Retos de Seguridad y Soluciones para las Industrias

Agenda

El conflicto entre operaciones y seguridad.

Mejorando la seguridad.

Soluciones de protección para industrias.

El conflicto entre operaciones y seguridad

Fábrica de Papel Georgia-Pacific

18 de febrero 2014

Fábrica de papel despide a su gerente de sistemas.
Brian Johnson **regresa vía VPN.** En dos semanas de haber ingresado al sistema de Georgia-Pacific, causo un daño en la producción estimado en $1.1MM USD. Su ataque fue a la fábrica de la empresa localizada en Port Hudson, Louisiana, la cual produce toallas y pañuelos de papel 24 horas al día.

No tenia auditoria
Tomo 13 días para encontrar cuales cambios se hicieron y quien los hizo

Acceso al VPN no fue revocado
Las cuentas de IT no están sincronizadas con Recursos Humanos

Falta de monitoreo de ICS
La compañía no tenía conocimiento de los cambios realizados

Ataque Red Eléctrica Ucraniana

23 de Diciembre de 2015

Ciberataque de la red eléctrica ucraniana
Aunque el ataque en sí mismo se desencadenó el 23 de diciembre de 2015, se planificó cuidadosamente: las redes y los sistemas se vieron comprometidos **ocho meses antes**

Falta de auditoria
Información forense limitada, malware tenia funciones de borrado

túnel SSH to OT comprometido
Uso de malware para obtener credenciales desde un computador.

Falta de Monitoreo de ICS
Apago el UPS e inhabilito Dispositivos con firmware falso

Fuentes de ataques

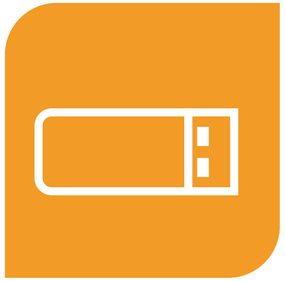
Your great subtitle in this line

Spearphising

La forma mas fácil que todavía está operando. Astutos emails son muy efectivos usando triggers emocionales (urgencia, management)

Watering Hole + Vulnerability

Uso de una página Web común para iniciar un ataque por una vulnerabilidad



USB Key

La herramienta perfecta para infectar varias maquinas.

Ex-empleados

La forma de ataque mas peligrosa.

Mejorando la Seguridad de Redes Tecnológicas Operacionales

Mejor Seguridad

Back to the basics

> *Las empresas están invirtiendo mas para proteger sus activos digitales, pero los crímenes cibernéticos siguen creciendo en frecuencia y en severidad. Lo que se necesita ahora no es mas seguridad pero mejor seguridad*
> *– Morgan Stanley Research*

- Industria 4.0 : Seguridad incluye la seguridad cibernética
- La seguridad cibernética debe ser tomada en cuenta
- Usar protocolos estándares como OPC UA
- Auditar todos los accesos a la Red Operacional

El próximo paso

Back to the basics

Dos Factores de Autenticación

Implementar dos factores de autenticación para cualquier acceso remoto. Restringir Fuente de IP

OT Security

Proteger y monitorear comportamientos peligrosos y horas después del trabajo pueden ser objeto de ataques

USB Key

Políticas estrictas de USB para prevenir scripts/ejecutables

Enable Auditing

La mayoría de los programas de software como Windows y otras aplicaciones comunes ya tienen sistemas de auditoria incluido

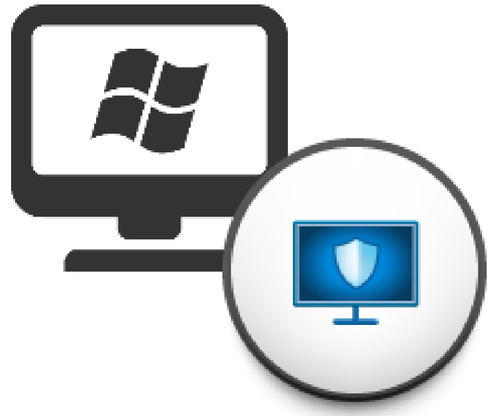
Control de Acceso

Empleados que dejen la empresa en puestos claves. Políticas que actualicen el control de acceso.

Soluciones Stormshield para diferentes industrias

Una solucion global para las industrias de seguridad

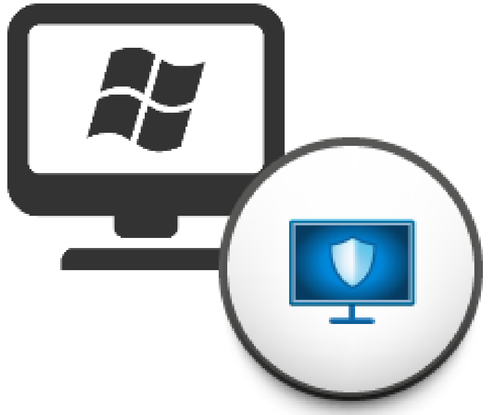
STORMSHIELD NETWORK SECURITY



STORMSHIELD ENDPOINT SECURITY

- Multiples factores para sus necesidades
- Convergencia IT/OT en todo los productos SNS
- Stormshield Management Center para administrar todo los SNS desde un solo punto
- Stormshield Visibility Center una vision 360° del Firewall de la red y de todos los computadores

Seguridad de Largo Plazo con SES



SES ofrece seguridad de largo plazo para los sistemas operativos que no se benefician de los parches de seguridad

OS	Microsoft EOL	SES Support
XP SP3	Abril 8, 2014	2020
2003 Server	Julio 14, 2015	2020

Muchas gracias