Universidad del valle de Guatemala

Erick Guerra

Tarea 6. Desarrollo Seguro Parte 1

Capítulo 3: “The Texas Prison Hack” de The Art of Intrusion.

Descripción:

Dos reclusos de la Unidad Wynne (Texas), William y Danny, descubren que comparten pasión por la informática. Con piezas introducidas por personal complaciente y sin controles de inventario, montan varios PC, los conectan por cableado Ethernet que ellos mismos tienden entre dependencias y acaban consiguiendo acceso a Internet usando credenciales de un guardia. Además, modifican y ocultan software de acceso remoto para observar a personal de la prisión sin ser detectados. Durante meses consumen música, vídeos y chatean, a la vez que aprenden redes y sistemas, con varios sustos pero sin que los pillen en el acto.

Vulnerabilidad explotada:

Veo que el mayor problema se dio uno tras otro por fallas físicas, operativas y de red que encadenaron y permitieron a dos internos montar y ocultar su propia infraestructura. Operaron con credenciales prestadas en una red sin segmentación ni control, obtuvieron salida a Internet mediante líneas y módems no supervisados, y usaron software de acceso remoto no autorizado que mantuvieron oculto para pasar inadvertidos.

Propuestas de solución:

- Gestión de activos y configuración con auditorías periódicas para detectar instalaciones no autorizadas.
- Gestión de cuentas y privilegios, intentando cumplir con la política de la menor cantidad de permisos posibles.
- Registros constantes de cualquier acción por usuario.
- Mayor control de red y comunicaciones con detección y bloqueo de acceso no autorizado.