2022 / Documento técnico

Star2M
INNOVATIVE COMMUNICATIONS

# Introducción al riesgo tecnológico

## Cómo se relaciona esto con las ayudas a la navegación

iridium connected

**Un ataque cibernético debido a disposiciones de seguridad inadecuadas o desactualizadas puede comprometer la seguridad de la información de identidad personal (PII), desconectar los sistemas y deshabilitar por completo las operaciones comerciales.**

**La ingeniería cibernética analiza el diseño, la implementación, el mantenimiento y las medidas de mejora para proteger la integridad, la confidencialidad y la disponibilidad de los sistemas y la información.**

2022 / Documento técnico

## Tecnología digital en la industria AtoN

La tecnología ha evolucionado con el tiempo para convertirse en un elemento clave para gestionar las ayudas a la navegación. Aunque el uso de dispositivos portátiles para acceder a la información bajo demanda es conveniente, no está exento de riesgos.

Las disposiciones de seguridad inadecuadas u obsoletas a nivel empresarial, de sistemas y de usuario pueden tener consecuencias nefastas. Un ataque puede comprometer la seguridad de la información de identidad personal (PII), desconectar los sistemas y puede desactivar por completo las operaciones comerciales.

La mayoría de las organizaciones ya habrán considerado el riesgo y la importancia de una estrategia de ciberseguridad. La ingeniería cibernética analiza el diseño, la implementación, el mantenimiento y las medidas de mejora para proteger la integridad, la confidencialidad y la disponibilidad de los sistemas y la información.

Para las organizaciones que no cuentan con una estrategia formal, nunca ha sido tan crítico evaluar su nivel de vulnerabilidad.

**El momento de actuar es ahora.**

## Por qué la ciberseguridad es imprescindible

Los ataques cibernéticos a las empresas son cada vez más frecuentes y, en particular, en los últimos 10 a 15 años, los casos de filtraciones de datos y registros expuestos han crecido significativamente. La empresa de ciberseguridad Varonis compiló **más de 100 estadísticas y tendencias para 2021** que ayudan a identificar la necesidad de medidas más estrictas.

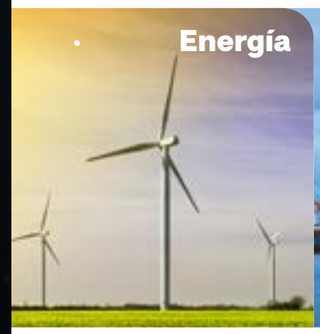
Los sectores que son los mayores objetivos son:

- Energía
- Transporte
- Minería
- Construcción

Estas industrias son lucrativas para los atacantes y es por eso que la ciberseguridad es imprescindible para las organizaciones que operan en estos mercados.

Incluso algunas de las organizaciones más grandes y con conocimientos técnicos (Facebook, Microsoft, Yahoo) han reconocido públicamente que han sido atacadas por malware. Estos ataques pueden ser a través de grupos de piratas cibernéticos, o incluso sancionados por los gobiernos; para interrumpir o deshabilitar operaciones, obtener acceso a datos personales/información de crédito o por un rescate.

La emisión de ransomware para iniciar un bloqueo del sistema es una de las principales razones detrás de un ataque. El motivo principal es extorsionar dinero. Interrumpir los servicios es un objetivo secundario. A diferencia de otras industrias, en la industria marítima, la probabilidad de un ataque terrorista se considera relativamente baja. Sin embargo, a medida que la industria avanza hacia la automatización, el impacto podría ser mucho más significativo.



2022 / Documento técnico

## Convergencia de OT e IoT -Qué significa esto para la seguridad de los datos

Los sistemas de tecnología operativa (OT) y SCADA han sido tradicionalmente los medios para acceder a los datos de monitoreo. Eran esencialmente sistemas de silos que capturaban y transmitían datos para un propósito comercial específico.

Los tipos de monitoreo incluyen:

- Red telefónica pública conmutada (PSTN) a través de interfaces de acceso telefónico para iniciar alarmas. Esto fue fundamental para la industria en las décadas del 80 y 90.
- RF se hizo popular desde el comienzo como una solución de última instancia. Encontró su lugar donde las redes PSTN no podían dar servicio. Requiere aprobación regulatoria en la mayoría de los países excepto para la banda ISM. Todavía se usa mucho hoy en día.
- GSM es un servicio confiable. Sin embargo, todavía tiene una cobertura limitada en muchas áreas y está sujeto a un ciclo de actualización de tecnología
- Bluetooth y Zigbee se utilizan para opciones de conectividad de corto alcance y siguen siendo populares para la comunicación con sensores y dispositivos auxiliares.
- El satélite se ha vuelto más competitivo en cuanto a lo monetario y la tecnología ha avanzado a un ritmo acelerado. Ofrecer una cobertura verdaderamente global es la opción preferida para ubicaciones remotas o en alta mar, y donde el servicio GSM no es confiable.

La popularidad de Internet de las cosas (IoT) en los últimos veinte años está cambiando nuestro comportamiento y los medios en los que nos comunicamos. El acceso a las aplicaciones, los datos y la funcionalidad está al alcance de la mano y ha seguido alimentando nuestro creciente apetito por un mundo cada vez más conectado.

La alta demanda de los consumidores ha llevado a los proveedores de OT a repensar su estrategia de sistemas de silos y pasar a las mismas redes de TI utilizadas por IoT. El resultado es una red de tecnología híbrida con protocolos abiertos, tiene acceso público y como tal tiene un alto riesgo de ser comprometida.

## Riesgo para AtoN: ¿por qué?

El uso de la tecnología en sí es un riesgo. Los piratas informáticos tienen la capacidad de escanear e interceptar datos y dispositivos. GSM, Bluetooth, PSTN, WiFi, TCP y RF cumplen su propósito, pero todas son redes abiertas que permiten que cualquier persona intercepte, decodifique y use los datos para su beneficio. Esto hace que estas redes y los sistemas conectados a ellas sean más susceptibles a ataques.

El riesgo accidental puede estar sujeto al factor humano, por lo que los activos se configuran incorrectamente o se apagan accidentalmente. Las actualizaciones de software automatizadas pueden corromper los datos y desactivar por completo un sistema, desactivar activos o brindar información errónea.

El riesgo de conectividad puede resultar de la interferencia de la red, por lo que una persona que opera en la misma frecuencia puede desconectar la red, un riesgo que es imposible de evitar.

En relación con las ayudas a la navegación, las plataformas de gestión de datos son ideales para consolidar mensajes en un solo centro, pero son las más susceptibles al riesgo de un ciberataque. En organizaciones con cientos de activos y con mucho personal accediendo a estos sistemas, los protocolos de seguridad insuficientes o desactualizados pueden conducir a una brecha de seguridad grave.

## Consideraciones clave de diseño

Las consideraciones clave de diseño para un sistema de gestión de datos deben incluir:

- Un mínimo de cifrado AES-256 y protección de datos SHA-256 para hash para proteger la información de identificación personal (PII) y los datos de activos.
- Segregación de PII y datos de configuración de datos de activos
- Utilice la autenticación multifactor para usuarios (MFA), al aplicar contraseñas complejas y actualizaciones frecuentes de contraseñas.
- Asegúrese de que el "Directorio activo" no sea de acceso público.
- Cree capas de acceso para separar la base de datos, la API y los sistemas front-end.
- Habilite el cifrado de extremo a extremo para los usuarios – Certificados SSL/TLS.
- Realice pruebas de penetración continuamente para ayudar a comprender las amenazas de red en curso.
- Políticas de gestión de datos de copia de seguridad y restauración para mitigar la posibilidad de pérdida.

## Planificación para el futuro

El mayor riesgo para las organizaciones son sus sistemas de datos y, a medida que los ciberdelincuentes se vuelvan más sofisticados, la amenaza de ataque y su costo para las empresas seguirán aumentando.

Para mitigar mejor el riesgo, se recomienda:

- Desarrolle una estrategia formal de seguridad cibernética y una política de TI: aplique y revise con la frecuencia que sea necesaria.
- Realice una evaluación de riesgos del sistema de gestión de datos, para ayudar a abordar posibles puntos de entrada para una infracción y desarrollar un plan de acción en caso de que ocurra una intrusión.

Por ahora, debido al retraso en la conectividad, el riesgo para los datos de AtoN es relativamente bajo, pero en el futuro, es probable que esto cambie. A medida que avanza la tecnología, las organizaciones deben planificar la protección de todos sus datos a medida que los atacantes se vuelven más específicos en su enfoque.

## Obtener más información:

Mire el seminario web a pedido "**Seguridad cibernética en AtoN**" donde **Jens Ohle, Gerente de ingeniería** de Sealite, presentó a los **miembros de IALA** sobre este tema.

La carrera de ingeniería de Jens se inició en Telkom Sudáfrica. Jens también trabajó como líder de equipo – Integración de sistemas para una empresa de valores global.

## ¿Cómo funciona Star2M?

La plataforma Star2M reúne todos sus activos en un solo centro.

Utiliza encriptación AES-256 de grado militar junto con archivos de datos a largo plazo de alta integridad. Star2M funciona de dos maneras:

- Por IOT y conectando sus activos (como luces de obstrucción y linternas marinas) digitalmente al portal. Esto permite al usuario monitorear y controlar sus activos para satisfacer sus necesidades operativas.
- Al registrar los datos y las condiciones de los activos directamente en la plataforma a través del portal web o la aplicación móvil.

Esto permite al usuario realizar tareas clave como la planificación, el seguimiento y la programación para respaldar el rendimiento óptimo de los activos.

El Portal Star2M está disponible a través de cualquier tableta, teléfono celular o PC conectado a Internet. La aplicación Star2M también está disponible para teléfonos inteligentes iOS y Android.

Operando como un servicio de suscripción, Star2M es impulsado por Iridium®, la compañía de servicios de satélite global de órbita terrestre baja. Ofrece cobertura de polo a polo, en cualquier lugar y en cualquier momento.

## ¿Quiere obtener más información?

Para obtener más información sobre cómo Star2M puede ayudar a su negocio, visite nuestro sitio web en www.star2m.com.

Alternativamente, puede comunicarse con uno de nuestros representantes utilizando los detalles a continuación.

**Oficina central**
+61 (0)3 5977 6128
sales@star2m.com

**Américas**
+1 (603) 737 1311
sales@star2m.com

**Reino Unido**
+44 (0) 1502 588026
sales@star2m.com

**Asia**
+65 6908 2917
sales@star2m.com