convergint® | utilities

Guía de buenas prácticas, **2024: Servicios públicos**

El sector de los servicios públicos está experimentando **una escalada de riesgos físicos y cibernéticos a escala nacional y mundial** que obliga a priorizar la planificación de la seguridad y la mitigación de los procedimientos. El equipo especializado en servicios públicos de Convergint ofrece estrategias de protección de alta seguridad, implementación metódica de programas y soluciones integrales centradas en impulsar tanto la seguridad como la eficiencia operativa en este sector. Con un profundo conocimiento de las amenazas de la industria y los requisitos de cumplimiento normativo, Convergint despliega un diseño en capas para garantizar un rendimiento y una funcionalidad óptimos.

Incidentes y riesgos de seguridad en los servicios públicos

Las ubicaciones de operaciones críticas han presentado durante mucho tiempo un mayor riesgo para las empresas de servicios públicos debido a su abundancia de activos. Sin embargo, se ha demostrado que incluso los emplazamientos situados aguas abajo requieren protección y mitigación de riesgos debido a las repercusiones para las empresas y la comunidad y a la atención mediática nacional que conlleva un incidente de seguridad.

En última instancia, cuando se trata de evaluaciones de riesgos para la identificación de activos, la estrategia de protección y la planificación de la mitigación de riesgos, **es esencial realizar evaluaciones por subverticales** para adaptar las soluciones a los activos, normativas, operaciones empresariales y riesgos únicos asociados a un sector específico.

Centrales nucleares

La energía nuclear es única por estar tan intensamente regulada y altamente vigilada. El razonamiento es claro. Un ataque con éxito, ya sea físico o cibernético, podría dar lugar a una liberación incontrolada de radiactividad con importantes repercusiones para el medio ambiente y la salud, incluida la posibilidad de víctimas mortales a corto y largo plazo. Las instalaciones nucleares están obligadas por la normativa de la Comisión Reguladora Nuclear (NRC) a adoptar un enfoque muy prescriptivo de la seguridad para prevenir o mitigar el impacto de los incidentes.

Las centrales nucleares son estructuralmente robustas con intención y disuaden las intrusiones físicas por diseño. Además, un riguroso enfoque por capas de la protección física proporciona refuerzo e incluye una fuerza de respuesta humana de estilo militar. Las amenazas cibernéticas también se abordan con diligencia y protocolos exhaustivos que se aplican para gestionar el riesgo, supervisar constantemente los acontecimientos y proporcionar un nivel de separación de las redes externas. En definitiva, este subsector está bien protegido, pero se somete a pruebas periódicas para que los equipos y protocolos se reevalúen continuamente con el fin de garantizar la protección y la evolución de las amenazas.

Servicios eléctricos

Las compañías eléctricas recurren a agencias de respuesta in situ o externas para interceptar a los posibles malhechores de la amenaza. La escalada del riesgo podría obligar a reevaluar esta estrategia. Según el Departamento de Energía, en el primer semestre de 2023 se produjeron 95 incidentes relacionados con personas, incluidos actos vandálicos y ciberataques, lo que supera cualquier periodo de la historia.

Los ataques físicos siguen siendo la principal preocupación de este sector. En concreto, el terrorismo nacional ha causado estragos en las operaciones sobre el terreno y en las comunidades a las que prestan servicio las estaciones de transmisión eléctrica. El sur de EE.UU. y el noroeste del Pacífico se han visto especialmente afectados desde 2022, y la situación no parece mejorar. Esto exige una defensa a varios niveles, adoptada cada vez más por las subestaciones de todo el mundo.

Servicios de agua

Las amenazas físicas están aumentando para las empresas de suministro de agua, lo que hace que se preste especial atención a la protección de los activos más vulnerables a los ataques. Como en el caso de las instalaciones eléctricas, lo más prudente es adoptar un enfoque de defensa en profundidad.

Lamentablemente, las ciberamenazas están aumentando al mismo tiempo para las empresas de suministro de agua. Los sistemas SCADA (Supervisory Control and Data Acquisition) son fundamentales para la supervisión operativa y el control de los activos clave para mantener el almacenamiento limpio y la distribución de agua a los consumidores. Mantener un estricto control y observación de estos sistemas, además de mantener buenas prácticas de ciberseguridad en los sistemas empresariales, es clave para prevenir o mitigar los ciberataques. Esta necesidad queda ejemplificada por el reciente ataque a un edificio de la autoridad del agua en el condado rural de Allegheny, Pensilvania, aparentemente perpetrado por un agente de un Estado nación. La autoridad fue capaz de desconectar y reanudar las operaciones manualmente sin incidentes, pero el mensaje se recibió alto y claro: los esfuerzos de seguridad física deben ir en paralelo con las protecciones cibernéticas.

Renovables: Solar, eólica y bioenergía

Aunque menos prominentes en el panorama de las empresas de servicios públicos, las renovables tienen una huella nacional cada vez mayor, lo que significa un aumento de los objetivos y riesgos potenciales. Las renovables tienen activos que también son vulnerables y se han visto obligadas a preparar defensas tanto físicas como cibernéticas. Un incendio provocado en 2023 en una instalación de paneles solares de Las Vegas como "declaración política" es sólo un indicio de

lo que puede venir si este subsegmento no está preparado con una respuesta adecuada a las amenazas emergentes.

El sector en su conjunto

La seguridad física parece ser la principal preocupación de las empresas de servicios públicos, y con razón. El coste de las intrusiones es evidente en los titulares del país. Dicho esto, **las amenazas cibernéticas son cada vez más prominentes, ya que los sistemas obsoletos** y las redes abiertas crean una clara oportunidad de acceso. Y los agentes del Estado-nación se están convirtiendo en una amenaza cada vez más importante, lo que aumenta el riesgo más allá de la simple piratería informática.

Es esencial que el sector adopte una postura firme frente a la ciberdelincuencia e invierta adecuadamente para disuadir y mitigar las amenazas, al tiempo que aplica estrategias integrales de seguridad física.

El coste de los ataques físicos o cibernéticos

Hay cuatro categorías clave de pérdidas resultantes de una intrusión física o cibernética para los servicios públicos:

1. **Reputación/confianza:** Aunque las empresas de servicios públicos no inviten a que se produzcan incidentes, la percepción de falta de preparación puede erosionar la confianza de los clientes y dañar su reputación en la comunidad. En muchos casos, cambiar a un competidor no será una opción, pero un golpe a la percepción de la marca sigue siendo significativo para una empresa de servicios públicos.
2. **Pérdida de negocio**: Los cortes de suministro forzados por ataques físicos o cibernéticos crean una pérdida de negocio tangible, y una disminución medible de los flujos de ingresos.
3. **Multas:** Las multas por incumplimiento físico de las empresas eléctricas pueden superar el millón de dólares al día por ubicación y, dada la visibilidad de los servicios públicos, la normativa se aplica con firmeza. Posteriormente, se han documentado casos de multas de más de 50 millones de dólares en una sola ubicación. Otros sub-verticales tienen una estructura de multas similar. Las sanciones cibernéticas no están tan codificadas, pero el incumplimiento sigue siendo una empresa costosa dadas las sanciones.
4. **La vida humana**: Obviamente, el resultado más preocupante de un ataque físico es la pérdida de vidas humanas. Las ramificaciones en sentido descendente quedan claramente ejemplificadas por un incidente en Carolina del Norte, donde un activo de nivel inferior fue atacado físicamente con importantes repercusiones para una comunidad de más de 50.000 habitantes. Las personas perdieron la vida debido a la imposibilidad de alimentar el aire acondicionado durante una sofocante ola de calor.

Riesgos futuros más amenazadores

Las amenazas físicas ya han mostrado ramificaciones tangibles, y la creciente respuesta de las empresas de servicios públicos y de la supervisión gubernamental da fe de la gravedad de este problema en evolución. Y a medida que las ciberamenazas adquieran mayor relevancia, es probable que veamos más directrices, más restricciones y más requisitos de protección. La rápida escalada de la amenaza cibernética exigirá que la respuesta se mantenga a la altura. Dicho esto, la naturaleza fluida de la ciberamenaza se traduce en una respuesta tecnológica menos prescriptiva y más proactiva.

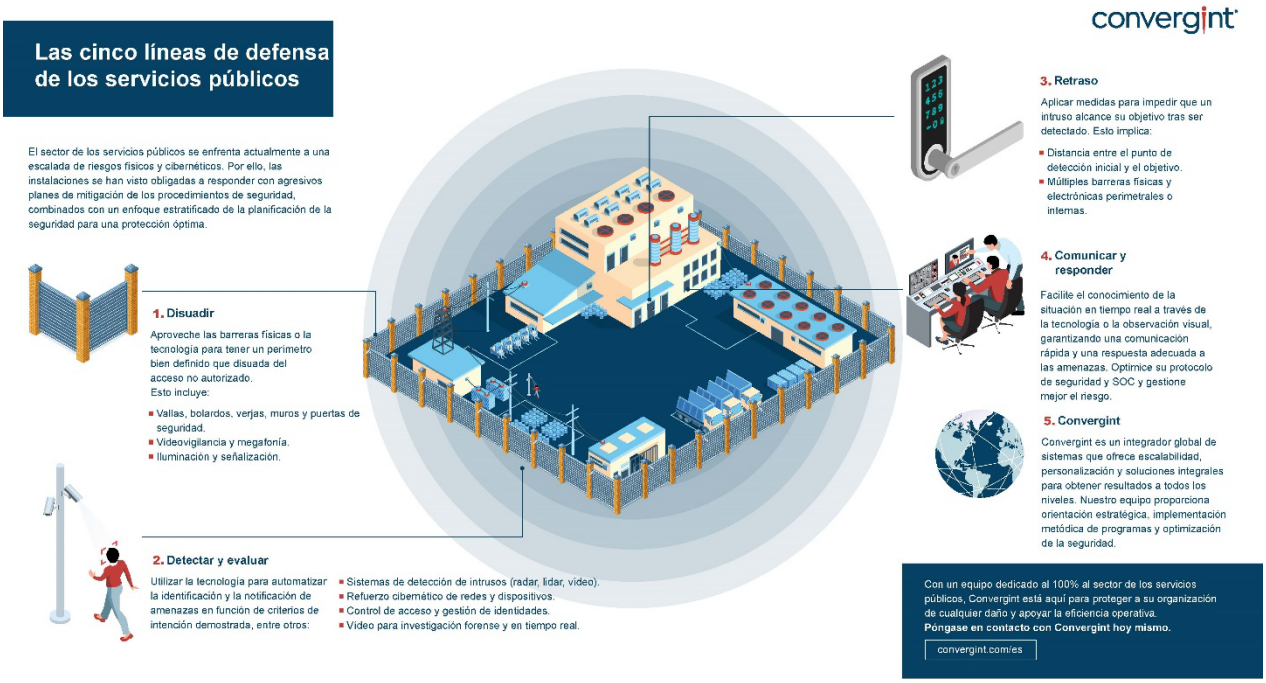
En conjunto, las normas de seguridad y las recomendaciones de mitigación para los servicios públicos se ajustarán continuamente para proporcionar una orientación adecuada ante el creciente número de ataques y el aumento de los niveles de sofisticación. Esto afectará incluso a los activos que antes se consideraban de nivel inferior en términos de riesgo. En última instancia, se establecerán unas medidas de seguridad mínimas que no serán negociables.

Contramedidas tecnológicas de seguridad

Convergint recomienda que **las empresas de servicios públicos contrarresten las amenazas físicas y cibernéticas emergentes con un enfoque de seguridad de defensa en profundidad**. Cualquier sistema de seguridad puede ser desafiado con tiempo y dinero suficientes; por lo tanto, la preparación depende de la complejidad y de una estrategia integral. Los acontecimientos actuales impulsan a las empresas de servicios públicos a responder con planes agresivos de mitigación de procedimientos y soluciones de seguridad de múltiples capas para:

- **Disuadir:** Aprovechando las barreras físicas o la tecnología para tener un perímetro bien definido que disuada del acceso no autorizado.
- **Detectar y evaluar**: Utilizando la tecnología para automatizar la identificación y notificación de amenazas con criterios definidos de intención demostrada.
- **Retraso.** Mediante la aplicación de medidas para retrasar a un intruso de llegar a los activos de destino deben superar la disuasión.
- **Comunicar y responder:** Aprovechando el conocimiento en tiempo real a través de la tecnología y la observación visual para garantizar una comunicación rápida y una respuesta adecuada a las amenazas.

convergint | utilities



En última instancia, **las medidas de defensa en profundidad detienen a los agresores en su camino o proporcionan alertas y notificaciones para coordinar una respuesta**. Las infiltraciones físicas o cibernéticas que logran atravesar una capa se ven ralentizadas o bloqueadas por la siguiente, lo que da aún más tiempo para mitigar o prevenir un resultado negativo para un activo o las operaciones.

Mejorar la eficacia del personal de seguridad/reducir costes

Las empresas de servicios públicos se enfrentan a retos operativos únicos. Muchos de ellos gestionan tanto una infraestructura como una plantilla que envejecen. Por lo tanto, es esencial que mejoren la eficacia del personal de seguridad mediante el aumento de la tecnología de seguridad física y electrónica.

La evolución de las amenazas obliga a reevaluar los procesos de las políticas, los procedimientos, las estrategias de aplicación, la caracterización de los activos y la clasificación de cada impacto empresarial. Además, las entidades necesitan aprovechar de forma cruzada el gasto multidepartamental para cada ubicación, cosiendo las operaciones de seguridad para una seguridad óptima y unos resultados empresariales más impactantes. La inclusión y participación de todas las unidades de negocio en una utilidad para una estrategia de seguridad organizativa proporciona una mayor concienciación, propiedad y responsabilidad en materia de seguridad, lo **que se traduce en un programa empresarial más sólido**.

Gestión del presupuesto de seguridad

Los presupuestos deben tener en cuenta las condiciones medioambientales, los riesgos y la clasificación de los activos. Además, recomendamos:

1) **A corto plazo:** Las empresas de servicios públicos dejan de centrarse exclusivamente en reducir el coste del presupuesto de seguridad y, en su lugar, tratan de sacar más provecho del gasto. Se puede obtener más valor replanteando la seguridad en términos de beneficios operativos y mayor eficiencia. - Gráfico de eficiencia operativa
2) **A largo plazo:** Las empresas de servicios públicos se plantean aprovechar "la ciudad" a la que prestan servicio: administraciones públicas, sanidad, escuelas, etc. Pregúntese qué hacen los clientes/adjuntos en materia de seguridad y cómo la integración puede hacer que todos sean más eficientes. Evalúe si existe una dualidad para la seguridad y las operaciones y, potencialmente, incluso para la seguridad en el futuro, que podría facilitar estratificando sus esfuerzos. Piense en la capacidad proactiva de aprovechar la tecnología de seguridad en todos los sectores verticales existentes, sobre todo teniendo en cuenta el ritmo de los avances. Los datos bidireccionales y la integración permitirían a las empresas de servicios públicos ir más allá de un enfoque aislado de la seguridad, mejorando la eficacia de una manera muy eficiente. La seguridad podría dejar de ser un centro de costes y convertirse en un centro de beneficios con medidas como compartir los SOC. Esto puede ser difícil de imaginar ahora mismo. Dicho esto, a medida que se gestionan las ciberamenazas, es inevitable pasar a un entorno basado en la nube, lo que facilitará la integración.

Utilizar la tecnología de seguridad para mejorar la competitividad de las empresas o marcas

En última instancia, aprovechar la tecnología de seguridad de vanguardia para aumentar la seguridad y apoyar la eficacia operativa mejora el rendimiento general de la empresa y garantiza una experiencia óptima para el cliente. Y, de paso, aumenta la seguridad y la satisfacción de los empleados.

Resumen de recomendaciones, 2024

A medida que la huella física y digital del sector de los servicios públicos sigue ampliándose y evolucionando para satisfacer una demanda de los consumidores cada vez mayor, también deben hacerlo las protecciones de los activos existentes y nuevos. Las amenazas a la industria son continuas, y la batalla constante entre el sector de los servicios públicos con sus socios en seguridad y los malos actores significa que debe haber un proceso continuo de auditoría y evaluación del ciclo de vida. Esto se traduce en una reevaluación constante de políticas, procesos, procedimientos y tecnologías para garantizar que la empresa de servicios públicos mantiene un alto nivel de concienciación sobre las amenazas y un sólido programa de seguridad que pueda responder a los impactos o mitigar los riesgos para las operaciones empresariales y el personal. Esto se complementa con la caracterización recurrente de los activos, las evaluaciones de vulnerabilidad y las evaluaciones de amenazas que deben probar a fondo las estrategias de mitigación, incluidas las mejoras y modificaciones tecnológicas.

La carga financiera que supone el desarrollo de una estrategia de protección más sólida y estratificada no tiene por qué cubrirse únicamente con los presupuestos típicos de los

departamentos de seguridad. El gasto multidepartamental puede aprovecharse empleando tecnologías multiuso que impulsen la eficiencia operativa y mejoren la seguridad. Los sistemas de vídeo y control de accesos a nivel de empresa pueden servir de plataforma integrada para aportar todo tipo de información de uso operativo. Los sistemas que incluyen la supervisión de activos, los sensores medioambientales, la calidad del aire, los sistemas de protección de la vida y otros sistemas de seguridad pueden aprovechar una plataforma única para transmitir información a las distintas partes interesadas y departamentos. Las notificaciones posteriores, rápidas y en tiempo real, pueden reducir la demanda de recursos sobre el terreno para el mantenimiento y facilitar las pistas de auditoría.

En última instancia, la comunicación es clave, y ningún problema debe resolverse en el vacío. La colaboración constante con otros sectores o empresas que se enfrentan a amenazas similares puede ayudar a determinar qué soluciones son realistas para satisfacer y garantizar las necesidades de la empresa. Las perspectivas operativas a través de la evaluación comparativa y los foros de usuarios pueden incluir casos de uso relevantes y mejores prácticas que, a su vez, pueden aprovecharse para las solicitudes de financiación y el desarrollo de estrategias de despliegue de la innovación. La comunicación con los organismos de respuesta, como las fuerzas de seguridad locales o los organismos reguladores del sector, puede ayudar a mantener actualizada a una empresa sobre las amenazas locales o específicas del sector.

Una estrategia de seguridad debe tener varios niveles y diseñarse teniendo muy en cuenta las necesidades empresariales y operativas específicas, utilizando todos los recursos disponibles y la experiencia pertinente. Convergint es la guía perfecta para conducir a las empresas de servicios públicos a través de ese viaje. **Aprovechamos la evaluación comparativa de la industria, los socios tecnológicos y los expertos en seguridad dedicados** a todos los sub-verticales de los servicios públicos en apoyo del desarrollo de una solución optimizada y personalizada para satisfacer esas necesidades.