SECUTIL: Soluciones de seguridad y ciber-seguridad en Utilities para protección de infraestructuras críticas

Description

El objetivo principal del proyecto consiste en el desarrollo de soluciones de soporte a la seguridad en previsión de unaumento masivo en la sensorización, volumen de datos, tipología de datos críticos, incremento de los elementos decontrol y supervisión, robustez ante desastres naturales y también ante la tendencia de ataques intencionados.

En concreto, se pretende llevar a cabo el desarrollo de un sistema de gestión integral de la cadena de seguridadaplicada a las Utilities, garantizando la privacidad y la integridad de la información mediante la encriptación yseguridad funcional, así como la sensorización de instalaciones y control de accesos, con el fin demejorar la seguridad física, control de acceso y ciber-seguridad en redes e infraestructuras implicadas en la gestión de recursos.

Asimismo, se van a definir estrategias de resiliencia, tolerancia a fallos y capacidad de recuperación, para redes einfraestructuras en relación a los elementos críticos, puntos débiles y seguridad funcional.

En líneas generales, los objetivos perseguidos son los siguientes:

- Soluciones de privacidad y seguridad en los dispositivos.

- Detección de ataques y anomalías

- Gestión unificada de seguridad lógica y física

- Diseño de estrategia para la resiliencia (Security-by-design)

- Evaluación de resultados

Cabe destacar, que el desarrollo del presente proyecto es completamente relevante para su aplicación en redes einfraestructuras para la gestión de recursos de las Utilities, ya que el futuro crecimiento de nuevas tecnologías en lasáreas de Computación en la nube, el Internet de las Cosas (IoT) y el Big Data son prácticamente ilimitadas, lo que setraduce en nuevas amenazas y la necesidad de diseñar y desarrollar nuevas soluciones.

En este sentido, cabe destacar que la entrada de nuevas amenazas y ataques cibernéticos pueden derivar en grandespérdidas para la sociedad y las empresas, e incluso afectar a las relaciones entre países. A modo resumen, losciberataques pueden suponer:

- Pérdidas financieras.

- Daños a la reputación de la organización.

- Pérdidas de propiedad intelectual, incluyendo material patentado y marcas registradas, información comercial sensible y lista de clientes.

- Penalizaciones (legales y reglamentarias).

Proyecto financiado por el Fondo Europeo de Desarrollo Regional de la Unión Europea en el marco del Programa Operativo FEDER 2014-2020.

Barcelona Supercomputing Center - Centro Nacional de Supercomputación

---