Principios de cyber-security para entornos corporativos

Matías Cuenca-Acuna, Leonardo Frittelli, Marcelo Lorenzati,
María Emilia Torino y Gustavo Domingo Yaguez
INTEL

Resumen

Hoy en día, empresas y negocios se encuentran más que nunca expuestos a diferentes amenazas cibernéticas. Desde ataques simples y genéricos a operaciones ofensivas personalizadas (APTs, *advanced persistent threats*). En este ámbito, no es efectivo sólo implementar técnicas de protección. Detección y remediación de incidentes son igualmente importantes.

El presente curso tiene como objetivo presentar como se estructura la seguridad de una empresa a los fines de proteger y defender la misma. También cubriremos algunas tácticas, técnicas y procedimientos (TTPs) conocidos que están siendo utilizados en ciber-ataques.

El curso estará dictado por cinco profesionales de Intel Security (ex McAfee) que trabajan en el área de seguridad corporativa. Este equipo trabaja en la creación de productos para ataques avanzados para las top 2000 empresas globales. El curso se dará en castellano con material en Ingles. Cada día corresponde a un módulo que será presentado por uno de los profesionales antes mencionados.

Temario

- Anatomía de un ataque y el *Cyber Kill Chain* (día 1)
  - ¿Cuáles son las ciber amenazas que empresas y gobiernos se enfrentan hoy en día?
  - Tipos de ataques
  - Fases involucradas en un ataque: reconocimiento, creación del arma, entrega, explotación, instalación, comandos & control y acciones sobre objetivos
  - Detalles de cómo funcionaron algunos de los ataques más famosos, como el ocurrido a Target en 2013

- Seguridad en redes e infraestructura de una empresa (día 2)
  - Topologías de redes y protocolos (repaso)
  - Arquitectura de una red corporativa.
  - Componentes principales (intranet/DMZ, NATs, *gateways*, DNS/DHCP/*Web*/*Email*/VPN/*Domain servers*, *endpoints)*

- Defensa en profundidad (día 3)
  - Seguridad de la información. Confidencialidad, integridad, disponibilidad, autentificación, no repudio
  - Políticas de seguridad
  - Planes de continuidad y recuperación a desastres
  - Control de acceso
  - Respuesta a incidentes

- Inteligencia sobre amenazas (*threat intelligence*)

- Protegiendo redes corporativas (día 4)
    - Firewalls, NGFWs (next generation firewalls), IPSs (intrusion prevention systems), IDSs (intrusion detection systems), SIEMs (security information and event management), web proxies, email gateways, honeypots, honeynets, sandboxes

- Protegiendo *endpoints corporativos* (día 5)
    - *Workgroups* y cuentas locales. Active Directory, Kerberos, NTLMv2, *smart cards*
    - Políticas de seguridad
    - *Anti-viruses*, HIPS *(host intrusion prevention system),* EDR (*endpoint detection and response*), *firewalls*, encryptación de discos, DLP (*data lost prevention*)
    - Seguridad en dispositivos móviles

Bibliografía

1. Data-Driven Security: Analysis, Visualization and Dashboards, Jay Jacobs; Bob Rudis.
2. Introduction to Computer Networks and Cybersecurity, Chwan-Hwa Wu; J. David Irwin.
3. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, Eric M. Hutchins∗ , Michael J. Cloppert† , Rohan M. Amin,
   Ph.D.http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf