CÓMO GARANTIZAR LA CIBERSEGURIDAD EN EL SECTOR NUCLEAR. ESTRATEGIAS PARA MANTENER UN ENTORNO SEGURO

ANTONIO FÉLIX SÁNCHEZ-ORO PORTILLO
Técnico en Seguridad de la Información
ENUSA, INDUSTRIAS AVANZADAS, S.A, S.M.E

INTRODUCCIÓN

"El único sistema verdaderamente seguro es aquel que está apagado, encerrado en un bloque de cemento, sellado en una habitación revestida de plomo y custodiado por guardias armados —y aún así tengo mis dudas".

Con esta frase Gene Spafford, conocido por ser un prestigioso experto en ciberseguridad y computación forense, quiso resaltar, con un cierto toque de ironía, una verdad muy poderosa en el ámbito de la ciberseguridad: no existe la seguridad absoluta. Solo niveles de riesgo aceptable. Ya que, incluso un sistema que aparentemente está aislado puede ser vulnerado, bien por un fallo humano, una amenaza interna o una vulnerabilidad desconocida.

Esta verdad incómoda preocupa, sobre todo, cuando hablamos de sistemas críticos de los cuales nuestra sociedad depende para funcionar.

TRANSFORMACIÓN DIGITAL Y SUS RIESGOS INHERENTES

Vivimos una era en la que la transformación digital ya no es una opción, sino una realidad irreversible. Tradicionalmente, el sector nuclear ha sido conservador por naturaleza y a la vez por necesidad, pero no ha podido evitar sumarse también a esta corriente global. Automatización, monitorización remota o sistemas inteligentes son solo algunos ejemplos de cómo la tecnología ha mejorado nuestra eficiencia operativa, nuestra precisión y, en muchos casos, nuestra seguridad.

Pero, sin embargo, toda moneda tiene dos caras. Esta digitalización ha traído consigo la ampliación de la superficie de exposición a ciberamenazas. Y es aquí donde aparece el verdadero reto: la ciberseguridad ha dejado de ser un complemento o un "lujo técnico" para convertirse en un eje esencial de la seguridad nuclear, formando un pilar silencioso y vital, que consigue que las instalaciones sigan operando con seguridad y eficacia.

El sector nuclear es testigo y a la vez protagonista de esta transformación digital en la que nos vemos inmersos. Y aunque ello ha traído grandes beneficios, también nos ha obligado a adoptar una nueva mentalidad: pensar como un atacante.

Cada nuevo dispositivo, flujo de trabajo o cada mejora tecnológica representa también un potencial vector de ataque para quienes buscan vulnerar sistemas. Por eso, el equilibrio entre innovación y seguridad debe ser cuidadosamente gestionado.

En ciberseguridad, un descuido puede comprometer toda la infraestructura informática. Porque, en esta realidad actual, no se trata de si seremos atacados o no. Sino de cuándo, cómo y con qué nivel de preparación responderemos.

VECTORES DE ATAQUE MÁS COMUNES

Los sistemas informáticos han experimentado, de forma general, un aumento en las prestaciones en cuanto a ciberseguridad se refiere. Actualmente la ciberseguridad se tiene en cuenta en todas las fases de creación de un producto software o hardware, dando como resultado sistemas y dispositivos ciberseguros frente a ataques. Debido a ello, los ciberdelincuentes han aumentado su presión sobre el nuevo eslabón más débil de la cadena: las personas. Son el objetivo principal de un atacante. Hay mayor probabilidad de éxito al realizar un ciberataque si es contra un grupo de usuarios que contra una infraestructura informática.

Las técnicas empleadas para llevar a cabo estos ataques se denominan Ingeniería Social, cuyo principal objetivo es robar

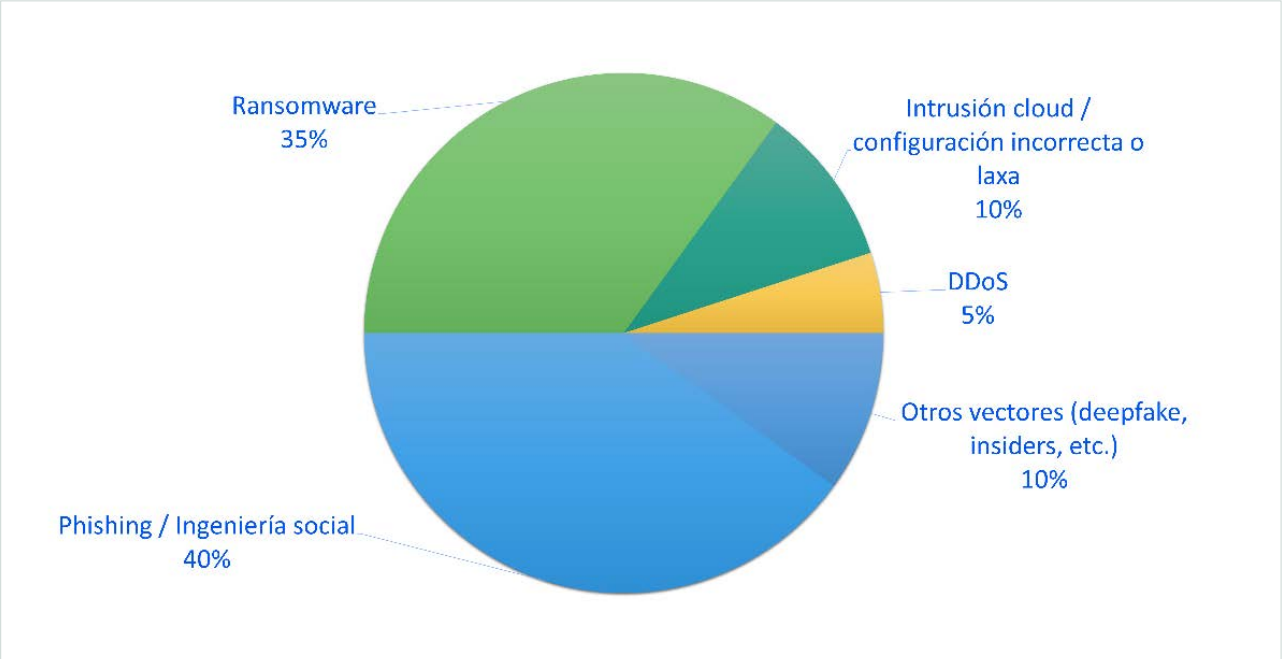

Figura 1. Principales vectores de ataque.

credenciales o infectar con un software malicioso un equipo de la organización.

En una primera fase se engaña al usuario mediante un correo electrónico, un WhatsApp o una llamada telefónica. El objetivo es obtener datos o comprometer su equipo. Y una vez dentro de la red empresarial, el atacante pasa a una segunda fase en la que realiza los llamados movimientos laterales consiguiendo ampliar sus vectores de ataque y seguir penetrando en la red de la empresa.

Cuando el atacante tiene suficiente información sobre la empresa, puede pasar a realizar acciones ofensivas como, por ejemplo, infectar la red con *ramsomware*. Se trata de un software malicioso que, al infectar un equipo informático, encripta la información y, generalmente, los atacantes piden una cuantía económica por su rescate. Este tipo de ataques llevan siendo muy populares en la última década, debido a su alta efectividad y su gran capacidad lucrativa, donde la principal fuente de entrada sigue siendo por *phishing*.

Al margen de la ingeniería social, o el *ramsomware*, hay otros vectores de ataques típicos como por ejemplo el uso de configuraciones laxas. Un ejemplo común es no obligar a los usuarios a usar un doble factor a la hora de entrar por VPN a la red interna de sus organizaciones. En este caso un ciberatacante, con solo un nombre de usuario y su contraseña comprometidos, bastaría para que pudiera penetrar de la red de una organización.

Otra amenaza que además tiene una tendencia alcista en los últimos años, son los ataques provenientes de los *"Insiders"*. Este término anglosajón se refiere a las personas que están dentro de la organización y de forma deliberada realizan acciones malintencionadas o negligentes. Suele ser incómodo hablar de cómo tu propio personal podría causar un daño en la organización, pero existe una tendencia creciente que indica que debemos aumentar los planes de respuestas ante esta amenaza.

Y en último lugar, mencionar también los ataques de denegación de servicio (DDoS), que consisten en colapsar un servicio informático enviando peticiones masivas. Este tipo de ataques es popular debido a su bajo coste, y su alto impacto en las organizaciones, siendo capaces de dejar sin disponibilidad servicios esenciales.

EL DESAFÍO DE LOS SISTEMAS LEGACY

He mencionado cuáles son los principales ataques informáticos en las empresas, pero los sectores industriales, y por ende las infraestructuras críticas, tienen una particularidad en común si hablamos de amenazas. Se trata de un reto interno especialmente complicado de proteger: los sistemas *legacy* (heredados). Dicho de otra manera, sistemas longevos que se encuentran en estaciones críticas de trabajo cuya sustitución o actualización no es posible.

Muchos de estos equipos fueron diseñados en épocas donde la conectividad era mínima y la ciberseguridad, una preocupación inexistente. Como no se pueden actualizar o sustituir, la organización debe hacer convivir estas estaciones de trabajo con los sistemas modernos.

Los ciberatacantes son conocedores de este problema y saben que afectan también a los entornos críticos. No por tener redes aisladas, debemos de caer en la falsa percepción de seguridad de que nuestra red está bien "protegida".

A continuación, vamos a ver ejemplos reales de redes aparentemente aisladas y seguras que fueron vulneradas durante años.

STUXNET

Imaginemos por un momento que estamos en una sala de control subterránea, en el corazón de la planta nuclear de Natanz, en Irán. Todo parece normal: los monitores muestran valores estables, los operarios observan sus pantallas sin señales de alarma, y las líneas de producción, continúan su

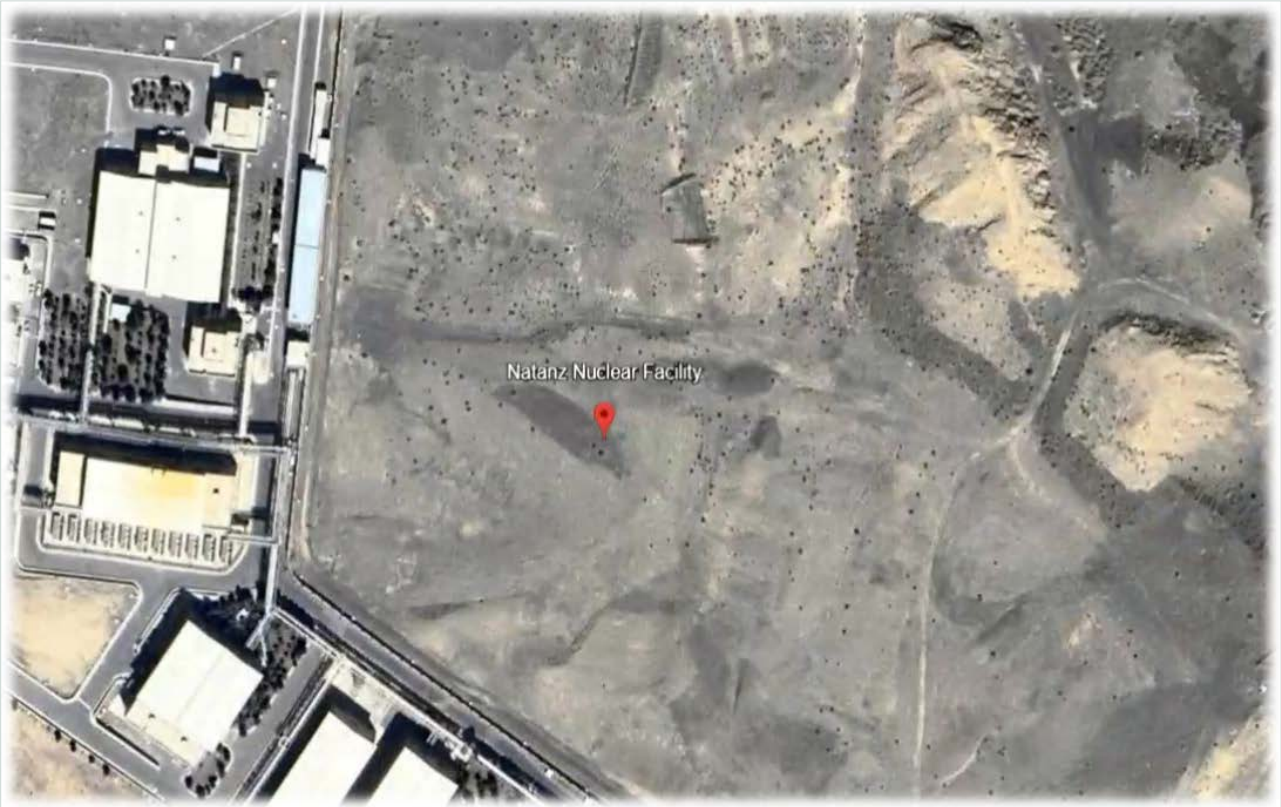

Figura 2. Fotografía satelital de la planta nuclear de Natanz, Irán.

trabajo aparentemente sin alteraciones. Sin embargo, algo está ocurriendo detrás de esas pantallas.

Un software ha tomado el control de los sistemas industriales. Modifica la velocidad de rotación de las máquinas, acelerándolas y frenándolas en ciclos programados, para provocar microfracturas, tensiones internas y con el tiempo su destrucción.

Se trata de Stuxnet. Un gusano informático desconocido, que marcaría un punto de inflexión en la ciberseguridad global. Descubierto en 2010, pero activo desde al menos un año antes, fue el primer *malware* del mundo diseñado no para robar información, sino para destruir infraestructura física.

Stuxnet sorprendió al mundo por su elevado grado de sofisticación. La infección a la planta nuclear se produjo por medio de una memoria USB. Una vez conectada a un equipo interno, el virus se propagó por las redes internas que se encontraban aisladas de internet. Stuxnet era capaz de permanecer dormido hasta reconocer sistemas en una configuración industrial idéntica a la de Natanz. Solo entonces actuaba.

Una de las curiosidades de Stunext era que mientras saboteaba los sistemas, alimentaba a los técnicos con datos falsos. Les hacía creer que todo funcionaba con normalidad, atacando los sistemas desde dentro sin dejar rastro.

Ningún país ha reconocido oficialmente ser el creador de este gusano informático. Pero todas las investigaciones apuntan a una operación secreta entre Estados Unidos y el gobierno de Israel, cuyo nombre en clave es *Operation Olympic Games*. Su objetivo era frenar el programa nuclear iraní sin necesidad de bombardear la planta.

Y lo lograron, ya que el virus destruyó aproximadamente un 20% de las centrifugadoras de la planta, retrasando significativamente el desarrollo nuclear del país.

Stuxnet se propagó a otras plantas nucleares de todo el planeta. Ha sido detectado en India, Indonesia, Pakistán o Azerbaiyán, pero sin activarse ya que su programación lo evitaba.

Este gusano hizo comprender a la sociedad que una línea de código puede tener el mismo poder destructivo que un misil, ya que este software podría catalogarse como un arma de guerra.

Desde el conocimiento público de este gusano, la ciberseguridad se ha convertido una cuestión de Estado, de defensa nacional y de supervivencia operativas.

BLACKENERGY

Cinco años más tarde, el 23 de diciembre de 2015, en Ucrania es pleno invierno. Las familias se preparan para la festejar la navidad. Las ciudades están cubiertas por la nieve, todo parece en calma. Y entonces la luz se apaga.

En cuestión de minutos, cientos de miles de personas quedan sin electricidad: semáforos apagados, los ascensores se detienen, las calefacciones dejan de funcionar, las personas dejan de tener agua en sus casas. No es una catástrofe natural, tampoco es un fallo técnico. Es un ciberataque. Es la primera vez que una sociedad presencia un apagón provocado por un ciberataque real.

Detrás de este suceso estaba BlackEnergy, un *malware* que no solo comprometía sistemas, sino que abría una nueva puerta al sabotaje digital. No era un simple virus, era un conjunto de *malwares*, diseñados para infiltrarse y permanecer ocultos en la red, moverse lateralmente y finalmente atacar los sistemas.

En este caso la infección comenzó con un correo electrónico. Una campaña de *phishing* cuidadosamente elaborada, enviada a empleados de compañías eléctricas. Un archivo adjunto que un trabajador abrió permitiendo comprometer su equipo. Durante meses, los atacantes efectuaron movimientos laterales por las redes sin ser detectados: copiaron credenciales, cartografiaron los sistemas SCADA, estudiaron los protocolos.

Finalmente, el 23 de diciembre, en una operación coordinada, los atacantes tomaron el control remoto de las subestaciones eléctricas. Ejecutaron el ataque y desconectaron el suministro eléctrico de parte de Ucrania. Pero el ataque fue especialmente destructor por dos motivos: el primero, fue encadenar BlackEnergy con el lanzamiento de otro *malware* cuyo objetivo era impedir la recuperación de los sistemas, borrar los discos duros y otros registros. Y el segundo fue por el lanzamiento de un ataque de denegación de servicio para silenciar las llamadas de auxilio, bloqueando los centros de atención a emergencias. La sociedad no tenía forma de pedir ayuda.

El resultado del ataque afecto a más de 230.000 personas que se quedaron sin electricidad ni calefacción en una noche helada.

Esa misma noche los técnicos de los sistemas observaban con incredulidad como alguien, desde otra parte del mundo, operaba sus sistemas mejor que ellos.

Este hecho nos vuelve a hace pensar que la guerra moderna se libra desde teclados y pantallas.

Aunque ningún gobierno lo confirmó oficialmente, hay indicios que indican que el responsable del ataque fue un grupo llamado Sandworm, vinculado al servicio de inteligencia militar ruso, el GRU.

Queda claro que las infraestructuras críticas no bastan con protegerlas con alambradas, también es necesario proteger la infraestructura informática que nos cuesta más ver. Y no basta con tener redes aisladas, porque siempre hay formas de vulnerar sistemas.

Estos eventos marcaron un antes y un después. Y dejaron claro que las infraestructuras críticas, como las nucleares, no están exentas.

ESTRATEGIAS DEFENSIVAS

Para dar respuesta a los problemas de ciberseguridad vistos, una de las estrategias más efectivas es la defensa en profundidad. Consiste en implementar un enfoque de múltiples capas de protección con el objetivo de ralentizar, detectar y mitigar ciberataques. Cada una de estas capas se aplican en un ámbito distinto de la infraestructura informática: barreras físicas, seguridad perimetral lógica, seguridad en la red interna, protección en dispositivos de punto final, control de acceso discrecional, concienciación y gestión de incidentes son las claves para poder hacer frente a la nueva superficie de ataque a la que nos vemos expuestos.

Todas estas medidas, requieren un estudio exhaustivo de cada caso. Desde un punto de vista global a continuación, indicaré las diez principales medidas que consiguen obtener esa visibilidad y respuesta ante ciberataques ataques:

1. Segmentación de redes IT/OT

En primer lugar, se debe de implementar una división lógica de la red de IT y OT, estableciendo barreras mediante electrónica de red, zonas desmilitarizadas (DMZ) y sistemas de control de tráfico. Esta separación minimiza la superficie de ataque y evita que una intrusión en el entorno corporativo afecte los sistemas de control industrial.

2. Aplicación de política de parches por anillos

Es muy recomendable aplicar una política de gestión de vulnerabilidades basada en un modelo de anillos, donde los parches se implementan de forma escalonada. Este enfoque permite validar la compatibilidad y estabilidad de las actualizaciones antes de aplicarlas a todo el conjunto de sistemas.

3. Control estricto de accesos y privilegios

Hay que reforzar el principio de mínimo privilegio mediante controles granulares de acceso, autenticación multifactor y segregación de roles. De modo que cada usuario solo tenga acceso a los sistemas y recursos estrictamente necesarios para el desempeño de sus funciones, limitando así las posibilidades de movimientos laterales en caso de compromiso.

4. Monitorización del tráfico y comportamiento en redes industriales

El uso de sistemas de monitorización continua, como IDS/IPS, es imprescindible. Ya que estos sistemas permiten detectar patrones de comportamiento anómalos, tráfico no autorizado o posibles intentos de intrusión, facilitando una respuesta temprana ante incidentes de seguridad.

5. Formación continua del personal

El factor humano es el vector de ataque principal, como hemos visto, por ejemplo, en el caso de BlackEnergy. Por lo tanto, es fundamental implementar programas de formación y concienciación continuos dirigidos a todo el personal, para reforzar las buenas prácticas en ciberseguridad y reconocer comportamientos maliciosos de ingeniería social, como el *phishing*.

6. Reducción de la exposición a Internet

También hay que proteger la información pública de nuestra organización en el ciberespacio. Por ello, hay que identificar y asegurar después todos los dispositivos expuestos públicamente, aplicando medidas como el cierre de puertos innecesarios, la desactivación de servicios vulnerables y, en casos necesarios, el aislamiento completo de sistemas críticos de cualquier tipo de conectividad externa. También hay que tener en cuenta la vigilancia digital, para evitar casos como una posible usurpación de identidad.

7. Protección de estaciones críticas

Las estaciones críticas deben de estar protegidas mediante *firewalls*, limitando el número de equipos esenciales que

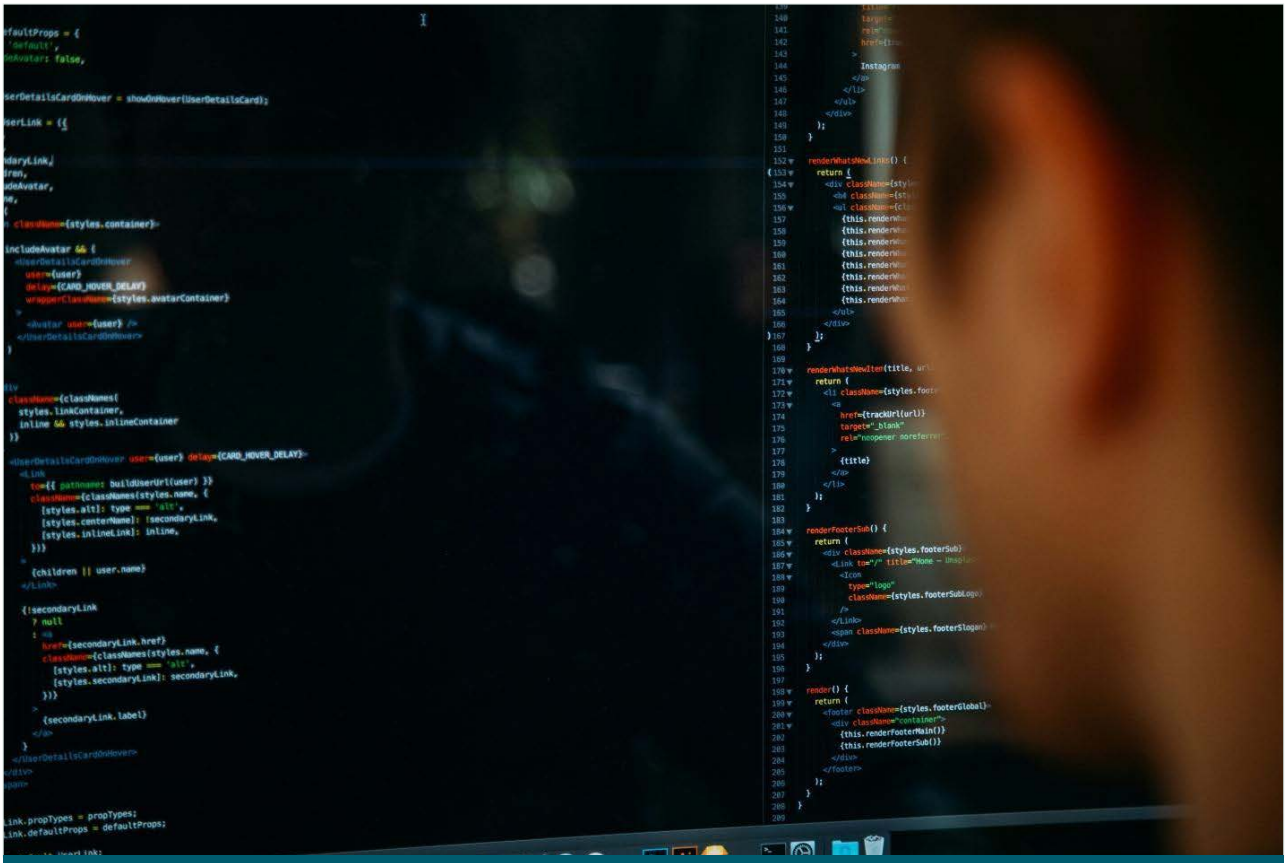

Figura 3. Técnico informático trabajando.

pueden tener acceso. Llegando incluso si fuera necesario, a mantenerlos en redes totalmente aisladas.

8. Gestión de dispositivos finales

Hay que implementar políticas específicas para el control de dispositivos portátiles, incluyendo ese gran olvidado: los teléfonos móviles. Se debe de equiparar la línea base de seguridad de los portátiles a los dispositivos móviles con medidas como escaneos antimalware automáticos, bloqueo de puertos y análisis del tráfico, para prevenir la introducción de software malicioso desde cualquier dispositivo externos con conectividad a la red de la organización.

9. Refuerzo de la seguridad en aplicaciones públicas

Para aquellas aplicaciones o portales accesibles desde el exterior, se deben de implementar distintas soluciones de protección como Web Application Firewalls (WAF), autenticación de múltiple factor, cifrado de extremo a extremo y monitoreo continuo del tráfico.

10. Concienciación sobre phishing y dispositivos extraíbles

Por último, es recomendable desarrollar campañas constantes de concienciación sobre los riesgos asociados al *phishing* y el uso indebido de dispositivos de almacenamiento extraíbles, fomentando prácticas seguras y controles automatizados para mitigar estos vectores de ataque, que como hemos visto, fueron utilizados con Stuxnet.

PROTECCIÓN DE EQUIPOS *LEGACY*

Dentro de los riesgos comentados, no he dado hasta ahora una respuesta al problema de los equipos *legacy*.

Aparentemente, es un problema que no tiene solución. Desde mi punto de vista la mejor estrategia, teniendo en cuenta que estas estaciones pueden verse afectadas en rendimiento y estabilidad si introducimos software moderno, es optar por emplear técnicas pasivas de seguridad sobre ellos, implementando:

- ***Gateways* de seguridad:** que actúan como filtros entre los sistemas *legacy* y el resto de la red.
- **Sondas de monitorización:** que permiten estudiar comportamiento de la red de forma pasiva y sin comprometer el entorno operativo de la línea de producción.
- **Aislamiento y segmentación de la red:** dividimos las redes en zonas más pequeñas con mayor control y mediante el uso de redes virtuales para crear barreras lógicas entre los dispositivos heredados y el resto.

Ante este reto, la clave está en adaptar la protección al contexto sin poner en riesgo la operación.

RESPUESTA ANTE INCIDENTES Y CULTURA ORGANIZATIVA

Además de las medidas anteriores, que protegen nuestra actividad en tiempo real, es crucial contar con medidas de protección pasivas que actúan en caso de un ataque; la

prevención es esencial, pero también lo es nuestra capacidad de respuesta ante incidentes. Tenemos que ser capaces de responder con eficacia e inteligencia.

Por lo tanto, hay que contar con:

- Planes de contingencia, respuesta ante incidentes y planes de recuperación ante desastres adaptados a distintos escenarios.
- Inventario de activos actualizado en tiempo real para tener un conocimiento del alcance de nuestros sistemas.
- Simulacros periódicos, que nos permiten probar procedimientos, detectar debilidades y mejorar continuamente.

Ante una amenaza hay que responder de manera reglada, con procedimientos y experiencia ante incidentes. Proceder con "el plan" establecido es vital para ser rápidos y efectivos ante un problema de ciberseguridad.

CONCLUSIONES

Hemos visto cómo la transformación digital nos trae ventajas y a la vez inconvenientes que es necesario conocer para estar preparados para enfrentar los nuevos retos en materia de seguridad de la información.

La ciberseguridad no es un destino, sino un viaje constante. Un proceso de mejora continua que exige visión, compromiso y acción. Exige humildad para reconocer riesgos, pero también valentía para afrontarlos.

Creo en una seguridad digital que esté integrada en la cultura corporativa. Que no solo proteja, sino que inspire confianza. Que sea una ventaja competitiva, pero también un compromiso con nuestros valores.

La seguridad nuclear del siglo XXI, como han podido ver, no se defiende solo con plomo y hormigón. También se defiende con bytes, protocolos, procesos y personas. ■