Capítulo tercero

Ciberseguridad, geopolítica y energía

Alberto Pinedo Lapeña

Resumen

El sector eléctrico se enfrenta a la creciente amenaza de ciberseguridad por parte de grupos de ciberdelicuentes que lanzan cada vez ataques más sofisticados, y a pesar de que las empresas cada vez están más preparadas, una reciente encuesta de Utility Dive sitúa la ciberseguridad como la segunda mayor prioridad donde las empresas creen que deben centrarse. Los expertos están de acuerdo, señalando por un lado el aumento de los niveles de gasto que se están viendo alrededor de la seguridad y la expansión en el uso de sus estándares y por otro en el intercambio cada vez mayor de información dentro de la industria.

El sector de las utilities además ha visto un claro aumento en el gasto en seguridad desde el año 2015, cuando la red eléctrica de Ucrania se vio afectada por un ataque que provocó un largo apagón y que afectó a casi 250.000 personas. O ataques como los más recientemente sufridos en Florida a la cadena de suministro que han venido a reafirmar que la ciberseguridad es un tema al que se le debe dar prioridad. Además, tenemos delante de nosotros la transición global de los combustibles fósiles a las energías renovables y los recientes cambios geopolíticos en el

ámbito internacional que han hecho que la ciberseguridad sea un elemento consustancial a los nuevos equilibrios de fuerzas entre Estados. En este capítulo repasaremos el contexto actual energético, las nuevas amenazas globales y las recomendaciones de ciberseguridad en el sector.

Palabras clave

Ciberseguridad, cibercrimen, amenazas.

Cybersecurity, geopolitics and energy

Abstract

The electricity sector faces a growing cybersecurity threat from cybercriminals launching increasingly sophisticated attacks; and despite companies getting wiser to it, a recent Utility Dive survey ranks cybersecurity as the second greatest priority that companies believe they should focus on. Experts agree, pointing, on the one hand, to the increasing levels of spending on security and the expansion in the use of security standards, and on the other, to the ever-increasing exchange of information within the industry.

The Utilities sector has also seen a clear increase in spending on security since 2015, when Ukraine's power grid was hit by an attack that caused a lengthy blackout, affecting nearly 250,000 people. Or, more recently, like the attacks in Florida to the supply chain that have reaffirmed cybersecurity as an issue that should be given high priority. In addition, we have before us the global transition from fossil fuels to renewables energies and the recent geopolitical changes in the international arena that have made cybersecurity an inherent element of the new balance of forces between states. In this chapter, we will review the current energy context, new global threats, and cybersecurity recommendations for the sector.

Keywords

Cybersecurity, cybercrime, threats.

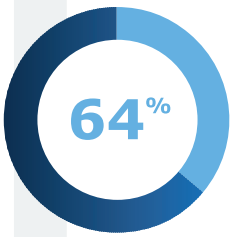
ESTADO DE LOS SISTEMAS INDUSTRIALES AUDITADOS

71%

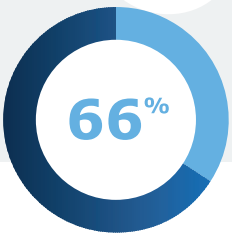
DE LAS INFRAESTRUCTURAS AUDITADAS POR MICROSOFT EN EL ENTORNO DEL IIoT/ICS* TENÍAN **SISTEMAS MICROSOFT WINDOWS NO SOPORTADOS**** QUE YA NO RECIBEN PARCHES DE SEGURIDAD, **LO QUE LOS HACE ESPECIALMENTE VULNERABLES.**

62%

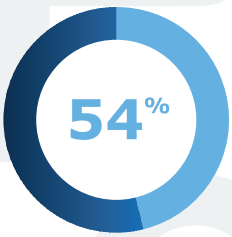
EL **PORCENTAJE DE INFRAESTRUCTURAS OT CON SISTEMAS WINDOWS NO SOPORTADOS** SIGUE SIENDO ALTO, INCLUSO EXCLUYENDO LOS SISTEMAS WINDOWS 7 QUE QUEDARON FUERA DE SOPORTE EN ENERO DE 2020.



DE LAS INFRAESTRUCTURAS OT TENÍAN **CONTRASEÑAS SIN CIFRAR CIRCULANDO POR SUS REDES,** LO QUE FACILITA EL COMPROMISO DE LOS SISTEMAS SIMPLEMENTE HACIENDO SNIFFING DE RED.



DE LAS INFRAESTRUCTURAS **NO ACTUALIZABAN AUTOMÁTICAMENTE LOS SISTEMAS WINDOWS** CON LAS ÚLTIMAS DEFINICIONES DE ANTIVIRUS.



DE LAS INFRAESTRUCTURAS TENÍAN **DISPOSITIVOS A LOS QUE SE PODÍA ACCEDER DE FORMA REMOTA DESDE REDES INTERNAS**, LO QUE PERMITIRÍA A LOS ATACANTES MOVERSE SIN SER DETECTADOS A OTROS ACTIVOS CRÍTICOS.

* **IIoT:** INTERNET OF INDUSTRIAL THINGS / **ICS:** INDUSTRIAL CONTROL SYSTEMS

** **SISTEMAS MICROSOFT WINDOWS NO SOPORTADOS:** WINDOWS 2000, WINDOWS XP Y WINDOWS 7

EL MERCADO DE LAS CIBERAMENAZAS

GRUPOS DE CIBERDELINCUENTES A SUELDO Y BIEN PREPARADOS PUEDEN COMPROMETER UNA INFRAESTRUCTURA POR UNOS POCOS DÓLARES.

ATACANTE A SUELDO

DESDE
$250
POR TRABAJO

SPEAR PHISHING A SUELDO

ENTRE
$100 Y
$1.000

ROBO DE CREDENCIALES

$0,97
POR CADA 1000
(DE MEDIA)

KITS DE RANSOMWARE

DESDE
$66
(O 30% DE LOS BENEFICIOS/ MODELO DE AFILIACIÓN)

EXPLOIT KITS

$1.400
/MES

BREACHING SERVICES

$10.500
(DE MEDIA)

ZERO DAYS

ENTRE
$50K Y
$3,5M

DENEGACIÓN DE SERVICIO

$311,88
/MES

ADEMÁS, **SE TRATA DE UN MERCADO EN CONTINUA EVOLUCIÓN**, DONDE LOS PRECIOS ESTÁN EN NIVELES MUY BAJOS, LO QUE HACE QUE **RESULTE MUY BARATO EFECTUAR UN ATAQUE.**

Contexto energético actual

La transición global de los combustibles fósiles a las energías renovables conducirá sin duda a un cambio geopolítico en el tablero internacional. El proceso estará definido por la evolución en lugar de la revolución y la geopolítica basada en el petróleo se verá desafiada pero no abandonada completamente.

Actualmente ya se están produciendo cambios fundamentales en el sistema energético mundial, cambios que afectarán a casi todos los países y que tendrán consecuencias geopolíticas de gran alcance. Durante muchos años las estrategias basadas en combustibles fósiles han ido dando forma al mapa geopolítico mundial. Los llamados Estados petrolíferos, naciones cuyas economías dependen en gran medida de la extracción y exportación de petróleo y gas natural, han obtenido un gran poder utilizando su capacidad de reducir o incluso eliminar las exportaciones de petróleo, gas natural y sus derivados. Además, los ingresos obtenidos por dicha exportación han permitido influir en las políticas de otras naciones y afectar así a las sociedades en su conjunto.

Este poder político y económico de los Estados petrolíferos disminuirá gradualmente a medida que las fuentes de energía renovables se generalicen, lo que puede significar que ciertos Estados pierdan su estatus como potencias en la geopolítica de la energía. Esto puede llegar a crear cierta inestabilidad interna con posibles riesgos de contagio en otras regiones. De hecho, países ubicados en el Cuerno de África ya se están enfrentando a una descarbonización a medida que los ingresos del petróleo, su principal producto de exportación, se desploman. Esto deja a dichas naciones ante la situación de no ser capaces de alcanzar acuerdos políticos a nivel nacional donde, en ausencia de estructuras de gobernanza mundial, pueden surgir nuevos conflictos principalmente debidos a tres hechos:

- En primer lugar, el cambio de economías basadas en carbono a economías basadas en energías renovables.
- En segundo lugar, la nueva definición del futuro geopolítico a través de nuevas formas de gobernanza que estarán estrechamente conectadas a tecnologías energéticas específicas y diferentes a las actuales.
- En tercer lugar, la demanda mundial de minerales para producir energía renovable se acelerará y llevará a nuevos Estados al centro de la competencia geopolítica.

El poder de cortar los suministros de petróleo y gas ha dominado dicha geopolítica desde del siglo XX, los combustibles fósiles se concentraron en ubicaciones geográficas muy específicas con una gran capacidad de influencia. Con la transición hacia fuentes de energía renovables como la energía eólica, y solar en todas sus vertientes, reducimos esa dependencia de las energías fósiles como el petróleo. Además, dichas energías renovables se generan de forma descentralizada lo que hace muy difícil su uso como arma de energía política.

Ante esta situación surgen nuevas amenazas, la principal, los cortes de suministro producidos por ciberataques a las infraestructuras críticas de energía. Y esos ataques pueden darse en cualquier parte y desde cualquier parte del mundo. En 2015 un ciberataque a la red eléctrica de Ucrania dejó a un cuarto de millón de personas sin electricidad.

A medida que las empresas que dan servicios energéticos en el mundo recurren a fuentes de energía renovable, y utilizan soluciones digitales e inteligentes, el riesgo aumenta y el sabotaje de dichas infraestructuras a pequeña escala es una de las amenazas clave del sector y en consecuencia de la nueva geopolítica energética.

Los ciberataques contra actores geopolíticos clave como EE. UU., Europa, China, Irán o India ilustran como las grandes naciones pueden también ser golpeadas por los ciberdelincuentes. A medida que el mix energético evoluciona desde una energía basada en combustibles fósiles a una energía moderna y renovable, también lo hacen las herramientas que los ciberdelincuentes utilizan para interrumpirla y controlarla.

Autonomía energética y amenazas de ciberseguridad globales

Paralelamente, las diferentes tecnologías allanan el camino para gestionar estructuras de gobernanza mucho más específicas. Las estrategias para asegurar un flujo estable y asequible de energía basada en el carbono ocuparon un lugar muy destacado en la agenda geopolítica del siglo XX e involucraron intervenciones, acuerdos y creación de organismos internacionales como la AIE, la Agencia Internacional de la Energía y la OPEP.

Además, las vastas y costosas técnicas necesarias para extraer, procesar y transportar energía basada en carbono requerían por un lado la participación de los Gobiernos, y por otro, otras formas

centralizadas de control. Sin embargo, las energías renovables pueden generarse mediante sistemas más pequeños y accesibles para un conjunto mayor de empresas y particulares.

Todo esto, tiene unas implicaciones políticas y económicas, pero también tiene implicaciones desde el punto de vista de la ciberseguridad.

Si bien, estas infraestructuras energéticas a pequeña escala son menos vulnerables a ciberataques y la generación de energía distribuida a pequeña escala reduce su vulnerabilidad estratégica, el control sobre estos sistemas altamente interconectados y digitalizados, se suele ejercer a nivel subnacional. Por ejemplo, a través de cooperativas energéticas o a través de redes comunitarias de energía.

Esta generación de energía descentralizada permite cierta independencia energética a nivel local y regional. Sin embargo, en el contexto político esto puede debilitar el poder de los Gobiernos centrales, disminuir sus ingresos fiscales y empoderar a las comunidades, dado que aumenta la autosuficiencia energética de los Estados, y también reduce la competencia geopolítica. Esto sin duda altera las alianzas políticas y las jerarquías basadas en los combustibles fósiles de antaño.

Por otro lado, estos sistemas, que proporcionan una mayor autosuficiencia y flexibilidad, podrían hacer que los Estados sean más propensos a los conflictos en el escenario internacional que si dependieran de los monopolistas de la energía. La Unión Europea podría haber adoptado una postura más dura sobre el conflicto de Ucrania si no fuera por la dependencia del gas ruso.

El futuro previsible sin embargo será una mezcla de ambas geopolíticas, ya que los sistemas de energía seguirán siendo híbridos junto con el establecimiento de más sistemas de energía basados en energías renovables. Los combustibles fósiles conservarán sus posiciones estratégicas y el desarrollo de grandes unidades centralizadas de generación de energía como plantas de energía nuclear y proyectos de presas hidroeléctricas se expandirán.

Así pues, la tecnología y las estrategias de ciberseguridad se tendrán que adaptar a las nuevas fuerzas geopolíticas y evolucionar para mantener seguras las infraestructuras energéticas existentes que pertenecen a la geopolítica tradicional y proteger las nuevas formas de energía renovables.

En la era del carbono y equivalentes la base de la geopolítica energética eran los hidrocarburos. El cambio a las energías renovables pone a las nuevas materias primas en el corazón de la geopolítica energética y las cadenas de suministros de materiales críticos para producción de tecnologías verdes alterarán dicha geopolítica.

La transición verde a menudo es bienvenida como una oportunidad para abandonar la política asociada al suministro de petróleo y gas, que como hemos comentado, dio forma a gran parte de la geopolítica del siglo XX. Sin embargo, las tecnologías de energía renovable requieren grandes cantidades de minerales no renovables, lo que implica una carrera global para asegurar suministros estables.

Se prevé, que la demanda de dichos minerales críticos para la transición, como el cobre, el cobalto, el litio y los llamados elementos de tierras raras crezcan exponencialmente a medida que las economías avanzadas construyan vehículos eléctricos, paneles solares, turbinas eólicas y sistemas para almacenar y distribuir dicha energía renovable.

El que controle el suministro de estos materiales tendrá influencia geopolítica en un mundo poscarbono. Su distribución geográfica se está convirtiendo rápidamente en un elemento clave. La Unión Europea, la Agencia Internacional de Energías Renovables y la Agencia Internacional de la Energía ya han puesto el foco en ello ya que abusar en el control sobre el suministro de dichos materiales con fines políticos puede poner en peligro la sostenibilidad de la transición verde.

Si bien es cierto que muchos minerales críticos para la transición son abundantes, la mayoría de las naciones carecen de la tecnología para procesarlos o no pueden extraerlos de manera rentable dadas las estrictas regulaciones ambientales. La extracción de tierras raras, cobre y litio es notablemente intensiva en combustible y agua y tiene unos altos costes ambientales por poner un ejemplo.

En la actualidad, los elementos críticos para las tecnologías verdes provienen de un número limitado de países. Asumir dichos costes ambientales y sociales, pueden traducir la abundancia de dichos minerales críticos en influencia política, podrían convertirse en los países de la OPEP de la era poscarbono. De hecho, el

exsubsecretario de Estado de los EE. UU. para Asuntos de África ya postuló que la República Democrática del Congo se convertirá en el golfo Pérsico del siglo XXI. Sin embargo, el Congo y otros productores de minerales críticos para la transición también pueden sufrir el destino de Nigeria y ser víctimas del equivalente poscarbono, con su riqueza mineral, formando una fuente de intervenciones encubiertas, conflictos civiles y subdesarrollo.

Todo este marco geopolítico unido a la digitalización de las cadenas de suministro hace que los riesgos de ciberseguridad sean un elemento para tener en cuenta en la estrategia de políticas de energía renovable, ya que la falta de medidas de protección y gestión de dichas infraestructuras digitales puede suponer un riesgo para el país.

La ciberseguridad está en todos los eslabones de dicha cadena de suministro, pero también en los sistemas de gestión de las infraestructuras renovables, desde la materia prima como comentábamos hasta la producción y manufactura de las instalaciones energéticas renovables de plantas solares y eólicas. Pero además los sistemas de telecontrol y automatismos, sistemas de gestión de montaje de infraestructuras, y sistemas de operación y mantenimiento de instalaciones.

Consideraciones de ciberseguridad en el sector energético

Los sistemas de energía eléctrica en todo el mundo están experimentando una evolución radical durante este siglo XXI, y están adoptando cada vez más conceptos transformadores como la descentralización, la automatización y la digitalización como ya comentábamos brevemente con anterioridad. Este cambio de paradigma ha llevado al despliegue de miles de millones de dispositivos en las redes y a una expansión continua de las redes de comunicaciones hacia el perímetro de la red. Si bien esta transición ha llevado a una visibilidad y control sin precedentes para el sector energético, también ha ampliado en gran medida el área de superficie potencial expuesta para los ciberataques, incrementando los riesgos cibernéticos asociados. Por otro lado, estamos observando un crecimiento exponencial en el número de ataques y la proliferación de grupos de adversarios (Estados nación, cibercriminales, hacktivistas) que de modo creciente están poniendo foco en las empresas energéticas, lo que está dando forma a un entorno empresarial en el que la pregunta a la que se enfrentan ahora las empresas es, cuándo ocurrirá un incidente, no si este ocurrirá.

Por otro lado el futuro de la regulación y la monitorización del cumplimiento normativo estará habilitado digitalmente. Así que, se debería comenzar por inventariar los procesos actuales, priorizarlos para la digitalización y luego identificar soluciones que respalden un marco de cumplimiento integrado y eficiente de las diversas actividades en todos los aspectos del negocio. Se debe poner un especial cuidado en seleccionar las soluciones más adecuadas, ya que de otro modo, puede resultar en implementaciones de calidad inferior o en sistemas inflexibles que no pueden mantenerse al día con un panorama regulatorio en constante cambio. Por otro lado, es importante involucrar a los usuarios finales en el proceso de transformación digital de manera temprana y con la mayor frecuencia posible. Esto puede ayudar a mejorar la adopción de dichas soluciones, que en última instancia son la clave para la mejora sostenible del negocio.

La industria de la energía, en los momentos de crisis como el vivido durante la pandemia de la COVID-19 han centrado la atención en dos cosas: cómo mantener a las personas seguras y cómo continuar suministrando energía a los clientes. En estos momentos de crisis, trabajar de forma remota ha sido la prioridad número uno para todas las empresas energéticas. Pero esta realidad también ha expuesto a la industria energética a nuevos riesgos cibernéticos provenientes tanto de dentro como de fuera de las defensas establecidas. Las empresas necesitan proteger a sus trabajadores y evitar interrupciones. Por lo que además las empresas deben considerar que:

- El trabajo remoto está creando nuevos riesgos cibernéticos.
- Los atacantes buscarán explotar nuevos puntos débiles en la infraestructura de las organizaciones.

El sector de la energía a nivel mundial se enfrenta a esa creciente amenaza de ciberseguridad con adversarios cada vez más sofisticados, pero diferentes encuestas muestran que las empresas generalmente creen que están bien preparadas. Los expertos están de

acuerdo, señalando el aumento de los niveles de gasto relacionados con la ciberseguridad, la expansión de los estándares de seguridad y la mejora en el intercambio de información en toda la industria.

El sector energético ha experimentado un aumento del gasto en seguridad desde 2015, cuando la red eléctrica de Ucrania sufrió el ciberataque antes mencionado que dejó sin energía a casi 250.000 personas. Según Guidehouse Insights, se espera que el gasto mundial en ciberseguridad en el ámbito de redes inteligentes aumente a casi 3.200 millones en 2026.

La industria energética tradicionalmente ha confiado en los sistemas de detección y prevención de intrusiones (ID/PS), firewalls y otras herramientas para proteger la mayor parte de sus recursos, pero dichas herramientas se limitan a la detección de malware basada en firmas y fallan frente el data fuzzing y las amenazas internas. Además, los analistas no disponen de los procesos de negocio de ciberseguridad requeridos para integrar nuevos productos en sus redes de confianza. Esto es crucial para las compañías energéticas, ya que su misión es proporcionar energía fiable y segura para satisfacer las demandas dinámicas de los consumidores.

El objetivo principal de un marco de ciberseguridad es no solo asegurar los sistemas energéticos de forma global, sino también proteger la infraestructura crítica de los ciberataques:

- A nivel de dispositivos: dotando de seguridad a los dispositivos físicos y sus interfaces (usuario y máquina).
- A nivel de comunicaciones: dotando de seguridad a la red de comunicación que los dispositivos utilizan para enviar y recibir paquetes de información.
- A nivel de aplicación: proporcionando seguridad a las aplicaciones para el procesamiento y análisis y que, proporcionan información de alto nivel a los analistas y operadores.

Dicho marco debe colocar las múltiples tecnologías de seguridad necesarias en un sistema de interconexión de sistemas abiertos (OSI), que aplique evaluaciones continuas e incorpore algoritmos inteligentes para garantizar la ciberseguridad.

Redes OT

Las redes OT utilizadas en entornos de empresas energéticas y que son consideradas infraestructuras críticas, tradicionalmente estaban alejadas de las redes de TI corporativas y de Internet,

pero la transformación digital ha aumentado tanto la conectividad como el número de dispositivos en estos entornos, lo que ha llevado a un mayor riesgo.

Muchos de los protocolos que se utilizan en IIoT (Internet Industry of Things) y en las redes OT son heredados y los dispositivos integrados en estos entornos fueron diseñados hace años, carentes de controles como el cifrado o una autenticación sólida, y además las propias redes OT a menudo son planas, sin segmentación y sin políticas de confianza cero de las que hablaremos más adelante.

Según un estudio de Microsoft realizado en 2020 a través de su filial CyberX, el 71% de las infraestructuras IIoT/OT auditadas tenían sistemas operativos Windows no soportados, como Windows 2000, Windows XP y Windows 7, que ya no reciben parches de seguridad, y que los hacen especialmente vulnerables a ransomware y malware. Incluso excluyendo los sistemas Windows 7 que quedaron fuera de soporte en enero de 2020, el porcentaje de infraestructuras OT con sistemas Windows no soportadas seguía siendo bastante alto, un 62%.

Además el 64% de las infraestructuras IIoT/OT tenían contraseñas sin cifrar circulando por sus redes, lo que sin duda facilita el compromiso de los sistemas simplemente monitorizando la red.

El 66% de las infraestructuras no actualizaban automáticamente los sistemas Windows con las últimas definiciones de antivirus, infraestructuras en las que el 54% tenían dispositivos a los que se podía acceder de forma remota desde redes internas y usando protocolos de administración estándar como RDP, SSH o VNC, lo que puede permitir a los potenciales atacantes moverse sin ser detectados a otros activos críticos.

Un ejemplo de estas situaciones de riesgo se produjo durante el ataque Triton a los sistemas de seguridad de una instalación petroquímica, el adversario aprovechó el protocolo RDP para moverse desde la red TI a la red OT con el fin de desplegar un malware zero-day.

Abordar el riesgo de ciberseguridad en el entorno energético

Con el avance de las nuevas tecnologías y sobre todo con la conexión de estas redes OT y sistemas IIoT a Internet por parte de miles de millones de dispositivos nuevos cada año, es más importante que nunca protegerlos. Es por ello por lo que se debe

abordar la transformación de dichos sistemas para facilitar la protección de los datos, garantizar la privacidad y la seguridad física.

Solo algunos proveedores de nube y empresas especializadas en el desarrollo de soluciones de seguridad IIoT/OT permiten trabajar con chips certificados que agregan capas de protección y seguridad y que permiten gestionar la confianza en las comunicaciones entre dispositivo y la nube o infraestructuras on-premise.

A medida que los sistemas industriales y la tecnología operativa continúan evolucionando y creciendo, también lo hacen las responsabilidades de los CISOs. Los CISOs ahora necesitan mitigar los riesgos inherentes de la tecnología actual conectada a la nube, los sistemas de almacenamiento y los dispositivos inteligentes desplegados en cientos de plantas de trabajo. La gestión de esos riesgos de seguridad incluye la necesidad de garantizar el correcto funcionamiento de las instalaciones de petróleo y gas, renovables, redes de distribución, transporte, así como el resto de las infraestructuras críticas del sector.

Los analistas predicen que en 2025 tendremos aproximadamente 21.500 millones de dispositivos industriales conectados en todo el mundo, lo que aumentará drásticamente el área expuesta a ataques por parte de los ciberdelincuentes. Debido a que dichos dispositivos a menudo no disponen de una buena política de actualizaciones, los CISOs necesitan nuevas estrategias para mitigar estos nuevos riesgos que difieren de manera sustancial de los que habitualmente encontramos en el área de las tecnologías de la información (TI). Dicha diferencia debe ser abordada por las juntas directivas de las compañías y por sus equipos de finanzas. Las costosas interrupciones de producción, los fallos de seguridad, que incluso pueden provocar lesiones o pérdidas de vidas humanas, los daños ambientales, todos, son escenarios potenciales que han trasladado el mundo de los dispositivos industriales al centro de la gestión de amenazas cibernéticas.

Un panorama de amenazas en evolución

Tanto los sistemas industriales como las redes OT se consideran sistemas ciberfísicos (o CPS de sus siglas en inglés); es decir, abarcan tanto el mundo digital como físico. Esto hace que cualquier CPS sea un objetivo deseable para ciberdelincuentes que buscan causar daño o una interrupción operativa. La historia reciente demuestra que dichos ataques ya son, lamentablemente, parte de nuestras vidas. Ataques como el originado en

Oriente Medio (Triton[1] que mencionamos antes), o el ataque a la red eléctrica ucraniana[2] son buenos ejemplos de este nuevo escenario. En 2017, el ransomware NotPetya[3] paralizó la poderosa línea naviera Maersk y detuvo cerca de una quinta parte de la capacidad logística mundial. Dicho ataque también se extendió al gigante farmacéutico Merck, a FedEx y a numerosas empresas europeas antes de regresar a Rusia para atacar a la compañía petrolera estatal, Rosneft.

En 2019, Microsoft observó un ataque patrocinado por el Estado ruso utilizando dispositivos inteligentes de IoT[4] (teléfonos, impresoras de oficina y decodificadores de video) como puntos de entrada a las redes corporativas, desde las cuales intentaron elevar los privilegios. Los atacantes incluso han llegado a comprometer sistemas de control de acceso a la construcción[5] para pasar a las redes corporativas utilizando ataques distribuidos de denegación de servicio (DDoS) en el que un sistema informático se viene abajo y se bloquea ante la avalancha de tráfico que recibe.

Todos estos son ejemplos del panorama actual que vivimos en el sector energético, y solo hemos citado algunos de los muchos que lamentablemente hay.

El mercado de las ciberamenazas

Pero sin duda lo que más preocupa hoy en día es el creciente mercado de ciberamenazas, donde las empresas están expuestas a un mercado que corre paralelo al de las soluciones de ciberseguridad. Mientras unos tratan de protegernos de los ciberdelincuentes, otros tienen a su disposición grupos a sueldo y bien preparados que pueden comprometer una infraestructura por unos pocos dólares. También hemos observado un aumento de la madurez de los modelos de negocio de los atacantes donde los ciberdelincuentes pueden ser muy efectivos utilizando kits

1 https://www.darkreading.com/operations/industrial-safety-systems-in-the-bullseye/d/d-id/1330912.

2 https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

3 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

4 https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/.

5 https://www.cpomagazine.com/cyber-security/hackers-use-smart-building-access-control-systems-to-launch-ddos-attacks/.

de ataque apoyados por modelos de afiliación (donde los nuevos criminales pagan a los autores del kit un porcentaje de las ganancias en lugar de comprarlo directamente).

Desde hace 3 años aproximadamente venimos observando que dicho mercado ha experimentado pocos cambios en los precios de ciertos productos, pero en el que se pueden encontrar exploit kits por $1.400/mes, breaching services por $10.500 de media, zero days entre $50K y $3,5M, y kits de ransomware desde $66 con modelos de afiliado en el que el atacante paga hasta el 33% de los beneficios al desarrollador del kit. Además, existe todo un mercado en continua evolución tal y como se puede apreciar en la figura, donde los precios para ataques de compromiso a pc/móviles, robo de credenciales y ataques DDoS son bastante asequibles, lo que hace que resulte «muy barato» efectuar un ataque.

Se da la circunstancia que algunos de los ataques existentes han ido evolucionando, como el caso del mass distribution malware, hacia un malware adaptado o dirigido a organizaciones individuales, y que finalmente se ha convertido en la tendencia habitual en nuestros días. Otros ataques como file-less malware, con una mayor inversión en técnicas de evasión en la detección en los últimos años usando técnicas que permiten cargar el código del atacante directamente en la memoria. O los ataques malware-less que es otra evolución del tradicional ataque malware, donde con

Figura 2. Mercado de ciberamenazas. Elaboración propia

frecuencia se dirigen a plataformas SaaS y usan métodos de ingeniería social (robo de credenciales y falsificación de correos electrónicos).

Pero sin duda la combinación de ataques a la cadena de suministro, más los denominados ataques modern cross domain junto con el ransomware son los que están haciendo más daño a las empresas en su conjunto y a las energéticas en particular.

El modelo actual

Desde la década de 1990, la Arquitectura de Referencia Empresarial de Purdue, también conocida como el Modelo Purdue, ha sido el modelo estándar para organizar –y segregar– las funciones de red de cualquier sistema de control empresarial e industrial (ICS). Purdue divide la empresa en varios «niveles», cada uno de los cuales representa un subconjunto de sistemas. Los controles de seguridad entre cada nivel están tipificados por una «zona desmilitarizada» (DMZ) y un firewall.

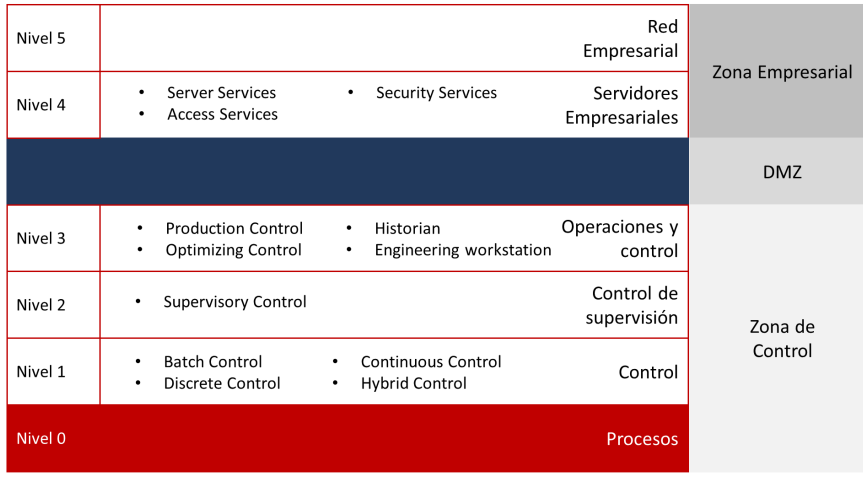


Figura 3. Modelo Purdue. Niveles. Elaboración propia

Los enfoques convencionales restringen el acceso en el nivel 3 desde los niveles 4, 5 (e Internet). Hacia arriba, solo los niveles 2 o 3 pueden comunicarse con los niveles 4 y 5, y los dos niveles más bajos (control y procesos) deben mantener sus datos y comunicaciones dentro del OT de la organización.

Pero en nuestra era industrial, los datos ya no fluyen de manera jerárquica como lo prescribe el Modelo Purdue. Con el auge de

la computación perimetral (Edge), los sensores y controladores inteligentes (niveles 0 y 1) evitan los firewalls y se comunican directamente con la nube, creando nuevos modelos y aumentando la exposición del sistema.

Modernizar este modelo con una aproximación basada en los riesgos planteados por la propia infraestructura puede ayudar a que los sistemas industriales y la TI tradicional de una empresa, y en concreto una del sector energético, cumpla plenamente con los requisitos para esta nueva era.

Una nueva estrategia

A tal efecto después de tantos años era necesario evolucionar la aproximación Purdue y apostar por nuevas metodologías. Desde el laboratorio nacional de Idaho se desarrolló la denominada Consequence-Driven Cyber-Informed Engineering[6] que aborda los riesgos planteados por los sistemas industriales. A diferencia de los enfoques tradicionales de la ciberseguridad, CCE ve la consecuencia como el primer aspecto de la gestión de riesgos y diseña proactivamente los posibles impactos. Según CCE, hay cuatro pasos que una organización, debe priorizar:

- Identificar los procesos más importantes: concentrándose en proteger las funciones críticas «que no deben fallar» y cuyo fallo podría causar daños a la seguridad, daños operativos o ambientales.
- Mapear la infraestructura digital: examinando todas las vías digitales que podrían ser explotadas por los ciberdelincuentes, identificando todos los activos conectados (TI, IIoT, sistemas de gestión de edificios, OT, dispositivos personales inteligentes, etc.) y detallando quién tiene acceso a qué, incluyendo proveedores, personal de mantenimiento y trabajadores remotos.
- Rutas de ataque potenciales: analizando las vulnerabilidades para determinar las potenciales rutas de ataque que conducen a los procesos más importantes, incluyendo los posibles esquemas de ingeniería social y el acceso físico a las instalaciones.
- Mitigar y proteger: priorizando las opciones que permitan «diseñar» los riesgos cibernéticos que presentan mayores

[6] https://inl.gov/cce/.

consecuencias. Implementar políticas de segmentación y una estrategia de confianza cero para separar dispositivos IIoT y OT de otras redes TI, reduciendo así el número de puntos de entrada accesibles a Internet y sobre todo parchear las vulnerabilidades en las posibles rutas de ataque.

Todo esto fundamenta lo que debe ser la nueva estrategia, pasando de un modelo basado en niveles a un modelo basado en riesgos y con la premisa de confianza cero en lo relacionado con la ciberseguridad. Sin embargo, tan importante como una buena estrategia es definir cómo vamos a medir el beneficio que esta proporciona.

Medir el beneficio de la estrategia

A menudo las empresas se plantean los retornos de inversión a partir de los ingresos que un nuevo software o sistema proporciona a la cuenta de resultados. Pero los rendimientos de una estrategia no se pueden ver solo a través de las cuentas anuales de una empresa, los beneficios hay que agruparlos en varios conceptos que proporcionan beneficios directos e indirectos. Esta agrupación debe tener en consideración estos cuatro pilares:

- Evitar los costes de seguridad o ambientales: los fallos de seguridad en instalaciones energéticas, químicas, mineras, petroleras, de transporte u otras instalaciones industriales pueden causar consecuencias más graves que una violación de la seguridad IIoT/OT o TI de una compañía. Se pueden perder vidas, se puede dejar a toda una ciudad sin energía durante días, los costes incurridos por impactos medioambientales o las responsabilidades legales de los daños producidos así como el propio daño reputacional de la marca, pueden llegar a costar cientos de millones de euros.
- Minimizar el tiempo de inactividad: como demostraron los ataques NotPetya y LockerGoga[7], el tiempo de inactividad incurre siempre en pérdidas financieras reales que afectan a todos, desde el personal de la planta hasta los accionistas. Además de las consecuencias graves en la sociedad al considerarse infraestructuras críticas que afectan al correcto funcionamiento de la economía de un país.

[7] https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms/.

- Detener el robo de propiedad intelectual: las empresas de la industria energética, la alta tecnología y empresas que se dedican a innovar en el ámbito de las energías renovables gastan millones de euros en investigación y desarrollo. Las pérdidas por el robo de su propiedad intelectual por parte de los Estados nación o competidores también se pueden medir en cientos de millones de euros. Su protección debe formar parte de las métricas de beneficio de una nueva estrategia.
- Evitar multas por incumplimiento regulatorio: sectores industriales como el energético que están mayormente enfocadas en combustibles fósiles como el petróleo y el gas, o empresas dedicadas a la distribución energética, están fuertemente reguladas. Por lo tanto, son vulnerables a sanciones si se produce una violación de seguridad en sus sistemas y esto les lleva a incumplir alguna de las regulaciones que se les aplica. Con todos estos elementos es necesario definir un plan de acción.

Plan de acción

Para el CISO de hoy, asegurar la infraestructura, significa ser responsable de toda la seguridad digital: TI, OT, IIoT, instalaciones, etc. Esto requiere un enfoque integrado, que abarque a las personas, los procesos y la tecnología. Este enfoque integrado debe incluir:

- Unos objetivos comunes para los equipos de IT y OT dirigidos a soportar la organización.
- Establecer mecanismos ágiles de comunicación entre todos los equipos responsables de los diferentes sistemas tanto industriales como de TI para que todos tengan una visión lo más completa posible de la organización.
- Proporcionar herramientas que permitan a los equipos dar visibilidad al equipo de ciberseguridad lo que redundará en un aumento de la eficiencia en la lucha contra las ciberamenazas.

Actualmente con los ciberdelincuentes trabajando tanto en entornos TI como OT las organizaciones deben centrar sus esfuerzos en protegerse con soluciones XDR (Extended Detection & Response) para entornos industriales y TI que además deben estar integradas en los sistemas SIEM/SOAR para facilitar el seguimiento de las amenazas de forma global. Estas herramientas deben:

- Facilitar el descubrimiento de activos TI e IIoT/OT.

- Gestionar las vulnerabilidades para identificar los riesgos de TI y de IIoT/OT, detectando cambios no autorizados y priorizando la mitigación.
- Realizar análisis de comportamiento para detectar amenazas avanzadas de forma rápida y precisa.
- Tener la capacidad de integrar terceras herramientas (ticketing, CMDB).

Estrategia de ciberseguridad para sector energético

Nuevos aspectos que considerar

Las empresas del sector energético han confiado su seguridad tradicionalmente en sistemas de protección basados en red y en otras herramientas con mecanismos de detección basados únicamente en firmas, que no son capaces de seguir el dinamismo de las amenazas, son ineficaces frente a distintas técnicas de ataque disponibles para los adversarios y que tienen tasas de fallo elevadas.

Como indicábamos anteriormente, a la hora de rediseñar el marco de seguridad, se debe considerar el sistema energético en su conjunto, protegiendo las infraestructuras críticas de los ataques con un enfoque basado en tres puntos: los dispositivos, las comunicaciones y las aplicaciones.

Lo más importante es construir una base de principios generales que permitan una defensa en profundidad, como se indica en el siguiente diagrama:

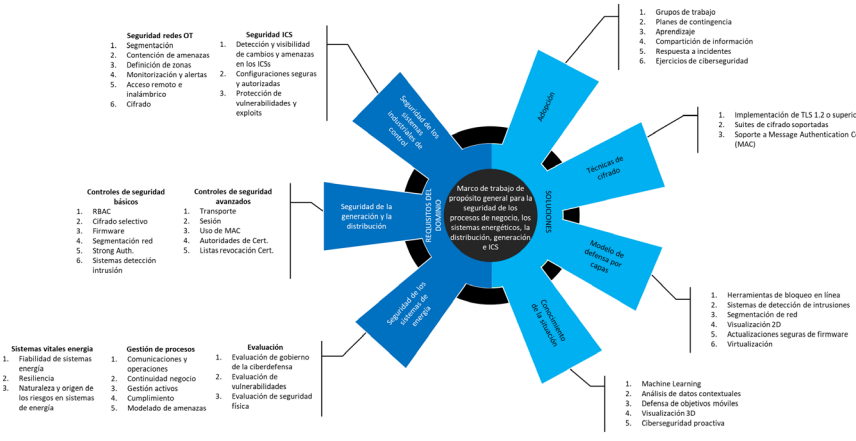


Figura 4. Principios generales que permiten una defensa en profundidad. Elaboración propia

Los cambios en el entorno de las compañías energéticas, tanto internos como externos, obligan a desarrollar el plan sobre esos principios, para que sirvan de base para mejorar y construir una sólida estrategia de ciberseguridad y cumplimiento considerando también:

- Proteger los flujos de trabajo remotos: las empresas energéticas están realizando cambios fundamentales en sus flujos de trabajo de producción de energía, y los métodos y arquitecturas de ciberseguridad también deberán renovarse de forma acorde. Se debe analizar y adaptar el enfoque de los sistemas que asumen que los trabajadores están físicamente presentes en las plantas o desplazados. Por ejemplo, las plantas generalmente prohíben los dispositivos portátiles, pero la mayoría de los trabajadores ahora están fuera de la planta, con acceso a esos dispositivos «prohibidos» o con acceso a plataformas de redes sociales. Cualquier plan diseñado para esta nueva realidad necesita proteger y monitorizar los nuevos flujos de trabajo remotos en este nuevo contexto.
- Conexiones seguras: los empleados sin acceso seguro no pueden trabajar de manera efectiva, lo que hace que dicho acceso sea necesario, pero no suficiente para ese plan de ciberseguridad. Los operadores de planta deben definir proactivamente quién debe acceder a qué activos e instituir los controles pertinentes antes de aprobar el acceso remoto a los activos.
- Monitorización de anomalías: trabajar desde casa hace que algunas prácticas de seguridad sean más difíciles. Por ejemplo, tanto las acciones válidas como las maliciosas ahora podrían provenir desde fuera de la planta, lo que hace más complejo discernir qué representa un comportamiento normal y legítimo frente a uno malicioso. Esta consideración aumenta la importancia de la monitorización como una herramienta para hacer la distinción entre empleados, terceros usuarios autorizados y atacantes, estableciendo líneas base dinámicas que permitan detectar rápidamente desviaciones o anomalías que puedan servir para identificar un potencial ataque. Estos procesos de monitorización deben diseñarse con el objetivo de poder ser automatizados gradualmente, a medida que se va ganando confianza en la precisión de dichas detecciones y en las acciones de respuesta y remediación, liberando tiempo para que los analistas puedan realizar tareas de mayor valor añadido. En definitiva, aprovechar las capacidades tecnológicas para la recopilación de grandes volúmenes de datos para

su tratamiento ágil utilizando procesos analíticos basados en Inteligencia Artificial/Machine Learning, de forma que los equipos se liberen de las tareas más repetitivas y que puedan ser automatizadas, para pasar a centrar sus esfuerzos en la identificación de nuevos casos alineados con las necesidades del negocio, la búsqueda activa de nuevas vulnerabilidades o amenazas presentes en la infraestructura, y el análisis de la inteligencia de amenazas para poder anticiparse a los movimientos de los adversarios. Esto proporcionará una mejor postura de seguridad lo que a su vez tendrá un impacto elevado en la retención del talento, tan escaso en el mercado de la ciberseguridad.

- Asumir la brecha y estar preparado para responder ante un posible incidente: las plantas necesitan un plan de respuesta a incidentes que funcione cuando la mayoría de los empleados no están en su puesto de trabajo. Este plan debe ponerse a prueba mediante simulacros para identificar deficiencias y adaptaciones que puedan ser necesarias en función de la evolución del entorno. Se debe estar preparado para poder activar la respuesta a incidentes en el menor tiempo posible, con soporte limitado y con un soporte experto remoto distribuido. Considerando que uno de los objetivos más frecuentes de los atacantes puede consistir en tener una presencia persistente en el entorno para poder planificar de forma más efectiva los siguientes pasos, la eliminación o el reinicio de los sistemas pueden no ser una opción útil.

En definitiva, se debe abordar una estrategia basada en el principio de confianza cero que detallaremos a continuación.

Estrategia confianza cero

El modelo de seguridad basado en confianza cero, más conocido en su terminología inglesa como Zero Trust, supone un cambio de paradigma respecto a los modelos de ciberseguridad tradicionales. En lugar de establecer un perímetro muy robusto que separe un entorno interno de confianza y la zona exterior donde se supone que están los mayores riesgos, considera un nuevo paradigma en el cual se debe asumir la posibilidad de sufrir una brecha de seguridad en cualquier momento, que toda la actividad de los usuarios sobre los recursos internos debe verificarse explícitamente y que se debe proporcionar un acceso limitado a los usuarios, reduciendo al mínimo el número de usuarios privi-

legiados y sus permisos de acceso, mediante un proceso ágil de autorizaciones temporales. En el caso de entornos industriales y particularmente en empresas energéticas, se establece un límite estricto en torno a los datos corporativos y de los clientes, pero también de los sistemas industriales.

Basado en el principio de «nunca confiar, siempre verificar», Zero Trust ayuda a asegurar los recursos corporativos al eliminar dispositivos desconocidos y no administrados y limitar el movimiento lateral. La implementación de un verdadero modelo de confianza cero, requiere que todos los componentes estén validados y demuestren ser confiables.

En un entorno de confianza cero, es necesario cubrir los siguientes seis riesgos clave:

1. Identidad: automatizando la detección de riesgos y proporcionando acceso seguro a los recursos con una autenticación sólida en toda la infraestructura digital.
2. Punto de conexión: defendiendo toda la superficie de ataque creada por el creciente y diverso número de puntos de conexiones, utilizando un enfoque flexible e integrado de la gestión.
3. Datos: clasificando, etiquetando y protegiendo los datos en entornos on-premise y nube para ayudar a evitar que se compartan de forma inapropiada y reducir así los riesgos internos.
4. Aplicaciones: manteniendo un acceso seguro de los empleados a los diferentes entornos donde se ubican las aplicaciones, incluyendo el acceso remoto a las mismas.
5. Red: reduciendo las vulnerabilidades de seguridad de las soluciones basadas en el perímetro, incluyendo la necesidad de VPNs, y mejorando la escalabilidad de las soluciones para todos los entornos, on-premise/nube.
6. Infraestructura: protegiendo la infraestructura, incluyendo entornos de TI, IIoT/OT tanto on-premise como en la nube con una gestión más eficiente y automatizada.

Mediante una estrategia confianza cero lo que se crea es una plataforma de acceso unificada que se puede utilizar para mejorar la seguridad general de todo un ecosistema. Para su correcta ejecución hay cuatro fases clave, que en términos generales, se describen a continuación:

- Fase de verificación de la identidad: en primer lugar debemos implementar una autenticación de múltiples factores (MFA) a través de sistemas biométricos o cualquier otro sistema que al menos incluya algo que se tiene o algo que se es. La rápida adopción de dispositivos móviles para el trabajo –que requieren conexión a los recursos corporativos– impulsó la evolución de la experiencia MFA incorporando soluciones más modernas como servicios de autenticación con soporte para biometría. Y a medida que avanzamos desde el punto de vista tecnológico se acentúa más el desarrollo de soluciones basadas en la eliminación de las contraseñas.
- Fase de verificación del dispositivo: garantizar el correcto funcionamiento del dispositivo mediante el despliegue de soluciones que permitan inscribir dichos dispositivos de usuarios en soluciones de gestión de activos. Soluciones, que permiten la verificación de todos los requisitos de conexión del dispositivo (parches, políticas de seguridad, etc.). Esta capacidad es esencial para establecer la política de salud del dispositivo de cara a acceder a los recursos corporativos. Se debe comenzar exigiendo que los dispositivos estén gestionados y a continuación, exigir que los dispositivos estén «sanos» para acceder a las principales aplicaciones de productividad.
- Fase de verificación del acceso: en esta tercera fase, se debe definir un plan para minimizar los permisos de acceso a los recursos corporativos y exigir la verificación de la identidad y el estado de los dispositivos para todos los métodos de acceso. A medida que se trabaja para que los principales servicios y aplicaciones sean accesibles a través de Internet, los métodos de acceso pasarán de ser heredados (red corporativa), a Internet primero (Internet más VPN cuando sea necesario), y luego a solo Internet (Internet sin VPN). Esto reducirá el acceso de los usuarios a la red corporativa en la mayoría de los casos. A pesar del fuerte enfoque en los dispositivos, algunos escenarios requieren que los usuarios trabajen desde dispositivos no gestionados, por ejemplo, en los casos de personal de proveedores, o escenarios relacionados con la ejecución de proyectos, estos últimos también hay que considerarlos.
- Fase de verificación de servicios: en esta fase se debe ampliar la verificación desde la identidad y el dispositivo hasta el propio servicio, lo que permitirá garantizar su disponibilidad al inicio de cada interacción.

El siguiente diagrama proporciona una arquitectura de referencia simplificada de lo que sería un enfoque de implementación de confianza cero. Un enfoque global como este debe extenderse a toda la infraestructura digital, incluyendo identidades, puntos de conexión, red, datos, aplicaciones y la propia infraestructura. Una arquitectura de confianza cero requiere la integración de todos los elementos.

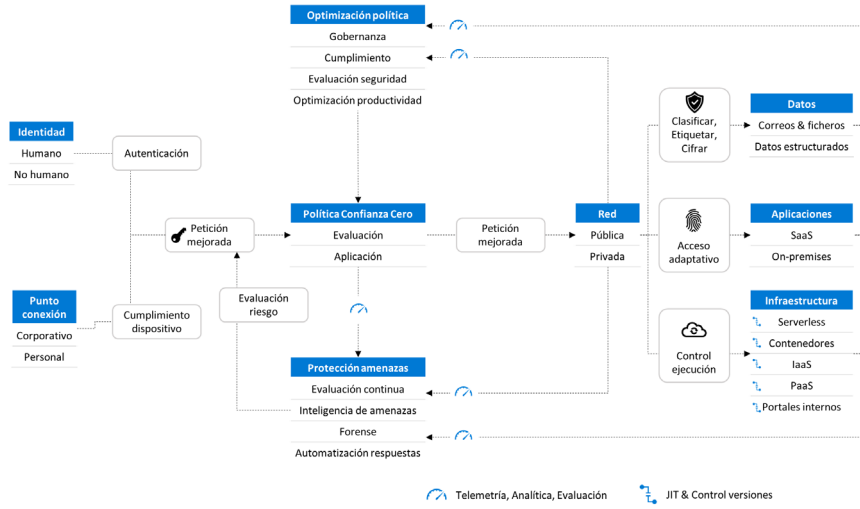


Figura 5. Arquitectura de referencia. Elaboración propia

La base de la seguridad son las identidades. Tanto las identidades de las personas como las de los dispositivos (industriales o no) necesitan una autenticación sólida, conectándose desde puntos de conexión que pueden ser personales o corporativos y siempre con un dispositivo que cumpla con las políticas, solicitando el acceso que debe estar siempre fundamentado en los principios de confianza cero de verificación explícita, acceso con los mínimos privilegios y siempre asumiendo la brecha.

Las políticas de confianza cero interceptan la solicitud y verifican explícitamente las señales de los seis elementos de riesgo antes comentados basándose siempre en la configuración definida y aplicando el acceso con el menor número de privilegios. Dichas señales incluyen al usuario, la ubicación, el grado de cumplimiento del dispositivo, la sensibilidad de los datos, la sensibilidad de la aplicación y muchos más parámetros que podremos definir en dicha política. Además, la telemetría, la información de estado y la evaluación de riesgos contra amenazas, alimenta el motor de dichas políticas para responder automáticamente a las

mismas en tiempo real. La política de confianza cero se aplica en el momento del acceso y se evalúa continuamente a lo largo de la sesión.

Otros elementos para tener en consideración son la gobernanza y el cumplimiento, que son fundamentales para una buena implementación de la seguridad basada en confianza cero. La evaluación de seguridad y la optimización se realizan a través de la telemetría lo que nos permite vigilar el comportamiento de todos los servicios y sistemas. Además, la telemetría y la analítica se enriquecen con inteligencia de amenazas que generan evaluaciones de riesgo de muy alta calidad y que pueden ser investigadas manualmente o automatizadas. Los ataques se producen a gran velocidad, y los sistemas de defensa deben actuar de igual manera, lo que hace que los humanos no puedan reaccionar con la suficiente rapidez ni cribar todos los riesgos, por eso se hacen indispensables herramientas de automatización para la respuesta a incidentes.

El filtrado y la segmentación del tráfico también se aplican a la evaluación y el cumplimiento de la política de confianza cero antes de conceder el acceso a cualquier red pública o privada. La clasificación, el etiquetado y el cifrado de datos deben aplicarse a los correos electrónicos, los documentos y los datos estructurados. Y el acceso a las aplicaciones debe ser adaptable, ya sea en modalidad nube o en infraestructura on-premise. El control debe aplicar a toda la infraestructura, tanto en servicios serverless, contenedores, IaaS, PaaS así como portales internos, con controles just in time (JIT) y de versiones. Y, por último, la información de la telemetría, el análisis y la evaluación de la red, los datos, las aplicaciones así como la infraestructura, se devuelven a los sistemas de optimización de políticas y protección contra amenazas para seguir mejorando el proceso.

Proteger las identidades

Se ha demostrado que las credenciales tienen un 99,9% menos de probabilidades de ser comprometidas cuando se utilizan mecanismos de autenticación multifactor (MFA). No en vano, las pérdidas de datos suelen empezar con una sola cuenta comprometida. En 2020, tras una investigación realizada por Microsoft se publicaron unas conclusiones en las que destacaba entre ellas un aumento del 230% en ataques de password spray.

Y es que, con el aumento masivo de los ataques relacionados con la identidad, detectar y responder rápidamente cuando se ven

cuentas comprometidas es fundamental para limitar el impacto de una brecha de seguridad. Utilizar técnicas de Machine Learning avanzado para ofrecer una detección continua en tiempo real es crucial. Aprovechar dichas tecnologías para incorporar la remediación automatizada y la inteligencia conectada para investigar los inicios de sesión sospechosos para posteriormente abordar las posibles vulnerabilidades lo es aún más.

Esta aproximación debe basarse en:

- Implementar soluciones de autenticación multifactor. Una buena base son las medidas de seguridad aportadas por el Esquema Nacional de Seguridad dentro del marco operacional en lo relacionado con los controles de acceso «4.2.5 Mecanismo de autentificación» [op.acc.5].
- En línea con dichas soluciones de autentificación, habilitar los mecanismos de autentificación sin contraseña.
- Bloquear sistemas de autentificación anticuados.
- Incluir herramientas para detectar el compromiso ante la suplantación de identidades, mientras al mismo tiempo se simplifica la experiencia del usuario.
- Reforzar las políticas de acceso condicional incorporando herramientas que permitan evaluar en tiempo real los riesgos ante inicios de sesión.
- Incorporar herramientas para investigar y corregir dichos riesgos (inicios de sesión).

Proteger el punto de conexión

También es esencial evaluar la seguridad de los sistemas IIoT/OT con el mismo rigor y enfoque completo que los sistemas TI. Como hemos observado, los atacantes tienden a elegir los «objetivos más fáciles» como punto de entrada, y los puntos de conexión a los sistemas es uno de los eslabones más débiles. El phishing dirigido o ataques similares permiten el acceso a sistemas TI que luego pueden proporcionar una vía para que los atacantes lleguen a los sistemas OT, y también es posible lo contrario. Cualquier dispositivo con conectividad puede presentar una puerta de entrada para un atacante determinado y con suficientes conocimientos técnicos puede hacerse con el control de una infraestructura.

A modo de ejemplo, en el caso del incidente de ciberseguridad Triton que comentábamos al principio, este dirigió su ataque

contra los controladores de seguridad en una instalación petroquímica de Oriente Medio, tenía la intención de causar daños estructurales importantes a la instalación que podrían haber tenido como consecuencia posible, la pérdida de vidas humanas. Los atacantes obtuvieron su punto de acceso inicial en la red TI y posteriormente utilizaron tácticas conocidas como living off the land[8] para obtener acceso remoto a la red OT, donde implementaron un malware especialmente diseñado para dicho entorno.

Como hemos comentado anteriormente, si bien muchas organizaciones están evolucionando su enfoque de seguridad de TI, alejándose de un modelo de seguridad basado en el perímetro a un modelo de confianza cero, los dispositivos IIoT/OT a menudo se pasan por alto o se retrasa su inclusión. Como ejemplo, es común el cifrado de datos confidenciales de las aplicaciones, pero muchas organizaciones no han considerado que sus sistemas de control se basan en el protocolo Modbus, que por diseño carece de cualquier tipo de autenticación y envía datos sin cifrar. Otro ejemplo comparativo, es una práctica muy habitual que los PC tengan certificados actualizados, pero los dispositivos IIoT a menudo se despliegan con contraseñas predeterminadas de fábrica. Los compromisos en estos sistemas IIoT/OT pueden interrumpir las operaciones. Los atacantes también se están centrando en cómo interactúan los dispositivos IIoT y OT, dichos sistemas de control industrial a menudo se actualizan o modernizan con capacidades remotas, introduciendo nuevos vectores de ataque que permiten que los ataques virtuales causen daño en escenarios físicos. A principios de 2021, una planta de tratamiento de agua en Florida[9] fue víctima de un atacante que accedió de forma remota a sistemas críticos e intentó alterar la cantidad de productos químicos en el suministro de agua.

Es fundamental comprender la seguridad de los sistemas que no están en la red de TI/OT de la organización, pero que, sin embargo, podrían tener impacto en las operaciones. Así como una organización siempre busca mejorar la eficiencia y la sostenibilidad, sus proveedores también lo hacen. Estos sistemas integrados en la cadena de suministro pueden conectarse fuera de la red de una empresa para medir y monitorizar el funcionamiento de los dispositivos, optimizar los ahorros de energía y

[8] https://www.mandiant.com/resources/attackers-deploy-new-ics-attack-framework-triton.

[9] https://www.techrepublic.com/article/fbi-secret-service-investigating-cyberattack-on-florida-water-treatment-plant/.

ofrecer más tiempo de actividad. Los compromisos en los componentes de la infraestructura que son administrados externamente pueden afectar directamente al negocio. Por ejemplo, se podría apagar la climatización de un edificio lo que podría detener las operaciones y estropear el inventario, los sensores de calidad del aire podrían no alertar a los trabajadores sobre condiciones ambientales inseguras, etc. Si bien el uso de los dispositivos IIoT puede contribuir a implantar mejores prácticas ambientales, es esencial que todos los sistemas conectados, que pueden estar en funcionamiento durante periodos muy prolongados de tiempo, se diseñen, evalúen y operen de forma segura.

La protección de los dispositivos IIoT y OT frente a los riesgos provenientes del entorno TI se vuelve más relevante a medida que estos entornos convergen. Es habitual que el análisis de riesgos se aborde de forma aislada para cada uno de los entornos. Para tener el éxito en la lucha contra los ataques, los riesgos deben abordarse de manera integral y, al mismo tiempo, dar cabida a la experiencia en el dominio en cada área. También es fundamental garantizar que los entornos digitales modernos no se vean frenados por las amenazas de la tecnología heredada y conectada a los sistemas OT. La mitigación requiere un enfoque integrado que abarque toda la empresa y sus proveedores. Las organizaciones deben buscar oportunidades para endurecer, parchear o segmentar los sistemas para reducir la superficie de ataque.

Proteger los datos

Los recientes avances en la gestión y el despliegue de la energía, como las redes inteligentes, solo han complicado la situación para las empresas energéticas. Esto no ha pasado desapercibido para los Gobiernos nacionales y regionales. La Comisión Europea, por ejemplo, creó el Smart Grid Task Force en 2009 para asesorar sobre cuestiones relacionadas con el despliegue y desarrollo de redes inteligentes.

Las redes inteligentes se consideran una forma esencial de gestionar el suministro de energía en el futuro, lo que permite a las empresas responder a los cambios locales en el uso. Pero como reconoció dicho grupo de trabajo, los clientes deben aceptar el uso de redes inteligentes lo que, a su vez, requiere que se les dé control sobre sus datos de consumo de energía. También es esencial que la nueva tecnología no ponga en peligro la privacidad de los datos personales y que los consumidores se sientan

seguros de que sus datos se mantendrán protegidos y se respetará su privacidad.

El grupo examinó los posibles riesgos en el tratamiento de los datos, la seguridad y la protección (incluidas las cuestiones de intercambio de datos), la identificación de la propiedad de los datos y los derechos de acceso así como las partes responsables de dicha protección. Y examinó la legislación europea sobre protección de datos y si debían establecerse nuevas medidas adicionales. Uno de los elementos clave en la estrategia de confianza cero que antes comentábamos, debe tener en cuenta estas recomendaciones y por tanto incluir mecanismos para la protección de los datos. Entre las acciones que se deben acometer se consideran imprescindibles las siguientes:

- Aplicar políticas de protección para proteger los datos con o sin la inscripción del dispositivo. Esto permite proteger la información de la empresa incluso en dispositivos no gestionados.
- Aplicar las directivas de gestión de aplicaciones móviles a sus aplicaciones de negocio existentes y de forma que no sea necesario realizar cambios en dichas aplicaciones.
- Permitir a los usuarios ver de forma segura el contenido de los dispositivos dentro de su ecosistema de aplicaciones mediante el uso de navegadores gestionados o versiones específicas de catálogo de aplicaciones empresariales.
- Cifrar los datos de la empresa dentro de las aplicaciones utilizando el nivel más alto posible y soportado por los dispositivos.
- Proteger los datos de la empresa aplicando políticas credenciales y doble factor de autenticación.
- Estableciendo sistemas de protección de la información y DLP a nivel documental para evitar que las potenciales perdidas accidentales de información comprometan a la empresa y sus clientes.
- Definir una clasificación de la información para toda la compañía, teniendo en cuenta tanto a usuarios internos como clientes y proveedores.

Además los retos asociados a las normativas de privacidad se dividen normalmente en tres ámbitos: legal y de cumplimiento, tecnológicos y de datos. Hay que poner énfasis en la responsabilidad de la empresa que requiere a su vez un sólido modelo de gobernanza de la privacidad, lo que lleva a las empresas a

revisar la forma en que redactan las políticas de privacidad, para que sean más fáciles de entender y cuenten con las protecciones adecuadas en todo el ciclo de vida de la gestión de la información personal. Los requisitos de privacidad afectan a la forma de diseñar y gestionar las tecnologías. El concepto de «privacidad desde el diseño» se ha consagrado en la legislación a través de mecanismos como la Data Protection Impact Assessment (DPIA). Las personas y los equipos responsables de la gestión de la información se enfrentan al reto de proporcionar una supervisión transparente del almacenamiento y el linaje de los datos. Y es necesario mejorar la comprensión de los mecanismos de recopilación de dichos datos –así como los protocolos de almacenamiento– lo que a la larga facilitará el cumplimiento de los derechos de los clientes.

En última instancia, la privacidad de los datos no debe considerarse un mero ejercicio de cumplimiento normativo. Por el contrario, es una oportunidad importante para que las empresas energéticas impulsen el rendimiento y el crecimiento del negocio a través de la mejora de la eficiencia, la gestión de riesgos y la innovación relacionada con los riesgos asociados a la gestión de los datos y las prácticas empresariales.

Proteger las aplicaciones

En el sector energético a menudo conviven soluciones basadas en DCS, SCADA, RTU, con soluciones TI, e incluso con soluciones Legacy. Es muy importante de cara a proteger todas las aplicaciones aplicar controles y soluciones para descubrir todo el shadow IT existente para tenerlo inventariado y poder determinar qué medidas de protección se establecen. Aproximadamente el 15% de las aplicaciones que se despliegan en una empresa de tamaño medio no están gestionadas o simplemente no existen a los ojos de los administradores, lo que hace de esta gestión algo muy importante.

Además, se deben garantizar los permisos adecuados a cada una de las aplicaciones del catálogo empresarial, limitar el acceso basándose en el análisis en tiempo real y dotarse de herramientas de supervisión para identificar comportamientos anómalos.

Todas las acciones de los usuarios que puedan comportar riesgos de seguridad se deben controlar, así como validar las diferentes opciones de configuración segura de las aplicaciones que manejen información sensible dentro de una organización.

Conectando las aplicaciones a soluciones Cloud Application Security Broker (CASB) podemos conseguir su protección y analizar el comportamiento de los usuarios utilizando técnicas de Machine Learning para identificar amenazas.

Proteger la red

Ya no estamos en la era de las redes claramente definidas y específicas para una determinada ubicación. En lugar de una red contenida y definida que hay que asegurar, hemos pasado a un conjunto muy elevado de dispositivos y redes. Esto es un reto para muchas empresas que a menudo tienen pocos recursos y una arquitectura de red plana y abierta unido a una mínima protección contra amenazas y un tráfico interno no cifrado. Esta situación se puede agravar si la tendencia hacia infraestructuras energéticas a pequeña escala como cooperativas energéticas o redes comunitarias energéticas crece y no se tienen en cuenta estos riesgos.

La ciberseguridad será aún más importante en estos entornos, y las empresas que se dedican a dotar de soluciones de ciberseguridad deberán apostar por desarrollar soluciones específicas para este tipo de redes en entornos de cooperativas o comunidades energéticas.

Adoptar un marco de seguridad de confianza cero es la clave para superar estas limitaciones. En lugar de creer que todo lo que hay detrás del cortafuegos de la empresa es seguro, debemos asumir que las brechas serán inevitables. Esto significa que se debe verificar cada solicitud como si se originara en una red no controlada. En dicho marco de la confianza cero, hay tres objetivos clave cuando se trata de asegurar una red:

- Estar preparado para manejar los ataques antes de que se produzcan.
- Minimizar el alcance de los daños y la rapidez con la que se propaga.
- Aumentar la dificultad de compromiso de los sistemas, estén en infraestructuras on-premise o en la nube

Proteger la infraestructura

Las infraestructuras de IIoT/OT y TI incluyen una amplia gama de tecnologías, como hardware, dispositivos, sistemas industriales de control, máquinas virtuales, software, microservicios, redes y etc.

Muchas organizaciones tienen dificultades para proteger este entorno porque la gestión de los permisos suele ser una gestión semimanual y suele carecer de una gestión eficaz de la configuración de todos los activos. La implementación de un marco de confianza cero de extremo a extremo facilita:

- Asegurar que el software y los servicios están actualizados.
- Gestionar todas las configuraciones de forma centralizada con un enfoque multiinfraestructura.
- Prevenir, detectar y mitigar los ataques.
- Identificar y bloquear comportamientos de riesgo.

Dado que las redes están sujetas a ataques continuos y cada vez más sofisticados, es especialmente importante proteger su infraestructura de red con soluciones de seguridad que reconozcan de forma inteligente las amenazas desconocidas y se adapten para prevenirlas en tiempo real.

Se debe establecer una línea base prioritaria para la forma en que se administra una infraestructura. Se pueden aprovechar las instrucciones NIST 800-53, que definen un conjunto de requisitos. Esta base mínima debe tener en cuenta al menos estos elementos:

- El acceso a datos, redes, servicios, dispositivos, utilidades, herramientas y aplicaciones debe controlarse mediante mecanismos de autenticación y autorización.
- Los datos deben cifrarse en tránsito, en reposo y en uso con tecnologías como Confidential Computing[10].
- Restringir los flujos de tráfico de red.
- Visibilidad del equipo de seguridad para todos los activos.
- La supervisión y la auditoría deben estar habilitadas y configuradas correctamente de acuerdo con las directrices organizativas.
- El antimalware debe estar actualizado y en ejecución.
- Es necesario realizar análisis de vulnerabilidades y corregirlas, según las directrices organizativas.

Para medir e impulsar el cumplimiento de esta línea base mínima, se deben contemplar todas las infraestructuras, tanto on-premise

[10] https://confidentialcomputing.io/.

como nube. La red igual que la identidad es el nexo de unión de todos los activos y disponer de una herramienta de vigilancia es indispensable.

Conclusión

Nos gustaría concluir con tres mensajes claros al respecto de los puntos tratados en este capítulo en el que hemos hablado del contexto energético actual, los riesgos de ciberseguridad en el entorno energético y como abordar una estrategia de ciberseguridad. Hemos de ser conscientes que las empresas de sector energético deben tener la ciberseguridad como una de las principales prioridades y comprometerse a trabajar con el resto de los actores de la industria para proteger a sus clientes y las infraestructuras.

Por eso pensamos que la mejor respuesta que puede dar el sector energético debe tener una visión ambiciosa y basada en las tres «D». Diplomacia, Disrupción y Defensa.

Diplomacia

Hemos tratado durante la explicación del contexto actual diferentes temas relacionados con la situación geopolítica. Los Gobiernos continúan invirtiendo en capacidades ofensivas en el ciberespacio, y los ataques Estado-nación sobre población civil van en aumento. Los ciberataques han pasado a formar parte de lo que se ha venido a llamar guerra híbrida. El mundo necesita nuevas reglas internacionales para proteger «lo público» de dichas amenazas y del cibercrimen. Deberíamos trabajar en fomentar una diplomacia digital fomentando el encuentro entre todos los Estados en iniciativas como la Paris Call[11] o la Convención de Génova que nos permitan establecer nuevos tratados y protocolos para esta nueva realidad.

Disrupción

También hemos hablado de los riesgos en el entorno energético. No hay una sola empresa hoy en día que pueda por si sola luchar contra el cibercrimen de forma efectiva. Es necesario que el sector público y el sector privado colaboren a través de pro-

[11] https://pariscall.international/en/.

gramas de protección conjunta, compartan inteligencia de seguridad, y ahonden en los protocolos de actuación y respuesta a incidentes. Desde España la labor que desempeña en esta línea el CCN-CERT[12], INCIBE[13] y el DSN[14] en el ámbito de sus respectivas competencias es esencial para continuar la línea marcada en las diferentes estrategias de seguridad nacional, pero además es importante colaborar con el resto del sector privado especializado en el ámbito de la ciberseguridad sobre todo con aquellos cuya inteligencia de seguridad sea global y aporte una visión integrada a nivel mundial.

Defensa

En cuanto a la estrategia, es necesario potenciar estrategias como confianza cero (Zero Trust) en todos los ámbitos, pero sobre todo en el de las infraestructuras críticas. Abrazar esta aproximación para abordar la seguridad en un mundo cada vez más global, híbrido y remoto utilizando una aproximación basada en nunca confiar, siempre verificar en todos los ámbitos tecnológicos para reducir el avance de los ciberataques.

12 https://www.ccn-cert.cni.es/.
13 https://www.incibe.es/.
14 https://www.dsn.gob.es/es/.