الفصل الثاني عشر

أمن الحكومة الإلكترونية[1]

1- نشر الوعي الأمني المعلوماتي:

لا يمكن تجنب الأخطار المذكورة وإعتماد سياسات دفاع إلكترونية من دون وعي كامل وشامل لهذا الموضوع الخطير، وإذا لم يستطع رأس الهرم من رجالات الدولة ومدراء القمة في الحكومة الإلكترونية أن يستوعبوا تلك الحقيقة فمن غير الممكن لمن دونهم من الموظفين أن يأخذوها على محمل الجد ويعطوها الاهتمام الكافي لدرء مخاطرها. وبناءً عليه من المهم، بل من الضروري، أن تقوم الحكومة الإلكترونية بحملة توعية عامة حول أمن البلاد الإلكتروني تشمل رأس الدولة وصولاً إلى موظفيها وجمهور المواطنين وتشرح لهم المخاطر الأمنية الإلكترونية وكيفية تفاديها وما هي الإجراءات التي قامت بها الحكومة في هذا المجال ومن الممكن إصدار نشرة إعلامية (مجلة، جريدة، تلفزيون...) شهرية خاصة بهذا الموضوع.

2- الاستراتيجيات التنظيمية والهيكلية:

بما أن موضوع الأمن الإلكتروني سوف يمس أمن البلاد بشكل عام، فمن المهم أن تقوم الحكومة بإجراءات وقائية تتناسب مع ذلك الموضوع ومنها ما هو على المستوى التنظيمي والهيكلي، إذ لا يجوز إعطاء مسؤولية الأمن الإلكتروني لمجموعة من الأشخاص داخل الدولة كجزء إضافي من مهامهم ولا بد من إنشاء تشكيلات خاصة بالأمن الإلكتروني قد تكون تابعة لأجهزة الدولة الأمنية بحيث يكون تطوير الأمن الإلكتروني ورسم سياسات الدفاع والهجوم الإلكتروني في صلب مهامها وقد نذكر على سبيل المثال وحدة الأمن الإلكتروني ووحدة الرقابة الأمنية الإلكترونية التي سوف تتأكد من أن جميع إدارات الدولة تقوم بتنفيذ إجراءات الوقاية الأمنية المقررة والمرسومة من قبل الدولة.

---

[1] لمزيد يمكن العودة إلى: http://www.egovconcepts.com/getContent.do?cid=31 |أمن الحكومة الإلكترونية|~~~|26-8-2008

لمجموعة من الأشخاص داخل الدولة كجزء إضافي من مهامهم ولا بد من إنشاء تشكيلات خاصة بالأمن الإلكتروني قد تكون تابعة لأجهزة الدولة الأمنية بحيث يكون تطوير الأمن الإلكتروني ورسم سياسات الدفاع والهجوم الإلكتروني في صلب مهامها وقد نذكر على سبيل المثال وحدة الأمن الإلكتروني ووحدة الرقابة الأمنية الإلكترونية التي سوف تتأكد من أن جميع إدارات الدولة تقوم بتنفيذ إجراءات الوقاية الأمنية المقررة والمرسومة من قبل الدولة.

٣- تطوير الاتفاقات الأمنية الخارجية:

لا يوجد دولة في العالم لا تملك اتفاقات أمنية ثنائية أو جماعية مع الدول الخارجية، ومن المفيد أن يتم تطوير تلك الاتفاقات الأمنية لكي تشمل قضايا ومواضيع الأمن الإلكتروني وأوجه التعاون المحتملة، وعلى سبيل المثال قد تتعاون الحكومة مع حكومات خارجية لمنع الاعتداء الإلكتروني الصادر من أراضي تلك الدول وعبر شبكاتها وفي المقابل من الممكن أن يتم تبادل الخبرات الامنية الإلكترونية مع تلك الحكومات.

٤- استراتيجية الترغيب والترهيب:

ويشتمل الترغيب هنا على عدة نقاط ومنها تشجيع المواطنين على الإبلاغ عن محاولات الاعتداء الإلكتروني بدون أن يتم الكشف عن المخبرين ويمكن للدولة أن تعمد إلى تخصيص خط هاتف ساخن (**Hotline**) من أجل استقبال ملاحظات المواطنين في هذا المجال، من جهة أخرى، ينبغي على الحكومة أن تضع العقوبات الرادعة لمرتكبي الجرائم الإلكترونية بحيث تقوم بإرهابهم قبل أن يفكروا بإرهابها ومحاولة الاعتداء إلكترونياً عليها، وفي هذا المجال سيأتي الدور الحيوي للهيئات التشريعية في الدولة من أجل سن القوانين الرادعة المناسبة.

٥- اعتماد مفاتيح التشفير:

تعتمد تكنولوجيا التشفير الحديثة على النظرية التالية: تمتلك كل جهة أو فرد مفتاحين لتشفير وفك تشفير البيانات، المفتاح الاول وهو المفتاح الخاص

ويكون فقط بحوزة الجهة المخولة، والمفتاح الثاني وهو المفتاح العام ويتم نشره على الإنترنت أو على شبكة الحكومة الإلكترونية من أجل استخدامه من قبل الجهات الأخرى لتشفير الملفات والمعلومات المراد إيصالها إلى الطرف الآخر. وعلى سبيل المثال من أجل تشفير المعلومات المرسلة من قبل المواطن إلى دائرة الآليات من أجل تسجيل سيارته، فإن المواطن يستخدم المفتاح العام الخاص بدائرة الآليات لتشفير المعلومات قبل إرسالها وتستخدم الدائرة مفتاحها الخاص لفك تشفير المعلومات بعد استقبالها، وتدعم هذه التقنية مستويات تشفير عالية تصل إلى ١٢٨ بت (**bits** ١٢٨) وهو ما أثبت فعاليته ضد محاولات الكسر.

وباستخدام نفس التقنية، سوف يصبح الإمضاء الإلكتروني حقيقة تقنية واقعية، ولكن سوف تحتاج الدوائر وأجهزة الدولة إلى آلية لإصدار وإدارة المفاتيح العامة والخاصة وهذا ما اتفق الجميع على تسميته : " البنية التحتية للمفاتيح العامة **Infrastructure Public Key**".

٦- الهوية الإلكترونية الموحدة:

موضوع الهوية الإلكترونية ووسائلها من المواضيع الجديدة على ساحة النقاش الإلكترو- حكومي وهو لم يصل إلى مرحلة النضج الكامل بالرغم من إدعاءات الكثير من مزودي البرامج بوجود حلول مناسبة، ومجمل القصة هي أن الحكومة المادية قادرة على التعرف على مواطنيها من خلال الباسبور أو الهوية الورقية ولكن كيف ستتمكن الحكومة الإلكترونية من التعرف إلى مواطنيها؟ ببساطة يجب أن تكون هناك هوية رقمية أو إلكترونية قادرة على التعريف عن الأشخاص وغير قابلة للنقل من شخص إلى آخر وأمينة وموثوقة. وتدرس بعض الحكومات إمكانية استخدام مكونات مادية (أجهزة صغيرة) وليس فقط مكونات منطقية (برامج) لمعالجة كل الجوانب المحيطة بالهوية الإلكترونية.

٧- تقنية الترخيص الإلكتروني:

سوف تخدمنا الهوية الإلكترونية للتعريف عن أنفسنا لدى الحكومة

الإلكترونية وبالتالي الولوج داخل الحدود الإلكترونية للبلاد ولكن هذا لا يعني أننا سوف نصبح في مقام يسمح لنا بتنفيذ وطلب جميع الخدمات الإلكترونية، فبعض الخدمات سوف تكون مقصورة على الرؤساء وغيرها خاص بالمؤسسات وأخرى خاصة بالأفراد وهكذا وباختلاف الناس ومقاماتهم سوف تختلف درجات الترخيص ونطاقها وعلى سبيل المثال يمكن للحكومة أن تعطي تراخيص البحث عن معلومات تجارية لأصحاب المؤسسات المسجلة لدى الدولة والتي تدفع الضرائب بشكل منتظم ويمكن إصدار الترخيص الإلكتروني الخاص باستخدام أجهزة الأمن والعسكر للأفراد المولجين بهذه المهام. من ناحية أخرى، فإن تقنية الترخيص الإلكتروني قد تستخدم للمحافظة على خصوصية معلومات المواطن والمؤسسات فمن غير الصروري للشخص الحاصل على رخصة إلكترونية لإجراء خدمة معينة أن يكشف كافة معلوماته الشخصية الموجودة في الهوية فقد يحتاج إلى تقديم معلومات الرخصة والتي عادة ما تحتوي على أدنى حد مقبول من معلومات.

٨- تشفير المعلومات المنقولة والمحفوظة:

لا يمكن غض النظر عن أمن وسرية المعلومات التي تنتقل من طرف إلى آخر عبر شبكة الإنترنت وتركها عرضة لعيون المتنصتين، ومن الواجب اعتماد تقنيات تشفير عالية بحيث تظهر تلك المعلومات بصورة مبهمة تماماً لكل من يحاول التنصت عليها عبر الشبكة السلكية أو اللاسلكية وأحد التقنيات المستخدمة في هذا المجال هي تقنية "SSL" المتوفرة عالمياً وفي معظم البرامج والأنظمة الإلكترونية هذا على صعيد المعلومات المنقولة وينبغي إتخاذ نفس الإجراءات بالنسبة للمعلومات الحساسة المحفوظة في الأجهزة بحيث يتم حفظها وهي مشفرة.

٩- تسجيل الأثر الإلكتروني:

تحتاج الرقابة الإلكترونية اللاحقة إلى معلومات تستند إليها لمعرفة من فعل ماذا ومتى من أجل التدقيق في الأعمال المريبة ومساءلة الأشخاص المسؤولين عنها، لذلك يكون من الضروري أن تعمد الحكومة الإلكترونية إلى إنشاء خدمات

لتسجيل الأثر الإلكتروني لطالب الخدمة وعلى سبيل المثال يمكن تسجيل معلومات عن اسم المستخدم وتاريخ طلب الخدمة ووقتها وعنوانه على الشبكة والبلد الذي طلب منه الخدمة بالإضافة إلى عدد محاولاته للدخول إلى الشبكة وستكون جميع هذه المعلومات بخدمة قسم الرقابة الإلكترونية لاحقاً.

كلمات مرور معقدة وديناميكية: لقد تكلمنا سابقاً عن إمكانية توليد كلمات السر إلكترونياً وما هي التقنيات المستخدمة لذلك، ومن أجل تفادي هذا الأمر من الضروري أن تكون كلمات السر تطابق الحد الأدنى لمواصفات الأمن والسرية بحيث تكون طويلة كفاية ولا تستخدم الكلمات المفتاحية أو أسماء العلم أو الحيوانات أو الكلمات التي يحتمل وجودها في معاجم اللغة، ويمكن زيادة تعقيد هذه الكلمات بجعلها تتغير اوتوماتيكياً مع مرور الوقت عليها.

١٠- محاكاة أساليب الهجوم الإلكتروني :

ويسمى هذا الأسلوب في بعض الأحيان بالمناورات الأمنية الإلكترونية وتعمل خلالها أجهزة الأمن الإلكتروني على القيام بهجوم تجريبي غير ضار على أنظمة إدارات الدولة المختلفة للتحقق من صلابتها ومقاومتها وقد يتم هذا الهجوم بدون سابق إنذار للتأكد من فعالية أجهزة الحماية ومستوى تطبيق الإدارات الحكومية لمعايير الأمن الإلكتروني. الحماية المادية للأجهزة والأنظمة كما في حالة بقية الأجهزة والإدارات الحكومية حيث تخصص الدولة فرق حماية مكونة من عناصر الشرطة والأمن، تحتاج مواقع الحكومة الإلكترونية وأماكن تواجد أنظمتها إلى حماية أمنية للتأكد من عدم تجرؤ أطراف عدوة على العبث والتخريب وتدمير المكونات المادية للحكومة الإلكترونية وقد ينفع من فترة إلى أخرى إجراء مسح راداري لاسلكي للتأكد من عدم وجود أجهزة تنصت إلكترونية في نطاق عمل الحكومة الإلكترونية.

يوجد العديد من تقنيات الدفاع الإلكتروني على المستوى التفصيلي وقد ذكرنا أهمها مع عدم إغفالنا للاستراتيجيات الداعمة لوجود حكومة إلكترونية أمينة وموثوقة.