Seminario Fundación Socinfo

“Ciberseguridad (12): Defensa ante ciberataques masivos”

13 de julio de 2017

Defensa ante ciberataques masivos

La experiencia en el Ayuntamiento de Madrid en la reacción ante amenazas globales de malware

Juan Miguel Moreno Pérez
morenopjm@madrid.es
Jefe de Servicio de Innovación
O.A. Informática Ayuntamiento de Madrid

Reacción ante amenazas globales de malware

- WannaCry:
  - **Viernes** 12 de mayo, avisos de: CCN-CERT, proveedores TIC, **prensa**, **afectados** (Telefónica), **usuarios** internos.
  - 14 de **marzo**, Microsoft publicó la vulnerabilidad. "Prueba de concepto" a los pocos días. (¿Zero Day?)
  - Viernes 12 de mayo: inicio investigación efectos, solicitud de información SAT-INET, primera vacuna CCN-CERT, …
  - Sábado 13 de mayo: vacuna **revisada** CCN-CERT, avisos específicos Microsoft, …
  - Lunes 15 de mayo: verificación y parcheo infraestructuras, coordinación unidades NNTT municipales, detección de posibles incidentes, …
  - 16, 17, 18, …. de mayo … … … **y explicar a la dirección**.

Reacción ante amenazas globales de malware

- ¿Qué prefiere el defensor, un ataque masivo o uno específico?
- Masivo ≠ sofisticado

Usuarios "desprevenidos" abren un correo "dudoso"	Usuarios conocedores de que existe una campaña de correos "maliciosos"
"Tu factura" ¡ hay que seguir avisando aunque la amenaza sea antigua !	"Renta 2017", "WannaCry", …

- El correo electrónico, siempre el correo

Reacción ante amenazas globales de malware

- Mantras:
  - La prevención tecnológica no es suficiente:
    - Filtros anti spam (servidor de origen del spam está "limpio", destinatarios "limitados", …)
    - Antivirus actualizados (mutaciones / firmas desconocidas, zero days, …)
    - Esta idea debe permear en la organización
  - A veces, no se está actualizado:
    - Actualizaciones automáticas no completadas (5 %)
    - Actualizaciones que han de ser manuales
    - Sistemas fuera de mantenimiento
    - Sistemas "de terceros no controlados" (interconexiones, asistencias, …)

Reacción ante amenazas globales de malware

- Mantras:
  - Alertar (no alarmar) / Tranquilizar
    - ¿Cortar Internet?, ¿Cortar correo? (depende de situación, organización,)
    - Avisar mediante correos electrónicos, avisos en la Intranet, …
    - Elegir al destinatario según objetivo del aviso: toda la plantilla, centros directivos promotores de contratos, …
    - Insistir cuando haga falta (nuevas "primeras" infecciones, …)
  - Colaborar
    - Difusión prensa, información, concienciación, …
    - CCN-CERT: información, vacuna, …
    - Microsoft, desarrollos para sistemas sin mantenimiento.
    - Desarrollos específicos de empresas de antimalware
    - Afectados recomendando cortar comunicaciones VPN con ellos

Reacción ante amenazas globales de malware

- Mantras:
  - Investigar
    - Conexiones sospechosas: Sonda CCN-CERT
    - Monitorizaciones propias
    - Fallos en actualizaciones automáticas PCs.
    - Actualizaciones Servidores. 500 m2 de CPD
      ¿Cuántos servidores físicos? ¿cuántos virtuales? ¿cuántas licencias (a dispositivo, a usuario, flotantes)?
    - Infraestructura de acceso. ¿situación de "terceros"?
  - Coordinación Interna
    - Sistemas / Comunicaciones / Puestos de trabajo
    - Puestos de trabajo (generales, específicos, a disposición del público, …)

- Mantras:
  - Conocer antes de actuar
    - De nada sirve aplicar algunas medidas si el equipo no está "limpio"
    - ¿vacunar / parchear inmediatamente?
    - ¿Cortar vía de propagación? ¿qué pasa si bloqueo SMB?
  - No spammear a usuarios
    - Insensibilidad por desgaste
    - Los departamentos técnicos deben recibir toda la información posible y discriminar

Reacción ante amenazas globales de malware

- Mantras:
  - Creatividad
    - “honey pot”
  - Identificar daños
    - Recursos afectados
  - Recuperar
    - Limpiar y proteger equipos/aplicaciones
    - Información en copias de respaldo limpias y con poca diferencia temporal
    - Estrategias de recuperación para cientos de miles de ficheros

- Mantras:
  - Aprender
    - Revisar qué ha funcionado mejor / peor /como se espera
    - Comunicar a la dirección y a los usuarios con mensajes / normas revisadas
    - Insistir en la corrección de “vulnerabilidades resistentes” (aplicaciones y equipos en sistemas que deben de ser migrados, implantación de una excesiva variedad de tecnologías poco manejables para equipos TIC poco numerosos)
    - Disipar una falsa sensación de seguridad

- Cuando las barbas de tu vecino veas cortar …

EXPLICAR VULNERABILIDADES
HABER AVISADO
…
OPORTUNIDAD

OPORTUNIDAD
. Visualizar trabajo "invisible"
. Palpar riesgos
. Solicitar recursos