



Informe sobre la Protección de Infraestructuras Críticas en España

La exposición a internet de los sistemas tecnológicos y su diseño inestable, principales factores de riesgo para un ciberataque

- Iniciativas lideradas desde el más alto nivel estatal y la colaboración entre empresas del sector privado, que configuran el 80% de los operadores en este área, son fundamentales para aumentar la seguridad de las infraestructuras críticas españolas.
- Según un estudio realizado por S2 Grupo, los nuevos paradigmas de seguridad implican amenazas desconocidas que exigen esquemas de defensa flexibles y con rápida capacidad de respuesta para garantizar una correcta protección.

Valencia 28 de noviembre de 2011.- La protección de infraestructuras críticas^(*) (PIC) es una preocupación de los gobiernos de todo el mundo porque puede suponer una amenaza para el sistema o la población. Por ello, su seguridad es completamente necesaria. A pesar de esto, la **exposición a internet de los sistemas SCADA** (entornos tecnológicos que controlan operaciones de las infraestructuras críticas) y que éstos no hayan sido diseñados con la **seguridad como premisa básica**, hacen que un posible ataque remoto desde cualquier parte del mundo pueda tener éxito y se convierten en algunos de los principales factores de riesgo para un ciberataque en España, según se extrae del informe realizado por la empresa de seguridad digital S2 Grupo sobre la "**Protección de Infraestructuras Críticas en España**".

Como ha señalado la compañía, la seguridad de las infraestructuras críticas debe garantizarse desde cualquier punto de vista. Si bien la protección física en nuestro país es generalmente correcta, la seguridad lógica (aplicación de barreras para resguardar el acceso a datos y restringir el acceso sólo a personal autorizado) es mejorable, especialmente la de los sistemas de control industrial, desde el punto de vista de su control de acceso y de la robustez de las aplicaciones.

Adicionalmente, según se indica en el estudio, la defensa de las infraestructuras críticas (centrales nucleares, transporte, red eléctrica, suministro de agua, instalaciones portuarias, etc.) es muy compleja por **tres factores principales**: existen gran número de **agentes involucrados** en su protección (gubernamentales, autonómicos, etc.), muchas de ellas son **interdependientes** y el 80% de sus operadores pertenecen al **sector privado** (muchos de ellos, multinacionales).

(*)¿Qué es una infraestructura crítica? Según el Plan Nacional de Protección de Infraestructuras Críticas, se trata de aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas. Algunos ejemplos serían sector energético, el sistema financiero o tributario, la industria nuclear, el sector sanitario, las TIC o el transporte.

Por este motivo, desde S2 Grupo han señalado que es necesario potenciar la colaboración y el intercambio de información entre los actores participantes en la PIC nacional en todos los niveles, desde el estratégico al operativo, y en todos sus ámbitos de actuación ya sean públicos o privados. Además, el informe considera que estos últimos, debido a su gran peso en la PIC, deben reforzar su colaboración y olvidar que son competencia en pro de la seguridad nacional.

Solución: sistemas de protección flexibles

Por otro lado, el informe destaca que la continua aparición de nuevas amenazas hace que la **flexibilidad** en los sistemas de PIC y su alta **capacidad de respuesta** sean la clave de una óptima protección frente a posibles ciberataques. En definitiva, están obligados a contar con un alto grado de resiliencia para poder recuperarse de problemas de todo tipo, conocidos o desconocidos, porque si no se fracasará en su protección con la amenaza que ello supone para el entorno.

Aunque en España se trabaja intensivamente en la PIC, todavía queda mucho camino por recorrer a nivel nacional. Por eso, desde S2 Grupo consideran que para que las iniciativas sean exitosas deben cumplir dos parámetros: estar lideradas desde el más alto nivel estatal y estar orientadas a la protección integral y a la resiliencia de las infraestructuras. Su finalidad debe ser garantizar que el país es capaz de adaptarse rápidamente a nuevas situaciones que quizás ahora mismo nadie sea capaz de plantear.

Como se indica en el estudio, a corto y medio plazo deberían seguirse **6 líneas de actuación** para **mejorar la seguridad** de las infraestructuras críticas:

- Potenciar la **colaboración** y el intercambio de información entre todos los participantes en este ámbito.
- Promover la **participación activa** del sector privado y la colaboración público-privada.
- Impulsar los cambios orgánicos necesarios al **máximo nivel** del Estado para garantizar la gestión correcta de los nuevos paradigmas de la seguridad y la defensa.
- Garantizar la **adaptabilidad** de la protección a nuevas situaciones que sean radicalmente opuestas a las conocidas, permitiendo la resiliencia de las infraestructuras críticas.
- Abordar la protección de infraestructuras críticas desde el punto de vista físico y desde el punto de vista lógico con una **gestión integrada**.
- Mejorar la seguridad lógica de las infraestructuras críticas haciendo especial hincapié en la **protección adecuada de los sistemas de control**.

Sobre S2 Grupo

Fundada en 1999, es la primera empresa de la Comunidad Valenciana especializada en servicios globales de seguridad digital. En este ámbito, destaca su trabajo de consultoría para el diseño e implantación de Sistemas de Gestión de la Seguridad en todo tipo de organizaciones y procesos. La compañía prevé cerrar 2011 con una facturación de 3,85 millones de euros, lo que refleja un crecimiento del 21% respecto al ejercicio anterior, motivado por un aumento de la cartera de clientes y de la actividad de innovación. La inversión en I+D+i es uno de los ejes vertebradores de la compañía que en 2011 ha destinado 1,2 millones de euros a diferentes proyectos nacionales y europeos, lo que supone un 30% de su facturación.

Para más información:

Tinkle : Patricia Berzosa/ Miguel Cegarra
600 591 801 / 609 688 809
pberzosa@tinkle.es / mcegarra@tinkle.es