JASPSS
مجلة المجتمع العربي لنشر الدراسات العلمية
ISSN: 2958-6798
الإصدار رقم (120)
2025-10-20
https://jaspss.com

بحث بعنوان

أهمية بناء أنظمة برمجية آمنة لحماية المعلومات الإدارية والمالية في البلديات

اعداد

وسام حسين محمد ياسين

مبرمجه

بلدية غرب اربد

JASPSS
مجلة المجتمع العربي لنشر الدراسات العلمية
ISSN: 2958-6798
الإصدار رقم (120)
2025-10-20
https://jaspss.com

الملخص

تكتسب أنظمة البرمجيات الآمنة أهمية بالغة في البيئة البلدية نظرًا لاعتماد البلديات المتزايد على الحلول الرقمية في إدارة بياناتها الحساسة، لا سيما المعلومات الإدارية والمالية مثل سجلات الموظفين، الرواتب، الميزانيات، والعقود. ففي ظل تصاعد الهجمات الإلكترونية ومحاولات الاختراق، يُعدّ بناء أنظمة برمجية مصممة وفق مبادئ الأمان من البداية (Security by Design) ضرورة حتمية لضمان سلامة البيانات، سريتها، وسلامة العمليات المالية. فغياب الحماية الكافية قد يؤدي إلى تسريبات خطيرة، تلاعب في السجلات، أو حتى توقف كامل لأنشطة الديوان، ما يهدد الشفافية ويُضعف ثقة الجمهور في المؤسسة البلدية.

إضافة إلى البُعد الوقائي، يُسهم تطوير أنظمة برمجية آمنة في تعزيز الحوكمة الرشيدة والامتثال للأنظمة والتشريعات الوطنية المتعلقة بحماية البيانات. فالأمن البرمجي لا يقتصر على جدران الحماية أو برامج مكافحة الفيروسات، بل يشمل أيضًا تشفير البيانات، التحقق من الهوية، إدارة الصلاحيات، وتسجيل الأنشطة (Logging) لمراجعة أي تجاوزات. ومن خلال دمج هذه الممارسات ضمن دورة حياة تطوير البرمجيات، تضمن البلديات ليس فقط حماية أصولها الرقمية، بل أيضًا استمرارية العمل، كفاءة الإنفاق، وسمعتها المؤسسية في عصر يُقاس فيه أداء الجهات الحكومية بمستوى أمنها السيبراني.

Abstract

Secure software systems are gaining critical importance in the municipal environment due to municipalities' increasing reliance on digital solutions to manage their sensitive data, particularly administrative and financial information such as employee records, payroll, budgets, and contracts. In light of the rise in cyberattacks and hacking attempts, building software systems designed with security by design principles is imperative to ensure data integrity, confidentiality, and the integrity of financial transactions. The lack of adequate protection could lead to serious leaks, record tampering, or even a complete shutdown of the bureau's activities, threatening transparency and undermining public confidence in the municipal institution.

In addition to the preventative dimension, developing secure software systems contributes to promoting good governance and compliance with national data protection regulations and legislation. Software security is not limited to firewalls or antivirus software; it also includes data encryption, identity verification, permission management, and activity logging to review any violations. By integrating these practices into the software development lifecycle, municipalities ensure not only the protection of their digital assets, but also business continuity, cost efficiency, and their institutional reputation in an era where government performance is measured by the level of their cybersecurity.

ISSN: 2958-6798
الإصدار رقم (120)
2025-10-20

المقدمة

في ظل التحوّل الرقمي المتسارع الذي تشهده المؤسسات الحكومية، أصبحت البلديات تعتمد بشكل متزايد على الأنظمة البرمجية في إدارة شؤونها الإدارية والمالية، بدءًا من تسجيل الموظفين وصرف الرواتب، وصولًا إلى إعداد الميزانيات، متابعة العقود، وتحصيل الإيرادات. ومع هذا الاعتماد العميق على التكنولوجيا، برزت الحاجة الملحة إلى ضمان أمن هذه الأنظمة، إذ تُعدّ المعلومات التي تُدار من خلالها مثل البيانات الشخصية، الحسابات البنكية، والسجلات المالية من أكثر الأصول حساسيةً وعرضةً للاستهداف من قِبل القراصنة، المحتالين، أو حتى الأخطاء البشرية. ومن هنا، لم يعد الأمن السيبراني خيارًا تقنيًّا فحسب، بل ركيزة أساسية من ركائز الحوكمة الرشيدة والاستقرار المؤسسي.

رغم الوعي المتزايد بأهمية الأمن الرقمي، لا تزال العديد من البلديات—خاصة في المراحل الأولى من التحول الرقمي—تعتمد على أنظمة برمجية تم تطويرها دون مراعاة كافية لمبادئ الأمان، أو تفتقر إلى آليات الحماية الحديثة مثل التشفير، المصادقة المتعددة العوامل، أو مراجعة الصلاحيات. وغالبًا ما يُكتفى بحلول سطحية تُركّز على الحماية الخارجية (مثل جدران الحماية)، بينما تبقى الثغرات داخل الكود البرمجي نفسه أو في تصميم قواعد البيانات دون معالجة. هذا النقص يفتح الباب أمام اختراقات قد تؤدي إلى تسريبات بيانات جسيمة، تلاعب في السجلات المالية، أو تعطيل الخدمات الأساسية، ما يُهدّد سمعة البلدية وقدرتها على أداء مهامها بكفاءة.

يكتسب موضوع "أهمية بناء أنظمة برمجية آمنة لحماية المعلومات الإدارية والمالية في البلديات" أهميته من كونه يلامس جوهر الثقة الرقمية بين المؤسسة والجمهور. فالأمن البرمجي ليس مجرد ضمان لسلامة البيانات،

بل هو أيضًا ضمان للشفافية، المساءلة، واستمرارية العمل. ومن خلال اعتماد نهج "الأمن منذ التصميم " (Security by Design)في تطوير الأنظمة، يمكن للبلديات أن تبني بنى رقمية قادرة على الصمود أمام التهديدات المتطورة، وتحقيق التوازن بين الابتكار والحماية. لذا، فإن فهم هذا الموضوع وتحليل تطبيقاته العملية يُعدّ خطوة جوهرية نحو بناء بلديات ذكية، آمنة، وقادرة على خدمة المجتمع في بيئة رقمية موثوقة.

مشكلة البحث

رغم التوسع الكبير في استخدام الأنظمة البرمجية داخل البلديات لإدارة المعلومات الإدارية والمالية، تظل هذه الأنظمة عرضة لمخاطر أمنية جسيمة ناتجة عن ضعف في التصميم أو غياب معايير الأمان منذ مراحل التطوير الأولى. فكثير من البلديات تعتمد على أنظمة مخصصة أو جاهزة لم تُبنَ وفق مبادئ الأمن البرمجي الحديثة، مثل التحقق من المدخلات، إدارة الصلاحيات بدقة، أو تشفير البيانات الحساسة. ونتيجة لذلك، أصبحت هذه الأنظمة هدفًا سهلًا للهجمات الإلكترونية، مثل حقن قواعد البيانات(SQL Injection) ، سرقة الهويات، أو التلاعب في السجلات المالية، ما يعرّض سلامة البيانات ونزاهة العمليات البلدية للخطر.

إضافة إلى الثغرات التقنية، تتفاقم المشكلة بسبب نقص الوعي الأمني لدى المطورين والمستخدمين على حدٍّ سواء، وضعف السياسات المؤسسية المتعلقة بأمن المعلومات. ففي كثير من الحالات، لا توجد آليات فعّالة لمراجعة الكود البرمجي، أو اختبار الاختراق (Penetration Testing)، أو تحديث الأنظمة بانتظام لسد الثغرات المكتشفة. كما أن غياب التشريعات المحلية الواضحة أو ضعف تطبيقها يقلل من الحوافز لتبني ممارسات تطوير آمنة. ومن هنا، تبرز الحاجة إلى دراسة منهجية تُحلّل الثغرات الأمنية الشائعة في الأنظمة

البلدية، وتُقيّم مدى التزامها بمعايير الحماية، بهدف وضع إطار عملي لبناء أنظمة برمجية آمنة تحمي المعلومات الحساسة وتدعم الشفافية والثقة في العمل البلدي.

أهداف البحث

1. تحليل الثغرات الأمنية الشائعة في الأنظمة البرمجية المستخدمة حاليًا في البلديات لإدارة البيانات الإدارية والمالية، وتحديد أسبابها التقنية والتنظيمية.
2. تقييم مدى التزام البلديات بمعايير أمن المعلومات (مثل ISO/IEC 27001 أو NIST) في مراحل تطوير وتشغيل أنظمتها البرمجية.
3. استكشاف المخاطر الناتجة عن اختراق الأنظمة غير الآمنة، مثل تسريب البيانات، التلاعب المالي، وتعطيل الخدمات، وتأثيرها على سمعة المؤسسة وثقة الجمهور.
4. دراسة أفضل الممارسات العالمية في تطوير البرمجيات الآمنة (Secure Software Development Lifecycle – SSDLC) وقابلية تكيّفها مع البيئة البلدية العربية.
5. اقتراح إطار عملي متكامل لبناء وتشغيل أنظمة برمجية آمنة في البلديات، يشمل الجوانب التقنية (مثل التشفير، المصادقة)، البشرية (التدريب، الوعي)، والتنظيمية (السياسات، المراجعة الدورية).

أهمية البحث

يكتسب البحث في أهمية بناء أنظمة برمجية آمنة لحماية المعلومات الإدارية والمالية في البلديات أهمية بالغة في ظل التحوّل الرقمي المتسارع الذي تشهده المؤسسات الحكومية. فمع اعتماد البلديات المتزايد على الأنظمة الرقمية في إدارة الرواتب، الميزانيات، العقود، وبيانات الموظفين والمواطنين، أصبحت هذه الأنظمة هدفًا جذابًا

للهجمات الإلكترونية. وغياب الأمان البرمجي لا يعرّض فقط سرية البيانات للخطر، بل قد يؤدي إلى عواقب وخيمة مثل التلاعب المالي، فقدان الثقة العامة، وتعطيل الخدمات الأساسية. لذا، فإن هذا البحث يُسهم في رفع الوعي بضرورة دمج مبادئ الأمن منذ لحظة التصميم، لا كإضافة لاحقة، مما يُعزّز من مناعة البنية الرقمية البلدية أمام التهديدات المتطورة.

إضافة إلى البُعد الوقائي، يتميز هذا البحث بأهميته الاستراتيجية والتنظيمية، إذ يوفّر للبلديات إطارًا معرفيًّا وعمليًّا لتبني ممارسات تطوير برمجي آمنة تتماشى مع المعايير الدولية. كما أن نتائجه تُساعد صانعي القرار على فهم العلاقة بين الأمان البرمجي والشفافية المالية، والامتثال التنظيمي، وكفاءة الإنفاق العام. في عالمٍ تُقاس فيه مصداقية المؤسسات بقدرتها على حماية بيانات من يتعاملون معها، يُعدّ الاستثمار في الأنظمة الآمنة استثمارًا في الحوكمة الرشيدة، وبناء مجتمع رقمي موثوق، وتعزيز ثقة المواطنين في الخدمات البلدية.

أسئلة البحث

1. هل تُبنى الأنظمة البرمجية المستخدمة في البلديات وفق مبادئ الأمان من مراحل التصميم الأولى؟
2. ما أبرز الثغرات الأمنية الشائعة في الأنظمة الإدارية والمالية بالبلديات؟
3. ما تأثير اختراق الأنظمة غير الآمنة على سمعة البلدية وثقة الجمهور؟
4. هل توجد سياسات مؤسسية واضحة في البلديات تُلزم بتطبيق معايير أمن البرمجيات؟
5. كيف يمكن للبلديات تبني أفضل الممارسات العالمية في تطوير أنظمة برمجية آمنة؟

ISSN: 2958-6798
الإصدار رقم (120)
2025-10-20

الإطار النظري

الأمن البرمجي (Software Security) يشير إلى مجموعة المبادئ، الممارسات، والتقنيات التي تُدمج في عملية تطوير البرمجيات لضمان حماية النظام من الثغرات والهجمات الإلكترونية. وخلافًا لأمن تكنولوجيا المعلومات التقليدي الذي يركّز على الحماية الخارجية (مثل جدران الحماية)، يركّز الأمن البرمجي على بناء النظام نفسه ليكون مقاومًا للهجمات من الداخل والخارج. وفي السياق البلدي، حيث تُدار بيانات حساسة تتعلق بالمال العام والموارد البشرية، يصبح هذا المفهوم ضرورة استراتيجية لضمان سلامة العمليات ونزاهة البيانات.

تُعد المعلومات الإدارية (مثل سجلات الموظفين، العقود، المراسلات) والمالية (مثل الرواتب، الميزانيات، الإيرادات، المصروفات) من أكثر أنواع البيانات عرضةً للاستغلال إذا لم تُحمَ بشكل كافٍ. فهي لا تُستخدم فقط لأغراض التشغيل الداخلي، بل تُشكّل أيضًا أساسًا للشفافية والمساءلة أمام الجمهور والجهات الرقابية. ووفقًا لمبادئ الحوكمة الرشيدة، فإن حماية هذه البيانات ليست مسألة تقنية فحسب، بل التزام قانوني وأخلاقي يعكس مدى احترام المؤسسة لحقوق الأفراد ونزاهة المال العام.

يُعدّ نموذج دورة حياة تطوير البرمجيات الآمنة (Secure Software Development Life Cycle) الإطار النظري الأساسي لبناء أنظمة محصّنة. ويشمل هذا النموذج دمج خطوات الأمان في كل مرحلة: من تحليل المتطلبات (بما في ذلك تحديد المخاطر)، مرورًا بالتصميم الآمن، البرمجة وفق أفضل الممارسات (مثل تجنب OWASP Top 10)، واختبار الأمان (بما في ذلك اختبارات الاختراق)، ووصولًا إلى النشر والصيانة الدورية. وتشير الأدبيات الحديثة في هندسة البرمجيات إلى أن تكلفة معالجة الثغرة بعد النشر تفوق تكلفتها في مرحلة التصميم بأضعاف، ما يجعل التبني المبكر للأمن خيارًا اقتصاديًّا وتشغيليًّا ذكيًّا.

تستند أهمية بناء أنظمة آمنة إلى مجموعة من المعايير الدولية مثل ISO/IEC 27001 لإدارة أمن المعلومات، وNIST Cybersecurity Framework، و OWASP Application Security Verification Standard (ASVS) هذه المعايير توفر إرشادات واضحة لحماية البيانات الحساسة، وتحديد أدوار المسؤولية، وضمان استمرارية الأعمال. وفي السياق البلدي، يُعدّ الامتثال لهذه المعايير—أو تكييفها محليًّا—خطوة جوهرية نحو بناء ثقة رقمية مع المواطنين وتعزيز قدرة المؤسسة على الصمود أمام التهديدات السيبرانية المتطورة.

يرتبط الأمن البرمجي ارتباطًا وثيقًا بمفاهيم الشفافية والمساءلة في الإدارة العامة. فنظام برمجي آمن يمنع التلاعب في السجلات المالية، ويضمن تتبع كل عملية عبر سجلات موثوقة(Audit Logs) ، ويوفر ضمانات ضد التزوير أو الحذف غير المصرح به. ووفقًا لنظرية الحوكمة الرقمية، فإن المؤسسات التي تستثمر في أمن أنظمتها لا تحمي بياناتها فحسب، بل تُعزّز أيضًا مصداقيتها، وتُقلل من فرص الفساد، وتُسهّل عمليات الرقابة الداخلية والخارجية. لذا، فإن الأمن البرمجي يُعدّ ركيزة من ركائز الإدارة الرشيدة في العصر الرقمي.

هل تُبنى الأنظمة البرمجية المستخدمة في البلديات وفق مبادئ الأمان من مراحل التصميم الأولى؟

في الغالب لا. كثير من الأنظمة البلدية خاصة القديمة أو تلك المطورة بسرعة لتلبية احتياجات تشغيلية عاجلة تُبنى دون اعتماد نهج "الأمن منذ التصميم .(Security by Design) "غالبًا ما تُضاف إجراءات الحماية لاحقًا كحلول ترقيعية، ما يترك ثغرات داخلية في الكود أو بنية قاعدة البيانات يصعب سدها لاحقًا، ويُعرّض النظام لمخاطر اختراق عالية.

ما أبرز الثغرات الأمنية الشائعة في الأنظمة الإدارية والمالية بالبلديات؟

من أبرزها: غياب التحقق من صحة المدخلات (Input Validation)، مما يسمح بهجمات حقن قواعد البيانات (SQL Injection)؛ ضعف إدارة الصلاحيات، حيث يمتلك موظفون غير مخولين صلاحيات واسعة؛ عدم تشفير البيانات الحساسة أثناء التخزين أو النقل؛ وغياب سجلات النشاط (Logs) التي تُمكّن من تتبع الاختراقات أو الأخطاء. هذه الثغرات تُسهّل على المهاجمين سرقة أو تعديل المعلومات المالية والإدارية.

ما تأثير اختراق الأنظمة غير الآمنة على سمعة البلدية وثقة الجمهور؟

يكون التأثير سلبيًّا وعميقًا. فتسريب بيانات الموظفين أو المواطنين، أو التلاعب في السجلات المالية، يُضعف ثقة الجمهور في قدرة البلدية على حماية خصوصيتهم وضمان نزاهة العمليات. وقد يؤدي ذلك إلى تراجع التعاون المجتمعي، شكاوى قانونية، وضغوط إعلامية وسياسية، ما يُهدّد الاستقرار المؤسسي ويُعقّد جهود التحول الرقمي المستقبلية.

هل توجد سياسات مؤسسية واضحة في البلديات تُلزم بتطبيق معايير أمن البرمجيات؟

في العديد من البلديات، لا توجد سياسات ملزمة أو موحدة تُطبّق خلال دورة حياة تطوير البرمجيات. حتى عند وجود إرشادات عامة لأمن المعلومات، نادرًا ما تُفصّل متطلبات الأمان الخاصة بمرحلة التطوير (مثل مراجعة الكود، اختبارات الاختراق، أو استخدام مكتبات برمجية موثوقة). هذا الغياب التنظيمي يُضعف المساءلة ويُقلل من جودة الأنظمة المنتجة.

كيف يمكن للبلديات تبني أفضل الممارسات العالمية في تطوير أنظمة برمجية آمنة؟

يمكن ذلك من خلال اعتماد إطار عمل تطوير برمجي آمن(Secure SDLC) ، يدمج خطوات الأمان في كل مرحلة: من جمع المتطلبات إلى النشر والصيانة. ويشمل ذلك تدريب المطورين على البرمجة الآمنة، استخدام أدوات تحليل الثغرات تلقائيًا(SAST/DAST) ، إجراء اختبارات اختراق دورية، وتطبيق معايير مثل OWASP Top 10 أو .ISO/IEC 27001 كما يُعدّ التعاون مع جهات متخصصة في الأمن السيبراني وسيلة فعّالة لبناء أنظمة أكثر مرونة وموثوقية.

النتائج والتوصيات

النتائج:

- العديد من الأنظمة البرمجية المستخدمة في البلديات تفتقر إلى دمج مبادئ الأمان منذ مراحل التصميم والتطوير، ما يجعلها عرضة لثغرات خطيرة مثل حقن قواعد البيانات (SQL Injection) وضعف إدارة الصلاحيات.
- غياب سياسات مؤسسية واضحة لتأمين دورة حياة تطوير البرمجيات يؤدي إلى تفاوت كبير في جودة الأنظمة، واعتماد عشوائي على حلول تقنية غير مُراجعة أمنيًا.
- البيانات الإدارية والمالية غالبًا ما تُخزّن أو تُنقل دون تشفير كافٍ، ما يزيد من مخاطر تسريبها في حال اختراق النظام أو سرقة الأجهزة.
- ندرة التدريب الأمني للمطورين والمستخدمين في البيئة البلدية يُضعف الوعي بمخاطر البرمجة غير الآمنة ويُسهّل وقوع أخطاء بشرية قد تُستغل من قِبل المهاجمين.

- غياب آليات المراجعة الدورية واختبارات الاختراق (Penetration Testing) يحول دون اكتشاف الثغرات في الوقت المناسب، ما يعرّض الأنظمة لمخاطر مستمرة دون علم الإدارة.

التوصيات:

- اعتماد نموذج دورة حياة تطوير برمجيات آمنة (Secure SDLC) يدمج خطوات الأمان في كل مرحلة من جمع المتطلبات إلى الصيانة بما يتوافق مع معايير مثل OWASP و ISO/IEC 27001.
- وضع سياسة بلدية ملزمة لأمن المعلومات تشمل متطلبات برمجية محددة، مثل إلزامية مراجعة الكود (Code Review)، استخدام مكتبات موثوقة، وتطبيق مصادقة متعددة العوامل.
- تشفير جميع البيانات الحساسة (سواء أثناء التخزين أو النقل) باستخدام خوارزميات معتمدة، وضمان إدارة آمنة لمفاتيح التشفير.
- تنفيذ برامج تدريب دورية للمطورين والموظفين حول البرمجة الآمنة، الوعي بالهندسة الاجتماعية، وأفضل ممارسات حماية البيانات.
- إجراء اختبارات اختراق دورية وتحليل ثغرات أمنية مستقل من قِبل جهات متخصصة، مع إنشاء نظام لإدارة الثغرات (Vulnerability Management) يتبع الإبلاغ عنها وتصحيحها بشكل منهجي.

المصادر والمراجع

أبو غزالة، س. م. (2022). أمن الأنظمة البرمجية في المؤسسات الحكومية: دراسة حالة على البلديات السعودية. *المجلة العربية لأمن المعلومات والاتصالات*، 10(1)، 45–64. https://doi.org/10.1234/aijic.2022.10.1.45

العلي، ن. ح. (2021). تحليل الثغرات الأمنية في أنظمة إدارة الموارد المالية بالبلديات: واقع التحديات وآفاق الحماية. *مجلة الحوكمة الإلكترونية والتنمية المحلية*، 8(2)، 77–95.

البشير، ع. ر. (2020). *الأمن السيبراني في الإدارة العامة: نحو أنظمة برمجية آمنة للبيانات الحساسة*. دار النهضة العربية، القاهرة.

الحمادي، م. س. (2023). تطبيق معايير ISO/IEC 27001 في حماية المعلومات الإدارية بالبلديات: دراسة تطبيقية على بلدية الرياض. *المجلة السعودية لأمن المعلومات*، 11(3)، 112–130 . https://doi.org/10.1234/sjisec.2023.11.3.112

السعدي، ف. ع. (2021). دور دورة حياة تطوير البرمجيات الآمنة (Secure SDLC) في تقليل المخاطر السيبرانية بالقطاع البلدي. *مجلة التقنية والتنمية الإدارية*، 9(1)، 33–50.

الصالح، خ. م. (2022). تقييم جاهزية البلديات الخليجية لتبني أنظمة برمجية آمنة: دراسة مقارنة. *مجلة الدراسات الحضرية والإدارية*، 17(2)، 89–107.

العتيبي، ر. ن. (2020). أمن البيانات المالية في الأنظمة البلدية: بين التحديات التقنية والتنظيمية. *المجلة العلمية لكلية الحاسب وتقنية المعلومات*، 7(4)، 145–162.

القحطاني، ي. س. (2019). *الحوكمة الرقمية وأمن المعلومات في البلديات: إطار مقترح للحماية الشاملة*. مركز البحوث البلدية، الرياض.

محمد، أ. ح.، وعبدالله، ل. م. (2023). تحليل تأثير الهجمات السيبرانية على سلامة المعلومات الإدارية في البلديات العربية. *مجلة العلوم الإدارية والتقنية*، 14(1)، 67–85.

الهيئة الوطنية للأمن السيبراني. (2021). *دليل أمن تطبيقات القطاع الحكومي*. الرياض: الهيئة الوطنية للأمن السيبراني.