المؤتمر الحادي عشر للملاحة الجوية

مونتريال، ٢٢/٩-٣/١٠/٢٠٠٣

البند ٢: سلامة وأمن ادارة الحركة الجوية
البند ٢-٥: سلامة وأمن البنية الأساسية لادارة الحركة الجوية

منهجية أمن الكمبيوتر في شبكات تشغيل الهيئة الفرنسية للملاحة الجوية

(وثيقة مقدمة من فرنسا)

ملخص

تضطلع أجهزة الكمبيوتر حاليا بدور رئيسي في الملاحة الجوية، وتعتبر سلامة وأمن الأجهزة أمرا هاما للقيام بهذه المهام المرتبطة بخدمات الملاحة الجوية.

والغرض من هذه الوثيقة هو عرض المنهجية التي اعتمدتها الهيئة الفرنسية للملاحة الجوية للتعامل مع مشكلة أمن أجهزة الكمبيوتر التي تدير نظامها للمعلومات التشغيلية.

يرد الاجراء المعروض على المؤتمر في الفقرة ٥.

١- خلفية الموضوع: مشكلة أمن وسلامة أجهزة الكمبيوتر في الهيئة الفرنسية للملاحة الجوية

١-١ يمكن تعريف الحفاظ على سلامة نظام معلومات على أنه ضمان توفره وتكامله وسريته. والأمن، الذي يعتبر كمجموعة فرعية من سلامة نظام معلومات، يهدف على وجه الخصوص الى حماية سلامة نظام المعلومات ضد أعمال الانتهاك.

احتلت أجهزة الكمبيوتر حاليا مكانا مرموقا في الملاحة الجوية، كما تعتبر سلامة وأمن نظام المعلومات كأمر حيوي للقيام بمهام خدمات الملاحة الجوية.

وحتى بضع سنوات مضت، كان نظام معلومات الملاحة الجوية مغلقا، كما أنه أتاح تعاملا ضئيلا مع العالم الخارجي أو لم يتحه بالمرة. وكانت مقاومته كبيرة أمام التهديدات الأمنية لمجرد أنه كان يصعب الاطلاع من خلال جهاز

الكمبيوتر الى نظام المعلومات من أي مكان خارجه. وأمكن في مثل هذه الظروف أن يقتصر **الأمن** على حماية التوصل المادي لنظام المعلومات.

١-٢ ورأينا لعدة أعوام أنه مع زيادة أهمية نظام المعلومات للملاحة الجوية، فانه أصبح أكثر تعقيدا تدريجيا، وتطور بحيث أصبح موصلا بنظم وشبكات أخرى خارج نطاق تحكم خدمة الملاحة الجوية. وهذا التوصل لازم لضرورة التعامل وتبادل البيانات مع شركاء خدمات الملاحة الجوية (الشركات الأوروبية، شركات الطيران، الخ). وفي الوقت ذاته، ينخفض انتشار التكنولوجيات "الخاصة" تدريجيا أمام التكنولوجيات الموحدة مثل بروتوكول الانترنت (IP) بالنسبة للشبكات أو نظام UNIX بالنسبة لنظم التشغيل.

جعلت كل هذه العوامل نظام المعلومات أكثر حساسية وزادت من خطر التعرض للتهديدات الخارجية. مما أدى الى الزيادة الكبيرة لخطر انتهاك أمن نظام المعلومات من قبل عناصر مخربة.

١-٣ اتضح بالتالي للهيئة الفرنسية للملاحة الجوية أن عليها ايلاء المزيد من الانتباه لمشكلة الحفاظ على أمن وسلامة نظام المعلومات لديها، وحمايته على وجه الخصوص من أي انتهاكات خارجية.

٢- التعامل مع المشكلة

٢-١ بغية التمكن من تخفيض التهديدات التي تواجه نظام المعلومات لتصل الى مستوى مقبول، ينبغي تحديد تدابير حماية فنية وتنظيمية واجرائية تستطيع تصحيح نقاط الضعف في نظام المعلومات. وينبغي تقسيم مثل هذه التدابير الى قواعد من حيث ما يلي:

— معالجة المشكلة بشكل كامل.

— تحديث تدابير حماية موحدة.

— تحديد تدابير حماية تكون قابلة للتطبيق ومعترفا بها ومطبقة.

٢-١-١ ان معالجة المشكلة بشكل كامل تعني تغطية جميع الجوانب التي قد يكون لها أثر على الأمن بما في ذلك: اتصال نظام الكمبيوتر بالعالم الخارجي، والتوصيلات الداخلية (بين المواقع على شبكة الانترنت) والاستخدام، والتشغيل وصيانة أجهزة الكمبيوتر، والتغيرات الفنية والوظيفية، وتنظيم الموارد البشرية ومسؤولياتها، وادارة أمن الحوادث أو الوقائع. وبغية أن تكون التغطية شاملة ينبغي أن يؤخذ في الاعتبار جميع العناصر في نظام المعلومات التي لها "مقتضيات سلامة" أو التي قد يؤثر الانتهاك الأمني على أداء مهام الملاحة الجوية بها.

٢-١-٢ ينبغي أن تكون تدابير الحماية في نظام الكمبيوتر موحدة. فليس المستوى الفعال لحماية نظام الكمبيوتر الا بمثابة أوهن حلقة. لذا يكون من المجدي محاولة تطبيق تدابير حماية شديدة الاعاقة والتكلفة على جزء من النظام اذا ترك جزء آخر له نفس درجة الحساسية بقدر ضئيل من الحماية.

٢-١-٣ ينبغي أن تكون تدابير الحماية قابلة التطبيق وينبغي أن تأخذ في الاعتبار القيود وطبيعة السياق الخاصة. فعند تحديد القواعد الأمنية، تنبغي مراعاة التكنولوجيا المستخدمة والقيود على أمن التشغيل وعادات وممارسات المنتفعين

والمشغلين، الخ. وأخيرا بغية تطبيق هذه القواعد فعلا، فانه من الضروري أن يقبلها مشغلو نظام الكمبيوتر والمنتفعون به، وأن يكونوا على دراية بها، وأن تكون قابلة التطبيق مثل القواعد القائمة لتشغيل واستخدام النظام.

٢-٢ أخذا في الاعتبار جميع هذه العوامل، سعت فرنسا لاضفاء المنحة الرسمية على سياسة عامة رفيعة المستوى لأمن أجهزة الكمبيوتر. ويهدف هذا المشروع، المسمى *سياسة أمن أجهزة كمبيوتر ادارة الملاحة الجوية* (PSINA)، الى تعريف القواعد العامة لأمن أجهزة الكمبيوتر بالنسبة لجميع نظم "التشغيل" للملاحة الجوية التي تشكل جزءا من نظام معلومات مراقبة الحركة الجوية.

ينبغي أن ترد هذه السياسة العامة للأمن في وثيقة تحتوى على الفصول التالية:

— أهداف وحدود سياسة أمن أجهزة كمبيوتر ادارة الملاحة الجوية: تعريف يستخدم لنظام المعلومات، والمبادئ المعتمدة، والتهديدات التي يتم التعامل معها، ووضع هذه السياسة مقابل القواعد القائمة الأخرى.

— تصنيف مكونات نظام المعلومات: تعرف أربعة مستويات من الحساسية بالنسبة للمكونات الوظيفية والمادية لنظام المعلومات، مع معايير لتصنيف مكونات مختلف المستويات. ويجري التصنيف على ثلاثة جوانب: التوفر والتكامل والسرية.

— توصل المنتفع لنظام المعلومات: قواعد الخلوص الأمني، بالنسبة للاعتماد والتوثيق وامكانية تقفي الاجراءات وللاستخدام عندما يكون الموظفون الخارجيون عاملين بالهيئة العامة للطيران المدني.

— الحماية المادية: قواعد لحماية وسائط المعلومات الحساسة (الوسائط المنقولة أو المحمولة، الخ)، وحماية نظم أجهزة الكمبيوتر وموقعها المادية.

— صيانة وادارة نظام المعلومات: قواعد الخلوص الأمني، والتحقق من موظفي الصيانة، وتعيين فنيين خارجيين للصيانة، وامكانية متابعة عمليات صيانة وادارة النظام.

— توصيل النظام وتبادل البيانات داخل نظام المعلومات: اعتماد "مناطق جديرة بالثقة" تحدد جوانب وقواعد أمنية موحدة لاستخدام الشبكات الخاصة والعمومية للتوصيل الداخلي.

— التوصيل بهيئات خارجية وتبادل المعلومات معها: قواعد للتوصل لنظام معلومات من الخارج والتوصل لهيئات خارجية عن نظام المعلومات، وقواعد لاستخدام الشبكات العمومية أو الشبكات الخاصة بالتوصيل الخارجي، وقواعد لاصدار واستقبال بيانات أجهزة الكمبيوتر فيما بين نظام المعلومات والهيئات الخارجية.

— تطور نظام المعلومات: اعادة تقييم تصنيف مكونة ومستويات السلامة كلما تم تعديل نظام المعلومات، وقواعد لتكامل مكونات جديدة أو سحب المكونات القديمة.

— الوقائع والحوادث الأمنية: تعريف حادث أو واقعة أمنية وتصنيف الوقائع والكشف عنها، والاجراءات التي ينبغي أن تتخذ عند الكشف عن واقعة أمنية، وقواعد الاتصال الداخلي والخارجي بشأن الوقائع

والحوادث الأمنية، وتعريف مبادئ الجزاءات والاجراءات المطبقة على منتهكي النظام داخل الهيئة العامة للطيران المدني وخارجها.

— تنظيم الموارد البشرية المرتبطة بأمن نظام المعلومات: وعي المنتفع بالمسائل المرتبطة بالأمن/السلامة، والوعي فيما بين صانعي السياسة بالمسائل الأمنية، وتخويل مسؤولي "الأمن"، وقواعد لادارة وصيانة الأمن، الخ.

٢-٣ بغية ضمان أن القواعد الواردة تحت هذه السياسة الأمنية تكون قابلة التطبيق وأن يكون العاملون بنظام المعلومات على دراية مباشرة بها، تم تكوين مجموعة عمل وكلفت بمهمة تصميم اقتراح لهذه السياسة. وتتكون مجموعة العمل من ممثلي العديد من العاملين بخدمات الملاحة الجوية. اضافة الى ذلك بغية ضمان أن سياسة أمن أجهزة كمبيوتر ادارة الملاحة الجوية يدركها العديد من المشغلين والمنتفعين، فانها تعتمد من قبل لجنة اشرافية ترأسها هيئة الملاحة الجوية، مما يضمن ضرورة التطبيق.

٢-٤ ترد أدناه بعض الأمثلة على القواعد الأمنية المصممة في اطار سياسة أمن أجهزة كمبيوتر ادارة الملاحة الجوية.

— يجب أن يخول أي توصيل بنظم خارجية رسميا من قبل المسؤول الأمني استنادا الى ملف الأمن الذي ترد به بوضوح نتائج دراسة التهديدات التي أجريت من قبل.

— يجب التحقق الكترونيا من أي توصيل بالخارج. والغرض الرئيسي من ذلك هو ضمان أنه لا يتم التوصل في أي وقت الا الى الخدمات المخول بها لمثل هذا التوصيل وأن المراسلين المخولين فقط هم الذين يستطيعون استخدامها (المنتفعون أو النظم)، الخ. كذلك، ينبغي أن يتيح التحقق ضمانا بأنه لا يمكن استخدام الا الخدمات الفنية (مثل بروتوكولات الشبكة) اللازمة بوجه حصري للخدمات الوظيفية المخولة من خلال التوصيل.

— يمنع بالنسبة لمعظم العناصر الحساسة من نظام المعلومات، اجراء أي توصيل باستخدام الشبكات العمومية (RTC، الانترنت، الخ.).

٣- استراتيجية تطبيق الطريقة المعتمدة

٣-١ نظرا لنطاق مشروع سياسة أمن أجهزة كمبيوتر ادارة الملاحة الجوية، وبغية التعامل تدريجيا مع جميع جوانبها، تم تحديد بعض الأولويات فيما بين الأهداف.

الهدف الأول هو ضمان محيط نظام معلومات الملاحة الجوية بحيث يتم التعامل مع التهديدات الخارجية. ويتم ذلك بتعريف الوظائف والقواعد الأمنية التي ينبغي أن تكون مطبقة عند حدود نظام المعلومات.

ما أن يتم حماية هذا المحيط، سوف يكون التعامل مع الأمن الداخلي متاحا. ويصعب تعريف الاستجابة للتهديدات الداخلية كما تكون وسائل المكافحة كبيرة، نظرا لاستحالة "اغلاق" النظام بأكمله، فينبغي أن يكون نظام المعلومات قابلا للاستخدام ويتسم بفعالية، لذا فليس من الممكن اعتماد تدابير حماية شديدة وبسيطة نسبيا مثل تلك المستخدمة ضد التهديدات الخارجية. وذلك هو أحد الأسباب الرئيسية التي أدت الى الانتباه الى هذا الجانب بعد التعامل مع التهديدات الخارجية أولا.

٢-٣ والهدف النهائي ، من خلال هذه الأهداف المتتالية، هو استطاعة توفير أمن "راسخ" لنظام المعلومات، ذي محيط دفاعي يستخدم تكنولوجيا المراقبة والأمن، يعني بالشبكات وتوصيل الشبكات، وآلية دفاع داخلية تستخدم تكنولوجيا أمنية ترتكز على الشبكة الداخلية وعلى النظم ذاتها.

٤- الخلاصة

٤-١ تواصل فرنسا العمل حاليا على تعريف شكل مبدئي لسياستها لأمن أجهزة الكمبيوتر. وصاغت مجموعة العمل اقتراحا لوضع الفصول الأولى كحجر الأساس لهذه السياسة (أهداف وحدود السياسة، قواعد تصنيف مكونات نظام المعلومات)، كما تواصل حاليا عملها للتوصيل بالهيئات الخارجية. وسوف يعرض هذا الاقتراح المبدئي عما قريب على اللجنة الاشرافية.

٤-٢ ما أن يضاف الى هذه الفصول المبدئية، فصل عن تنظيم الموارد البشرية وأمن أجهزة الكمبيوتر، سوف يتاح رسميا تنفيذ الشكل المبدئي لسياسة أمن أجهزة كمبيوتر الملاحة الجوية في الهيئة الفرنسية للملاحة الجوية.

٤-٣ تلك مهمة على الأمد الطويل تستلزم جهدا متواصلا بغية التوصل الى سياسة أمنية شاملة متوافقة مع أهدافها.

٥- الاجراء المعروض على المؤتمر

٥-١ المؤتمر مدعو لما يلي:

أ) الأخذ في الاعتبار التهديدات التي تواجه أجهزة كمبيوتر الملاحة الجوية.

ب) وضع قواعد توصيات لضمان أمن أجهزة الكمبيوتر.

ج) تكليف مجموعة من الخبراء بمهمة وضع دليل عام لمساعدة الدول في تنفيذ سياستها للسلامة والأمن، ويكون ذلك على سبيل المثال في شكل قائمة تشير الى النقاط والأسئلة التي تتطرق اليها سياسة السلامة والأمن، والسبل التي تضمن بها أمن نظام الكمبيوتر.

— انتهـــى —