identificar Amenazas sobre Activos de Información
- Determinar Probabilidades e Impactos
- OUTPUT: Riesgo Residual > 0 (SIEMPRE)
  - Multiplicatoria y Sumatoria
- Priorizar: ΔRiesgo(después) / ΔCosto(ahora)
- Riesgo: Mitigar, Evitar, Transferir
- Controlar, practicar, ensayar, documentar
- Retroalimentar y reevaluar (aprendizaje)

Para no partir desde cero

- Incremental
- Estandarizaciones ISO/IEC 27001/27005
  - Recopila experiencia y prácticas. No reinventar la rueda
  - Se puede comenzar teniéndola en mente
- Sistema de Gestión de la Seguridad de la Información (SGSI)
  - Ej: Verinice (GPLv3). ¿Planilla de Cálculo? (complejo)
- Metodologías
  - MAGERIT, OCTAVE, NIST SP 800-39/800-30, MEHARI, AS/NZS
  - Consulte a su CERT local (clCERT)

Actividad Personal

- Suponga que vende sus sonrisas por Internet
  - Suponga un costo, un precio y una demanda. ¿Simple?
- Y aloja su sitio web en su computador personal casero con conexión a Internet casera. ¿Simple?
  - Especule sobre todos los motivos **técnicos** que se le ocurran que puedan afectar sus ventas (no mercado)
- Muchas cosas fallan: webcam, disco duro, CPU, conexión, ancho de banda, latencia... robos, incendio... phishing, ataques, desconfiguraciones...
- Tipping point: ¿A partir de qué punto comenzaría a tomar medidas paliativas y a qué precio?
  - Simple, ¿cierto? (pun intended)