Warith Scientific Journal

إجراءات مقترحة للتدقيق الداخلي لمخاطر أنترنت الأشياء

Proposed procedures for internal auditing of Internet of Things risks

أ.د ناظم حسن رشيد
Nadhim H. Rasheed
كلية الإدارة والاقتصاد/ جامعة الحمدانية
University of AL-Hamdaniya
dr.nadhim1962@uohamdaniya.edu.iq

م.د يوسف عبد السلام عبدي
Yossef abdel salam abdi
كلية الإدارة والاقتصاد/ جامعة الحمدانية
University of AL-Hamdaniya
yosufabdulsalam@uohamdaniya.edu.iq

المستخلص

يهدف البحث إلى التعرف على مفهوم انترنت الأشياء، وأهم التحديات الأمنية، وخطوات تدقيقه، ولفت نظر المدققين الداخليين إلى الأساليب والاجراءات المقترحة التي يمكن للتدقيق الداخلي من خلالها التدقيق، والتقييم وتقديم المشورة فيما يتعلق بانترنت الأشياء، وتحديد أهم الضوابط العامة لتكنولوجيا المعلومات المستخدمة في عمليات تدقيقه.

ولتحقيق أهداف البحث استخدم الباحثان المنهج الاستدلالي في الدراسة والتحليل باستخدام الدوريات والكتب والمواقع الإلكترونية التي تتناول موضوع البحث، خاصة فيما يتعلق بمجالات: إنترنت الأشياء، التحديات الأمنية التي ترافقه، ودور التدقيق الداخلي في التقييم والتدقيق والمشورة.

وتوصل البحث إلى مجموعة من الاستنتاجات أهمها:

1. تجاهل إدارة المنظمة والتدقيق الداخلي لأمن انترنت الأشياء يمكن أن يؤدي إلى آثار خطيرة على نجاح المنظمة، ومن ثمَّ خروقات في البيانات، والخسائر المالية، والمشكلات القانونية، فضلاً عن الإضرار بسمعة المنظمة.
2. تقع على عاتق العاملين في التدقيق الداخلي مسؤولية مراقبة مشهد انترنت الأشياء عن كثب لتحديد ومنع مجالات المخاطر هذه من التأثير على الأعمال.
3. يمكن وضع برنامج عمل تدقيق يتضمن الاجراءات اللازمة لتقييم وتدقيق جوانب ذات الصلة بالمخاطر انترنت الأشياء.

بناءً على استنتاجات البحث، تم تقديم مقترحات تتفق مع هذه الاستنتاجات، وأهمها:

ضرورة قيام الجهات المهتمة بمهنة التدقيق الداخلي بعقد الندوات للمدققين وإقامة ورش عمل مختصة للتعريف بأنترنت الأشياء، ولفت نظر المدققين الداخليين إلى الطرق التي يمكن أن يوفر بها التدقيق الداخلي التقييم والتدقيق فيما يتعلق بانترنت الأشياء، وعدها جزء أساسي من مهمة المدقق الداخلي الناجح الذي يضيف قيمة للشركة التي منحته ثقتها.

الكلمات المفتاحية: انترنت الأشياء، أمن انترنت الأشياء، التدقيق الداخلي لانترنت الأشياء، الضوابط العامة لتكنولوجيا المعلومات.

Abstract

The research aims to identify the concept of the Internet of Things (IoT), the most important security challenges, and the steps for auditing the IoT, and to draw the attention of internal auditors to the proposed methods and procedures through which internal audit can audit, evaluate, and provide advice regarding the IoT s, and to identify the most important general controls for information technology used in IoT audits.

To achieve the research objectives, the researchers used the deductive approach in this research and analysis using journals, books, and websites that address the research topic, especially with regard to the areas of: The IoT, the security challenges of the IoT, and the role of internal audit in evaluation, auditing, and advice.

The research reached to a set of findings, the most important of which are:

1. Ignoring the organization's management and internal audit of IoT security can lead to serious impacts on the organization's success, resulting in data breaches, financial losses, and legal problems, as well as damage to the organization's reputation.
2. It is the responsibility of internal audit professionals to closely monitor the IoT landscape to identify and prevent the risk areas to impacting the business.
3. An audit work program can be developed that includes the necessary procedures to evaluate and audit aspects related to Internet of Things risks.

Based on the research conclusions, recommendations were presented that are consistent with these conclusions, the most important of which are:
It is necessary for parties interested in the internal audit profession to hold seminars for auditors and hold specialized workshops to introduce the Internet of Things, and to draw the attention of internal auditors to the ways in which internal audit can provide evaluation and audit in relation to the Internet of Things, and consider this an essential part of the task of the successful internal auditor who adds value to the company. That gave him her trust.
Keywords: Internet of Things, Internet of Things security, Internet of Things, internal audit, general information technology controls.

1- المقدمة:

يعد انترنت الأشياء Internet of Things (IoT) موضوعًا ساخناً وقد فتحت التطورات في السنوات القليلة الماضية نافذة على فرص تحويلية مذهلة إنترنت الأشياء عبارة عن شبكة من الأجهزة المترابطة التي تقوم بجمع البيانات وتبادلها، على الرغم من أن تطبيقه لا يزال في مرحلة الوليدة، إلا أن تطبيقه في المؤسسات الكبيرة قد نما بشكل ملحوظ، مما يسهل جمع البيانات بشكل أسهل وأكثر كفاءة ويخلق إنترنت الأشياء فرصاً لإعادة هندسة العمليات الصناعية وإحداث ثورة في تجارب الزبائن، مع تحسين كفاءة وفعالية العمليات التجارية.

اليوم، أصبح إنترنت الأشياء جزءًا لا يتجزأ من حياتنا اليومية. لقد حولت تكنولوجيا إنترنت الأشياء قطاعات مختلفة، بما في ذلك الرعاية الصحية والتصنيع والنقل والزراعة، من المنازل الذكية إلى المدن الذكية. ومن خلال الاستفادة من إنترنت الأشياء، يمكن للمؤسسات تحسين تجارب الزبائن وتحسين استخدام الموارد.

يتمتع إنترنت الأشياء (IoT) بإمكانية تحقيق فوائد هائلة في البيئات التنظيمية. ولسوء الحظ، تأتي هذه التقنيات أيضاً مصحوبة بعدد لا يحصى من نقاط الضعف التي يمكن أن تكون بمثابة قنوات للهجمات السيبرانية، ومن ثمَّ كانت هناك تحركات لمعالجة هذه المخاوف، بما في ذلك تطوير المعايير والمبادئ التوجيهية والأطر التنظيمية الدولية والمحلية ودور التدقيق الداخلي.

يلعب التدقيق الداخلي دوراً حاسماً في مواجهة هذه التحديات من خلال التقييم والتدقيق وتقديم المشورة بشأن الوضع الأمني لأجهزة إنترنت الأشياء، وتقييم ممارسات خصوصية البيانات، وضمان قابلية التشغيل البيني والتوافق بين الأنظمة المترابطة ومن خلال معالجة هذه المخاطر والتحديات، يمكن للمؤسسات الاستفادة من الإمكانات الكاملة لإنترنت الأشياء مع الحفاظ على أمان وخصوصية أنظمتها وبياناتها.

2- منهجية البحث

2-1 مشكلة البحث: تتمثل المشكلة الأساسية للبحث في تساؤل رئيس وهو :

ما هي الأساليب والإجراءات المقترحة التي يمكن للتدقيق الداخلي من خلالها تقديم التقييم والتدقيق والمشورة فيما يتعلق بمخاطر إنترنت الأشياء؟

ويتفرع من هذا التساؤل الأسئلة الفرعية الآتية:

1. ما هي أهم التحديات الأمنية لإنترنت الأشياء؟ لماذا يعد أمن إنترنت الأشياء ضرورياً لنجاح الشركة؟
2. ماهي خطوات تدقيق انترنت الاشياء؟ ما الذي تم تضمينه في تدقيق إنترنت الأشياء؟
3. ما هي الأسئلة الأساسية التي يجب مراعاتها عند وضع خطط التدقيق والنظر في دورها في إنترنت الأشياء؟ وماهي الخطوات الموصى به في نشاط التدقيق الداخلي لإنترنت الأشياء؟
4. أهم ضوابط تكنولوجيا المعلومات العامة المستخدمة في عمليات تدقيق إنترنت الأشياء؟

2-2أهمية البحث:

تأتي **أهمية البحث** من أهمية موضوع انترنت الاشياء، إذ أحدث ثورة في حياتنا الشخصية والمهنية، يلعب إنترنت الأشياء دوراً محورياً في مشهد الأعمال. فهو يسمح للآلات بإكمال المهام الشاقة دون تدخل بشري، ويمكن للشركات أتمتة العمليات وتقليل تكاليف العمالة وتقليل الهدر وتحسين تقديم الخدمات، وهذا يساعد المنظمة على تقليل تكلفة تصنيع البضائع وتسليمها، ويوفر الشفافية في معاملات الزبائن.، مما يوفر رؤى حول كل شيء بدءًا من أداء الآلات وحتى سلسلة التوريد والعمليات اللوجستية.

ومن هنا فإن موضوع انترنت الأشياء مهم لمجالس الإدارة وإدارة المخاطر والتدقيق الداخلي، إذ إنه موضوع حيوي وهام في الممارسات المهنية للتدقيق الداخلي، مع وصف وتحليل دور التدقيق الداخلي في التدقيق والتقييم والمشورة.

ويعد البحث بمثابة دعوة لمجالس الإدارة والتدقيق الداخلي وإدارة المخاطر للتعرف على مخاطر إنترنت الأشياء بوصفها تهديداً للمنظمة، مع ضرورة التعاون فيما بينهم بوصفهم شركاء في إدارة مخاطر وتحديات المنظمة. انترنت الأشياء.

وعليه فإن هذه الدراسة تعد من الدراسات الجديدة التي لم يتم التطرق إليها من قبل بالشكل الكافي. ولذلك يعد هذا البحث من المحاولات العلمية الهادفة إلى إثراء الإنتاج الفكري في موضوع التدقيق على إنترنت الأشياء.

2-3أهداف البحث :يهدف البحث إلى تحقيق الأهداف الآتية:

1. التعرف على مفهوم انترنت الأشياء وأبعاده.
2. التعرف على أهم التحديات الأمنية لإنترنت الأشياء.
3. الاطلاع على أهم خطوات واجراءات التدقيق الداخلي المقترحة لانترنت الأشياء، وما الذي يتضمنه التدقيق على إنترنت الأشياء؟
4. تحديد الأسئلة الرئيسة التي يجب مراعاتها عند تطوير خطط التدقيق والنظر في دورها في إنترنت الأشياء.
5. التعرف على أهم ضوابط تكنولوجيا المعلومات العامة المستخدمة في عمليات تدقيق إنترنت الأشياء.

2-4 فرضيات البحث :

1. تعمل وحدات التدقيق الداخلي إلى تكثيف جهودها لمواجهة التحدي المتمثل في ضمان عمل الضوابط المتعلقة بمخاطر أنظمة إنترنت الأشياء بفعالية، وعدم تفويت الفرص.
2. يمكن للتدقيق الداخلي أن يلعب دوراً في تحديد مخاطر انترنت الأشياء الناشئة والدفاع ضدها.
3. يمكن وضع برنامج عمل للتدقيق الداخلي يتضمن الجوانب المتعلقة بمخاطر إنترنت الأشياء.
4. يمكن تحديد الإجراءات المقترحة للتدقيق الداخلي لإجراء التدقيق والتقييم وتقديم المشورة فيما يتعلق بمخاطر انترنت الأشياء في المنظمات.

2-5 منهج البحث:

يعتمد البحث على استخدام المنهج الاستدلالي في الدراسة والتحليل من خلال استخدام الدوريات والكتب والمواقع الالكترونية التي تتناول موضوع البحث، خاصة فيما يتعلق بمجالات: مفهوم انترنت الأشياء وأبعاده، التحديات الأمنية لإنترنت الأشياء، تدقيق انترنت الأشياء، الضوابط العامة لتكنولوجيا المعلومات المستخدمة في عمليات تدقيق على إنترنت الأشياء.

وعليه فقد تم تقسيم البحث على وفق الخطة الآتية :

المبحث الأول: الإطار النظري لإنترنت الأشياء وأبعاده

المبحث الثاني: التحديات الأمنية لإنترنت الأشياء

المبحث الثالث: موقف التدقيق الداخلي من انترنت الأشياء

المبحث الرابع: تدقيق الداخلي لأنترنت الأشياء- الاجراءات المقترحة

3- المبحث الاول: الإطار النظري لأنترنت الأشياء وأبعاده

يشمل النمو الهائل للتكنولوجيا، الذي أدى إلى الثورة الصناعية الرابعة، مجموعة متنوعة من الابتكارات الجديدةَ، والتقنيات التي تغير الحياة كما نعرفها بشكل يومي.

تعد إنترنت الأشياء، والحوسبة السحابية، وسلسلة الكتل، والذكاء الاصطناعي عدداً قليلاً ًمن التقنيات العديدة التي تشكل مستقبل كيفية إدارة الأعمال في العالم الحديث، إنترنت الأشياء وتطورها في السنوات الأخيرة خلق فرصاً مالية، إلى جانب العديد من التهديدات الأمنية (O'Flaherty, 2020,3)

يشير إنترنت الأشياء إلى شبكة من الأجهزة والأشياء والأنظمة المترابطة التي تتواصل وتتبادل البيانات مع بعضها البعض، تتضمن هذه الشبكة الأشياء اليومية مثل الأجهزة الذكية والأجهزة المنزلية والآلات الصناعية. تكمن أهمية إنترنت الأشياء في قدرتها على جمع وتحليل كميات هائلة من البيانات، مما يمكّن المؤسسات من اتخاذ قرارات تعتمد على البيانات وتحسين الكفاءة التشغيلية (Greengard,2024,1-2)

فضلاً عن ذلك تظهر أهمية إنترنت الأشياء في قدرتها على دفع الابتكار وتحسين الإنتاجية وتحسين نوعية الحياة بشكل عام. من خلال ربط الأجهزة والأنظمة المختلفة، يمكّن إنترنت الأشياء المؤسسات الحصول على رؤى وأتمتة العمليات وإنشاء نماذج أعمال جديدة، يمكن لإنترنت الأشياء تحسين الإنتاجية من خلال تحسين استخدام الموارد على سبيل المثال، في مصانع التصنيع، يمكن لأجهزة استشعار إنترنت الأشياء مراقبة أداء المعدات والكشف عن الحالات الشاذة، مما يتيح إجراء صيانة استباقية وتقليل وقت التوقف عن العمل وهذا يؤدي إلى زيادة الكفاءة وتوفير التكاليف للمؤسسات(Tamboly,2024)

يعمل إنترنت الأشياء على تبسيط وأتمتة المهام المعقدة والتي تتجاوز في بعض الأحيان نطاق القدرات البشرية، يبلغ عدد الأجهزة المتصلة التي تشكل إنترنت الأشياء اليوم إلى المليارات.

ببساطة، أجهزة إنترنت الأشياء هي أجهزة كمبيوتر لديها القدرة على جمع ومعالجة كميات كبيرة من المعلومات الحساسة. على سبيل المثال، قد تشمل أجهزة إنترنت الأشياء الكاميرات والأجهزة الطبية المتصلة بالشبكة وأنظمة التحكم الصناعية (ICS) والطابعات ومجموعة واسعة من الأجهزة الأخرى. يجب حماية البيانات التي يمكن الوصول إليها من التعرض المحتمل (Davis & Anwar,2020,7).

اليوم، أصبحت شبكة الإنترنت منتشرة في كل مكان، حيث تصل إلى كل ركن من أركان العالم تقريباً، وتؤثر على حياة الإنسان بطرق لا يمكن تصورها. ومع ذلك، فإن الرحلة لم تنته بعد، نحن ندخل الآن عصراً من الاتصال الأكثر انتشاراً والذي سيتم فيه توصيل مجموعة واسعة جداً من الأجهزة بالإنترنت، نحن في عصر "إنترنت الأشياء تم تعريف هذا المصطلح من قبل مؤلفين مختلفين بعدة طرق مختلفة من أهم هذه التعريفات:

1. إنترنت الأشياء عبارة عن شبكة من الأجهزة المادية يمكن لهذه الأجهزة نقل البيانات فيما بينها دون تدخل بشري، لا تقتصر أجهزة إنترنت الأشياء على أجهزة الكمبيوتر أو الآلات يمكن أن يتضمن إنترنت الأشياء أي شيء مزود بمستشعر تم تعيين معرف فريد له (UID) الهدف الأساسي لإنترنت الأشياء هو إنشاء أجهزة الإبلاغ الذاتي التي يمكنها التواصل مع بعضها البعض (والمستخدمين) في الوقت الفعلي(Schulze 2024)

2. إنترنت الأشياء عبارة عن بنية تربط الأجهزة المادية ببعضها البعض باستخدام شبكة مثل الإنترنت. يمكن للأجهزة التي تعمل بأنظمة تشغيل مختلفة التواصل مع بعضها البعض عبر الشبكة، مما يسمح لها بمشاركة المعلومات والتحكم في الأجهزة المتصلة وأتمتة العمليات في بيئة الأعمال، يقوم إنترنت الأشياء بمراقبة العمليات الموجودة مسبقاً وإنشاء عمليات جديدة، يشتمل إنترنت الأشياء على العديد من المكونات الأساسية التي تنشئ نظاماً بيئياً سلساً ومترابطاً(Pawlan ,2024)

3. يُعرّف إنترنت الأشياء بأنه تفاعل بين العالمين المادي والرقمي. يتفاعل العالم الرقمي مع العالم المادي باستخدام عدد كبير من أجهزة الاستشعار والمحركات (Friess& Guillemin,2011,9-10)

4. شبكة من الاشياء المادية التي ترتبط رقمياً بأجهزة استشعار والمراقبة والتفاعل داخل المنظمة ، وبين المنظمة وسلسلة التوريد الخاصة بها، مما يسمح المرونة والرؤية والتتبع وتبادل المعلومات لتسهيل التخطيط والتحكم والتنسيق في الوقت المناسب لجميع العمليات (Daya & Bahroun, 2019,719)

وعليه يمكن تعريف انترنت الاشياء:

مجموعة واسعة من الأشياء المادية المجهزة بأجهزة استشعار وبرامج تمكنها من التفاعل مع القليل من التدخل البشري من خلال جمع البيانات وتبادلها عبر الشبكة. يتضمن إنترنت الأشياء العديد من الأجهزة "الذكية" الشبيهة بالكمبيوتر والتي أصبحت شائعة جداً اليوم، والتي يمكنها الاتصال بالإنترنت أو التفاعل عبر الشبكات اللاسلكية، وتشمل هذه "الأشياء" الهواتف وأجهزة تنظيم الحرارة وأنظمة الإضاءة وأنظمة الري والكاميرات الأمنية والمركبات والمدن.

يشير إنترنت الأشياء إلى نوع جديد من العالم حيث تكون جميع الأجهزة والأجهزة التي نستخدمها تقريباً متصلة بالشبكة. يمكننا استخدامها بشكل تعاوني لإنجاز المهام المعقدة التي تتطلب درجة عالية من الذكاء.

ولتحقيق هذا الذكاء والترابط، تم تجهيز أجهزة إنترنت الأشياء بأجهزة استشعار ومحركات ومعالجات وأجهزة إرسال واستقبال مدمجة إنترنت الأشياء ليس تقنية واحدة؛ بل هي بالأحرى مجموعة من التقنيات المختلفة التي تعمل معاً جنباً إلى جنب (Sethi& Sarangi,2017,1-2)

إن الاستراتيجية الوطنية لإنترنت الأشياء، إذا تم تصميمها وتنفيذها بشكل صحيح، من شأنها أن تزيد من فرصة إنترنت الأشياء لتحقيق فوائد اجتماعية واقتصادية كبيرة ولن تتمكن أي دولة من الحصول على هذه الفوائد بنجاح من خلال ترك تطوير إنترنت الأشياء للسوق فقط، تماماً كما لن تتمكن أي إجراءات حكومية من الحصول على كل الفوائد المحتملة دون وجود قطاع خاص قوي قادر على الإبداع دون أن يثقل كاهله قيود تنظيمية مفرطة، ومع إدراك البلدان على نحو متزايد لإمكانات إنترنت الأشياء، ينبغي لها أن تعمل على وضع استراتيجيات وطنية شاملة تعمل بشكل استباقي على تعزيز تطوير التكنولوجيا وتبنيها مع الحد من الحواجز التنظيمية التي تقيد نموها (New & Castro,2015,15)

تواجه الهيئات التنظيمية وهيئات الرقابة تحديات عندما يتعلق الأمر بوضع معايير لأمن البيانات لأن عوالم التكنولوجيا وتقييم التهديدات تتغير باستمرار وخطيراً.

ولسوء الحظ فإن إنترنت الأشياء مليء أيضاً بالآثار السيئة الناجمة عن انتهاكات البيانات، وحوادث الخصوصية، وهجمات حجب الخدمة الموزعة يعد كل جهاز في الشبكة نقطة دخول محتملة للمتسللين الضاريين، وحتى الاستخدام العادي للبيانات من قبل الشركات المصنعة وشركات السلع الاستهلاكية يمكن أن يكون محفوفاً بالمخاطر التنظيمية الدولية .

لقد أنشأت إنترنت الأشياء نموذجاً جديداً حيث تقوم شبكة من الآلات والأجهزة القادرة على التواصل والتعاون مع بعضها البعض بقيادة ابتكارات العمليات الجديدة في المؤسسات (Lee, 2019,1-2),تسببت هجمات الأمن السيبراني المنتشرة والمتزايدة باستمرار على أنظمة إنترنت الأشياء في حدوث مجموعة واسعة من المشكلات للأشخاص والمؤسسات فيما يتعلق بالسمعة والامتثال والتمويل والعمليات التجارية. ترجع الزيادة السريعة في الهجمات الإلكترونية جزئياً إلى النمو الهائل لأجهزة إنترنت الأشياء في مجالات مثل الشبكات الذكية، والمراقبة البيئية، وأنظمة مراقبة المرضى، والتصنيع الذكي، والخدمات اللوجستية. تمثل إدارة أمن إنترنت الأشياء تحدياً بسبب الطبيعة الديناميكية والعابرة للاتصال بين الأجهزة، وتنوع الجهات الفاعلة القادرة على التفاعل داخل أنظمة إنترنت الأشياء وقيود الموارد (Malik & Singh,2019,697-798).

1-3 المعايير والتشريعات الأساسية لأمن إنترنت الأشياء

فيما يلي، أهم المعايير والتشريعات الأساسية لأمن إنترنت الأشياء. وهذه الأمور مهمة لأنها توجه عملية تطوير ونشر أنظمة إنترنت الأشياء الآمنة والمتوافقة (Wrotniak,2023)(Illing, Dawn,2023) (Ioannis,2021)

1 .اللائحة العامة لحماية البيانات :(GDPR) لائحة في الاتحاد الأوروبي (EU) تحمي الخصوصية والبيانات الشخصية للأفراد. ويتضمن أحكاماً تتعلق بأمن أجهزة إنترنت الأشياء ومعالجة بيانات إنترنت الأشياء.

2 .إطار عمل NIST للأمن السيبراني في الولايات المتحدة الأمريكية: قام المعهد الوطني للمعايير والتكنولوجيا (NIST) بتطوير إطار عمل لتحسين إدارة مخاطر الأمن السيبراني عبر مختلف القطاعات، بما في ذلك إنترنت الأشياء. فهو يوفر إرشادات وأفضل الممارسات والمعايير لتأمين أجهزة وأنظمة إنترنت الأشياء.

يتطلب قانون تحسين الأمن السيبراني لإنترنت الأشياء لعام 2020 من NIST نشر معايير وإرشادات للوكالات بشأن "الاستخدام المناسب والإدارة من قبل الوكالات لأجهزة (IoT)صدرت NIST الإصدار النهائي من إرشادات الأمن السيبراني لإنترنت الأشياء للوكالات الفيدرالية - سلسلة NIST SP 800-213، في ديسمبر 2021.

3 .إطار الامتثال لأمن إنترنت الأشياء: هذه مبادرة من مؤسسة أمان إنترنت الأشياء لإنشاء إطار شامل لضمان أمان أنظمة إنترنت الأشياء. ويتضمن مجموعة من المتطلبات والإرشادات وقوائم المراجعة للمؤسسات لتقييم وتحسين أمان منتجات وخدمات إنترنت الأشياء الخاصة بها.

4. قانون أمن المنتجات والبنية التحتية للاتصالات: ينص هذا التشريع في المملكة المتحدة على أن الأجهزة الذكية الاستهلاكية يجب أن تتمتع بالقدرة على التخفيف من الهجمات السيبرانية والحماية منها، مما يضمن مستوى أعلى من الأمان لأجهزة إنترنت الأشياء في السوق.

4- المبحث الثاني: المخاطر والتحديات المحتملة في إنترنت الأشياء

على الرغم من أن إنترنت الأشياء يقدم العديد من الفوائد، إلا أنه يطرح أيضاً مخاطر وتحديات جديدة يجب معالجتها لضمان التشغيل الآمن والموثوق للأنظمة المترابطة.

مع استمرار توسع إنترنت الأشياء، فإنه يجلب العديد من المخاطر الأمنية التي يجب النظر فيها بعناية. أحد الاهتمامات الرئيسة في إنترنت الأشياء هو أمان الأجهزة والشبكات، ومع تزايد عدد الأجهزة المتصلة، يمكن استغلال نقاط الضعف في أجهزة إنترنت الأشياء للوصول غير المصرح به، أو شن هجمات إلكترونية، أو المساس بالبيانات الحساسة. ويشكل هذا تهديداً كبيراً لخصوصية وأمن الأفراد والمنظمات على حدٍ سواء

(Tamboly,2024)

لقد توسع اعتماد إنترنت الأشياء بشكل كبير في السنوات الأخيرة تتمتع الأجهزة "الذكية" بالعديد من التطبيقات والفوائد المحتملة للمستهلكين والشركات على حد سواء. على سبيل المثال، يمكن لأجهزة إنترنت الأشياء زيادة الكفاءة التشغيلية من خلال تمكين مراقبة وإدارة المعدات المركزية أو البنية التحتية الحيوية أو المواقع البعيدة.

يأتي تطوير تطبيقات إنترنت الأشياء مصحوباً بمجموعة من التحديات الأمنية الشائعة، ويتضمن ذلك معالجة نقاط الضعف في البرامج الثابتة للجهاز وبروتوكولات المصادقة فضلاً عن ذلك، فإنه يستلزم أيضاً ضمان النقل الآمن للبيانات وتخزينها.

1-4 ما هو أمن إنترنت الأشياء؟

يعد أمان إنترنت الأشياء مصطلحاً شاملاً يغطي الاستراتيجيات والأدوات والعمليات والأنظمة والأساليب المستخدمة لحماية جميع جوانب إنترنت الأشياء. يتضمن أمان إنترنت الأشياء حماية المكونات المادية والتطبيقات والبيانات واتصالات الشبكة لضمان توافر وسلامة وسرية النظم البيئية لإنترنت الأشياء.

يشير أمن إنترنت الأشياء إلى الممارسات والبروتوكولات التي تضعها لحماية أمان وخصوصية أجهزة إنترنت الأشياء ويهدف إلى حماية النظام البيئي المترابط للأجهزة ضمن إنترنت الأشياء تشمل المكونات الرئيسة للنظام البيئي لإنترنت الأشياء أجهزة الاستشعار والمحركات والشبكات وغيرها.

التحدي الذي يواجه الأجهزة الذكية هو أنه كلما زاد اتصالها، أصبح من الأسهل على المتسللين التدخل فيها، لا تتحمل الشركات المصنعة غالباً أي مسؤولية عن هذه المشكلات الأمنية (Jansasoy,2023)

إن الطبيعة الديناميكية لأمن إنترنت الأشياء مليئة بالتحديات المستمرة، وذلك بسبب الاكتشاف المنتظم للعيوب في أنظمة إنترنت الأشياء تعتمد الإدارة الأمنية الفعالة على عدة ممارسات أساسية(Wrotniak,2023):

أ. تحصين مكونات النظام.

ب. الحفاظ على البرامج الثابتة المحدثة.

ج. تنفيذ إدارة الوصول.

د. مراقبة التهديدات النشطة.

ه. والاستجابة السريعة للثغرات الأمنية التي تم تحديدها.

من خلال تأمين أجهزة إنترنت الأشياء وبيئات الاعمال، يمكنك تقليل خطر أن تصبح نقاط دخول إلى أجزاء أخرى من الشبكة.

2-4 أهم تحديات ومخاطر إنترنت الأشياء التي يجب معالجتها

وفقاً لدراسات :(MicroAI , 2023) (Chalishazar,2023) (Chakray,2024)

تتمثل التحديات الأمنية الشائعة لأجهزة إنترنت الأشياء ما يلي:

1. عدم كفاية حماية البيانات /نقص التشفير

بالنسبة لمعظم أجهزة إنترنت الأشياء، يعد الافتقار إلى تشفير البيانات مشكلة أمنية كبيرة كما يعد الافتقار الى التشفير في كل عملية إرسال أحد أكبر التهديدات الأمنية لإنترنت الأشياء.

2. البرمجيات الضعيفة: لا يتبع منشئو أجهزة إنترنت الأشياء دائماً أفضل الممارسات، بما في ذلك استخدام المكتبات ذات السمعة الطيبة والمحدثة تتفاقم هذه المشكلات بسبب صعوبة تصحيح أجهزة إنترنت الأشياء في كثير من الأحيان، مما يترك نقاط الضعف المعرضة للاستغلال.

3. واجهات غير آمنة

غالباً ما تستخدم أجهزة إنترنت الأشياء واجهات وبروتوكولات شبكة غير آمنة على سبيل المثال، تسمح بعض أجهزة إنترنت الأشياء بالاتصالات عبرTelnet ، مما يعرض بيانات الاعتماد والبيانات الأخرى بنص عادي على الشبكة.

4. الافتقار إلى التوحيد: أحد المساهمين الرئيسيين في ضعف أمن إنترنت الأشياء هو الافتقار إلى معايير ومتطلبات الأمان. بالنسبة لأجهزة إنترنت الأشياء، فإن معظم معايير الأمان هي توصيات اختيارية، إن وجدت على الإطلاق.

5. الوعي الأمني والتعليم

يمثل الافتقار إلى الوعي الأمني والتعليم أيضاً تحدياً كبيراً في مجال إنترنت الأشياء لا يدرك العديد من المستخدمين والشركات تماماً المخاطر المرتبطة بأجهزة إنترنت الأشياء وقد لا يتخذون الاحتياطات اللازمة لحماية أنظمتهم وبياناتهم.

6. انخفاض التكاليف

ومن أجل خفض التكاليف، يمكن لشركات التصنيع الحد من الاستثمار الأمني، ويمكن أن تكون النتيجة معدات لا يمكنها أبداً توفير الحماية الكافية. سيكون المستخدم النهائي دائماً في خطر، يمكن أن يكون تقليل تكاليف الأجهزة وكذلك التطوير في هذا السياق خطأً فادحاً. المستخدم هو الذي ينتهي بالدفع.

7.التهديد المتزايد للبرامج الضارة وبرامج الفدية الخاصة بإنترنت الأشياء

لقد زاد الخطر المحتمل للبرامج الضارة وبرامج الفدية التي تستهدف هذه الأجهزة، ويرجع ذلك إلى الانتشار السريع للأجهزة المتصلة بإنترنت الأشياء لقد حددهم مجرمو الإنترنت كأهداف جذابة لشن الهجمات.

8 .التعامل مع كميات كبيرة من البيانات وعدم الدقة في معالجتها

تقوم الكثير من أجهزة إنترنت الأشياء بإنشاء وإرسال مجموعة من المعلومات الحجم الهائل للبيانات يجعل من الصعب الحفاظ عليها وحمايتها.

9. عدم وجود تحديثات في الوقت المناسب والبرامج القديمة
تعد التحديثات ضرورية للحفاظ على أمان أجهزة إنترنت الأشياء. ويجب تحديث الأجهزة في الوقت المناسب، مجرد اكتشاف ثغرات أمنية جديدة غالباً ما لا تعطي الشركات المصنعة الأصلية لأجهزة إنترنت الأشياء الأولوية للأمن السيبراني عند تصميم منتجاتها وينتج عن ذلك إنتاج أجهزة أكثر عرضة للهجوم السيبراني.
10. تنوع التقنيات والمعايير المستخدمة
إحدى الصعوبات الرئيسة التي تواجه أمن أجهزة إنترنت الأشياء هي تنوع التقنيات والمعايير المستخدمة مع وجود العديد من الشركات المصنعة والبائعين المشاركين في النظام البيئي لإنترنت الأشياء، تم تطوير العديد من الأجهزة والبروتوكولات بمستويات مختلفة من الأمان. وهذا يخلق تعقيداً إضافياً عند محاولة ضمان الأمان في جميع جوانب شبكة إنترنت الأشياء.
11. عدم الوضوح في المسؤوليات
فيما يتعلق بالسلامة في أجهزة إنترنت الأشياء، هناك ثلاثة لاعبين رئيسيين: الشركة المصنعة ومزود الخدمة والمستخدم. في حالة وقوع هجوم إلكتروني، فإن تحديد المسؤوليات ليس واضحاً تماماً ويمكن أن يؤدي إلى صراعات.
12 .مواقع النشر غير الموثوقة
في بعض الأحيان يتم استخدام أجهزة إنترنت الأشياء في مواقع غير آمنة لفترات طويلة من الوقت، وهذا يجعل من السهل على المتسلل مهاجمة هذه الأجهزة دون أن يتم اكتشافها.

3-4 لماذا يعد أمان إنترنت الأشياء ضرورياً لنجاح مشروعك؟
سيكون لإنترنت الأشياء تأثير كبير على جميع جوانب الأعمال والمجتمع تقريباً لقد ارتفع عدد الأجهزة والخدمات الجديدة المصممة لإنترنت الأشياء بشكل حاد في السنوات الأخيرة، ويتم استخدام الأجهزة المتصلة بشكل متزايد لتوليد رؤى جديدة حول صحة الإنسان، وتحسين السلامة العامة، والحفاظ على الموارد، وتعزيز الإنتاجية، ودعم الحكومة الأكثر فعالية (New & Castro,2015,2)
ستتوفر عشرات المليارات من أجهزة إنترنت الأشياء الجديدة بحلول عام 2025، مما سيؤدي إلى زيادة الناتج المحلي الإجمالي العالمي بعشرات التريليونات من الدولارات، ولكن هذا لن يحدث إلا إذا قمنا بالأمور في نصابها الصحيح وخرجت الأجهزة الجديدة من الرفوف وبدلاً من ذلك، رأينا مخاوف تتعلق بالسلامة والأمن والخصوصية والموثوقية تعوق اعتمادها (Ioannis,2021)
تهيمن إنترنت الأشياء على العناوين الرئيسية، على الرغم من أن القصص تتأرجح بين فوائد استخدام الأجهزة المتصلة رقمياً والمخاوف الأمنية المرتبطة بها.
مع نمو الإنترنت يستمر عدد الأجهزة المتصلة في الارتفاع كل يوم، وهذا الاتجاه لا يتباطأ وينطوي ذلك على زيادة هائلة في التهديدات الأمنية الجديدة، حيث أن العدد المتزايد من أجهزة إنترنت الأشياء يمنح المتسللين ومجرمي الإنترنت المزيد من نقاط الدخول. المشكلة الأمنية الرئيسية لإنترنت الأشياء هي التعرض للقرصنة (psa.inc, 2020)
يعد أمان إنترنت الأشياء أمراً مهماً نظراً لحساسية أجهزة إنترنت الأشياء والاستخدام المتزايد لأجهزة إنترنت الأشياء. تظل العديد من أجهزة إنترنت الأشياء غير مشفرة ويمكن أن تكون بمثابة بوابة للمتسللين، حيث يمكن لجهاز واحد مخترق أن يمنح شخصاً ما إمكانية الوصول إلى شبكته المتصلة بالكامل (Becher,2023)
أحد المخاوف الرئيسة هو احتمال وقوع هجمات إلكترونية. يمكن للمتسللين استغلال أجهزة إنترنت الأشياء الضعيفة لديك. يمكن أن يمنحهم وصولاً غير مصرح به إلى شبكتك أو بياناتك مما يؤدي إلى اختراق البيانات، والخسائر المالية، والإضرار بسمعتك.
إحدى النتائج الأخرى لإهمال أمن إنترنت الأشياء هي الامتثال التنظيمي. ويختلف هذا حسب مجال عملك ونوع البيانات التي تعالجها، قد تخضع للوائح محددة لحماية البيانات والخصوصية يمكن أن يؤدي الفشل في تلبية هذه المتطلبات إلى فرض عقوبات ومشكلات قانونية وفقدان ثقة الزبائن.
يمكن أن يكون لتجاهل أمان إنترنت الأشياء آثار خطيرة على نجاح مشروعك يمكن أن يؤدي إلى عواقب وخيمة، يمكن أن يشمل ذلك خروقات البيانات، والخسائر المالية، والمشكلات القانونية. وأخيراً، قد يؤدي الافتقار إلى الأمان إلى الإضرار بسمعتك، ومن خلال إعطاء الأولوية لأمن إنترنت الأشياء منذ البداية، يمكنك التخفيف من هذه المخاطر كما أنه سيغرس الثقة في المستخدمين، ويضع أساساً متيناً لنمو مشروعك ونجاحه من خلال قيام التدقيق الداخلي بتقييم وتدقيق انترنت الاشياء (Wrotniak,2023).

5-المبحث الثالث: موقف التدقيق الداخلي من انترنت الاشياء

لدى المدققين الداخليين أسباب مختلفة للتفكير فيما يعنيه إنترنت الأشياء لمؤسساتهم وقد يُطلب منهم تقديم المشورة للإدارة بشأن الفوائد والميزة التنافسية المحتملة التي يمكن أن توفرها إنترنت الأشياء ومع ذلك، يجب عليهم أيضاً مراقبة المخاطر الجديدة التي يقدمها والضوابط التعويضية المطلوبة لا يمكنهم تحمل افتراض أن شيئاً ما، بمجرد إصلاحه، سيظل على حاله مثلما يرفع المد المرتفع جميع القوارب، فإن دورة التطور السريع لإنترنت الأشياء تعني تطوراً سريعاً بنفس القدر للمخاطر، ويتعين على المدققين الداخليين أن يظلوا مطلعين على هذه التغييرات وأن يكونوا مستعدين لإبقاء مؤسساتهم على اطلاع Seago , 2016,27-(28)

صنفت الدراسات الاستقصائية للشركات المهنية، مثل استطلاع قدرات واحتياجات التدقيق الداخلي لعام 2016 الذي أجرته شركة Protiviti، إنترنت الأشياء ضمن أهم أولويات التدقيق الداخلي لهذا العام تشير العديد من الدراسات الاستقصائية الاخرى حول التوقعات ومستقبل التدقيق الداخلي إلى أن أصحاب المصلحة يتوقعون المزيد من التقارير التطلعية فضلاً عن ذلك الرؤى حول المخاطر والتخطيط الاستراتيجي وتكنولوجيا المعلومات وأداء الأعمال يجب معالجة الفجوات الرئيسة في مهارات معينة، بما في ذلك التحليلات وتكنولوجيا المعلومات والاتصالات من أجل زيادة التأثر والتأثير.

التحدي الذي يواجه المتخصصين في التدقيق والامتثال هو التطور السريع والتقدم في إنترنت الأشياء. تتغير المخاطر والضوابط المرتبطة بها وتتطور بسرعة، ويحتاج المدققون الداخليون إلى مواكبة تطورات وتقدمات إنترنت الأشياء حتى يتمكنوا من تدقيق وتقييم المخاطر والضوابط في مؤسساتهم (Tabuena ,2016)

يمكن تحديد موقف التدقيق الداخلي من انترنت الاشياء وفق دراسات عديدة منها: (Cia , 2019) (Tabuena,2016)

1. يمكن للتدقيق الداخلي، باعتباره خط الدفاع الثالث، أن يلعب دوراً في تحديد المخاطر التي تنشأ والدفاع عنها ومع كون الامتثال جزءًا من تقييم المخاطر على مستوى المؤسسة، هناك أيضاً أدوار لكليهما من حيث الأهمية والفوائد والميزة التنافسية التي يمكن أن يحققها إنترنت الأشياء.
2. يعد المدققون الداخليون عنصراً أساسياً في الدفاع ضد احتمالات القرصنة والجرائم الإلكترونية وقضايا الخصوصية التي تأتي مع العيش في عالم يعتمد على قوة الإنترنت تقع على عاتق العاملين في التدقيق الداخلي مسؤولية مراقبة إنترنت الأشياء لتحديد مجالات المخاطر هذه ومنعها من التأثير على الأعمال.
3. إن إنترنت الأشياء في جوهره ثورة رقمية يمكنها تجديد عقلية المدرسة القديمة التي تم استخلاص التدقيق الداخلي منها منذ فترة طويلة يمثل التحدي الذي يواجه كل من المتخصصين في التدقيق والامتثال هو السرعة التي يتطور بها إنترنت الأشياء، مع تقدم المخاطر والضوابط المرتبطة بها يحتاج المدققون الداخليون إلى البقاء في الطليعة ومواكبة تطورات إنترنت الأشياء من أجل اكتشاف مؤشرات التغيير وتأثيرها على مؤسساتهم.
4. يمكن لوظيفة التدقيق الداخلي تقديم المشورة للإدارة بشأن الأهمية والفوائد والميزة التنافسية التي يمكن أن تجلبها إنترنت الأشياء إلى المنظمة، يمكن للمدققين أن يوضحوا للإدارة كيف يمكن تنفيذ إنترنت الأشياء في عمليات مثل توزيع المبيعات ومراقبة المخزون.
5. من خلال وظيفة إدارة المخاطر، يمكن للمدققين الداخليين المساعدة في تسهيل جلسات تقييم المخاطر مع الإدارة وإجراء الأبحاث لفهم كيفية استخدام إنترنت الأشياء داخل بيئة التشغيل المحددة للمؤسسة وبطبيعة الحال، أثناء أداء مثل هذه الخدمات الاستشارية، يجب على المدققين الداخليين الحفاظ على موضوعيتهم وعدم تحمل مسؤولية الإدارة.
6. هناك توقعات أكبر للمدققين الداخليين لتولي دور شريك تجاري أكثر استراتيجية في مؤسساتهم إن وظيفة "المستشار الموثوق " هي أكثر من مجرد كلمة طنانة يتم طرحها حول جزء التدقيق، فهو في الواقع يحدد نوع الشركات الفردية وأصحاب المصلحة المطلوبين لشغل دور التدقيق الداخلي.
7. يعد فريق التدقيق الداخلي عنصراً رئيساً في تقييم المخاطر الإستراتيجية التي تؤثر على الأعمال، وفقاً لتلك التي يمثلها إنترنت الأشياء تعتمد الشركات على وظيفة التدقيق الداخلي لديها لاستفادة من الفرص المتعلقة بإنترنت الأشياء فضلاً عن ذلك المخاطر المحتملة.

6-المبحث الرابع: التدقيق الداخلي لانترنت الاشياء- الاجراءات المقترحة

من المهم أن يفهم قادة تكنولوجيا المعلومات عملية تدقيق إنترنت الأشياء للبدء هناك ثلاثة أنواع من عمليات التدقيق:

1. الطرف الأول يتم إجراء تدقيق الطرف الأول من قبل الادارات المسؤولة عن أنشطة إنترنت الأشياء.
2. الطرف الثاني يتم إجراء عمليات تدقيق الطرف الثاني من قبل قسم التدقيق الداخلي داخل المنظمة.
3. الطرف الثالث يتم اجراء عمليات تدقيق الطرف الثالث بواسطة شركة تدقيق خارجية.

هنا، من الضروري فحص عملية تدقيق الطرف الأول، للحصول على إرشادات حول الإعداد لإجراء تدقيق إنترنت الأشياء (Kirvan,2020)

عند التحضير لتدقيق إنترنت الأشياء، يجب عليك تأمين التفويض والميزانية لإجراء التدقيق، وتحديد من سيقوم بإجراء التدقيق بعد ذلك، يتم تحديد الضوابط التي من المحتمل أن تخضع للتدقيق في حالة تعين مدقق داخلي، تأكد من أن فريق التدقيق على دراية بتدقيق أنظمة تكنولوجيا المعلومات والفروق الدقيقة في تكنولوجيا إنترنت الأشياء تحديد فريق قسم تكنولوجيا المعلومات الذي سيدعم عملية التدقيق، وإنشاء منطقة عمل لفريق التدقيق. تأمين مجموعة متنوعة من المستندات والتقارير والمعلومات الأخرى وإعدادها كأدلة للفحص من قبل المدققين الداخليين.

6-1تدقيق انترنت الاشياء

إننا نمر حالياً بثورة تكنولوجية تُعرف باسم الثورة الصناعة 4.0، والتي تدور حول الأنظمة المستقلة وإنترنت الأشياء والتعلم الآلي وما إلى ذلك، وبما أن التقنيات الجديدة أصبحت جزءًا من أنظمة تكنولوجيا المعلومات في المؤسسة، يحتاج المدققون أيضاً إلى ترقية أنفسهم بالمعرفة بأحدث الأدوات والتقنيات.

في تدقيق إنترنت الأشياء، من الضروري تحديد الإجراءات خطوة بخطوة الذي يجب اتباعها إلى جانب التحديات المحتملة وحلولها التي قد يواجهها المدققون أثناء المشاركة في تدقيق أجهزة إنترنت الأشياء.

يمكن تحديد خطوات تدقيق انترنت الاشياء على النحو التالي:

6-2 موضوع التدقيق

الخطوة الأولى هي تحديد موضوع التدقيق، وهو ما يعني ما يجب تدقيقه، ولكن قد يكون التحدي هنا هو عدم وجود تعريف مقبول عالمياً لإنترنت الأشياء. ولذلك، فإن المفتاح هو تضمين جميع أجهزة إنترنت الأشياء المستخدمة في المؤسسة وتحديد موضوع التدقيق. يحتاج الى الإجابة على السؤال الرئيس: ما الذي تقوم بتدقيقه (Tyag ,2019)

لذا، للبدء في التحضير لتدقيق إنترنت الأشياء، قم بإنشاء قائمة بكل شيء قد يكون متصلاً بالإنترنت، وخاصة الأصول التي تؤثر على العمليات التجارية. يجب أن يشمل المخزون الشامل لإنترنت الأشياء أنظمة سطح المكتب وأجهزة الكمبيوتر المحمولة والطابعات والماسحات الضوئية وآلات النسخ وأجهزة الفاكس. قم بتضمين جميع الأجهزة المتصلة بالشبكة في مركز البيانات، سواء كانت موجودة محلياً أو في مكان آخر أو في الحوسبة السحابية فحص وسائل التواصل الاجتماعي، فضلاً عن ذلك المنظمات الخارجية التي لديها اتصالات متكررة، مثل الزبائن والموردين الرئيسيين(Kirvan,2020)

6-3تحديد هدف التدقيق

الخطوة الثانية هي تحديد هدف التدقيق وهو ما يعني سبب قيامنا بتدقيقه وينصح الباحثون بتبني وجهة نظر قائمة على المخاطر وتحديد الأهداف وفقاً لذلك تعد مخاطر الأعمال والمخاطر التشغيلية والمخاطر الفنية ثلاث فئات رئيسة من مخاطر إنترنت الأشياء(Tyagi ,2019)

وهذا يعني أنه بمجرد أن نقرر ما الذي نقوم بتدقيقه، نحتاج إلى تحديد هدف التدقيق لماذا نقوم بتدقيقها؟ من وجهة نظر المدقق، فمن المستحسن اعتماد وجهة نظر قائمة على المخاطر وتحديد الأهداف وفقاً لذلك.

ويمكن تعريف المخاطر التقنية على النحو التالي (ISACA,2017,9) :

1. تحديثات البرامج والتصحيحات. قد يكون الوقت اللازم لإصدار التصحيح أطول من الدورة النموذجية للأجهزة التي لا تعتمد على إنترنت الأشياء.
2. عمر الأجهزة. تتمتع أجهزة إنترنت الأشياء بدورة حياتها الخاصة، وغالباً ما تكون قديمة.
3. معرفات المستخدم وكلمات المرور للتحكم في الوصول إما غير موجودة أو أنها مشفرة بشكل ثابت.
4. يمكن أن تتعرض أجهزة إنترنت الأشياء للاختراق بسرعة، لكن تصحيحها يستغرق أياماً أو أسابيع وتبقى العواقب الأوسع مجهولة لأنه من الصعب معرفة ما تمت رؤيته أو تعديله أو سرقته.
5. يمكن للقراصنة استخدام أجهزة إنترنت الأشياء كنقطة دخول إلى شبكات المؤسسة.

6-4 تحديد نطاق التدقيق

عند تحديد أهداف التدقيق يجب تحديد نطاق التدقيق، والذي يتضمن تحديد أجهزة إنترنت الأشياء الفعلية التي تحتاج إلى التدقيق وستكون هذه مهمة صعبة لأن الأجهزة ليست مجرد أجهزة استشعار، بل تتضمن البنية التحتية الداعمة مثل طرق الاتصال وجمع البيانات ووسائل التخزين والخوارزميات المستخدمة لمعالجة البيانات، وفقا لآراء مختلفة، فإن إجراء التخطيط المسبق للتدقيق

من شأنه أن يساعد في التخفيف من التحديات يتضمن التخطيط المسبق للتدقيق إجراء تقييم للمخاطر، وتقييم سيناريوهات المخاطر، وإجراء مقابلات مع الجهة الخاضعة للتدقيق للاستفسار عن الأنشطة أو مجالات الاهتمام التي ينبغي تضمينها في نطاق المهمة (Tyagi ,2019)

5-6 تنفيذ التخطيط المسبق للتدقيق

والآن بعد أن تم تحديد سيناريوهات المخاطر، ينبغي تقييمها لتحديد أهميتها يعد إجراء تقييم المخاطر أمراً بالغ الأهمية في تحديد النطاق النهائي للتدقيق القائم على المخاطر(ISACA, 2016,8)

تشمل اعتبارات الضمان الخاصة بإنترنت الأشياء ما يلي (ISACA.2015,12) :

1. كيف سيتم استخدام الجهاز من منظور الأعمال؟ ما هي العمليات التجارية المدعومة وما هي قيمة الأعمال المتوقع إنشاؤها؟
2. ما هي بيئة التهديد للجهاز؟ ما هي التهديدات المتوقعة وكيف سيتم التخفيف منها؟
3. من سيتمكن من الوصول إلى الجهاز وكيف سيتم التعرف على هوياتهم والتحقق منها؟
4. ما هي عملية تحديث الجهاز في حالة نشر هجوم أو ثغرة أمنية؟
5. من المسؤول عن مراقبة الهجمات أو الثغرات الجديدة المتعلقة بالجهاز؟ كيف سيقومون بهذه المراقبة؟
6. هل تم تقييم جميع سيناريوهات المخاطر ومقارنتها بقيمة الأعمال المتوقعة؟
7. ما هي المعلومات الشخصية التي يتم جمعها أو تخزينها أو معالجتها بواسطة أجهزة وأنظمة إنترنت الأشياء؟
8. هل يعلم الأفراد الذين تنطبق عليهم المعلومات الشخصية أنه يتم جمع معلوماتهم واستخدامها؟ هل أعطوا موافقتهم على مثل هذه الاستخدامات والجمع؟
9. مع من سيتم مشاركة البيانات والإفصاح عنها؟

أخيراً ينبغي إجراء مقابلة مع الجهة الخاضعة للتدقيق للاستفسار عن الأنشطة أو مجالات الاهتمام التي ينبغي تضمينها في نطاق المهمة.

فيما يلي الأسئلة الأساسية التي يجب مراعاتها عند وضع خطط التدقيق والنظر في دورها في إنترنت الأشياء: (Reed,2016)

1. كيف يتم نشر إنترنت الأشياء في مؤسستنا اليوم؟ من يملك إنترنت الأشياء أو مكوناته؟
2. التفكير في المخاطر المرتبطة بوجود إنترنت الأشياء؟ كيف تم قياس تلك المخاطر والسيطرة عليها؟
3. هل نعرف ما هي البيانات التي يتم جمعها وتخزينها وتحليلها؟ هل تم تقييم الآثار القانونية والخصوصية والأمنية المحتملة؟
4. هل لدى الشركة خطط طوارئ لـ "أشياء" الإنترنت التي تم اختراقها أو تعديلها لأغراض غير مقصودة؟
5. إلى أي مدى تستخدم الأطراف الثالثة إنترنت الأشياء وتتصرف بالنيابة عنا؟ هل لدينا الإجراءات والاتفاقيات المناسبة المعمول بها لمراقبة تلك الأطراف الثالثة بشكل مناسب؟
6. ما هو الدور الذي يلعبه إنترنت الأشياء في استراتيجيتنا الحالية كمنظمة؟ كيف نقيس الإنجاز المتعلق بأية أهداف مرتبطة بالأهداف الإستراتيجية؟
7. ما هي مخاطر عدم النظر في إمكانيات إنترنت الأشياء أو الاستفادة منها بشكل أكبر؟ هل نستخدم تحليلات البيانات إلى أقصى إمكاناتها؟

6-6 الخطوة الرابعة هي تحديد إجراءات التدقيق وخطوات جمع البيانات

في هذه المرحلة من عملية التدقيق، يجب أن يكون لدى فريق التدقيق معلومات كافية لتحديد واختيار نهج أو استراتيجية التدقيق والبدء في تطوير برنامج التدقيق ومع ذلك يجب تحديد خطوات الاختبار.

لإجراء فحص لكل من الضوابط العامة لتكنولوجيا المعلومات (ITGC) يتم استخدام مجموعة من التقنيات التالية :(Kirvan,2020)

أ. القيام بإجراء مقابلة مع الموظفين والمديرين المسؤولين عن موارد إنترنت الأشياء.

ب. فحص الوثائق مثل الإجراءات المكتوبة والسياسات والأدلة الفنية.

ج. الحصول على أدلة مرئية، مثل لقطات الشاشة للتحقق من أداء عناصر تحكم محددة.

د. توثيق الملاحظات الشخصية - على سبيل المثال، ملاحظة كيفية أداء الموظفين للمهام المتعلقة بالرقابة.

ولذلك يُقترح مراجعة الجوانب المميزة لإنترنت الأشياء من خلال النظر:(ISACA, 2018,5)

1. الضوابط الأساسية العامة – الحد الأدنى من الضوابط التي يجب تطبيقها على جميع جوانب التكنولوجيا.

2. الضوابط المتعلقة بالبيانات – الضوابط التي تنطبق على البيانات التي تشكل جزءًا رئيساً من إنترنت الأشياء. مثل عناصر التحكم التي تنطبق على البيانات التي تشكل جزءًا رئيساً من إنترنت الأشياء.
3. التحليل والضوابط المتعلقة بالتعلم - الضوابط المعمول بها للتأكد من أن التحليل أخلاقي ويتيح الاستخدام الموثوق للبيانات وأن نتائج التحليل يمكن تطبيقها على اتخاذ القرارات التجارية.
4. محاذاة الأعمال والعمليات - الضوابط المتعلقة بالجوانب التي تضمن توافق تنفيذ إنترنت الأشياء مع احتياجات العمل وتقديم فوائد الأعمال على النحو المطلوب.

يساعد إنترنت الأشياء في خلق قيمة تجارية كبيرة وبالتالي سيبقى ويتحسن. ومع ذلك، نظراً للطبيعة الديناميكية للتكنولوجيا، فمن المستحسن اعتماد نموذج تدقيق مشترك من شأنه أن يجعل تدقيق إنترنت الأشياء أسهل وأكثر

6-7استراتيجيات تدقيق إنترنت الأشياء

نظراً للمخاطر والتحديات الفريدة التي تواجه إنترنت الأشياء يحتاج المدققون إلى اعتماد استراتيجيات محددة لتقييم سلامة الأنظمة المترابطة وسريتها وتوافرها بشكل فعال.

عندما يتعلق الأمر بتدقيق أنظمة إنترنت الأشياء يجب على المدققين ألا يركزوا فقط على الجوانب التقنية ولكن أيضاً أن يأخذوا في الاعتبار الآثار الأوسع للأجهزة المترابطة يتضمن ذلك فحص التأثير المحتمل على الخصوصية والأمان والعمليات التجارية بشكل عام.

فيما يلي إجراءات تقييم المخاطر والإدارة والامتثال والاعتبارات التنظيمية المتعلقة بإنترنت الأشياء:

(Tamboly,2024)(Salman, 2015,11)

6-8 تقييم المخاطر وإدارتها

قبل إجراء تدقيق لأنظمة إنترنت الأشياء، يعد إجراء تقييم شامل للمخاطر أمراً بالغ الأهمية وهذا يتضمن:

1. تحديد المخاطر المحتملة وتقييم احتمالاتها وتأثيرها. من خلال فهم المخاطر المحددة المرتبطة بأجهزة وشبكات إنترنت الأشياء، يمكن للمدققين تركيز جهودهم على تقييم المجالات الحيوية وتنفيذ الضوابط المناسبة.
2. يجب على المدققين أن يأخذوا في الاعتبار العواقب المحتملة لخرق الأمان أو خرق البيانات أثناء عملية تقييم المخاطر. وقد يشمل ذلك خسائر مالية وأضراراً بالسمعة وآثاراً قانونية. ومن خلال تحديد هذه المخاطر، يمكن للمدققين تحديد أولويات أنشطة التدقيق الخاصة بهم وتخصيص الموارد بشكل فعال.
3. يجب على المدققين النظر في الخصائص الفريدة لأنظمة إنترنت الأشياء التي قد تخلق مخاطر إضافية. على سبيل المثال، يمكن أن يؤدي العدد الهائل من الأجهزة المترابطة وتعقيد البنية التحتية للشبكة إلى زيادة مساحة الهجوم وزيادة صعوبة اكتشاف التهديدات والتخفيف من حدتها.
4. "يجب على المدققين إجراء تقييم لضعف هذه الأجهزة والنظر في إجراء اختبارات الاختراق على تلك الأنظمة بشكل دوري. وينبغي استخدام نتائج هذه الإجراءات لتعزيز أمن أنظمة إنترنت الأشياء.
5. يجب على المدققين الداخليين تقييم ما إذا كانت الضوابط موجودة لاستعادة أنظمة إنترنت الأشياء في حالة حدوث فشل.
6. يجب على المدققين الداخليين تحديد ما إذا كانت الإدارة تتفهم التأثير التجاري المحتمل لانقطاع نظام إنترنت الأشياء وما إذا كانت هناك السياسات والإجراءات والعمليات المناسبة والكافية مطبقة لاستعادة العمليات التجارية المتأثرة في الوقت المناسب في حالة حدوث انقطاع أو كارثة.

6-9 الامتثال والاعتبارات التنظيمية

يعد الامتثال للمتطلبات التنظيمية أمراً ضرورياً في عصر إنترنت الأشياء يتضمن دور التدقيق الداخلي بالاجراءات التالية: 35 (Tabuena ,2016) (Tamboly,2024)(O'Flaherty,2020)

1. تقييم ما إذا كانت المؤسسات متوافقة مع اللوائح ذات الصلة، مثل قوانين حماية البيانات والمعايير الخاصة بالصناعة.
2. تقييم فعالية الضوابط المعمول بها لضمان الامتثال والتوصية بالتحسينات إذا لزم الأمر.
3. عند تقييم الامتثال، يجب على المدققين التركيز على الضوابط الفنية والنظر في سياسات المنظمة وإجراءاتها وإطار الحوكمة. ويشمل ذلك تقييم مدى كفاية سياسات حماية البيانات، وخطط الاستجابة للحوادث، وبرامج تدريب الموظفين.
4. يجب على المدققين الداخليين مراعاة المعايير الخاصة بالصناعة وأفضل الممارسات ويجب على المدققين الداخليين تقييم ما إذا كان يتم اتباع هذه المعايير وما إذا كانت هناك حاجة إلى ضوابط إضافية للتخفيف من المخاطر الخاصة بالصناعة.

5. يجب أن يظل المدققون على اطلاع دائم بالمشهد التنظيمي المتطور ومعايير الصناعة الناشئة لتقييم الامتثال بشكل فعال في بيئة إنترنت الأشياء سريعة التغير.
6. تقييم ما إذا كانت أنظمة إنترنت الأشياء هذه قد خضعت لاختبار المناسب باستخدام حالات الاختبار المناسبة قبل نشرها في الإنتاج.
7.يجب وضع الضوابط لضمان إجراء الاختبارات الكافية قبل إجراء الترقيات والتصحيحات والتغييرات على أنظمة إنترنت الأشياء حيث تشكل الصحة والسلامة خطراً كبيراً.
8. تقييم ما إذا كانت هناك ضوابط مراقبة كافية وما إذا كانت جميع هذه الضوابط تعمل بفعالية مع مرور الوقت.
9. تقييم ما إذا كانت الاستثناءات والإخفاقات التي تحدث يتم تسجيلها بشكل مناسب ويتم تسجيل القرارات المتعلقة بالحوادث في الوقت المناسب.
10. يجب أن يكون المدققون يقظين لمعرفة أين ومتى يتم نشر أنظمة إنترنت الأشياء من قبل الإدارات المختلفة في المؤسسة وتحديد أولويات عمليات تدقيق أنظمة إنترنت الأشياء وفقاً لطبيعتها الحرجة والحساسة"
يمكن تلخيص خطوات اجراءات تدقيق إنترنت الأشياء بالآتي:
1. القيام بإعداد خطة تدقيق إنترنت الأشياء، والتي تتضمن نطاق التدقيق ونهج التدقيق والجدول الزمني.
2. مراجعة وتلخيص المعلومات التي تم جمعها للتدقيق، مثل الوثائق الفنية والاستبيانات وتقارير المخاطر ووثائق التدقيق السابقة، وتحديد الثغرات في الوثائق الموجودة، وتحديث المعلومات حسب الاقتضاء.
3. مراجعة وتطبيق المعايير واللوائح والتشريعات ووثائق الممارسات الجيدة للتحقق من صحة النتائج الأولية.
4. تحديد ضوابط التدقيق، وإعداد أوراق العمل التي تعكس مقاييس تدقيق إنترنت الأشياء التي تم تحديدها وتحديدها من قبل مجموعات المعايير والمنظمين والمشرعين وغيرهم.
5. بعد مقابلات التدقيق وأنشطة الاكتشاف، القيام بإعداد مسودة تقرير رأي حول تدقيق إنترنت الأشياء لمناقشتها مع الأطراف المهتمة في المؤسسة ثم اكمال تقرير تدقيق إنترنت الأشياء النهائي الذي يتضمن نتائج المناقشات والإجراءات الموصى بها.
6. أكمال خطة العمل والإطار الزمني لمعالجة نتائج وتوصيات تدقيق إنترنت الأشياء، والتأكد من تنفيذ خطة العمل لمعالجة نتائج تدقيق إنترنت الأشياء ضمن الإطار الزمني المتفق عليه.
7.قيام بجدولة تدقيق إنترنت الأشياء التالي، وقم بتضمين إنترنت الأشياء كجزء من عمليات تدقيق مستقبلية.

7-الاستنتاجات

1. إنترنت الأشياء (IoT) عبارة عن شبكة من الأشياء المادية التي تحتوي على إلكترونيات مدمجة في بنيتها من أجل التواصل واستشعار التفاعلات فيما بينها أو فيما يتعلق بالبيئة الخارجية في السنوات المقبلة، ستوفر التكنولوجيا القائمة على إنترنت الأشياء مستويات متقدمة من الخدمات وستغير عملياً الطريقة التي يعيش بها الناس حياتهم اليومية.
2. نظراً لمساحة الهجوم الموسعة للمخاطر الأمنية المتعلقة بالتوافر والنزاهة والسرية، يعد أمان إنترنت الأشياء أمراً بالغ الأهمية للمؤسسات لحماية بيئات شبكاتها من التهديدات المحمولة على أجهزة إنترنت الأشياء.
3. يمكن أن يكون تجاهل إدارة المؤسسة والتدقيق الداخلي لأمن إنترنت الأشياء آثار خطيرة على نجاح المؤسسة. يمكن أن يؤدي إلى عواقب وخيمة، ومن ثم خروقات البيانات والخسائر المالية والمشاكل القانونية فضلاً عن ذلك اضرار بسمعة المنظمة.
4. يجب على المدققين الداخليين فهم مفهوم وأبعاد إنترنت الأشياء لتقييم المخاطر وتقييم الضوابط والتأكد من الالتزام بالمتطلبات التنظيمية. من خلال اعتماد اجراءات تدقيق تكنولوجيا المعلومات، والاستفادة من التقنيات الناشئة مثل الذكاء الاصطناعي، وسلسلة الكتل، والحوسبة السحابية، والتعاون مع أصحاب المصلحة الآخرين.
5. تقع على عاتق فرق التدقيق الداخلي مسؤولية مراقبة مشهد إنترنت الأشياء عن كثب لتحديد مجالات المخاطر هذه ومنعها من التأثير على الأعمال.
6. يعد فريق التدقيق الداخلي عنصراً اساسياً في تقييم المخاطر الإستراتيجية التي تؤثر على الأعمال، وذلك وفقاً لتلك التي يمثلها إنترنت الأشياء. تعتمد الشركات على وظيفة التدقيق الداخلي لديها لزيادة مجالات الفرص المرتبطة بإنترنت الأشياء فضلاً عن ذلك المخاطر المحتملة.
7. يمكن وضع برنامج عمل للتدقيق الداخلي يتضمن الاجراءات اللازمة لتقييم وتدقيق الجوانب المتعلقة بمخاطر انترنت الاشياء.
8. لكي يقوم المدقق الداخلي بتدقيق إنترنت الأشياء، لابد لفريق التدقيق على دراية بمراجعة أنظمة تكنولوجيا المعلومات تحديد فريق تكنولوجيا المعلومات الذي سيدعم عملية التدقيق، وإنشاء منطقة عمل لفريق التدقيق تأمين مجموعة متنوعة من المستندات والتقارير والمعلومات الأخرى وإعدادها كأدلة للفحص من قبل المدققين الداخليين.

9. يحتاج المدققون الداخليون إلى البقاء في المقدمة ومواكبة تطورات إنترنت الأشياء من أجل اكتشاف مؤشرات التغيير وتأثيرها على مؤسساتهم.
10. تعد سرعة العمل هي حقيقة من حقائق الحياة المعاصرة، وهي أمر يجب أن يكون المدققون الداخليون قادرين على مواكبته ليكونوا فعالين. يستخدم عمل المدققين التكنولوجيا أكثر من أي وقت مضى بسبب إنترنت الأشياء ومع ظهور التعلم الآلي والذكاء الاصطناعي والأتمتة ولذلك يجب أن يكون المرشحون القادمون إلى مجال التدقيق الداخلي قادرين على إثبات المعرفة ذات الصلة بكيفية تطبيق التكنولوجيا في الممارسة العملية.

8- المقترحات

1. قيام المهتمون بمهنة التدقيق الداخلي بعقد ندوات للمدققين وعقد ورش عمل متخصصة للتعريف بإنترنت الأشياء وتوجيههم إلى الأساليب والإجراءات التي يمكن من خلالها أن يقدم التدقيق الداخلي التقييم والتدقيق فيما يتعلق بمخاطر إنترنت الأشياء، وبالتالي جزء أساسي من مهمة المدقق الداخلي الناجح مما يضيف قيمة للشركة وهذا ما منحه ثقتها.
2. يجب على الجهات المهتمة بالتدقيق الداخلي توجيه إدارات التدقيق الداخلي بوضع برنامج عمل للتقييم والتدقيق يدرس الجوانب المتعلقة بإنترنت الأشياء في المؤسسة وتحديد الأهداف الأساسية والنطاق والإجراءات اللازمة لتحقيق تلك الأهداف.
3. دعم المدققين الداخليين في تحسين إدارة المخاطر والحوكمة وعمليات التدقيق الداخلي للتخفيف من مخاطر إنترنت الأشياء من خلال تطوير مهاراتهم العلمية والعملية والتقنية في هذا المجال.

المصادر

1-Becher, Brooke(2023) IoT Security: What It Is and Why It's Important, https://builtin.com/internet-things/iot-security.

2- Ben-Daya, Mohamed, Hassini, Elkafi, & Bahroun, Zied. (2019). Internet of Things and Supply Chain Management: A Literature Review. International Journal of Production Research, Volume 57, 2019 - Issue 15-16: Special Issue.

3- Chakray (2024) 10 security problems of the IOT, https://www.chakray.com/10-security-problems-internet-of-things/ 10 security problems of the IOT.

4- careersinaudit (Cia) (2019) Internal Audit and the Internet of Things, https://www.careersinaudit.com/article/internal-audit-and-the-internet-of-things/

5-Chalishazar,Tej (2023)11 Biggest security challenges & solutions for IoT, https://www.peerbits.com/blog/biggest-iot-security-challenges.html.

6. Davis ,Brittany & Anwar, Mohd (2020) Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study, IEEE Internet of Things Journal March 2020.

7-Greengard, samul (2024) Internet of Things electronic network, https://www.britannica.com/science/Internet-of-Things.

8- ISACA (2018) COLUMNS IS Audit Basics: Auditing the IoT, https://www.isaca.org/resources/isaca-journal/issues/2018/volume-5/is-audit-basics-auditing-the-iot .

9- ISACA(2017) Assessing IoT Upsides, Downsides and Why We Should Care About Them, USA, www.isaca.org/Knowledge-Center/ Research/ResearchDeliverables/Pages/ Assessing-IoT.aspx.

10- ISACA (2016) Audit Plan Activities: Step-By-Step, USA,www.isaca.org/KnowledgeCenter/Research/Documents/Audit-PlanAct

11- ISACA(2015) Internet of Things: Risk and Value Considerations, USA, 2015, www.isaca.org/ knowledge-center/research/researchdeliverables/pages/internet-of-things-risk-and-valueconsiderations.aspx.

12 - Illing, Dawn (2023) The Cybersecurity Improvement Act 2020 & NIST Cybersecurity For IoT, https://www.globalsign.com/en/blog/cybersecurity-improvement-act-nist-iot

13- Ioannis , Fotios Chantzis (2021) Why Is IoT Security Important?, https://builtin.com/iot-internet-things/practical-iot-hacking

14- Jansasoy, Jessica (2023)10 IoT Security Challenges and Solutions To Protect Your Devices (2023 https://www.linkedin.com/pulse/10-iot-security-challenges-solutions-protect-your-2023-jansasoy.

15-Kirvan,Paul (2020) How to conduct an IoT audit for compliance, https://www.techtarget.com/searchcio/tip/How-to-conduct-an-IoT-audit-for-compliance.

16- Lee, I. (2019)The Internet of things for enterprises: An ecosystem, architecture, and IoT service business model. / Internet of Things 7 (2019) 100078journal homepage: www.elsevier.com/locate/iot

17- New, Joshua & Castro, Daniel (2015) Why Countries Need National Strategies for the Internet of Things, Center for Data Innovation, December 16, 2015
18-Malik, Vinita & Singh Sukhdip(2019) Security risk management in IoT environment, Journal of Discrete Mathematical Sciences and Cryptography ,Volume 22, 2019 - Issue 4.
19- MicroAI (2023) IoT Security – The Top Six Risks , https://micro.ai/blog/iot-security-the-top-six-risks .
20- O'Flaherty, Christopher James(2020)A BRAVE NEW WORLD: A SHORT INTRODUCTION TO THE INTERNET OF THINGS AND ITS EFFECTS ON SOCIAL ENGINEERING, BDO South Africa Services .
21- Friess O. Vermesan, , P. Guillemin et al.(2011) "Internet of things strategic research roadmap," in Internet of Things: Global Technological and Societal Trends, vol. 1,
22- psa.inc, 2020 Why IoT Security is Important, https://www.psa.inc/company/news/why-iot-security-is-important/
23- Pawlan, David (2024) What is Internet of Things (IoT): An IoT Overview in 2024, https://aloa.co/blog/what-is-internet-of-things-iot-overview-and-explanation
24-Reed, Jordan,(2016) Internal Audit and the Internet of Things, https://blog.protiviti.com/author/jordan-reed/
25-Salman, S.(2015) Auditing The Internet Of Things. https://iaonline.theiia.org
auditing-the-internet-of-things.
26-Sethi, Pallavi & R. Sarangi, Smruti (2017) Internet of Things: Architectures, Protocols, and Applications , Journal of Electrical and Computer Engineering , Volume 2017 , https://doi.org/10.1155/2017/9324035.
27- Seago, Jane (2016) The Internet of Things requires internal auditors to confrontrisks that are not so neatly contained, Internal Auditor(Vol. 73, Issue 4) https://iia-indonesia.org/files/magazine/Majalah_IA_Aug2016.pdf
28- Schulze ,Jessica (2024) What Is the Internet of Things (IoT)? With Examples, https://www.coursera.org/articles/internet-of-things
29- Tamboly,Niloufer (2024) IT Audit Implications of The Internet of Things (IoT) https://www.google.com/search?
30- Tyagi Aditya (2019)Auditing the IoT, https://www.linkedin.com/pulse/auditing-iot-aditya-tyagi
31- Tabuena, Jose (2016) Internet of Things' role in internal audit & compliance, https://www.complianceweek.com/internet-of-things-role-in-internal-audit-and-compliance/10350.article .
32- Wrotniak, Karol(2023) 8 Key IoT Security Challenges and Proven Solutions from the Field, https://www.thedroidsonroids.com/blog/iot-security-issues-internet-of-things-security.