JASPSS
مجلة المجتمع العربي لنشر الدراسات العلمية
ISSN: 2958-6798
الإصدار رقم (2)
02–كانون الثاني–2023
https://jaspss.com

"إدارة أمن المعلومات في البلديات"

إعداد الباحث

م. معاذ يوسف أحمد الحياري

مهندس حاسوب

بلدية عين الباشا الجديدة

الملخص

يهدف هذا البحث الى التوعية بأهمية وضع نظام إدارة أمن المعلومات في المؤسسات العامة و البلديات. حيث يوضح ما هو نظام إدارة أمن المعلومات وأهميته وأهدافه ومكوناته. كما يوضح الأنواع المختلفة للبيانات وكيفية التعامل معها بالإضافة الى بيان المخاطر الأمنية التي تهددها وكيفية تجنب هذه المخاطر.

المقدمة

في هذا العصر أصبحت التكنولوجيا جزء أساسي في مختلف نواحي حياتنا، وشهد قطاع التكنولوجيا تطور كبير و بشكل متسارع جداً، و زادت الحاجة الى استخدامها في مختلف المجالات و من قبل أغلب الناس، و أصبحنا نقضي معظم الوقت و نحن على إتصال بالانترنت من خلال مختلف الأجهزة. كما أن الدول و الحكومات تسعى لمواكبة هذا التطور وأصبحت تتجه الى ما يسمى بالحكومات الذكية لتقديم خدماتها للمواطنين على أفضل وجه وبشكل أسرع وبدقة عالية لذا يجب ان نكون على دراية هل المعلومات الحساسة التي لدينا آمنة؟.

و مع مرور الوقت تزداد أهمية أمن المعلومات، و تزداد الحاجة الى تطوير أنظمة إدارة أمن المعلومات، حتى تتمكن من التغلب على المخاطر الأمنية و الهجمات الإلكترونية و التي أصبحت أكثر تطورا و تعقيدًا، كما أصبحت تنطوي على البرامج الضارة و التصيد الاحتيالي و التعلم الآلي و الذكاء الاصطناعي وغير ذلك قد عرّضت بيانات وأصول المؤسسات والحكومات والأفراد لخطر دائم.

تعريف نظام إدارة أمن المعلومات في البلدية

يعرف نظام إدارة أمن المعلومات بأنه مجموعة من الأطر التي تحتوي على سياسات و إجراءات لحماية البيانات من الوصول غير المصرح به لتعديل المعلومات، سواء في التخزين و عملية المعالجة أو نقلها، و ضد الحرمان من الخدمة للمستخدمين المرخص لهم أو توفير الخدمة للمستخدمين غير المصرح بهم، بما في ذلك التدابير اللازمة للكشف عنها، و توثيقها و مواجهة مثل هذه التحديات.

يقوم نظام إدارة أمن المعلومات على ما يلي:

- ❖ وضع التشريعات اللازمة لتنفيذ إدارة أمن المعلومات.
- ❖ حماية الأجهزة في البلدية من المخاطر الأمنية.
- ❖ استمرارية و تنفيذ وتطوير وصيانة و تحسين أمن المعلومات.

أهداف نظام إدارة المعلومات في البلدية

يهدف نظام إدارة أمن المعلومات الى تحقيق كل من:

- ✓ **السرية:** حيث تشير السرية الى الصفة الخارجية التي تمنح للمعلومات، و التي تنطوي على التكتم و الخصوصية، و ذلك من خلال تحديد الضوابط و التعليمات التي تحدد الجهات المسموح لها بالإطلاع عليها، و من ثم حماية المعلومات في النظام بحيث لا يمكن للأشخاص غير المرخص لهم الوصول اليها.
- ✓ **التوافر:** و تعني ضمان توافر المعلومة للأطراف المخولين بالوصول الى المعلومات عند الحاجة. و تتحقق عند امتلاك هذه الأطراف المخولة القدرة على الوصول الى المعلومات و إمكانية إستخدامها بصورتها الحالية أينما كانت و كيفما تطلب الأمر.

- ✓ **سلامة المعلومات:** و تتضمن الصفات الجوهرية الخاصة بكمال المعلومات و تماسكها و إرتباطها بمجموعة القيم السائدة في المؤسسة . و تتحقق عند الحفاظ على دقة و إكتمال المعلومات و إتصافها بالصدق و الأصالة و عمق تطابقها مع الحقيقة و الواقع و ضمان أنه لم يتم إجراء أية تغييرات غير مصرح بها على هذه المعلومات.
- ✓ **المساءلة:** و تعني تحمل الشخص الذي قام بالوصول الى أي معلومة داخل النظام مسؤولية التغيير الذي حصل عليها أثناء وصوله اليها، سواء كان موظفاً مسؤولاً عن معالجة المعلومات أو أحد العملاء و هذا يشمل جميع الأفراد الذين يستطيعون الوصول الى المعلومة. و تتحق عندما يتم ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها، بحيث تتوفر لبقدرة على إثبات أن تصرفاً ما قد تم من شخص ما في وقت معين.
- ✓ **قابلية التدقيق:** و تشير الى عملية التقييم لحالة أمن المعلومات في المؤسسة مقارنة بمستوى العمل القياسي لها، و ضمان أن الموظفين يتصرفون وفقا للإجراءات المتبعة و المبادئ التوجيهية التي يمكن استخدامها لتعزيز حالة الأمن. و تتحقق عندما يتم التأكد من أن مقاييس أمن المعلومات مقبولة في إطار تطبيقات نظم المعلومات. و معرفة مدى تجاوز المستخدم التصريح الممنوح له، الى جانب التأكد من صحة البيانات و المعاملات و الوثائق.

مكونات نظام إدارة المعلومات

يشمل نظام إدارة أمن المعلومات كل من:

1) **أمن حماية البيانات.**
2) **الأمن السيبراني.**

3) **أمن الأجهزة الذكية.**

4) **الأمن المادي.**

5) **أمن وسائل التواصل الاجتماعي.**

أولاً: أمن حماية البيانات

تتضمن عملية حماية البيانات ما يلي:

- تحديد التصنيف الأمني للمعلومات.
- منع تسرب البيانات.

التصنيف الأمني للبيانات

تصنف البيانات الى ما يلي:

✓ **بيانات مفتوحة:**

و هي البيانات التي يتم الكشف عنها علناً للافراد و المنظمات الحكومية و غيرالحكومية ويمكن استخدامها و إعادة ارسالها لاطراف خارجية وفقا للشروط و الأحكام الموافق عليها.

✓ **بيانات سرية:**

و هذه البيانات قد تكون متاحة للتداول الخارجي و هي البيانات القابلة للمشاركة مع جهات حكومية محددة وفقا للمسؤوليات المهنية مع أذونات الترخيص و الوصول و للأغراض المصرح بها.

او متاحة للتداول الداخلي و هي المعلومات الخاصة و المتاحة للموظفين فقط و لا يسمح بالافصاح عنها لاية جهة خارجية.

✓ **بيانات حساسة:**

و هذه البيانات قد تكون متاحة للتداول الخارجي و هي البيانات القابلة للمشاركة مع مجموعات معينة و تخضع لضوابط صارمة مع ترخيص ذو صلة و أذونات الوصول و لأغراض مصرح بها.

او متاحة للتداول الداخلي و هي معلومات حساسة و مخصصة للاستخدام فقط من قبل أفراد محددين او مجموعات معينة من الموظفين أو داخ إدارات محددة.

✓ **بيانات سرية للغاية:**

معلومات سرية للغاية و يتم الإطلاع عليها من قبل أفراد محددين.

منع تسرب المعلومات

و الهدف منها هو مراقبة و منع إرسال البيانات غير المصرح بها الى جهات خارجية. و ذلك تجنب حودث أي من:

- فقدان البيانات الحساسة.
- التداعيات القانونية و الغرامات التنظيمية.
- التأثير على سمعة المؤسسة.
- التأثير على إيردات المؤسسة.

و لحماية البيانات من التسرب يجب ما يلي:

1) تجنب ارسال او إعادة توجيه البيانات للحسابات البريدية الشخصية.

2) تجنب ارسال البيانات عبر التطبيقات السحابية غير المصرح بها مثل: DropBox, Google Drive.

3) تجنب نشر المعلومات على مواقع التواصل الإجتماعي.

4) التأكد من تصنيف حفظ البيانات لتمييز البيانات قبل مشاركتها.

5) تجنب استخدام الصلاحيات المقدمة للموظف لنقل البيانات الى وسائط قابلة للحذف.

ثانياً: الأمن السيبراني

هو عملية حماية الأنظمة والشبكات والبرامج ضد الهجمات الرقمية. تهدف هذه الهجمات السيبرانية عادةً إلى الوصول إلى المعلومات الحساسة أو تغييرها أو تدميرها، بغرض الاستيلاء على المال من المستخدمين أو مقاطعة عمليات الأعمال العادية.

أنواع الأمن السيبراني:

1) **أمن الشبكات:** و فيه تتم حماية الأجهزة المربوطة على شبكة الحاسوب من الهجمات التي قد تتعرض لها سواء من داخل أو خارج الشبكة. و يوجد هناك العديد من التقنيات المستخدمة و التي تضمن السماح للأشخاص المخولين فقط بالوصول الى الشبكة و من أهم هذه التقنيات هو جدار الحماية و الذي يعمل واقيا بين الشبكة و المصادر الخارجية.

2) **أمن التطبيقات:** وفيه يجري حماية المعلومات المتعلقة بالتطبيقات التي يتم تثبيتها على الأجهزة، كإجراءات استخدام كلمات المرور قوية، وعمليات المصادقة الثنائية، وأسئلة الأمان التي تضمن التأكد من هوية مستخدم التطبيق.

3) **الأمن السحابي:** يلجأ الكثير إلى حفظ بياناتهم عبر التطبيقات السحابية عوضًا عن برامج التخزين المحلية مما أدى إلى ظهور الحاجة إلى حماية تلك البيانات، فيعنى الأمن السحابي بتوفير الحماية اللازمة لمستخدميها، مثل عمل نسخ احتاطية من البيانات و بشكل دوري.

4) **الأمن التشغيلي:** و يعنى بإدارة الأمن السيبراني الداخلي، عن طريق توظيف خبراء في إدارة المخاطر لكي يقوموا بوضع خطط بديلة في حال تعرض البيانات للخطر، بالإضافة الى توعية الوظفين و تدريبهم على أفضل الممارسات التي تضمن أمن معلوماتهم.

أنواع تهديدات الأمن السيبراني:

1) **تصيد المعلومات:** وهو عملية إرسال رسائل بريد إلكتروني احتيالية تشبه رسائل البريد الإلكتروني من المصادر الموثوقة.

والهدف هو سرقة المعلومات الحساسة مثل أرقام بطاقة الائتمان ومعلومات تسجيل الدخول، وهو أكثر أنواع الهجمات الإلكترونية شيوعًا.

وللحماية من هذا النوع من الهجوم يجب إتباع ما يلي:

- ✓ استخدام الحلول التقنية التي تعمل على تصفية رسائل البريد الإلكتروني الضارة.
- ✓ مراقبة مرسلي البريد الاكتروني الذين يستخدمون أسماء نطاقات مشبوهة.
- ✓ تجنب الضغط على الروابط او المرفقات من مرسلين لا تعرفهم.
- ✓ تجنب تقديم معلومات حساسة عبر البريد الإلكتروني.

من الأمثلة على عمليات التصيد:

التصيد المستهدف: حيث يكون اسم المرسل و البريد الإلكتروني غير مترابطين، كما يحتوي البريد الإلكتروني على روابط إلكترونية عشوائية.

تصيد المشاهير: حيث يكون البريد الإلكتروني مشبوه و يحتوي طلب غريب، بالإضافة الى التظاهر و الإدعاء بشخصية أخرى و يحتوي على العديد من الأخطاء اللغوية و النحوية.

التصيد عبر رسالة من مواقع مشاركة الملفات: حيث يكون المصدر مجهول و الموضوع لا علاقة له بالعمل، و يحتوي ملف غير متوقع و يكون غير قابل للتنزيل.

التصيد عبر الرسائل النصية: حيث تحوي على كلمات تنبيه او تخويف، بالإضافة الى كلمات ملحة و روابط قابلة للضغط، كما تحتوي على العديد من الأخطاء اللغوية و النحوية.

2) **هجمات كلمات المرور.**

- ✓ عدم استخدام كلمة مرور واحدة لأكثر من حساب.
- ✓ يجب ان تكون كلمة المرور قوية بحيث تحتوي على رموز و أرقام و أحرف كبيرة و أحرف صغيرة.
- ✓ عدم مشاركة كلمات المرور مع الأخرين.
- ✓ عدم استخدام اسم المستخدم و كلمة المرور على أجهزة الكمبيوتر العامة.
- ✓ تغيير كلمة المرور كل فترة.

3) **البرمجيات الخبيثة:** و هي نوع من البرامج المصممة للوصول غير المصرح به إلى جهاز الكمبيوتر أو إلحاق الضرر به.

و تحدث هجمات البرمجيات الخبيثة من خلال:

- فتح أو تنزيل مرفق في بريد الكتروني.
- فتح ملفات الفلاش.
- الضغط على رابط في رسالة بريد الكتروني.

و لتجنب هجمات البرمجيات الخبيثة:

✓ يجب البحث عن البرامج قبل تنزيلها او تثبيتها.

✓ اغلاق الرسائل المنبثقة دون الضغط على اي شيء بداخلها.

✓ التعامل مع الملفات المرفقة بحذر.

✓ فحص محركات اقراص الفلاش باستخدام برامج الأمان.

✓ تجنب خدمة مشاركة الملفات غير القانونية.

✓ عمل نسخ احتياطية من الملفات بإنتظام.

4) **التحايل بإستخدام الهندسة الإجتماعية:** و هي أسلوب يستخدمه الخصوم لاستدراج المستخدم إلى الكشف عن المعلومات الحساسة. حيث يمكنهم طلب الحصول على دفع نقدي أو الوصول إلى بياناتك السرية. ويمكن دمج الهندسة الاجتماعية مع أي من التهديدات المذكورة سابقًا لزيادة فرصة في النقر على الروابط أو تنزيل البرامج الضارة أو الوثوق بمصدر ضار.

و لتجنب هذا النوع من التهديد:

✓ عدم الإنخداع بالإلحاح الوهمي في المنشورات.

✓ الحذر من منح الآخرين بيانات حسابك او مشاركتهم كلمات المرور الخاصة بك.

✓ عدم منح أية معلومات أو بيانات تحت أي ضغط.

ثالثاً: أمن الأجهزة الذكية

أنواع التهديدات الأمنية المتعلقة بالأجهزةالمحمولة:

1) **التطبيقات الضارة:** و لتجنب هذا النوع من التهديدات يجب إتباع ما يلي:

- ✓ تنزيل التطبيقات من المصادر الموثوقة فقط.
- ✓ حذف التطبيقات التي لم تعد بحاجة اليها.
- ✓ ايقاف او منع تتبع الموقع الجغرافي.
- ✓ التأكد من أن التطبيقات لديها تقييم إيجابي و أنه يتم تحديثها بإستمرار.
- ✓ مراجعة خيارات الخصوصية.
- ✓ التحقق من أذونات اللتطبيقات بإنتظام.

2) **شبكات الانترنت الوهمية:** و لتجنب هذا النوع من التهديدات يجب إتباع ما يلي:

- ✓ التأكد من استخدام قنوات مشفرة آمنة.
- ✓ استخدام بيانات المحمول الخاصة ما أمكن ذلك.
- ✓ عدم استخدام شبكات الإنترنت العامة أو عدم مشاركة المعلومات الحساسة على شبكات الإنترنت العامة.

3) **فقدان او سرقة الجهاز:** و لتجنب هذا النوع من التهديدات يجب إتباع ما يلي:

- ✓ تفعيل خاصية تتبع الجهاز عن طريق الإنترنت، على سبيل المثال تفعيل خاصية العثور على أجهزة الـ iPhone.
- ✓ عمل نسخ احتياطية من البيانات.

✓ التعامل بحذر من الصور و مقاطع الفيديو المحفوظة في الجهاز.

رابعاً: الأمن المادي

أنواع التهديدات الأمنية المتعلقة بالأمن المادي:

1) **التتبع:** و لتجنب هذا النوع من التهديدات يجب إتباع ما يلي:

✓ عدم إعطاء حق الدخول للآخرين.

✓ استخدام الهوية الوظيفية من قبل الموظفين و استخدامها في أوقات العمل فقط و عدم ارتدائها في الأماكن العامة.

✓ عدم الدخول الى أماكن غير المصرح بدخولها الا من قبل أشخاص محددين.

2) **البيانات المكشوفة:** و لتجنب هذا النوع من التهديدات يجب إتباع ما يلي:

✓ عدم ترك البطاقة البنكية أو المحفظة او الجهاز المحمول دون رقابة داخل المكتب.

✓ عدم ترك أية مستندات هامة دون رقابة داخل المكتب.

✓ عدم ترك الأجهزة الإلكترونية دون رقابة في السيارة.

✓ القيام بعملية تسجيل الخروج او عمل قفل للأجهزة عند مغادرة المكتب حتى و لو لبضع دقائق.

3) **إنتحال الهوية الشخصية:** و لتجنب هذا النوع من التهديدات يجب إتباع ما يلي:

✓ عدم إعطاء الهوية الوظيفية للآخرين.

✓ عدم الثقة بأي شخص بصرف النظر عن مظهره أو بساطة طلبه.

خامساً: أمن وسائل التواصل الإجتماعي

أنواع التهديدات الأمنية المتعلقة بأمن وسائل التواصل الإجتماعي:

1) **الأخطاء البشرية:** و لتجنب هذا النوع من التهديدات يجب إتباع ما يلي:

- ✓ فكر قبل ان تنشر.
- ✓ معرفة ما ينشره الآخرين عنك.
- ✓ الحذر من رسائل البريد الإلكتروني التي تدعي أنها من مواقع التواصل الإجتماعي.

2) **أمن حسابات التواصل الإجتماعي:** و لتجنب هذا النوع من التهديدات يجب إتباع ما يلي:

- ✓ إغلاق أو مسح الحسابات الغير مستخدمة.
- ✓ تفعيل المصادقة الثنائية.
- ✓ التحقق من التطبيقات المتصلة بوسائل التواصل الإجتماعي الخاصة بك.
- ✓ عدم استخدام البريد الاكتروني الرسمي للتسجيل في اي من منصات التواصل الإجتماعي.

الخاتمة

إن المعلومات هي أصل مهم لجميع المؤسسات و الأفراد، حيث تستخدم المعلومات لخدمة الأشخاص واتخاذ القرارات و إنشاء معلومات جديدة. حيث تساعد تكنولوجيا المعلومات على معالجة جميع المعلومات وتخزينها وإدارتها، وبالتالي تعتبر حماية المعلومات وظيفة هامة يجب القيام بها على أكمل وجه.

إن سعي البلديات والحكومة و توجهاتها نحو حوسبة و أتمتة الخدمات المقدمة للمواطنين يجب أن يقابله إهتمام كبير بضمان أمن المعلومات، و عليه يجب العمل على تأسيس نظام إدارة أمن المعلومات في

المؤسسات العامة و البلديات بأسرع وقت ممكن لما له من أهمية بالغة، حيث يجب العمل على وضع خارطة طريق تضمن تحقيق الأهداف المرجوة منه و العمل على تطويره و تحسينه بشكل مستمر و ضمان ديمومة عمله على النحو الأمثل.

كما يتطلب إنجاح هذا النظام عقد دورات متخصصة و متقدمة لموظفي اقسام تكنولوجيا المعلومات في البلديات، بالاضافة الى حملات التوعية للموظفين و ذلك بالتنسيق مع الوزارات و الجهات ذات العلاقة.

أمن المعلومات ليست مهمة شخص معين، بل مهمة الجميع، فالجميع له دور معين بغض النظر عن طبيعة هذا الدور و حجمه و درجة تأثيره. و الكثير من الأشخاص قد لا يعون هذه الحقيقة.

المصادر و المراجع

رشا الصوالحة، (2021)، *أهمية الأمن السيبراني*، مقالة منشورة على موقع موضوع، متوفرة عبر الرابط الإلكتروني التالي: https://mawdoo3.com، تمت الزيارة بتاريخ 18–12–2022، الساعة 11:10 صباحاً.

المركز الوطني للأمن السيبراني في دولة البحرين، (2022)، *نماذج سياسات الأمن السيبراني*، متوفرة على الرابط الإلكتروني التالي: https://www.ncsc.gov.bh/ar/index.html ، تمت الزيارة بتاريخ 22–12–2022، الساعة 12:10 مساءً.

م الطائي و ي الكيلاني، (2015)، إدارة أمن المعلومات، محمد عبد حسين الطائي و ينال محمود الكيلاني، الطبعة الأولى، 247، دار الثقافة، عمان، الأردن.

Michelle Moore, (2022), *Top Cybersecurity Threats in 2022*, https://onlinedegrees.sandiego.edu/top-cyber-security-threats/ , visited in 19-12-2022, 13:00 PM

Cisco, *What Is Cybersecurity?,* https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html, visited in 18-12-2022, 13:55 PM

Trida Networks, *What Are the Different Types of Cyber Security?,* https://triadanet.com/different-types-of-cyber-security/ , visited in 20-12-2022, 10:40 PM

Abstract

This research is aims to increase the awareness of the importance for developing an information security management system in public institutions and municipalities. It explains the definition of the information security management system, its importance, objectives and components. It also explains the different types of the data and how to deal with them, in addition to clarify the security risks that may threat them and how to avoid these risks.