UNDÉCIMA CONFERENCIA DE NAVEGACIÓN AÉREA

Montreal, 22 de septiembre - 3 de octubre de 2003

Cuestión 2 del orden del día: Seguridad y protección en la gestión del tránsito aéreo (ATM)
2.5: Seguridad y protección de la infraestructura ATM

METODOLOGÍA PARA LA PROTECCIÓN DE COMPUTADORAS EN REDES OPERACIONALES DE LA OFICINA FRANCESA PARA LA NAVEGACIÓN AÉREA

(Nota presentada por Francia)

RESUMEN

Los sistemas de computadoras desempeñan actualmente una función primordial en la navegación aérea, y su seguridad y protección son vitales para llevar a cabo las tareas de los servicios de navegación aérea.

El objetivo de esta nota de estudio es presentar la metodología que ha adoptado la Oficina Francesa para la Navegación Aérea para tratar el problema de la protección de las computadoras de su sistema de información operacional.

Las medidas propuestas a la Conferencia figuran en el párrafo 5.

1. ANTECEDENTES: EL PROBLEMA DE LA PROTECCIÓN Y SEGURIDAD DE COMPUTADORAS EN LA OFICINA FRANCESA PARA LA NAVEGACIÓN AÉREA

1.1 El mantenimiento de la seguridad de un sistema de información puede definirse en términos de garantizar su disponibilidad, integridad y confidencialidad. La protección, que podría considerarse como un subelemento de la seguridad del sistema de información está destinada específicamente a proteger la seguridad del sistema de información contra ataques perniciosos.

Los sistemas de computadoras desempeñan hoy en día una función primordial en la navegación aérea, y la seguridad y protección del sistema de información son vitales para llevar a cabo las tareas de los servicios de navegación aérea.

Hasta hace unos pocos años, el sistema de información de navegación aérea funcionaba como un sistema cerrado que ofrecía poca o ninguna interacción con el mundo exterior. Era muy poco vulnerable a las amenazas de seguridad simplemente por el hecho de que era difícil tener acceso por

computadora al sistema de información desde el exterior. En tales circunstancias, la **protección** se limitaba a proteger el acceso físico al sistema de información.

1.2 No obstante, desde hace algunos años, se ha observado que si bien la importancia que tiene el sistema de información para la navegación aérea ha aumentado, éste se ha vuelto progresivamente más complejo y está evolucionando hacia un sistema cada vez más interconectado con otros sistemas y redes fuera del control del servicio de navegación aérea. Esta interconectividad es necesaria debido a que se requiere una interacción e intercambio de datos entre los asociados de los servicios de navegación aérea (asociados europeos, líneas aéreas, etc.). Al mismo tiempo las tecnologías "patentadas" han ido perdiendo terreno para dar lugar a tecnologías uniformes tales como el Protocolo de Internet (IP) para redes, o UNIX para los sistemas operativos.

Todos estos factores hacen que el sistema de información sea más susceptible y aumente el riesgo de su exposición a amenazas externas. Por consiguiente, aumenta considerablemente el riesgo de que se produzcan infracciones de seguridad del sistema de información por terceros con fines maliciosos.

1.3 En consecuencia, se hizo evidente para la Oficina Francesa para la Navegación Aérea que era necesario prestar más atención al problema de mantener la protección y seguridad de su sistema de información y específicamente protegerlo contra amenazas externas al soporte lógico.

2. ¿CÓMO ABORDAR EL PROBLEMA?

2.1 A fin de diminuir el riesgo del sistema de información a un nivel aceptable es necesario establecer medidas de protección técnica, de organización y de procedimientos que sean capaces de corregir la vulnerabilidad del sistema. Estas medidas deben concebirse en forma de reglas que:

— aborden el problema de forma exhaustiva;

— definan medidas de protección uniformes; y

— definan medidas de protección que sean aplicables, reconocidas y que se pongan realmente en práctica.

2.1.1 El abordar el problema de forma exhaustiva significa que deben cubrirse todos los aspectos que pueden tener repercusiones en la seguridad, incluyendo: la interconexión del sistema de computadoras con el mundo exterior, sus interconexiones internas (entre sitios), la utilización, funcionamiento y mantenimiento del equipo de computadoras, las modificaciones técnicas y funcionales, la organización y las responsabilidades de recursos humanos y la gestión de incidentes o accidentes de seguridad.

Para que sea exhaustiva, la cobertura debe tener en cuenta todos los elementos del sistema de información que tienen un "requisito de seguridad" o respecto de los cuales una infracción de seguridad tendría repercusiones en el desempeño de las tareas de navegación aérea.

2.1.2 Las medidas de protección deben ser uniformes dentro del sistema de computadoras. Obviamente el nivel de protección efectivo del sistema de computadoras es solo el que determine su eslabón más débil. Es inútil tratar de aplicar medidas de protección extremadamente complejas y onerosas a una parte del sistema cuando otra igualmente susceptible se deja con poca protección.

2.1.3 Las medidas de protección deben ser aplicables y deben tener en cuenta la naturaleza específica del contexto. Cuando se elaboran reglas de protección, deben tenerse en cuenta la tecnología utilizada, las restricciones en materia de seguridad operacional y las costumbres y prácticas de los explotadores, etc. Por último, a fin de que estas reglas puedan ponerse en práctica efectivamente, es

imperativo que sean reconocidas por los operadores y usuarios de los sistemas de computadoras, quienes deben estar familiarizados con éstos y deberían ser aplicables en la misma forma en que se aplican las reglas existentes para la operación y utilización del sistema.

2.2 Teniendo en cuenta todos estos factores, Francia ha emprendido la formalización de una política general de alto nivel para la seguridad de computadoras. El proyecto, denominado *Política de seguridad informática de la Dirección de Navegación Aérea* (PSINA), está destinado a definir reglas generales de protección de computadoras para todos los sistemas "operacionales" de navegación aérea que forman parte del Sistema de información de control del tránsito aéreo (SICTA).

Esta política general de seguridad debería consignarse en un documento que constaría de los siguientes capítulos:

— Objetivos y límites de la PSINA: definición utilizada para el sistema de información, principios adoptados, gestión de amenazas anteriores y el lugar de la PSINA en relación con otras reglas existentes;

— Clasificación de los componentes del sistema de información: se determinan cuatro niveles de sensibilidad con respecto a los componentes funcionales y físicos del sistema de información, junto con los criterios para la clasificación de los componentes en los diversos niveles. En la clasificación se tienen en cuenta tres aspectos: disponibilidad, integridad y confidencialidad;

— Acceso de los usuarios al sistema de información: reglas relativas a la autorización de seguridad, acreditación, certificación, rastreo de los movimientos realizados cuando se contrata personal del exterior para que preste servicios en la Dirección General de Aviación Civil;

— Protección física: reglas para la protección de los medios de información susceptibles (medios móviles, portátiles, etc.), protección y ubicación física de los sistemas de computadoras.

— Mantenimiento y administración del sistema de información: reglas relativas a la obtención de autorizaciones de seguridad, certificación del personal de mantenimiento, el empleo de técnicos del exterior para el mantenimiento y rastreo de las operaciones de mantenimiento y administración del sistema;

— Interconexión de sistemas e intercambio de datos dentro de un sistema de información: adopción de "campos fiables" definiendo parámetros y reglas de protección fiables para el uso de redes privadas y públicas para fines de interconexión interna;

— Interconexión e intercambio de datos con entidades externas, normas para tener acceso al sistema de información desde el exterior y para tener acceso a entidades externas al sistema de información, normas relativas al uso de redes públicas y privadas para la interconexión externa, normas relativas a la emisión y recepción de datos de computadora entre el sistema de información y las entidades externas;

— Evolución del sistema de información: una nueva evaluación de la clasificación de componentes y de los niveles de seguridad cada vez que se modifique el sistema de información; reglas para la integración de nuevos componentes o el retiro de los anteriores;

— Incidentes y accidentes de seguridad: definición de incidente o accidente de seguridad, clasificación y detección de incidentes, medidas que han de tomarse cuando se detecta un incidente de seguridad; reglas para las comunicaciones internas y externas relacionadas con incidentes y accidentes de seguridad; definición de los principios que rijan las sanciones y procedimientos contra partes maliciosas dentro y fuera de la Dirección General de Aviación Civil;

— Organización de los recursos humanos en relación con la seguridad del sistema de información: conocimiento del usuario sobre los problemas de seguridad/protección y conocimiento entre los encargados de tomar decisiones relacionadas con la seguridad, autorización de oficiales de "seguridad", administración de seguridad y reglas de mantenimiento, etc.

2.3 A fin de garantizar la aplicación de las reglas establecidas en el marco de esta política de seguridad y que los participantes en el sistema de información se familiaricen inmediatamente con las mismas, se ha creado un grupo de trabajo al que se ha asignado la tarea de redactar una propuesta de política. El grupo de trabajo está compuesto por representantes de diversos servicios operacionales de navegación aérea. Además, para asegurar que la PSINA sea reconocida efectivamente por los diversos operadores y usuarios, ésta será adoptada por un Comité de supervisión presidido por la Oficina Francesa de Navegación Aérea, asegurando así su poder de autoridad.

2.4 A continuación se indican algunos ejemplos de las reglas de seguridad elaboradas en el marco de la PSINA:

— Toda interconexión con sistemas externos debe ser autorizada oficialmente por un oficial de seguridad basándose en el registro de seguridad en el que están consignados específicamente los resultados de un estudio de riesgos realizado previamente.

— Toda interconexión con el exterior debe verificarse técnicamente. Esto tiene por finalidad, en particular, asegurar que en un determinado momento sólo los servicios autorizados para dicha interconexión sean accesibles y que sólo los corresponsales autorizados (usuarios o sistemas) pueden hacer uso de ella, etc. Además, la verificación también debe permitir asegurar que únicamente aquellos servicios técnicos (tales como protocolos de redes) que se requieren estrictamente para los servicios funcionales autorizados puedan usarse mediante esa interconexión.

— Para los elementos más susceptibles del sistema de información, se prohíbe establecer interconexión alguna utilizando redes públicas (RTC, Internet, etc.).

3. ESTRATEGIAS DE APLICACIÓN DEL MÉTODO ADOPTADO

3.1 Debido a la escala del proyecto PSINA y a fin de tratar gradualmente con todos sus aspectos, se han establecido algunas prioridades entre los objetivos.

El primer objetivo es asegurar el perímetro del sistema de información de navegación aérea a fin de tratar con los riesgos externos. Esto se lleva a cabo definiendo las funciones y reglas de protección que deben cumplirse en los límites del sistema de información.

Una vez que este perímetro está asegurado, será posible tratar con la seguridad interna. La respuesta a los riesgos internos es mucho más difícil de definir y los medios requeridos son mayores, ya que es imposible "bloquear" el sistema completo; en efecto, el sistema de información debe permanecer en uso y en forma eficiente y por consiguiente no es posible adoptar medidas de protección tan radicales

y relativamente sencillas como las que se utilizan contra los riesgos externos. Esta es una de las principales razones por las que se ha decidido tratar este aspecto después de haber abordado los riesgos externos.

3.2 Mediante esta secuencia de objetivos, el objetivo final es poder proporcionar un sistema de protección de la información "bien arraigado", con defensas de perímetro empleando control y tecnología de protección sobre las redes y las interconexiones de redes y un mecanismo de defensa interna que emplee tecnología de seguridad centrada en la red interna y en los propios sistemas.

4. CONCLUSIONES

4.1 Actualmente Francia prosigue su labor de definir una primera versión de su política de protección de computadoras. El grupo de trabajo ya ha redactado una propuesta para elaborar los primeros capítulos que constituirán la piedra angular de esta política (objetivos y límites de la política, reglas para la clasificación de los componentes del sistema de información), y ahora continúa su labor relativa a las reglas para la interconexión con entidades externas. En un plazo corto se presentará esta primera propuesta al Comité de supervisión.

4.2 Una vez que estos primeros capítulos se complementen con el capítulo sobre la organización de recursos humanos y protección de computadoras, será posible la implantación inicial en la Oficina Francesa de Navegación Aérea de una versión de la política de protección de computadoras de navegación aérea.

4.3 Esta es una tarea a largo plazo que requiere un esfuerzo sostenido a fin de lograr una política de seguridad exhaustiva conmesurable con sus objetivos.

5. MEDIDAS PROPUESTAS A LA CONFERENCIA

5.1 Se invita a la Conferencia a:

a) tener en cuenta los riesgos que amenazan a los sistemas de computadoras de navegación aérea;

b) elaborar normas y métodos recomendados (SARPS) para garantizar la protección de los sistemas de computadora; y

c) asignar a un grupo de expertos la tarea de producir una guía general para ayudar a los Estados en la implantación de sus políticas de seguridad y protección, por ejemplo en la forma de una lista de verificación en la que se indiquen los puntos y preguntas que deben tenerse en cuenta en una política de seguridad y protección y los medios para garantizar la protección del sistema de computadoras.

— FIN —