تطوير أنظمة حماية الكمبيوتر في المؤسسات الحكومية

Development of Computer Protection Systems in Government Institutions

مرام صالح محمد الجازي

Maram Saleh Mohammed Al-Jazi

مهندس حاسوب

Computer Engineer

بلديه الاشعري

قضاء أذرح، محافظة معان

المملكة الأردنية الهاشمية

الملخص

تنمو أنظمة المعلومات وتبادل البيانات بين المؤسسات الحكومية بسرعة في جميع أنحاء العالم، ومعها تتزايد التهديدات التي تتعرض لها المعلومات داخل الإدارات الحكومية. في السنوات الأخيرة، يبدو أن البحث في تطوير وبناء أنظمة المعلومات الآمنة في المؤسسات الحكومية فعال للغاية. بناءً على مبادئ نظام المعلومات، يقترح هذا البحث نموذجًا لتوفير وتقييم الأمن لجميع دوائر المؤسسات الحكومية. تبدأ متطلبات أي نظام معلومات بمحيط المنظمة وأهدافها. لم تأخذ معظم التقنيات السابقة في الاعتبار المكون التنظيمي الذي يعمل عليه نظام المعلومات، على الرغم من أهمية هذه الميزة في تطبيق طرق الوصول والتحكم من حيث الأمن. بناءً على ذلك، نقترح نموذجًا لتحسين الأمن لجميع إدارات المؤسسات الحكومية من خلال معالجة القضايا الأمنية في وقت مبكر من دورة حياة النظام، ودمجها مع العناصر الوظيفية طوال دورة الحياة، والتركيز على الجوانب التنظيمية للنظام. الجوانب الأمنية الرئيسية المشمولة هي إدارة النظام، والعوامل التنظيمية، وسياسة المؤسسة، والتوعية والجوانب الثقافية.

Abstract

Information systems and data exchange between governments institutions are growing rapidly all over the world and with it the threats to information within government departments are growing. In recent years, research into the development and construction of secure information systems in government institutions appears to be very effective. Based on the principles of the information system, this paper proposes a model for providing and evaluating security for all departments of government institutions. The requirements of any information system begin with the organization's surroundings and its goals. Most of the previous technologies did not take into account the organizational component on which the information system operates, despite the importance of this feature in the application of access and control methods in terms of security. Based on this, we propose a model for improving security for all government organization departments by addressing security issues early in the life cycle of the system, integrating them with functional elements throughout the life cycle, and focusing on the organizational aspects of the system. The main security aspects covered are system administration, organizational factors, enterprise policy, outreach and cultural aspects.

المقدمة

يعد تطوير البنية التحتية لأنظمة المعلومات أمرًا بالغ الأهمية لتحسين العمل الحكومي، ولكن القضية الرئيسية هي التهديدات والمخاوف الأمنية. هذه مخاوف تتعلق بالخدمات والبنية التحتية، حيث يمثل فقدان البيانات الحكومية، فضلاً عن انتهاك خصوصية المواطنين وسريتهم، تحديًا كبيرًا للمؤسسات الحكومية. الهدف الأساسي من البحث هو تطوير وتنفيذ نموذج لتوفير وتقييم أمن المعلومات في المنظمات. في السنوات الأخيرة، كانت أبحاث المؤسسات الحكومية في تطوير وبناء الأمن الآمن فعالة للغاية. ركزت بعض المساهمات على تكامل الجوانب الأمنية، ولا سيما آليات التحكم في الوصول، أثناء مرحلة التنفيذ، بينما ركزت مساهمات أخرى على تحديد وتحليل متطلبات الأمن. ومع ذلك، لا توجد طريقة لمعالجة المشكلة الكاملة لمتطلبات الأمان وتحولاتها في جميع مراحل دورة حياة نظام المعلومات.

يعتمد أداء العمل في المؤسسة على عوامل مهمة وحاسمة ، مثل التوافر والكفاءة والأمن وجودة المعلومات ووظيفة الخدمة والشفافية، وكل ذلك يساهم في تحسين أداء المؤسسة. إن تطوير وزيادة استخدام الأجهزة المحمولة والإنترنت للوصول إلى البيانات في المؤسسات الحكومية الحساسة يجعلها هدفًا جذابًا لمجرمي الإنترنت. ونتيجة لذلك، فإن اعتماد التكنولوجيا المتقدمة في المؤسسات يتطلب عادة تدريبًا ووعيًا متخصصًا للعاملين لاكتساب مهارات جديدة. ومع ذلك، فقد أدى تطبيق تقنيات المعلومات والاتصالات (ICT) في المؤسسات الحكومية إلى ظهور العديد من التحديات، لا سيما المخاوف المتعلقة بالخصوصية ونقاط الضعف المتعلقة بالقدرة على تزويد المواطنين بإمكانية الوصول إلى كميات كبيرة من البيانات. هناك أيضًا مخاوف بشأن الوصول إلى أنظمة معلومات المؤسسة وخطر الوصول غير المصرح به من داخل المنظمة.

الأمن هو جانب مهم من نظم المعلومات. حيث تطورت أساليب الأمن بطريقة مشابهة لنظم المعلومات. تشترك أنظمة الأمن والمعلومات في الأهداف والوسائل والتحديات، لذا فهي تعتمد على مراجعة المخاطر وتحليلها لتحديد الحماية المقبولة لنظام المعلومات.

يتزايد الاهتمام بالطرق والنماذج لفهم متطلبات الأمن لأنظمة المعلومات. ومن خلال هذا الاهتمام يبدو أن أساليب أمن نظم المعلومات لا يمكن أن تحقق النتائج المطلوبة ما لم تتكامل مع أساليب تطوير نظم المعلومات العامة. أدى التقارب بين المسارين إلى تطوير أساليب واضحة لتوفير ضوابط الأمن والسلامة لأنظمة المعلومات. وفقًا لذلك، تعتبر قضايا أمن المعلومات مسؤولية الإدارة لأنها تؤثر على وضع الشركة في السوق، وينصح هذا البحث المؤسسات باتباع نهج أكثر تقلبًا للمعلومات. تستلزم إدارة الأمن مشاركة الإدارة العليا، وإدارة الموارد البشرية، وتطوير وتنفيذ سياسة أمن المعلومات، والوعي بأمن المعلومات والتدريب، وإشراك صانعي القرار الاستراتيجيين. يناقش البحث الذي أجراه كراولي التدريب على أمن نظام المعلومات والديناميكيات التعليمية. تقدم هذه الورقة أيضًا تخصصًا في أمن نظام المعلومات على مستوى الدراسات العليا تم تطويره باستخدام هذه المعلومات. الغرض من هذه الورقة هو تحديد وترتيب أولويات القضايا الرئيسية التي يتعامل معها كبار مسؤولي المعلومات في الحكومة المحلية، أو يعتقدون أنهم سيتعاملون معها في المستقبل القريب، في مجال إدارة أمن نظم المعلومات.

الإطار النظري

أمن المعلومات

أمن المعلومات هو عملية تحديد المشكلات التي من المحتمل أن تتسبب في حدوث أضرار أو حالات تهديد وتنفيذ الحماية للقضاء على هذه الاحتمالية. سيتم تحقيق هذه العملية من التدابير المضادة من خلال العملية الأمنية.

يمكن الإشارة إلى أمن المعلومات في الحضارات القديمة عندما بدأت الحضارات في اتخاذ نماذج من أجل التواصل بحرية دون التعرض لخطر السمع. على سبيل المثال، بدأ المصريون في تبني علم التشفير في عام 3000 قبل الميلاد بتطبيق الهيروغليفية لإخفاء الكتابات من جهاز استقبال غير مقصود.

أدى تطوير التكنولوجيا الجديدة إلى إنشاء طرق أمنية مختلفة لتأمين المعلومات للأفراد والمؤسسات والجيوش والدول. تختلف هذه الأساليب من حيث السياق؛ استند بعضها إلى قواعد ولوائح وسياسات ومقاربات رياضية، واستند البعض الآخر إلى معرفة تشفير خالصة. منذ زيادة عدد النماذج الأمنية، استمرت التحديات في الزيادة واستمر الباحثون في التحقيق لاكتشاف حلول مختلفة عبر نماذج جديدة وتطوير القائمة مرة واحدة.

علاوة على ذلك، أدى التطور السريع لتكنولوجيا المعلومات والاتصالات إلى ظهور فرص كبيرة لتنفيذ الأدوات والتطبيقات المبتكرة مثل الحكومة الإلكترونية لتحسين جودة الخدمات المقدمة للجمهور من خلال الشبكات العالمية. هذا التطور السريع لا يمكن أن يكون خاليا من المشاكل. يعد أمن المعلومات وخصوصية المستخدم من القضايا الرئيسية التي يجب مراعاتها ومعالجتها من أجل إقناع الناس باستخدام خدمات الحكومة الإلكترونية بسلاسة. لذلك، فإن المسؤولية الحيوية لنظام الحكومة الإلكترونية هي الوفاء بخصائص الأمان الجوهرية؛ التوافر والسرية والمساءلة والنزاهة وضمان المعلومات.

ركز أمن المعلومات من قبل على سرية المعلومات المخزنة إلكترونيًا. إن التطور السريع في حجم هذه المعلومات وتأييد التجارة الإلكترونية داخل المنظمات قد أدى بشدة إلى ضرورة زيادة الأمن لحماية خصوصية هذه المعلومات ومنع أنشطة الوصول غير المصرح بها. هناك حاجة واعدة لتحسين أمن المعلومات والخصوصية والثقة في الحكومة من أجل زيادة الثقة في الحكومة الإلكترونية المعترف بها في البلدان المتقدمة والنامية.

تكامل نظام المعلومات في الحكومة الإلكترونية

تحتاج الحكومة الإلكترونية إلى تعاون داخل المؤسسات بسبب المتطلبات الوظيفية للحجم والموثوقية والتكامل. في سياق مجتمع الحكومة الإلكترونية، يوضح التكامل تلك العمليات التي تنقل المعلومات والخدمات للمستهلكين على جميع المستويات. التطورات في تكنولوجيا المعلومات والاتصالات، وفي القدرة على مشاركة هذه البيانات وتقديمها، تعمل

على تغيير الطريقة التي تتم بها الأعمال في نظام الحكومة الإلكترونية. في المقابل ، تتطور فكرة التكامل وتتوسع بسرعة التغييرات في التكنولوجيا التي تقودها.

هناك العديد من الصعوبات التي تواجه مشاركة مقنعة وفعالة للبيانات بين المؤسسات الحكومية من جهة، وبين الحكومات والشركات والمواطنين من جهة أخرى. تستند هذه التحديات إلى عدم الثقة والشفافية في تصميم نظم المعلومات، إلى القضايا الأخلاقية والقانونية عند دمج نظم المعلومات. هذا يضفي الشرعية على الحاجة إلى نظام أمان شامل يأخذ في الاعتبار مكونات تكامل الأنظمة.

الحاجة إلى الأمن

يتزايد حجم المعلومات الرقمية في العالم، ويتم مشاركة هذه المعلومات الرقمية في جميع أنحاء العالم. قدر تقرير صدر مؤخرًا عن مؤسسة Gartner أن حجم المعلومات التي تتعامل معها المنظمات سيكون أكبر بثلاثين مرة في أقل من عقد من الزمان.

بدأت تأثيرات أنظمة المعلومات على الحياة اليومية تصبح مهمة في أوائل التسعينيات مع إدخال أحد أكثر الاختراعات استثنائية في هذا القرن: الإنترنت. منذ ذلك الحين، أصبح الإنترنت جزءًا لا يتجزأ من الحياة البشرية الحديثة. ومع ذلك، إلى جانب فوائده الرائعة، هناك أيضًا مخاطر تتعلق بالإنترنت، ومعظمها يتعلق بقضايا الأمان. لم يكن إدراك هذا التهديد فوريًا. استغرق الأمر بعض الوقت لفهم مدى الخطر. عانت العديد من الشركات الكبيرة عبر الإنترنت مثل Yahoo و E-bay من العواقب الكارثية لهجمات الشبكات في الماضي القريب. بناءً على هذه العواقب، بدأ النهج العام لقضايا الأمن ينضج. يتم إنتاج وشراء حلول الأمان في جميع أنحاء العالم. ومع ذلك ، وفقًا لتوقعات العديد من المتخصصين في مجال الأمن، لا يمكن القضاء على جميع التهديدات؛ علاوة على ذلك، فإن معدل نمو التهديدات الأمنية سيكون أكبر من نمو الإنترنت. هذا يؤكد على ضرورة الاستثمارات الأمنية في أنظمة المعلومات: أجهزة الكمبيوتر منتشرة في الحياة الحديثة والإنترنت حقيقة لا مفر منها، لذلك يجب اتخاذ تدابير أمنية مناسبة.

في المستقبل، ستحتاج التكتلات والشركات الدولية والمنظمات غير الحكومية والمنظمات الحكومية والمدارس والجامعات والمؤسسات الصغيرة والمتوسطة وحتى الأفراد إلى استخدام أنظمة المعلومات إلى حد ما من أجل تحقيق النجاح في مجالات تخصصهم. من أجل التعامل مع كميات كبيرة من المعلومات، ستصبح المؤسسات أكثر اعتمادًا على تقنيات المعلومات، على الرغم من أوجه القصور والمخاطر الكامنة مثل الانتهاكات الأمنية وسرقة البيانات وفقدان البيانات، المدير الفني (CTO) ومؤسس Counterpane Internet Security، وهو أحد أشهر خبراء الأمن في العالم، وهو متأكد من أنه لا يوجد خيار آخر للشركات سوى ربط شبكاتهم بالإنترنت والمنافسة في العالم الرقمي.

المنافسة بين الشركات التي تخدم عملائها عبر الإنترنت عالية جدًا. من أجل البقاء ، تحاول الشركات تأمين المزايا التنافسية عبر برامجها وموقعها الإلكتروني وأنظمة المعلومات الأخرى. تقديم أفضل خدمة لعملائها قبل أن يصبح منافسوهم أمرًا بالغ الأهمية بحيث لا تركز الشركات في كثير من الأحيان بشكل كافٍ على الميزات المتعلقة بالأمان للبرنامج أو اختبار الأمان من أجل عدم تأخير عملياتهم ، على الرغم من أنهم على دراية بالتهديدات. في بعض الأحيان تتجاهل الشركات الأمن فقط ولا تعتبره مسألة مهمة. ينتج عن هذا الإهمال ترميز خالي من الأمان. يعد الترميز الخالي من الأمان للبرنامج تهديدًا خفيًا ويمكن تغطية هذا التهديد من خلال تدابير أمان الشبكة إلى حد ما، ولكن لسوء الحظ، لا يمكن تغطية التهديدات بشكل كامل.

تحديات أمن المعلومات في الحكومة الإلكترونية

1. أمن الشبكة

مع الحكومة الإلكترونية، تزداد الحاجة إلى الأمن في شبكات الاتصالات، والمرونة ضد هجمات الشبكة (الوصول، والتعديل، والحرمان من الخدمة) ذات أهمية محورية. تتغير التهديدات لأمن الشبكة (الإرهاب الإلكتروني، والتجسس الإلكتروني، والتهديدات المستمرة المتقدمة، والتهديدات المختلطة، وما إلى ذلك) باستمرار حيث يتم اكتشاف نقاط الضعف في كل من الأنظمة المنشأة والمقدمة حديثًا، والحاجة إلى حلول لمواجهة هذه

التهديدات. تشمل التدابير التي تضمن أمان الشبكة جدران الحماية والوكلاء لإبعاد الأشخاص غير المرغوب فيهم، وبرامج مكافحة الفيروسات ومجموعات برامج أمان الإنترنت، ومكافحة البرامج الضارة، والتشفير، والسياج الأمني، فضلاً عن هياكل الكمبيوتر المحسّنة، وما إلى ذلك.

2. الهوية

تثير مسألة تحديد الهوية العديد من الأسئلة المهمة المتعلقة بقضايانا. في مجال المشتريات، تعد مسألة التحقق من هوية الشركة أمرًا مهمًا، ليس فقط للتأكد من أن الشركة هي من يدعي العمل عند إبرام صفقة، ولكن أيضًا على المدى الطويل. هل ستكون الشركات قادرة على تحمل المسؤولية في المستقبل من خلال التوقيعات الرقمية التي استخدمتها عند إبرام الصفقات؟ هل هناك خطر من أن معلومات الهوية هذه قد تُفقد أو تُسرق أو تُحذف أو تصبح غير آمنة، وهل هذا ينطوي أيضًا على خطر عدم الالتزام بالاتفاقيات لأنه قد تكون هناك شكوك حول صحة تحديد الشركة؟ فيما يتعلق بجوازات السفر البيومترية، أثيرت شكوك حول ما إذا كانت البيانات البيومترية ستكون موثوقة وما إذا كانت ستتم حمايتها من المجرمين الذين يرغبون في تزوير البيانات وجوازات السفر البيومترية. على هذا النحو، فإن فعالية البيانات البيومترية ستكون مسألة سيتم تناولها. في الصحة الإلكترونية، تمثل مشكلة كيفية تعريف المرضى والأطباء وغيرهم من المهنيين الصحيين أنفسهم مشكلة. هل سيتم استخدام رمز PIN؟ أو بطاقة ذكية؟ ما هي وسائل التعريف المطلوبة لإنشاء بيانات المرضى وتعديلها والوصول إليها ومن المسؤول عن صحة السجل؟

3. سهولة الاستخدام

تركز قابلية الاستخدام على جعل التطبيقات والخدمات سهلة الاستخدام للأشخاص. ترتبط مسألة قابلية الاستخدام بالمخاوف الأمنية لأن محاولات زيادة أمان البيانات قد تقلل من قابليتها للاستخدام. فيما يتعلق بهذا المشروع، تتناول قابلية الاستخدام أيضًا كيفية استخدام البيانات ومن يستخدم البيانات. على هذا النحو، فإن

قابلية الاستخدام تستلزم تركيزًا قويًا على قضايا الثقة في الحكومة الإلكترونية التي يستحضرها التفاعل بين الجهات الفاعلة التي تتحكم في الخدمة أو تقدمها أو تستفيد منها. في المشتريات، تظهر مشاكل قابلية الاستخدام من المتطلبات الوطنية التي تتطلب ملفات الشركة، أو من مخططات التوقيع الإلكتروني. في الصحة الإلكترونية، تمتلك الأنظمة الصحية المختلفة أنظمة مختلفة لحفظ السجلات، وحتى داخل هذه الأنظمة، قد يكون هناك أيضًا أنظمة مختلفة للاحتفاظ بالسجلات. علاوة على ذلك، هناك مشكلة جعل أنظمة الاحتفاظ بالسجلات رقمية بالكامل والتأكد من أن الموظفين والمرضى يعرفون كيفية استخدام النظام الرقمي.

صلاحية التحكم صلاحية الدخول

ستكون جميع الأنظمة الإلكترونية التي تحتوي على معلومات حساسة ذات أهمية للأشخاص الذين قد يرغبون في استخدام هذه المعلومات لأغراض شائنة. ونتيجة لذلك، يلزم التحكم في الوصول إلى هذه الأنظمة من أجل منع الاستخدام غير المرغوب فيه للمعلومات المخزنة. التحكم في الوصول بشكل عام له تعريف واسع جدًا حيث يمكن أن يكون أي شيء من قفل السيارة إلى الرمز السري لبطاقة الائتمان الخاصة بك. لكن الوظيفة الأساسية هي رفض الوصول غير المرغوب فيه. في مجال الحكومة الإلكترونية، ستكون وسائل التحكم في الوصول بشكل أساسي إلكترونية أو مادية (الجدران، والبطاقات، والأجهزة المقاومة للعبث)، ويمكن أن تكون الأنظمة أي شيء من قواعد بيانات معلومات المواطن، والسجلات الصحية، والحسابات المصرفية، والعقود للتحكم في البنية التحتية مثل الكهرباء والطرق والمطارات، إلخ.

إدارة أمن المؤسسة

- الممارسات الشائعة

يوجد تخطيط مشترك ومجموعة إجراءات للمؤسسات التي لديها مجموعة من منتجات الأمان ، والتي تُستخدم بشكل عام عند إنشاء شبكة. أصبح هذا التصميم معيارًا واقعيًا لأي شركة مدركة للأمان. توجد منتجات مثل جدران الحماية وبرامج مكافحة

الفيروسات وأنظمة اكتشاف منع التطفل (IDS / IPS) في كل شبكة تقريبًا. إلى جانب هذه المنتجات الفعلية، أصبحت المنتجات الجديدة مثل مكافحة برامج التجسس وبرامج مكافحة البريد العشوائي وأدوات إدارة التصحيح منتشرة على نطاق واسع.

- صعوبات في التوسيع

استجابة للتهديدات الجديدة ونقاط الضعف ، يتم إنتاج برامج أمنية جديدة وإصلاحات. إذا لم يتم اتخاذ احتياطات إضافية ، فقد يتم استغلال نقاط ضعف جديدة واستخدامها ضد أصول أنظمة المعلومات الخاصة بالشركات. يعد سوق مكافحة الفيروسات مثالًا جيدًا على تطور أسواق الأمان. عند تقديمها لأول مرة ، كان يُعتقد أن برامج مكافحة الفيروسات تغطي المشكلات المتعلقة بالفيروسات. ومع ذلك ، في السنوات الأخيرة ، مع ظهور البريد العشوائي وبرامج التجسس والبرامج الإعلانية والتصيد الاحتيالي كتهديدات جديدة ، أصبح من الواضح أن هذه المناطق التي بها مشكلات لا تغطيها المجموعة الحالية من منتجات الأمان بما في ذلك برامج مكافحة الفيروسات. يتم توفير حلول لمناطق المشكلات الجديدة إما في شكل إضافة إلى المنتجات الحالية مثل وحدة البريد العشوائي لمنتج مكافحة الفيروسات أو في شكل برنامج جديد تمامًا مثل مرشح المحتوى.

هناك دورة إنتاج في الأمان، تبدأ باكتشاف الثغرات الأمنية. في الخطوة التالية من الدورة، يتم عمل تصحيحات وإصلاحات للمنتجات الحالية. إذا كانت الثغرة الأمنية معقدة للغاية بحيث لا يمكن تغطيتها بواسطة التصحيح، فسيتم إنتاج جهاز أو برنامج أمان جديد. في الخطوة الأخيرة من الدورة، تشتري المؤسسات برامج أمان جديدة أو تقوم بتحديث نظامها وفقًا لذلك. تبدأ الدورة من جديد باكتشاف ثغرة أمنية جديدة وتستمر بطريقة مماثلة. في نهاية كل دورة، تصبح شبكة المؤسسة مزدحمة ببرنامج جديد أو صندوق أمان أو أداة جديدة.

- معالجة السجل

جميع المعدات الأمنية لديها إمكانيات التسجيل. هذه القدرات ، إذا تم التعامل معها واستغلالها بشكل صحيح ، تكون مفيدة جدًا في إدارة الشبكة ومعالجة الحوادث ومهام

الشبكات الأخرى. من ناحية أخرى ، يمكن أن يصبح الأمر مرهقًا ويصبح عبئًا على المسؤولين إذا لم يتم إعطاء أهمية كافية لإدارة السجل. أشار إلى أهمية السجلات وإدارة السجلات:"بغض النظر عن أنواع الحلول الأمنية التي يتم تنفيذها ، يعد التسجيل أمرًا بالغ الأهمية لضمان أن تنفيذها يعمل بسلاسة بالإضافة إلى مراقبة ما يحدث في البيئة."

- مشكلة التعقيد وصعوبات الإدارة

تنمو الشبكات مع إضافة منتجات أمان جديدة، لها وحدات تحكم إدارية وشاشات وسجلات خاصة بها ليتم التعامل معها بواسطة مسؤول الأمان. هذه الأجهزة المختلفة لها مواقع مختلفة في تخطيط الشبكة. يتم إنتاج معظمها من قبل شركات مختلفة ويهدف إلى إدارتها بطريقة لامركزية. وبالتالي، فإن الإدارة اللامركزية ومعالجة السجلات هي الإعداد الافتراضي في العديد من المنظمات. نتيجة لذلك، لا يمكن التحقق من الارتباطات بين سجلات هذه الأنظمة المختلفة بسهولة، ولا يمكن اكتشاف العلاقات بينها بسهولة. لا يمكن اكتشاف المصادر والوجهات والأسباب والأساليب والعواقب للتدخلات المحتملة كما هو متوقع، وبالتالي قد لا تتحقق الفوائد المفترضة لمنتجات الأمان.

أصبحت إدارة أمان النظام في مؤسسة أكثر تعقيدًا نظرًا لأن مسؤولي الأمن غارقون في عدد كبير جدًا من السجلات القادمة من أجهزة أمان مختلفة مثل جدران الحماية وأنظمة اكتشاف / منع التطفل وأنظمة مكافحة الفيروسات وأجهزة التوجيه والمحولات وغيرها ملحقات. كل هذه الأجهزة المختلفة لها وحدات تحكم إدارية وواجهات وطريقة لعرض السجلات. تتطلب جميعها من المسؤولين قضاء بعض الوقت في إدارة الجهاز وتحليل سجلات الجهاز، وهو عامل قد يقلل من كفاءة المسؤولين. ومع ذلك، فإن التعامل مع الحوادث وإدارة الأمن، وهي المهام الرئيسية لمسؤول الأمن، تتطلب مراجعة جميع السجلات بطريقة منتظمة وفي الوقت المناسب والاستجابة السريعة من أجل منع أي نوع من محاولة اختراق الشبكة المعادية، والتعافي من الحادث في أقرب وقت ممكن.

على الرغم من توفر أجهزة وبرامج الإدارة المركزية المحسّنة اليوم ، إلا أنها باهظة الثمن ولا تزال تتطلب قدرًا كبيرًا من التفاعل البشري. ناقشنا أن كل طريقة لإدارة الأمن تتطلب وجودًا بشريًا إلى حد ما في كل جهاز أمني جنبًا إلى جنب مع المعالجة اليدوية وتقييم سجلات الأمان. ومع ذلك ، يُنظر إلى المراقبة عن بُعد والإدارة المركزية مع قدرات الترابط والتجميع على أنها حلول قابلة للتطبيق لإدارة أمن الشبكة.

الخاتمة

في هذا المقال، اقترح المؤلفون تصنيفًا واضحًا لتطبيقات الحكومة الإلكترونية وفقًا للمشاركين المعنيين في نظام الحكومة الإلكترونية. علاوة على ذلك، أظهر المؤلفون التحديات والعقبات في الحكومة الإلكترونية التي تم النظر فيها من أربعة جوانب: الجوانب التقنية، والسياسية، والثقافية، والقانونية. بالإضافة إلى تحديد التحديات والعقبات في الحكومة الإلكترونية، فقد اقترحوا ثلاثة عشر في الحكومة الإلكترونية من منظور شامل: المستخدم، والعملية، والقانونية، ووجهات نظر الأجهزة / البرامج. أخيرًا، يعد تطوير حلول عملية في الحكومة الإلكترونية موضوعًا مثيرًا للاهتمام لمزيد من البحث والمناقشة.

المصادر والمراجع

Chen, Z., Han, F., Cao, J., Jiang, X., & Chen, S. (2013). Cloud computing-based forensic analysis for collaborative network security management system. Tsinghua science and technology, 18(1), 40-50.

D. W. Seo, W. S. Yi, and K. S. Lee, "Information security activities model per e-government service promotion stage," in iiWAS2010 - 12th Int. Conf. Inf. Integr. Web-Based Appl. Serv., Nov. 2010, pp. 223–227, DOI: 10.1145/1967486.1967523.

D. Soares and F. De Sá-Soares, "Information systems security management key issues in local government," in ACM Int. Conf. Proceeding Ser., Oct. 2014, pp. 227–230, DOI: 10.1145/2691195.2691238

E. Niemimaa and M. Niemimaa, "Information systems security policy implementation in practice: from best practices to situated practices," Springer, European journal of information systems, vol. 26, pp. 1-20, Jan. 2017, DOI: 10.1057/s41303-016-0025-y.

E. Crowley, "Information system security curricula development," in Proc. 4th Conf. Inf. Technol. Curriculum, CITC4 2003, Oct. 2003, pp. 249–255, DOI: 10.1145/947121.947178.

Farn, K. J., Lin, S. K., & Fung, A. R. W. (2004). A study on information security management system evaluation—assets, threat and vulnerability. Computer Standards & Interfaces, 26(6), 501-513.

M. Franeková, P. Holečko, E. Bubeníková, and A. Kanáliková, "Transport scenarios analysis within C2C communications focusing on security aspects," ieeexplore.ieee.org, 2018, doi: 10.1109/SAMI.2017.7880354.

R. Gupta, S. K. Muttoo, and S. K. Pal, "Proposed framework for information systems security for e-governance in developing nations," in ACM Int. Conf. Proceeding Ser., vol. Part F128003, pp. 546–547, Mar. 2017, DOI: 10.1145/3047273.3047285.

R. Villarroel, E. Fernández-Medina, and M. Piattini, "Secure information systems development–a survey and comparison," Elsevier, Computers & Security, Vol. 24, pp. 308-321. Jun. 2005, DOI: 10.1016/j.cose.2004.09.011.

R. B. Vaughn, D. A. Dampier, and M. B. Warkentin, "Building an information security education program," dl.acm.org, Oct. 2004, pp. 41–45, DOI: 10.1145/1059524.1059533.

R. M. Schneider, "A comparison of information security risk analysis in the context of e-government to criminological threat assessment techniques," in Proc. 2010 Inf. Secure. Curric. Dev. Annu. Conf. InfoSecCD'10, Oct. 2010, pp. 107–116, DOI: 10.1145/1940941.1940966.

R. Ross, M. McEvilley, and J. C. Oren, "Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems," in NIST Special Publication, National Institute of Standards and Technology, 2016, 800-160, DOI: 10.6028/NIST.SP.800-160v1.

R. Ross, P. Victoria, G. Richard, B. Deborah, and M. Rosalie, "Developing cyber resilient systems: a systems security engineering approach," 2019, No. NIST Special Publication (SP) 800-160, vol. 2 (Draft). National Institute of Standards and Technology, 2019, DOI: https://doi.org/10.6028/NIST.SP.800-160v2.

S. Flowerday, T. T. & security, "Information security policy development and implementation: The what, how and who," Elsevier, 2016, DOI: 10.1016/j.cose.2016.06.002.

Shareef, S. M. (2016). Enhancing security of information in E-government. Journal of Emerging Trends in Computing and Information Sciences, 7(3), 139-146.

Z. Soomro, M. Shah, J. A.-I. J. of Information, "Information security management needs more holistic approach: A literature review," Elsevier, vol. 36, pp. 215–225, 2016, DOI: 10.1016/ j. ijinfomgt. 2015.11.009..