Ciberataques que pueden arrasar una ciudad!

La cosa esta calentita, ya sabemos el contexto de los sistemas de control industrial, como han evolucionado y los riesgos en general que pueden sufrir dichos sistemas debido a los ciberataques. Pero vamos a indagar un poco más dentro de esos riesgos, vamos a exprimir un poco el tema para entender la importancia de protegerlos. Y es que me gustaría recalcar que los sistemas de control industrial son inmensamente importantes en cualquier país del mundo, son los encargados de cosas muy importantes dentro de las infraestructuras de cualquier país y pueden generar consecuencias extremadamente dañinas.

Pensareis que estoy exagerando, que me gusta dramatizar, pero os voy a ir enseñando las cosas poco a poco. Para empezar ha llegado a mi poder el Informe de Amenazas CCN-CERT IA-04/16 (no es que lo haya conseguido a través de una fuente secreta en medio de una misión de vida o muerte, no, simplemente buscando en Google he dado con el). El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, que es el creador de la guía antes mencionada. En ese informe he tenido la oportunidad de recoger datos importantísimos para poder organizar adecuadamente este post, y así poder entender y explicaros la magnitud de las amenazas a los sistemas de control industrial y sus riesgos.

Los sistemas de control industrial están integrados en muchísimos sectores dentro de las infraestructuras de un país, por lo que se han clasificado en 4 grupos dependiendo de su naturaleza. En la siguiente tabla, veremos los distintos grupos en los que se han dividido los sistemas de control

industrial.

GRUPO	SECTOR
Grupo 1	Sistema financiero y tributario
	Instalaciones de investigación
	Administración
	Tecnologías de la Información y las Comunicaciones
Grupo 2	Transporte
	Agua
	Energía
Grupo 3	Alimentación
	Manufactura
	Salud
	Servicios
Grupo 4	Industria química
	Industria nuclear

En el primer grupo tenemos los sistemas que no forman parte del proceso principal de negocio pero sirven de sostén en procesos esenciales. El grupo número 2 si están los sistemas que son parte del proceso principal de negocio y además están muy extendidos geográficamente hablando. En el tercer grupo tenemos los sistemas acotados y en los que las consecuencias serían solamente en sus instalaciones. Por ultimo en el grupo cuarto tenemos lo que aun estando acotados en áreas pequeñas, las consecuencias serían muy extensas y devastadoras.

Para ir poniéndoos en situación y como anotación a este punto, vamos a ver algunos de los ejemplos de ciberataques a sistemas de control que aparecen en los grupos anteriores, y así ver de manera más nítida las posibles consecuencias de sus hackeos. Estaréis conmigo en que los más impactantes son los del grupo 4, ya que jugar con químicos o energía nuclear es muy peligroso, pero no son los únicos:

- **En 1982** Un Troyano camuflado causó una explosión en un gaseoducto transiberiano.

- **En 1985**Una fuga de productos químicos en Unión Carbide provoco 134 hospitalizados en Virginia.
- **En 1988** El gusano Morris, paralizó Internet y causó el**mayor daño por malware** visto hasta el momento.
- **En 2000**Un ex empleado al que despidieron de una planta de tratamiento de aguas vertió litros y litros de aguas residuales en ríos y parques de Maroochy en Australia.
- **En 2003**El gusano Slammer infectó la central nuclear de Davis-Besse en Ohio bloqueando el sistema durante varias horas. Todo por culpa de un ordenador portátil de una persona subcontratada.
- **En 2010**Uno de los más conocidos o más graves fue la detección de Stuxnet en las centrales nucleares. Logró parar la central nuclear de Natanz en Irán, destruyendo una quinta parte de los centrifugadores nucleares. Fue descubierto en más de 45.000 equipos alrededor del mundo.
- **En 2012**La friolera de 35.000 ordenadores de la petrolera Saudí Aramco, sufrieron el peor ciberataque de la historia, eliminándolos y causando que el 10% del petróleo que podía suministrar la empresa estuviera en peligro.
- **En 2014**Una empresa siderúrgica alemana sufrió graves daños al sufrir un ataque a través de phishing.
- **En 2015** El troyano BlackEnergy ataca a una planta de energía eléctrica en Ucrania, dejando a la mitad de hogares de Ivano –Frankivsk sin energía.
- **En 2016** El proveedor de dominios Dyn era víctima de un ataque DDoS (o de denegación de servicio) y con él, gran parte de las mayores páginas del país norteamericano.

Muchas de estas noticias se las tengo que agradecer a mi compañero de clase Luis Carlos Fernández y a sus fantásticos post en el año anterior. Como veis, fabricas nucleares, empresas de servicios y suministros y muchas más están en el objetivo de los hackers, concretamente sus sistemas de control industrial. Por último, analicemos bien esta fila de noticias y veremos que tipos de impactos surten estos ataques. Realmente son diferentes, muy diferentes a los hackeos convencionales o a los que estamos acostumbrados a ver, y es que estos dispositivos controlan dispositivos físicos por lo que sus impactos pueden ser totalmente nuevos a los ataques tradicionales. Como ejemplo veremos que pueden afectar a:

- **Impactos sobre la seguridad física y el entorno:**Teniendo en cuenta sobre todo el grupo 04, vemos que los impactos sobre las centrales nucleares podrían causar daños a nivel físico en las personas y medio ambiente, desde muertes a daños medio ambientales.
- **Impactos económicos:**Si atacáramos a una empresa de servicios cortando su distribución de suministro, el impacto económico sobre ella seria importante, además causaría problemas en la empresa y sus correspondientes consecuencias.
- **Impactos sociales y mediáticos:** Este impacto podríamos considerarlo como consecuencia del segundo punto o verlo también de manera independiente. Si una empresa deja de suministrar sus servicios, la gente perdería su

confianza en ella, Pero, aun sin ser una empresa de servicios, el mero hecho de ser una empresa vulnerable a la que han atacado y no ha podido defenderse, ya le da una imagen débil que provoca la pérdida de confianza de la gente sobre ella.

Como os he dicho anteriormente, os he explicado poco a poco los riesgos, dándoos los grupos de diferentes naturalezas y la importancia de cada uno, ejemplos de ataques a cada uno de eso grupos con sus impactos y la magnitud de dichos impactos. Supongo que ya tendréis claro la importancia de proteger esos sistemas de control industrial, pero tranquilos, no todo es negativo, también tenemos los controles para contener esos ataques y sobre todo para prevenirlos. En el siguiente post veremos los las soluciones que podemos darle a los malos, no os lo perdáis.