REFLEXIONES

Año 2. Número 5

SEGURIDAD
Ataques, Origen y Destino

Los sistemas de ataque están siendo modificados constantemente, siendo menores en número absoluto pero mucho más eficaces. La transformación de los ataques está permitiendo que, con combinación de técnicas físicas, lógicas y de engaños a las personas, se logren accesos a los diferentes anillos de seguridad de la empresa, difícilmente detectables.

Por su parte, la única forma de defenderse ante semejante nivel de ataques es teniendo una equilibrada estructura de defensa que proteja todos los activos con un nivel semejante de seguridad. Los atacantes siempre utilizan el eslabón más débil de la cadena para romperla. Los ejercicios de simulacro de ataque entre un Red Team (Equipo atacante) y el Blue Team (equipo de defensa) son una de las mejores prácticas para evaluar un ataque real dentro de una organización. Tipología del origen de los problemas:

- Fallo humano
- Accidente.
- Enemigo interno.
- Los "malos" clásicos

Los sectores más afectados son:

- Financiero
- Militar
- Gobierno/Administración
- Infraestructuras Críticas: Ley 8/2011
- Industria

Podemos estar seguros de que tendremos un problema de seguridad en nuestra empresa, el problema es identificar cuándo y qué impacto tendrá.

Patrocinado por :

Seguridad, prioridad de la Dirección

"Con*oce a tu enemigo. Conócete a ti mismo." (El arte de la guerra. Sun Tzu).*

Existe una diferencia patente entre el estado del arte de la Ciberseguridad Industrial entre distintos países. Europa está entre 5 y 10 años por detrás de EEUU en la implantación de controles de Ciberseguridad Industrial, y países como España se encuentran más de un lustro por detrás de otros países europeos como Holanda o el Reino Unido.

La atención limitada a la seguridad es un problema en muchas organizaciones porque no se trata con la debida diligencia. Se piensa que no da beneficios y no se establece como una prioridad. Sin embargo, está demostrado que es mucho mas costoso comenzar a prepararse, una vez que ya se ha sufrido las consecuencias de un problema de Seguridad.

Es necesario tapar todas las brechas del enorme perímetro digital de la empresa, y no olvidemos que la delincuencia está organizada y genera enormes beneficios.

Es recomendable que el **ciclo de vida de un proceso de seguridad** contenga las siguientes fases:

1.**Definición**: donde la organización debe desarrollar unos completos planes de seguridad que impliquen la identificación de las principales normativas, leyes y buenas prácticas en materia de seguridad que deben cumplir, para analizar los principales riesgos a los que está expuesta y formular un adecuado plan de seguridad. La creación o implantación de un sistema de gestión de seguridad será la mejor manera de tener el control total sobre los procesos de implantación de controles.

2.**Prevención**: las auditorías técnicas de seguridad, los servicios de inteligencia de las compañías, los planes de concienciación, y los simulacros que se realicen en la organización, son los únicos medios que dispone la Industria de cara tener una capacidad de prevención.

3.**Detección**: la detección precoz de un ataque es la forma más efectiva de contener lo inevitable. El fraude en los servicios de las empresas, la

Normas de Seguridad mas relevantes para las Industrias

Normativas de **Sistemas de Gestión** (SSGG):

- **ASIS SPC.1**-2009. Resiliencia organizacional: sistemas de gestión de la seguridad, la preparación y la continuidad.
- **ISO 9001**:2015. Sistemas de Gestión de la Calidad.
- **ISO 14001**:2015. Sistema de Gestión Ambiental.
- **ISO 20000**-1:2011. Sistema de Gestión del Servicio.
- **ISO 22301**:2012. Sistemas de Gestión de Continuidad de Negocio.
- **ISO 27001**:2013. Sistemas de Gestión de Seguridad de la Información.
- **OHSAS 18001**:2007. Sistemas de gestión de la seguridad y salud en el trabajo.

Normativas, estándares, Leyes

- **COBIT** v.5. Objetivos de Control para la Información y Tecnologías relacionadas. Versión 5.
- **ENS**. Esquema Nacional de Seguridad (Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Anexo II).
- **ISO 27002**:2013. Código de buenas prácticas para la Gestión de la Seguridad de la Información.
- **Ley 5/2014**, de 4 de abril, de Seguridad Privada.
- **Ley 8/2011**, de protección de las infraestructuras críticas (LPIC).

detección de la fuga de datos y los sistemas de monitorización son las únicas defensas con las que cuenta la organización.

4.**Respuesta**: no es posible admitir que un atacante no vaya a conseguir entrar en la Industria, por lo que es necesario contar con procesos de análisis forense y los procedimientos de gestión de gestión de crisis permitirán a la empresa tener un medio de contener el impacto del ataque.

5.**Recuperación**: la recuperación ante un ataque es fundamental y necesaria para devolver a la organización a su estado inicial en el menor tiempo posible, por lo que los procesos de resiliencia, y la continuidad de negocio son los únicos medios de tener la Industria preparada para su restauración tras un impacto en sus líneas de producciónnes que vela por cualquier forma de seguridad, generando ineficiencias, y costes.

Proteger los existente, construir deforma segura.

Términos de nuestro interés

La Deep Web, o Web profunda,

Es la zona de internet que no es accesible entre los buscadores típicos de Google o MSN. Representa más de 97% de las conexiones y el tráfico mundial, y es la zona de internet que más contenidos alberga.

Ciberseguridad Industrial

Es el conjunto de prácticas, procesos y tecnologías, diseñadas para gestionar el riesgo proveniente del ciberespacio derivado del uso, procesamiento, almacenamiento y transmisión de información utilizada en las organizaciones e infraestructuras industriales, utilizando las perspectivas de personas, procesos y tecnologías. (Fuente : CCI)

Próximo Encuentro, Miércoles 27 de Marzo de 2016, 19:30h

"Sistemas Cognitivos" Con el Patrocinio de

Elisa Martín Garijo
Directora de Tecnología e Innovación, IBM

Lugar : ETS Ingeniería del ICAI
C / Alberto Aguilera, 25 (Madrid)