الفصل الحادي عشر

المخاطر الإلكترونية المحيطة بالحكومة

هل فكرت يوماً ما يمكن أن يحصل إذا تم اختراق أنظمة الحكومة الإلكترونية؟ هل تأملت بمقدار الخسارة التي يمكن أن تلحق بمفهوم النموذج الإلكترو ـ حكومي من جراء ذلك؟ ماذا عن خصوصية معلوماتك كمواطن أو صاحب عمل؟ هل ستكون سعيداً بكشف بياناتك الصحية والاجتماعية والمالية والقضائية من قبل مجموعات متطفلة من الناس؟ قبل أن نحاول طرح أدوات الأمن المعلوماتي في الحكومة الإلكترونية يتوجب علينا تحليل المخاطر التي قد تنجم من جراء عدم الاهتمام بموضوع أمن وسرية المعلومات **ويشمل تحليل المخاطر جوانب عديدة منها**: الدوافع والنوايا ومصادر الخطر بالإضافة إلى وسائل الهجوم الإلكتروني وكيفية تجنبها باعتماد إجراءات الوقاية والدفاع الإلكتروني وما ينتج عنه من كلفة اقتصادية إضافية، ومن المهم أن لا نغفل عن تحديد أصول الحكومة الإلكترونية التي تحتاج إلى جهاز حماية فعّال.

1. مصادر الخطر المحتملة:

تعمل أجهزة الحكومة الإلكترونية في فضاء مفتوح يتداخل فيه جمهورها الخارجي (مواطنين، مؤسسات، حكومات أخرى) مع جمهورها الداخلي (وزراء، موظفين،...) وتصبح فيه أجهزة تلك الحكومة عرضة للعديد من أنواع الهجوم تحت دوافع مختلفة، ومن الممكن أن تتم مهاجمة أنظمة الحكومة الإلكترونية من داخلها وعبر أحد الموظفين الغاضبين أو من الخارج عبر مجموعات الهاكرز أو أجهزة الاستخبارات في بلدان عدوة وصولاً إلى المؤسسات التجارية الساعية إلى الحصول على معلومات تجارية تنافسية.

2. خطر المستخدم الشرعي:

المستخدم الشرعي هو المواطن أو صاحب المؤسسة الحاصل على إجازة من الحكومة في سبيل استعمال خدماتها الإلكترونية، وتكون الإجازة في معظم

دوافع مختلفة، ومن الممكن أن تتم مهاجمة أنظمة الحكومة الإلكترونية من داخلها وعبر أحد الموظفين الغاضبين أو من الخارج عبر مجموعات الهاكرز أو أجهزة الاستخبارات في بلدان عدوة وصولاً إلى المؤسسات التجارية الساعية إلى الحصول على معلومات تجارية تنافسية.

٢. خطر المستخدم الشرعي:

المستخدم الشرعي هو المواطن أو صاحب المؤسسة الحاصل على إجازة من الحكومة في سبيل استعمال خدماتها الإلكترونية، وتكون الإجازة في معظم الأحوال عبارة عن تأكيد هوية المستخدم إلكترونياً عبر شبكة الحكومة بعد أن يكون قد تم تسجيله سابقاً، وقد يحاول هذا المستخدم أن يوظف إمكانية دخوله إلى شبكة الحكومة من أجل تخريب الخدمات المتاحة في نطاق إجازته، وقد يحصل في بعض الأحيان أن هذا المستخدم يتمكن من الحصول على معلومات لا تخصه في حال وجود عيوب فنية في تصميم الخدمة الإلكترونية المتاحة له. من ناحية أخرى، من الممكن لهذا المستخدم أن ينكر قيامه بخدمات معينة في حين تؤكد أنظمة الحكومة قيامه بها.

٣. خطر موظفي الحكومة الإلكترونية:

وتشكل هذه المجموعة خطراً كبيراً على أنظمة الحكومة في حال أرادت ذلك، ونظراً لما يملكه بعض الموظفين في الحكومة الإلكترونية من حقوق دخول إلى الشبكة وإطلاع على الأنظمة فمن الممكن لهم أن يقوموا بأعمال تخريبية تؤدي إلى إيقاف الخدمة الإلكترونية وقد يكون هؤلاء الأشخاص مدفوعين بدوافع مادية أو نفسية أو لمجرد عدم الرضا عن وضعهم الوظيفي داخل الحكومة.

٤. خطر أجهزة المخابرات الخارجية:

من الممكن أن تعمد أجهزة المخابرات الصديقة أو العدوة على حد سواء إلى الحصول على معلومات عن أشخاص أو مؤسسات أو حتى أجندات الحكومة الداخلية عبر تنفيذ هجمات إلكترونية بهدف اختراق النظام الأمني المعلوماتي

للحكومة والدخول إلى مختلف الأنظمة فيها وقد توظف أجهزة المخابرات في هذه العملية كفاءات تقنية عالية وقادرة في كثير من الأحيان على اختراق أنظمة الحكومة الهدف.

٥. خطر المؤسسات التجارية:

تسعى المؤسسات التجارية دوماً إلى تحقيق السبق الاقتصادي والإعلامي والتجاري على منافساتها من المؤسسات وقد تحاول هذه المؤسسات أن تخترق أنظمة الحكومة الإلكترونية من أجل الحصول على معلومات عن منافسيها في السوق وقد تلعب أقسام المخابرات التجارية (Business Intelligence Departments) في المؤسسات الكبيرة دوراً خطيراً في هذا المجال وذلك في محاولة منها لإرضاء الإدارة العليا عبر تقديم معلومات تجارية تنافسية تملكها الحكومة ولم يتم نشرها.

٦. خطر المنظمات الإرهابية:

قد تحاول بعض المنظمات الإرهابية فرض أجنداتها السياسية على الحكومة عبر وسائل إرهابية عدة ومنها الحرب الإلكترونية، وربما تسعى إلى تعطيل خدمات الحكومة الإلكترونية بعد الحصول على مبتغاها منها من خلال هجوم إلكتروني مكثف قد يحدث في فترة زمنية قصيرة نسبياً، ويكمن خطر المنظمات الإرهابية في هذا المجال بكونها تتحرك من منطلقات تدميرية تكون معها مصلحة البلاد العليا نقطة هامشية أمام تحقيق أهدافها.

٧. خطر مزودي البرمجيات والعتاد:

يمتلك مزودو البرمجيات القدرة على التلاعب بالشيفرة البرمجية بحيث يتركون وراءهم ابواباً مفتوحة للأنظمة (Back Door) مما يمكنهم لاحقاً من الدخول إلى تلك الأنظمة بطريقة غير شرعية وتتجاوز بوابات الأمن المتاحة للجمهور، وعلى حد سواء يستطيع مزودو العتاد من أجهزة كمبيوتر وشبكات وغيرها أن يتركوا فيها عيوباً عن قصد بحيث يسهل عليهم تجاوز الإجراءات الأمنية الإلكترونية للحكومة.

٨. خطر الكوارث الطبيعية:

كما تؤثر الكوارث الطبيعية من زلازل وهزات أرضية وصواعق في الحركة العامة لأجهزة الحكومة ومستوى توافر خدماتها، فقد تلحق تلك الكوارث أضراراً كبيرة بأنظمة الحكومة الإلكترونية وقد تؤدي في بعض الأحيان إلى شلّ الخدمات الإلكترونية للحكومة في حال أصابت مواقع تشغيل تلك الخدمات.

٩. خطر عيوب التصميم والتشغيل:

وتشمل عيوب التصميم في مختلف مكونات الحكومة الإلكترونية من الشبكات وطريقة تصميمها إلى البرمجيات المستخدمة وخوارزميات التشفير ومستوياتها وصولاً إلى أساليب وطرق التثبت من الهوية الإلكترونية، وتقاس قوة جدار الأمن الإلكتروني الواقي بقوة الحلقة الأضعف في هذه المكونات بحيث يؤدي كسر تلك الحلقة الضعيفة إلى اختراق الجدار مهما كانت قوة مكوناته الأخرى. إن طريقة تصميم البنية التحتية لخدمات الحكومة الإلكترونية من الممكن أن يشكّل فارقاً مهماً في مستويات الأمن والسرية لتلك الخدمات، كما تعتمد الخدمات الإلكترونية على مبدأ "التوافرية **(Availability)** "الذي يقول بضرورة توفر الخدمة من خلال بدائل شبيهة في حال تم تدمير الخدمة الأصلية وفي حال لم يؤخذ هذا المبدأ بعين الاعتبار عند تصميم الخدمة فسوف تكون عرضة للانقطاع لاحقاً.

١٠. خطر التناثرية الأمنية:

في كثير من البلدان التي لا تملك مخططاً توجيهياً عاماً **(E -Government Master Plan)** لتطبيقات الحكومة الإلكترونية على مستوى كافة الإدارات الرسمية والوزارات، تعمد إدارات تلك البلدان إلى تطبيق مفهومها الخاص بالأمن والسرية الإلكترونية بدون الأخذ بعين الاعتبار أية معايير أو مقاييس تضمن كفاءة وفعالية تطبيقاتها، ويؤدي هذا الأمر بالتالي إلى نوع من تناثر وتنوع تطبيق مفاهيم الأمن والسرية عبر الإدارات وقد يشكل ضعف تطبيق إدارة أو وزارة واحدة لمبدأ

الحماية والأمن الحلقة الضعيفة في الجدار الواقي مما ينتج عنه بالنهاية اختراق هذا الجدار .

١١. خطر عدم الوعي بالمخاطر:

وأخيراً وربما ليس آخراً، يمثل عدم وعي مدراء القمة وموظفيهم في الحكومة الإلكترونية بالمخاطر المذكورة أعلاه الخطر الأعظم على النموذج الإلكترو-حكومي فالذي لا يعي المخاطر لا يمكن أن يضع خطط الدفاع والطوارئ.

لا يمكن لأي مشروع حكومة إلكترونية أن يزدهر وينجح بدون معالجة الأخطار المطروحة والجوانب المحيطة بها ، وربما من الأفضل للحكومة البقاء في فضائها المادي/الواقعي وعدم الشروع بدخول الفضاء الإلكترو- حكومي في حال لم تتسلح بأدوات الدفاع الإلكتروني المناسبة.