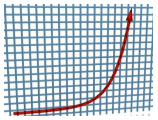
Casos de ciberataques a infraestructuras críticas

Julio César Ardita
Director CYBSEC
jardita@cybsec.com

SEMINARIO LA CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS
frente a un mundo tecnológicamente dependiente e interconectado

Incidentes de seguridad sobre infraestructuras críticas en Latinoamérica

Cada vez hay más incidentes de seguridad.



- Hay mas interconexión entre redes industriales y las redes corporativas e internet.
- Actualizaciones de sistemas. Sistemas antiguos legacy que se actualizan a nuevas versiones con nuevas tecnologías embebidas (sistemas abiertos, web, java, etc.).
- Desconocimiento de aspectos de seguridad técnicos.
- Hay muy poca conciencia de seguridad en los ingenieros locales, los representantes locales y los proveedores internacionales.
- Excusas de ahorro de costos y facilidad de operación por sobre temas de seguridad.
- Apertura de “back-doors” para el acceso administrativo y de proveedores.

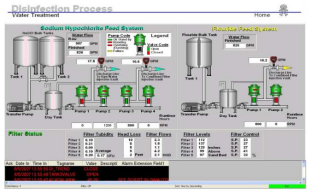
Análisis de un incidente

1. Un intruso externo envió mails de phishing a los administradores del sistema industrial (obtuvo información sobre las personas involucradas a través de redes sociales). Dos administradores accedieron al mail enviado y dejaron sus passwords de acceso a la red corporativa.
2. El intruso se conectó en forma remota via vpn utilizando como factor de autenticación ese user/pass. Logró ingresar a la red corporativa en forma remota.
3. Luego el intruso, con los mismos usuarios y passwords, ingresó en forma remota (via RDP) a los equipos de estos administradores, desde donde aprendió, investigó, conoció nuevos usuarios y passwords, leyó manuales, etc.
4. Instaló un Keylogger sobre las dos estaciones de trabajo (tenían privilegios de administrador).
5. Se conectó al sistema pivot para saltar a la red industrial (se autenticó con un user/pass que obtuvo) y un soft-token instalado en los equipos de estos administradores.
6. Desde el equipo pivot accedió vía web a la consola del sistema HMI para la gestión del sistema (eléctrico / gas / agua). Se autenticó con otro usuario y password que obtuvo con el Keylogger instalado en los equipos de los administradores.
7. El intruso aprendió a utilizar el sistema.
8. En el momento del ataque, el intruso accedió al sistema HMI (bloqueó subestaciones / cerró bombas / modificó la presión del gas) generando graves inconvenientes.
9. Luego el intruso ingresó a los servidores del sistema ICS a nivel de sistema operativo y borró las configuraciones del sistema principal y del sistema secundario. Luego apagó los sistemas.

SEMINARIO LA CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS
frente a un mundo tecnológicamente dependiente e interconectado

Incidentes de seguridad que investigamos en Latinoamérica

1. Infección de virus en equipos de la red industrial via pendrive por parte de un proveedor.
2. Intruso interno que generó un sabotaje utilizando el sistema industrial en forma no autorizada.
3. Intruso externo que ingresó a un sistema industrial via Internet y borró todos los servidores del sistema HMI.
4. Intruso externo que accedió vía internet al sistema de monitoreo y explotó vulnerabilidades.
5. Proveedor que ingresó con su equipo, se conectó a la red interna e infectó con un malware a toda la red corporativa e industrial.
6. Intruso interno que accedió al sistema HMI desde la red corporativa y provocó la parada de equipos de la red industrial.



¿Estamos preparados para responder a un incidente de seguridad?

La respuesta es **NO**.

Hay poca o nula relación entre los ingenieros que administran los sistemas industriales y las áreas de IT y Seguridad de la Información en las Organizaciones.

Hay pocos registros (logs) con información y casi siempre están implementados por defecto. Tener logs y monitoreo de alertas y eventos es crucial para poder detectar, frenar un ataque a tiempo y/o poder investigar que sucedió.

Hay desconocimiento técnico de seguridad informática entre los ingenieros. Cosas que técnicamente se pueden y no se pueden hacer. Por ejemplo: rootkits, explotación de vulnerabilidades, by-pass de medidas de protección, etc.

SEMINARIO LA CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS
frente a un mundo tecnológicamente dependiente e interconectado

Diferencias entre un ataque a una red industrial y a una red corporativa

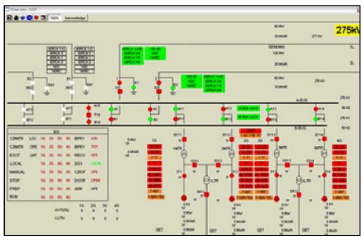
En un ataque a una red industrial:

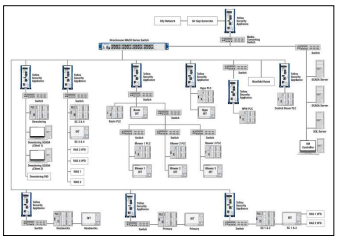
- Se debe conocer otras tecnologías y protocolos distintos con sus propios sistemas, aplicaciones y configuraciones.

- Se deben pasar medidas de seguridad más sólidas (doble factor de autenticación, IDS, IPS, firewalls internos, equipos pivot, etc).

- Se debe tener conocimiento y saber cómo operar un ICS (hay miles de sistemas HMI y configuraciones customizadas).

- Se necesita mucho más tiempo.

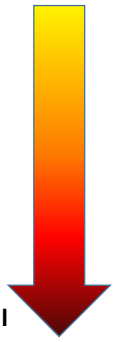




Diferencias entre un ataque a una red industrial y a una red corporativa

Nivel de dificultad en un ataque a un ICS (*):

+ Fácil



+ Difícil

- Comprometer la seguridad de un ICS
- Extraer información
- Hacer una parada del ICS
- Dañar (romper) el ICS
- Daño al equipamiento (sensores)
- Lograr un segundo ataque exitoso

(*) The Industrial Control System Cyber Kill Chain - SANS

SEMINARIO LA CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS
frente a un mundo tecnológicamente dependiente e interconectado

Objetivos de los intrusos sobre los ICS

Pérdida de visión (desde el centro de monitoreo / control)
Pérdida de acceso

Manipulación de la visión del ICS
Manipulación del control
Manipulación de los sensores e instrumentos

Bloqueo del acceso al ICS
Bloqueo del ICS

Daño al ICS
Daño a los sensores e instrumentos

Anatomía de un ataque externo e interno

Ataque externo

1. Interconexión a la red corporativa (VPN client/site o site/site, Terminal Server, Web, accesos remotos, etc).
2. Interconexión a la red industrial desde la red corporativa (equipos de administradores, pivot, firewall, etc.).
3. Interconexión a la red industrial desde Internet en forma directa.
4. Interconexión utilizando los accesos y mecanismos de autenticación de los proveedores externos.
5. Interconexión a las redes WIFI en los sites.
6. Interconexión física a la red industrial.
7. Malware y control remoto.

Ataque interno

1. Los ataques internos son los más complejos, porque son llevados a cabo por empleados, ex empleados o proveedores.
2. En estos casos, el intruso ya tiene el know-how y los mecanismos de acceso.
3. La única forma de detectar este tipo de ataques es con un monitoreo proactivo y con auditorias periódicas para detectar patrones anómalos sobre el sistema ICS.

SEMINARIO LA CIBERSEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS
frente a un mundo tecnológicamente dependiente e interconectado

Consejos y recomendaciones

Hacer un assessment de seguridad real sobre los sistemas industriales.

Definir e implementar mecanismos de seguridad sobre los ICS hasta el máximo nivel posible (acceso remoto con doble factor de autenticación, herramientas de seguridad, logs, configuraciones, concientizar a los administradores y operadores, etc.).

Exigir a los proveedores recomendaciones de seguridad y aplicar mejores prácticas.

Definir y acordar políticas y procedimientos para la gestión de incidentes de seguridad.

Realizar un monitoreo de seguridad proactivo sobre los sistemas involucrados para detectar intentos de intrusión con el fin de frenar a tiempo un ataque sobre un ICS.

Casos de ciberataques a infraestructuras críticas

Julio César Ardita
Director CYBSEC
jardita@cybsec.com

CYBSEC®
Desde 1996