Un día más…

Te pongo en situación: acabas de llegar a casa, por la tarde-noche, cansado de estar todo el día fuera de casa estudiando y trabajando. En ese momento, a alguien cercano a ti (tu madre, tu pareja, tu hermano, tu cabeza si es que vives sin compañía…) se le ocurre preguntar qué tal el día. Una pregunta aparentemente inofensiva (con responder *un día más…* ya valdría), podría generar más de un quebradero de cabeza para más de uno. A mi, por ejemplo, me dio que pensar sobre dos temas.

El primero, la típica respuesta de *un día más, un día menos*. ¿Qué tipo de respuesta es esa? una respuesta que indica que el día a día te supera. Que lo único que te hace levantarte de la cama es saber que a la noche vas a poder volver a ella. Una perspectiva realmente desoladora. ¿Qué tipo de razones puede tener una persona para no ser feliz? ¿Es realmente su culpa? Muchas veces tendemos a echarle la culpa al *sistema*, pero, ¿sabes qué? Malas noticias. No es más que una excusa barata. Eres parte del sistema y está en tu mano cambiarlo. Está en tu mano dejar ese trabajo que no te gusta, mandar a la mierda a ese compañero que te saca de tus casillas o llenar tu vida de cosas que te llenen de verdad. Y no sirve la excusa de necesito un trabajo para vivir o el acomodamiento. Porque dejar el trabajo por otro mejor no es la única solución. Una muy fácil y al alcance de cualquiera es cambiar la cara. Despertarte con la idea de enfrentar las cosas con una actitud diferente puede ser suficiente. Mucha es la gente que dice que la actitud es más de la mitad del camino a la hora de enfrentarte a un problema, y cuando el problema es la vida en general, parece de cajón afrontar el día a día con una actitud positiva. En el anterior post hablaba que tenemos que dejarnos a nosotros mismos sentir, todo el mundo debería tener unos días tristes. Pero eso, unos días tristes en medio de una vida feliz, y no una careta con una sonrisa escondiendo una persona infeliz. En resumen, siente, piensa, aprende y mejora, pero siempre sintiéndote por cómo eres y por qué es lo que haces.

Lo segundo que me da que pensar: ¿Cuántas veces piensas al día? ¿Nunca has tenido la sensación de tener todo el día programado? Te levantas de la cama, desayunas tu café y vas al trabajo. Trabajas, comes, trabajas y vuelves a tu casa. Estás reventado y ¿qué tal el día? Bien, supongo. Porque es la primera vez que piensas algo en el día. Todos somos homo sapiens sapiens, y una de las cosas que nos ha hecho sobrevivir es que nos adaptamos a todo. Sobre todo a una rutina fija. Nos gusta no tener que usar lo que tenemos encima de nuestros hombros, pero es lo que te puede hacer diferente del clon que tienes al lado. En la lego película, muestran una sociedad en la que todo el mundo es perfectamente normal, y el protagonista, es el más normal de la sociedad perfectamente normal. Sin embargo, es el protagonista. ¿Qué aprendemos de esto? ¿Que tenemos que ser aun más normales? No. Que por muy normal que te creas, siempre tienes algo dentro de ti que te hace diferente. Piensa en cómo puedes hacer el día más agradable a los que te rodean, muestrales que te

preocupas por ellos. Todas estas cosas están al alcance de cualquiera, incluso de la persona más *normal*. Lo único que hay que hacer es salir de la comodidad de la rutina y pensar, pensar un poco más. Incluso te puede venir bien para el punto anterior.

Dos cosas que cualquier entrenador *normal* pediría a sus jugadores: actitud y cabeza.

Hablando de emociones de una forma racional

Vas por la calle, un día cualquiera y alguien te pregunta qué tal estás. Simplificando existen dos respuestas a esta pregunta: estoy *positivo* o estoy *negativo*. Cuando la respuesta es *positiva*, se limita a estoy contenta o estoy feliz, pero cuando es *negativa*, la respuesta varía. Estoy asqueado, estoy indignado, decepcionada, desilusionada, aburrido… Y lo cierto es que parece que sabemos más palabras para emociones tristes o "*negativas*" que para las que nos generan satisfacción. Pero… ¿por qué pasa esto?

Las sensaciones negativas o las experiencias traumáticas se quedan más tiempo con nosotras y resultan más difíciles de superar. Además, la sociedad de hoy en día se centra en tratar (*destruir)* las emociones *negativas*. ¿Qué pasa con las emociones *positivas*? Esas como no son problemáticas que les jodan. Si existen movimientos que tratan de reforzar las emociones *positivas* como la psicología positiva, por qué estas no triunfan entre la forma de pensar de la gente. Parece que hay un *boom* de este tipo cuando luego lo único que hay es humo.

¿Por qué la tristeza es negativa?

¿Por qué la rabia es negativa?

¿Por qué la decepción es negativa?

Porque eso es lo que nos han enseñado. Nos han enseñado que hay que evitar estar triste y tenemos que estar contentas. Que un trabajador motivado produce mucho más que uno decepcionado. Pero, ¿realmente es malo sentir tristeza cuando un proyecto en el que tenías muchas esperanzas y se ha ido a la mierda? ¿Es malo estar decepcionado con una persona que no hace más que poner excusas para no quedar contigo? Lo primero de todo, antes que todo lo

demás, somos seres humanos y en el pack vienen las emociones. Nos tenemos que permitir sentir. Sentir lo que estamos sintiendo. Tengo el mismo derecho a estar triste que a estar feliz.

Cuando te permites sentir, es mucho más sencillo superar una emoción y ser más consciente de una misma. Y esto es lo que tienen que trabajar las empresas. Permitir a los trabajadores sentir lo que sienten y no tratar de curar la tristeza o ignorar la decepción. Se trata de entender al otro ser humano, de comprender por qué se siente así, independientemente si está triste o feliz, porque de las estas últimas tampoco nos podemos olvidar.

Entonces, como la culpa es de la sociedad y de las demás personas, no hay nada que un individuo pueda hacer. Y este es uno de los mayores errores que se puede cometer, no solo en el tema de las emociones sino en el tema de la vida. Sentirse indiferente ante una situación solo porque la gente lo hace así o porque la culpa es de la sociedad. Tenemos que mantener un espíritu crítico ante la sociedad, las demás personas y, sobre todo, ante nosotros. Tenemos que desconectar nuestro corazón de nuestra cabeza y dejar que cada cosa pase por su sitio. No podemos permitirnos que las emociones pasen por la cabeza antes y después de pasar por el corazón. No podemos seguir viendo caras de procesar. Necesitamos ver caras de sentir. Necesitamos poner más caras de sentir. Si las emociones vienen en el pack del ser humano, sería racional pensar que las emociones tienen que formar parte de nosotras.

Un pensamiento emocional que parece que no es muy informático o ingeniero, pero las emociones tienen más de ingeniero de lo que pensamos. Porque quizá a alguien le suene a algo pero *“las emociones ni se crean ni se destruyen, se transforman.”*

IIoT ¿Es el futuro?

Llegamos al final de este viaje, en el que hemos ido visitando muchas paradas que nos cuentan la actualidad y el contexto de los sistemas de control industrial, pero aún nos falta la última parada de todas: el futuro. Ya hemos comentado muchas veces el nuevo entorno que se presentó cuando el Internet entró en estos sistemas, pero lo cierto es que hoy en día se está abriendo otra puerta, con muchas otras amenazas y posibilidades. Hablamos de IIoT.

Ha habido bastante debate y especulación sobre el impacto potencial de Internet Industrial de las Cosas (IIoT) en el desarrollo, implementación y operación de sistemas de control industrial (ICS). Las predicciones van desde «Nada cambia» a «Va a cambiar todo lo que se hace». Como es habitual en situaciones como esta, tendremos que esperar a que el humo se aclare un poco para obtener una respuesta final. Independientemente de cómo se desarrolle finalmente, hay ciertos aspectos del control industrial que seguramente se verán afectados de alguna manera. Uno de estos es la ciberseguridad. Específicamente, ¿cuáles son los principios, estándares y prácticas

necesarios para garantizar que un sistema de control industrial funcione de manera segura y esté protegido de amenazas involuntarias, colaterales y deliberadas?

Algunos de los expertos más cínicos de la comunidad de ICS incluso han bromeado con que, en este contexto, el término IIoT debería considerarse como la abreviatura de «Internet industrial de amenazas» *threats* en inglés. Esto se basa principalmente en la expectativa de que el crecimiento en IIoT tiene el potencial de explotar la cantidad de posibles fuentes de ataque, también conocida como «superficie de ataque», mediante la introducción de un gran número de sensores ampliamente distribuidos y otros dispositivos que pueden o no haber sido diseñados de acuerdo con los estándares de seguridad industrial. Por otro lado, los optimistas entre nosotros pueden suponer que dado que la práctica del control industrial tiene una larga historia de conexión y recopilación de datos de dispositivos de un tipo u otro, entonces esto es más de lo mismo.

Sin embargo, otros sectores opinan que se presentan unas oportunidades que no se pueden dejar pasar. Por ello, dicen que es necesario generar unos estándares que estén a la altura de los que existen ahora mismo.

Ante esta nueva perspectiva, surgen una serie de preguntas, entre ellas se incluyen:

¿Hay riesgos adicionales introducidos por esta clase de tecnología?

¿Esto requerirá o justificará requisitos nuevos o significativamente modificados en los estándares?

¿Para qué debería el reconocimiento del impacto del IIo tener en cuenta los estándares existentes y planificados?

Dado que la complejidad del tema de seguridad, ya hay organizaciones que se han puesto , la esperanza es que podamos evitar crear otros adicionales dedicados a áreas tecnológicas específicas, como IIoT.

El enfoque preferido es analizar el impacto en la intersección de IIoT y seguridad cibernética, con el fin de identificar áreas específicas donde las normas y los informes existentes y en desarrollo pueden necesitar modificarse para agregar la consideración y énfasis apropiados de IIoT en los planes de despliegue y operaciones.

CyberX ha realizado un análisis de los riesgos a los que se exponen las industrias, y ha llegado una serie de conclusiones que se resumen en este infograma:

- Un tercio de los sistemas industriales están conectados a Internet.
- Más de tres cuartos de los sitios tienen versiones de Windows obsoletas.
- Autenticación débil

- Ausencia de antivirus
- Dispositivos no deseados y acceso inalámbrico
- Acceso remoto

De la mano de estos riesgos, llegan unas recomendaciones que las empresas deberían implantar para plantarle cara a los nuevos riesgos que aparecen.

- Ofrecer una formación para aumentar la conciencia sobre la seguridad y reforzar políticas corporativas fuertes
- Iniciativas organizacionales que rompan las barreras entre el mundo IT y el OT
- Usar controles compensatorios y defensas multicapa para detectar ataques y amenazas rápido
- Identificar de forma proactiva las vulnerabilidades más críticas

CSO ha publicado un informe en el que aparecen las 10 compañías más emergentes proporcionan soluciones de ciberseguridad en IIoT y ICS:

Applied Risk, Amsterdam

Bayshore Networks, New York

Claroty, New York, NY

Dragos, Washington, D.C.

Indegy, Tel-Aviv, Israel

mPrest, Petach Tikva, Israel

NexDefense, Atlanta

Nozomi Networks, San Francisco

Veracity, Alisa Viejo, Calif.

Waterfall Security, Rosh Ha’ayin, Israel

Obviamente, esta es una lista en la que no aparecen todas las empresas que tienen un impacto en el tema de la protección sino las más emergentes y de las que habrá que estar pendientes. En esta lista no se incluyen las grandes compañías como Airbus, BAE Systems, Cisco, IBM, Intel, Siemens o Symantec.

Una vez más, aparecen nuevos retos en la industria y solo las empresas que hayan aprendido del pasado serán capaces de emerger en el futuro.

Referencias:

Announcing the CyberX “Global ICS & IIoT Risk Report”. Visitado el 29 de noviembre de 2017. https://cyberx-labs.com/en/blog/announcing-cyberx-global-ics-iiot-risk-report/

How will ICS cybersecurity standards be impacted by IIoT? Visitado el 29 de noviembre de 2017.https://industrial-iot.com/2017/05/will-ics-62443-cybersecurity-standards-impacted-iiot/

ICS / IIoT Security Diary. Visitado el 29 de noviembre de 2017. https://cybersecurityventures.com/ics-iiot-security-report-diary/

10 emerging ICS and IIoT cybersecurity companies to watch. Visitado el 30 de noviembre de 2017. https://www.csoonline.com/article/3211372/security/10-emerging-ics-and-iiot-cybersecurity-companies-to-watch.html

IT vs. OT for the Industrial Internet – Two Sides of the Same Coin? Visitado el 30 de noviembre de 2017. https://www.globalsign.com/en/blog/it-vs-ot-industrial-internet/

2020: Future automation. Visitado el 30 de noviembre de 2017. https://www.controleng.com/single-article/2020-future-automation/c33ed4679973dcb1ed2f53411520088d.html

---

Controlemos esto

El camino que llevamos recorrido en el mundo de los sistemas de control industrial es largo ya. Hemos pasado por la historia que han tenido, el contexto en el que se encuentran y los riesgos a los que están expuestos debido a los avances en la tecnología sobre todo. Como ya hemos ido viendo, han sido, son y serán muchos los beneficios que ha traído la tecnología a la industria, pero también muchas han sido, son y serán las amenazas a los que los ha expuesto. Por ello, es necesario recopilar una información concreta que será clave a la hora de proteger y prevenir los daños.

Sistema de logs	Entradas del log del sistema	Log de aplicación	Mensajes de log de aplicación
	Errores/warning de sistema	Monitorización de rendimiento y estado	Estado del agente
	Accesos válidos e inválidos al sistema		Tiempo actividad del sistema
	Entradas del log del firewall		Uso de cpu, disco y memoria
	Accesos válidos e inválidos al perímetro		Tráfico de entrada y salida
	Excepciones de paquetes en el firewall	Monitorización de eventos de sistema	Inicios y terminaciones inesperadas de procesos
	Anomalías en paquetes de IDS (sistema de detección de intrusos)		Conexiones y desconexiones inesperadas de sockets
	Anomalías en el flujo de tráfico de IDS		Modificaciones inesperadas de registros
	Syslog general		Modificaciones inesperadas de archivos o programas
Configuración de sistema	Hardware		Cambios en dispositivos extraíbles
	Interfaces		Cambios o errores en los cambios de contraseñas
Ajustes del sistema	Políticas de logeo de sistema	Monitorización de listas blancas	Intentos de ejecución no autorizados
	Políticas de contraseñas de sistema		Actividad de cambios en las listas blancas
	Reglas del firewall	Gestión de listas blancas	Inventario de listas blancas
	Puertos y servicios permitidos o usados		Ajustes de políticas de cambio
Software y parches	Fecha de inventarios de software	Cuentas locales	ID de cuentas
	Fecha de instalación de parches		Tipos de cuenta, edad

Es una gran cantidad de información la que hay que guardar para después auditar y comprobar que todo está seguro. Para que esta gestión sea adecuada, es conveniente monitorizar, gestionar y proteger ciertas funciones de la empresa. Es recomendable monitorizar:

- Registro de eventos, correlación y archivo

- Vista unificada única
- Tableros de interfaz de usuario personalizables
- Arquitectura escalable

Además de lo anterior, gestionar:

- Integridad del archivo
- Monitorización de tráfico de red
- Proceso crítico y monitorización del servicio
- Reportar suscripciones
- Identificación de cambio de cuenta de usuario
- Archivo de archivo de configuración del dispositivo
- Red y sistema de salud y rendimiento
- Mantener la política de configuración central
- Recopilar e informar sobre ajustes, cuentas y configuraciones
- Analizar los cambios en la base de activos y el entorno
- Administrar el perímetro de seguridad electrónico reforzado
- Gestión de cambio de configuración
- Aplicar políticas de aplicaciones de nivel de host

Y proteger también:

- Prevenir aplicaciones maliciosas / malware
- Bloquear aplicaciones no autorizadas
- Hacer cumplir las políticas de cambio de confianza

Es una tarea que no solo no es fácil, sino que además es una tarea de vital importancia para la supervivencia de las empresas. Por ello, hay empresas que se han especializado en estos temas. INCIBE y el CCI (Centro de ciberseguridad industrial) son dos de las organizaciones que ofrecen su ayuda para que las empresas se protejan contra los ciberataques. El CCI en concreto ofrece una guía para la construcción de un sistema de gestión ciberseguridad industrial.

Ciertamente, es aliviador saber que finalmente, le están dando la importancia que se merece la seguridad de la industria.

Referencias:

Siem Industrial defender. Visitado el 21 de noviembre de 2017. http://www04.abb.com/global/dkabb/dkabb504.nsf/0/41f890a019314da9c1257afa002f2e65/$file/Sikkerhedsoverv%C3%A5gning+i+kontrolsystemer+-+Industrial+Defender.pdf

Instituto nacional de ciberseguridad de España. Visitado el 21 de noviembre de 2017. https://www.incibe.es/

Centro de ciberseguridad industrial. Visitado el 22 de noviembre de 2017. https://www.cci-es.org/web/cci/detalle-actividad/-/journal_content/56/10694/2

18112

Guía para la construcción de un SGCI (Sistema de Gestión de la Ciberseguridad Industrial). Visitado el 23 de noviembre de 2017. http://services.codeeta.com/widget/v3/65971

Riegos

Un estudio realizado por el Instituto SANS de cientos de profesionales de sistemas de control industrial (ICS) y las partes interesadas de seguridad cibernética en diversas industrias verticales, incluyendo la energía, la industria manufacturera, y el petróleo y el gas ha revelado que 4 de cada 10 profesionales del ICS carecen de visibilidad en sus redes ICS.

Esto significa que el 40% de los los defensores están trabajando con los ojos vendados. Siendo incapaces de detectar un ataque cibernético, averiguar de dónde viene y remediarlo en una cantidad de tiempo razonable. Una estadística aún más aterrador si se tomamos en cuenta todo lo que ya hemos comentado en posts anteriores: las amenazas a los sistemas de ICS son altos, o severa y crítica.

Al investigar sobre las amenazas que se detectan en la industria, las cuatro más apremiantes son:

- Añadir dispositivos que no pueden protegerse a sí mismos a la red.
- Incidentes internos estimulados por acciones accidentales.
- Amenazas externas de hacktivistas y ataques financiados.
- Extorsión – incluyendo ransomware.

Las amenazas de seguridad cibernética que afectan a los sistemas de control industrial están creciendo y la identificación de ataques sigue siendo un reto importante según la encuesta anual sobre los sistemas de control industrial llevada a cabo por el SANS Institute, en la que participaron algunos líderes de la industria como Nozomi redes. Esta encuesta llegó a la conclusión de lo que ya venimos comentando tiempo atrás: a pesar de que se hayan realizado avances en la protección de activos críticos e infraestructura, han surgido nuevas amenazas.

Como sugiere la frase inicial, cuatro de cada 10 profesionales de la seguridad ICS carecen de visibilidad en sus redes ICS, que es uno de los

principales impedimentos para asegurar estos sistemas. Por estos motivos, el ransomware fue recientemente identificada como una amenaza parte superior, junto con la creciente adición de dispositivos a la red.

A pesar de la cobertura de noticias casi a diario de los recientes ataques a los sistemas sin parches, SANS encontró que sólo el 46% de los encuestados se aplica regularmente los parches del fabricante; y 12% no aplica ni los parches de seguridad ni de capa de protección alrededor de los activos críticos del sistema de control.

Además de los riesgos ya comentados, existen muchas otras amenazas que acechan a los sistemas de control industrial. Entre ellos están:

- El alto número de cuentas privilegiadas o de administración que permiten al usuario o a las aplicaciones acceder al ICS
- El uso de cuentas compartidas que permite el acceso a sistemas críticos sin ningún tipo de supervisión.
- El uso de aplicaciones industriales con credenciales *hard-coded* embebidas.
- Es uso de estaciones de trabajo con privilegios administrativos completos.

Tal es el riesgo, que es necesario afrontar estas amenazas de una forma proactiva, de tal forma que prever el riesgo se vuelve una prioridad. Es tal, que están apareciendo en el mercado un sin fin de soluciones que permiten a las empresas gestionar sus riesgos y su seguridad de una forma más cómoda.

Como ya hemos comentado anteriormente, el gran problema, y de donde vienen la mayoría de los riesgos, es de conectar al Internet unos sistemas que no estaban pensados para ser conectados. Los sistemas SCADA son otro de los grandes riesgos que tiene la industria. Estos sistemas estaban pensados con una robustez innegable, y son impenetrables cuando son atacados desde los flancos para los que tienen sus defensas preparadas. Sin embargo, la conexión a Internet no es un flanco para el que estuvieran preparados. Además, a todo esto se suma la poca tolerancia a cambios que tienen los SCADA. Están pensados para ser instalados y durar décadas, no para que se les apliquen los frecuentes parches de firmware a los que tan acostumbrados estamos ya. Por ello, las compañías están dejando de utilizar estos sistemas, que han dejados de responder a una industria en constante cambio.

En conclusión, la mayoría de los riesgos surgen de la entrada de Internet en la industria, algo con muchas ventajas, de las que las empresas quisieron aprovecharse lo antes posible, pero descuidaron uno de los aspectos más

importantes: la seguridad.

Referencias:

Industrial Control Systems Security, consultado el 7 de noviembre. https://www.cyberark.com/solutions/security-risk-management/industrial-control-systems-security-compliance/

Applied Risk: An established leader in Industrial Control Systems security, consultado el 7 de noviembre. https://applied-risk.com/

https://www.technologyreview.com/s/511671/cybersecurity-risk-high-in-industrial-control-systems/

Prediciendo lo impredecible

El otro día, iba hablando hablado con un amigo por la calle y me dijo que se le había roto el coche y que no podía arreglarlo porque no tenía dinero para ello. Y estuvimos comentado que menuda putada era que justo se le hubiera roto el coche a él y que era imposible anticiparse a que le pasara. Sin embargo, le estuve dando vueltas al tema y llegué a una serie de conclusiones. El coche de mi amigo tenía 20 años, y no es nada descabellado pensar que un coche de 20 años vaya a sufrir problemas más a menudo que uno recién comprado. También estuve pensando sobre la tendencia que tenemos las personas de pensar que somos el centro del universo. Cuando a mi amigo se le rompió el coche dijo algo así como “¡Joder es que todo me pasa a mi!”. Una vez más, volvemos a lo de antes, un coche de 20 años no es tan raro que se rompa.
Esta anécdota me llevó a pensar en lo que llamamos imprevistos y en la forma de planificarnos alrededor de ellos. Para explicar estos imprevistos y las diferencias entre ellas voy a poner un ejemplo de una vida real, los gastos en mi vida. Como es lógico pensar, estos ejemplos se pueden extrapolar a la vida de cualquier persona o a cualquier ámbito, como es el mundo de las TIC.

El primer grupo se trata de los previstos. Todo el mundo tiene una agenda (bien sea en la cabeza, en el papel o en el móvil) que nos dice dónde tendríamos que estar en cada momento. De la misma forma, sabemos que hay gastos que van a llegar y en qué momento. Yo sé que el día 30 de cada mes me van a ingresar la nómina, pero también sé que el día 5 de cada mes, me van a pasar la factura de internet. La categoría de los previsibles abarcan todas aquellos factores que están programados. Están organizados y gestionados y

sabemos cómo tratar con ellos.

El segundo grupo es el de los imprevistos previsibles. A este grupo pertenece el “imprevisto” que tuvo mi amigo con el coche. Son esos imprevistos que sabemos que tarde o temprano van a llegar, pero que no queremos aceptar. Como jefe de equipo, eres consciente de que uno de los hijos de tus empleados va a llegar tarde algún día porque su hijo tiene fiebre. Es importante analizar nuestra situación para poder detectar estos factores que a simple vista no son tan fáciles de ver. Yo en mi vida sé que la lavadora de mi casa hay veces que lava mal la ropa y sale oliendo mal. No sé cuándo va a suceder, pero sé que va a pasar. Por ello, estoy preparado para que, el día que me toque, lavar la ropa a mano con el jabón especial.

El tercer, y último, grupo es de los imprevistos que no se pueden predecir. En este grupo entran aquellos factores que, generalmente, más impacto tienen en nuestra vida u organización, pero que son poco probables. Si nuestra empresa tiene contratado un servicio en AWS, y justo sufre un incendio en los servidores que nos daban servicio, experimentamos una bajada de la calidad de servicio. Como ya hemos comentado, intentar adivinar este tipo de factores es ciertamente complicado, por ello no hay que obsesionarse intentando controlar todos los aspectos.

Integrar esto en nuestra vida supone una carga de trabajo que mucha gente no está dispuesta a aceptar. Requiere tener un plan de vida creado y hoy en día poca gente se para a pensar cuáles son sus objetivos y su forma de obtenerlos. Sin este plan, es posible identificar estos imprevistos de los que hablábamos pero hallar la solución será una misión propia de Tom Cruise, imposible.

En conclusión, predecir lo impredecible es imposible, pero hay formas de esperar aquellas cosas que no esperamos.

ICS: una caja fuerte con demasiadas llaves

Uno de los mayores retos de las personas inteligentes de nuestra época es resumir todo lo que un concepto quiere decir en pocas palabras de forma que el resto de los seres humanos seamos capaces de entenderlo. Sin embargo,

muchas veces caemos en el error de creer que lo entendemos sin parar a mirar los detalles. En el campo de los Sistemas de control Industrial, es lo que ha hecho Amit Yoran:

> *Intrusions into systems that control operations in the chemical, electrical, water, and transport sectors have increased 17-fold over the last three years. The advent of connected and automated sensors aggressively exacerbates these issues. The growth in the use of cyber technology for terrorism, hacktivists, and other actors, combined with the weakness of ICS security generally, combined with the potential impact of bringing down a power facility or water treatment plant (hello, California), makes the critical breach of an ICS in 2016 extremely concerning and increasingly likely.[1]*

Realmente, en menos de 100 palabras ha definido cuál es el marco del riesgo en los ICS. Si analizamos la frase más a fondo, nos damos cuenta de las claves de las que habla

- **Fuentes y eventos de amenazas**: *"Growth in the use of cyber technology for terrorism, hacktivists, and other actors"*
- **Exploits, con probabilidad de éxito**:*"Intrusions into systems that control operations in the chemical, electrical, water, and transport sectors have increased 17-fold over the last three years"*
- **Vulnerabilidad, en el contexto de las condiciones de predisposición**: *"The advent of connected and automated sensors aggressively exacerbates these issues"*
- **Controles de seguridad, con efectividad**: *"The weakness of ICS security generally"*
- **Efecto adverso**: *"The potential impact of bringing down a power facility or water treatment plant (hello, California)"*
- **Riesgo, como una combinación de impacto y probabilidad**: *"The critical breach of an ICS in 2016 [is] extremely concerning and increasingly likely"*

Las empresas se están dando cuenta esta realidad hace mucho, pero esto no quiere decir que se hayan blindado contra estos riesgos. El día a día nos muestra como no estamos tan preparados como pensábamos para soportar estos ataques. Joel Brenner, un investigador del MIT, asegura que un ataque a algún sistema de control industrial puede resultar catastrófico para el sector en el que se centra el ataque. En foro de ciberseguridad europeo CyberSec[3] o en Cracovia que la amenaza venía de dos puntos distintos, de las naciones y de las organizaciones criminales. A pesar de que existen ciertos factores que disuaden a las naciones a llevar a cabo este tipo de ataques, estos factores no afectan a las organizaciones criminales.

En los últimos años ha habido numerosos ejemplos de ciberataques que han afectado a alguna infraestructura crítica de la sociedad. WannaCry afecto al servicio nacional de salud del Reino unido[4], los ciberataques contra el sistema de energía ucraniano[5], el ataque al proveedor de DNS Dyn[6] o el

ataque a Saudi Aramco[7]. A finales de 2016, la firma Kaspeski lab afirmó que el 24% se los ICS estaban bajo ataque.

Ya somos somos conscientes de cuáles son las causas que han generado estos problemas. La entrada de Internet en la industria sirvió para abrir muchas nuevas oportunidades para las compañías, que supieron aprovechar, pero cerrando los ojos a los riesgos o simplemente ignorándolos. Sin embargo, no todo esta perdido, desde el MIT llegan algunas recomendaciones para tratar de blindar el ICS:

1. Los controles clave de ICS deben aislarse de las redes públicas para que sean razonablemente seguros.
2. Los gobiernos deben respaldar un mercado para una tecnología de control más simple y segura.

Aislar el ICS del Internet puede ser una solución para eliminar las amenazas entrantes, pero negando todas las oportunidades por las que una vez el Internet entró en el sector.

¿Qué es lo más correcto ahora?¿Cortar por lo sano o invertir en seguridad y procesos de control de calidad?

Referencias

[1]<<Breaking Down the Risk of Industrial Control Systems Security>>, Acceso el 20 de octubre de 2017,http://www.aberdeenessentials.com/techpro-essentials/breaking-down-the-risk-of-industrial-control-systems-security/

[2]<<Industrial control systems under attack, warns MIT researcher>>, Acceso el 20 de octubre de 2017, http://www.computerweekly.com/news/450428010/Industrial-control-systems-under-attack-warns-MIT-researcher

[3] <<CYBERSEC FORUM>>, Acceso el 20 de octubre de 2017 https://cybersecforum.eu/en/

[4] <<WannaCry a signal moment, says NCA>>, Acceso el 20 de octubre de 2017, http://www.computerweekly.com/news/450421936/WannaCry-a-signal-moment-says-NCA

[5]<<Ukraine cyber attacks extend beyond power companies, says Trend Micro>>, Acceso el 20 de octubre de 2017, http://www.computerweekly.com/news/4500273017/Ukraine-cyber-attacks-extend-beyond-power-companies-says-Trend-Micro

[6]<<Dyn reveals details of complex and sophisticated IoT botnet attack>>,

Acceso el 20 de octubre de 2017, computerweekly.com/…/Dyn-reveals-details-of-complex-and-sophisticated-IoT-botnet-attack

[7] <<Saudi Aramco oil firm claims to be over cyber attack>>, Acceso el 20 de octubre de 2017, computerweekly.com/…/Saudi-Aramco-oil-firm-claims-to-be-over-cyber-attack

---

Sistemas de control industrial y riesgos

Caminar por la calle debería ser suficiente para darse cuenta del afán de los humanos por controlar todo. El tiempo, el clima, la calidad del aire, el numero de plazas en el parking de debajo de tu casa. Está por todos los lados. En las farmacias, en los escaparates de tu tienda de ropa o en el bar con tus amigos. Y lo cierto es que todo este control tiene un sentido. El control nos ayuda a comprender nuestro entorno, y por consiguiente predecirlo. Esto es algo que el ser humano no ha tardado mucho en darse cuenta, ya que la intención de controlar nuestros alrededores se remonta muy atrás, pero es actualmente cuando más controversia. Ante el control que el gobierno quiere imponer a los ciudadanos, estos se revelan para proteger su privacidad. Y siempre es por lo mismo, el afán de controlar y predecir. Este control también se extiende al mundo de la empresa y de la industria. Sería ideal controlar todas las variables que pueden inferir en el negocio, pero entran en juego dos variables que limitan este sueño: el tiempo y los recursos. Por ello, es cada vez más importante saber gestionar estos recursos e identificar las variables más importantes a controlar.

Antes de comprender el presente, intentemos comprender el pasado. Uno de los primeros mecanismos de control, se cree que fue un antiguo reloj de agua Ktesibios en Alejandría, Egipto. Sin embargo, se considera que el *boom* de los

sistemas de control industrial se inicio a medidos del siglo XVIII. Fue a finales de siglo cuando realmente se avanzó en la industria y campos específicos notaron considerables mejoras. En la industria naval, por ejemplo, se permitió la construcción de barcos más grandes gracias a la invención de los servomecanismos o servomotor. A mediados de 1950, empiezan a aparecer lo que conocemos como sistemas de control modernos. Los ingenieros se dieron cuenta de que las mediciones reales contienen errores y están contaminadas por el ruido, por lo que empezaron a aparecer nuevas formas de medir. Emergen también los PLC, o los controladores lógicos programables y términos como SCADA (*Supervisory Control and Data Acquisition*). Automatizar el control hizo que incrementara muchísimo la producción del sector industrial, pero de la misma forma que la tecnología y la información trae nuevas oportunidades, trae consigo también nuevos riesgos.

Los sistemas de control industrial se habían convertido en un activos muy fiables. Si bien es cierto que podían tener algún fallo interno, estaban completamente cubiertos en cuanto a los ataques externos se refiere. Sin embargo, los sistemas computacionales no son inmunes a las ciber-amenazas. La entrada del Internet en la industria, se abre un nuevo mundo para los ciberataques. Esto es una grave amenaza, que algunas empresas han sabido identificar mejor que otras, ya que se ha demostrado que un ataque de este tipo puede tener las mismas o peores consecuencias que un ataque físico. Ejemplos muy actuales demuestran la capacidad devastadora con la que cuentan. En esta imagen se muestran los 8 mayores ciberataques del 2016 según Forbes. Los sistemas de control industrial han pasado literalmente de tener cero días de ataques, a tener ataques de día cero.

A medida de que la industria avanza surgen nuevas tecnologías con las que controlar los procesos. Los sistemas de computación en la nube son cada vez más populares en el mundo de la industria, y términos como IIoT o la industria 4.0 están dejando de ser novedosos. El mundo de la industria está viviendo su cuarta revolución hacia un mundo totalmente nuevo, en el que las fábricas son más productivas, más flexibles y más eficientes. La computación en la nube ya es una realidad también en el mundo industrial. Nuevamente vuelven a surgir oportunidades y amenazas. En un mundo tan competitivo, donde se le otorga un altísimo valor a la información y el dato, ¿qué pasa cuando esos datos están en *la nube*? Los sistemas de control se tienen que extender mucho más allá de los límites de la organización.

Ciertamente, como con cada revolución, se plantea un futuro incierto pero ilusionante, donde se permite que el desarrollo y la innovación puedan volver a ser factores determinantes. Sin embargo, tenemos que aprender del pasado y aplicar esas lecciones al presente y al futuro. Innovación y desarrollo y control y seguridad tienen que ir de la mano. Olvidarlo es ser olvidado.

Referencias:

<<JOnline: Security of Industrial Control Systems>>, Acceso el 8 de octubre de 2017, https://www.isaca.org/Journal/archives/2010/Volume-4/Pages/JOnline-Security-of-Industrial-Control-Systems.aspx

<<Industrial Control Systems and Risks>>, Acceso el 8 de octubre de 2017, https://blogs.deusto.es/master-informatica/industrial-control-systems-and-risks/

<<Breaking Down the Risk of Industrial Control Systems Security>>, Acceso el 8 de octubre de 2017,http://www.aberdeenessentials.com/techpro-essentials/breaking-down-the-risk-of-industrial-control-systems-security/

<<Control system>>, Acceso el 8 de octubre de 2017, https://en.wikipedia.org/wiki/Control_system

<<Industrial Control Systems: A Primer for the Rest of Us>>, Acceso el 8 de octubre de 2017, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/industrial-control-systems-a-primer-for-the-rest-of-us.aspx

<<An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity>>, Acceso el 10 de octubre de 2017, https://ics.sans.org/media/An-Abbreviated-History-of-Automation-and-ICS-Cybersecurity.pdf

<<8 Major Cyber Attacks Of 2016 [Infographic]>>, Acceso el 10 de octubre de 2017, https://www.forbes.com/sites/kevinanderton/2017/03/29/8-major-cyber-attacks-of-2016-infographic/

<<Industria 4.0>>, Acceso el 10 de octubre de 2017, https://es.wikipedia.org/wiki/Industria_4.0