

دور أمن المعلومات في الحصول على ثقة الزبون

م.م بشرى علي

قسم ادارة الاعمال

جامعة جيهان- اربيل

المقدمة

• يعد أمن المعلومات احد اهم العوامل التي تؤدي الى الحصول على ثقة الزبون في المنظمات ومن خلال استخدام أمن المعلومات بالامكان ايجاد حلول على الاغلب لجميع المشاكل التقنية بالاضافة الى استغلال كافة الفرص التي تواجه المنظمة، وبسبب كون المعلومات من الموارد المهمة ،فانه بالامكان القيام بتوظيفها والاستفادة منها سواءً داخل المنظمة او في بيئتها الخارجية، وبالاعتماد على ما سبق فعلى المنظمات ان تبحث دوماً عن طرق مختلفة لرفع مستوى جودة قراراتها وذلك يتم من خلال الحفاظ على أمانة المعلومات المتوفرة لديها واطافة خصوصية كاملة لكافة بيانات زبائنها، والشركات وخصوصاً التي تعمل في مجال الاتصالات تعتمد بشكل كبير على استخدام ونشر انواع مختلفة من التقنيات التي تستهدف ادارة رأس المال الفكري لديها واستخدام أنظمة معلومات تتمتع باعلى مستويات الأمان والسرية والخصوصية، من خلال تجميع جميع البيانات المهمة في النظام وبعد ذلك القيام بمعالجتها وتحويلها الى معلومات قابلة للاستخدام في اتخاذ جميع القرارات الاستراتيجية والتكتيكية من قبل قادة المنظمة. من جانب آخر فإن ثقة الزبون تعد من المفاهيم المرتبطة بالعديد من المفاهيم الاخرى، مثال على ذلك سمعة المنظمة التي تعتمد على مدى ثقة الزبائن بتنفيذها لكافة وعودها لها في المستقبل ، وبما ان معظم الزبائن لديهم اهتمام كبير بالحفاظ على سلامة وخصوصية معلوماتهم الشخصية، وقد تم تقسيم هيكلية البحث الى ثلاثة محاور، المحور الاول منهجية البحث، اما المحور الثاني فتضمن الجانب النظري بمتغيريه الاول أمن المعلومات، والثاني ثقة الزبون، اما المحور الثالث فتضمن الجانب العملي للدراسة وتحليل اجابات عينة البحث، في حين تضمن المحور الرابع الاستنتاجات والتوصيات التي خرج بها البحث.

- المستقبل ، وبما ان معظم الزبائن لديهم اهتمام كبير بالحفاظ على سلامة وخصوصية معلوماتهم الشخصية، وقد تم تقسيم هيكلية البحث الى ثلاثة محاور، المحور الاول منهجية البحث، اما المحور الثاني فتضمن الجانب النظري بمتغيريه الاول أمن المعلومات، والثاني ثقة الزبون، اما المحور الثالث فتضمن الجانب العملي للدراسة وتحليل اجابات عينة البحث، في حين تضمن المحور الرابع الاستنتاجات والتوصيات التي خرج بها البحث.

مشكلة البحث

يمكن توضيح مشكلة البحث من خلال التساؤلات البحثية الآتية:

- هل تمتلك الشركات المبحوثة بنية تحتية أمنية كفوءة يمكن استخدامها لإدارة كافة معلوماتها والحصول على ثقة الزبون على المدى البعيد؟
- هل تمتلك الشركات المبحوثة الخدمات الكافية التي ترضي حاجات الزبائن وتساعد الشركات من الجانب الآخر على الحصول على الميزة التنافسية المستدامة؟
- هل تمتلك الشركات المبحوثة بنية تحتية أمنية قوية تحافظ على معلومات الزبون وسرية وخصوصية كافة المعلومات الشخصية الخاصة به؟

اهمية البحث

- والتي يمكن ايضاحها من خلال التالي:
- جاء هذا البحث للتركيز على أمن المعلومات والذي يعد من المواضيع التي عادة ما يتم الأغفال عنها خصوصاً في الشركات الخاصة بالاتصالات.
- تسليط الضوء اكثر على العلاقة ما بين متغيرات البحث والتي تتمثل بأمن المعلومات وثقة الزبون.
- الاستفادة من نتائج البحث لغرض تطوير وتحسين الانظمة المستخدمة من قبل الشركات المذكورة.

اهداف البحث

يهدف البحث الى الوصول الى مجموعة من الاهداف من أهمها التالي:

- توضيح العلاقة ما بين أمن المعلومات وثقة الزبون في شركات اسيا سيل، كورك تليكوم، نوروز.

- بيان تأثير أمن المعلومات على ثقة الزبون في الشركات المبحوثة.

- اعطاء اطار نظري لواحدة من اهم الحقول المستخدمة في مجال شركات الاتصالات والتي تتمثل بمتغيري أمن المعلومات وارتباطها بثقة الزبائن و اظهار امكانية استخدام تطبيقات وبرامجيات أمنة في شركات الاتصالات لغرض تحسين جودة الخدمات المقدمة من قبلها ولغرض الحصول على ثقة وولاء الزبائن بخدماتها على المدى البعيد.

فرضيات البحث

- يسعى البحث الحالي الى اختبار الفرضيات الآتية :
- الفرضية الأولى:
- H_0 : لا توجد علاقة ارتباط ذات تاثير معنوي مابين أمن المعلومات وثقة الزبون
- H_1 : توجد علاقة ارتباط ذات تاثير معنوي مابين أمن المعلومات وثقة الزبون
- الفرضية الثانية:
- H_0 : لا يوجد تاثير ذو دلالة معنوية لأمن المعلومات على ثقة الزبون.
- H_1 : يوجد تاثير ذو دلالة معنوية لأمن المعلومات على ثقة الزبون .

امن المعلومات

ويمكن تحديد مفهوم أمن المعلومات على انه المعيار المتبنى لمنع الاستخدام غير المخول او اساءة الاستخدام او التعديل والحرمان من استخدام المعرفة والحقائق و البيانات

متطلبات أمن المعلومات تتمثل بالاتي:

- تقدير الخطر والتعامل معه: اي القيام بتحليل لمخاطر أمن المعلومات للمنظمة.
- السياسة الأمنية: اي توجيه الادارة ومستوى الأمن.
- تنظيم أمن المعلومات: اي القيام بحوكمة أمن المعلومات.
- ادارة الموجودات (الاصول): اي اجراء جرد والقيام بتصنيف موجودات المعلومات.
- امن الموارد البشرية: اي الجوانب الأمنية المتعلقة بدخول وتحرك ومغادرة الموظفين للمنظمة.
- الأمن المادي والبيئي: اي حماية المعدات الحاسوبية .
- ادارة العمليات والاتصالات: ادارة السيطرة على الأمن التقاني في النظم والشبكات.
- الرقابة على الدخول: اي تحديد حقوق الوصول للشبكات والنظم والتطبيقات والوظائف والبيانات.
- امتلاك نظم المعلومات والقيام بتطويرها وصيانتها: اي بناء الأمن ليصبح جزءا من التطبيقات.
- ادارة الاحداث العرضية لأمن المعلومات: توقع اختراقات أمن المعلومات، والاستجابة لها بشكل مناسب.
- ادارة استمرارية الاعمال: اي حماية، وادامة (صيانة) واصلاح النظم وعمليات الاعمال الحرجة.
- المسايرة (المطاوعة): اي ضمان التوافق مع سياسة أمن المعلومات والمعايير والتشريعات والقوانين.

• **معيار ISO/IEC 27001**: ويعد من اهم معايير **IEC:ISO** يحدد هذا المعيار متطلبات انشاء، تنفيذ، تشغيل ومراقبة ومراجعة وادامة وتحسين نظم ادارة أمن المعلومات الموثقة.

• (NAKREM , 2007:16).

• **معيار التنفيذ الجيد لأمن المعلومات** : يتناول هذا المعيار أمن المعلومات من وجهة نظر الاعمال من اجل تقدير استعدادات المنظمة لتنفيذ أمن المعلومات, حيث انها تركز على الاستعدادات الخاصة بالمنظمة لجعل مخاطر الاعمال ذات العلاقة بنظم المعلومات الحساسة تحت السيطرة ضمن البيئة التنافسية والديناميكية المتواجدة اليوم (ZEGERS ,2006:35).

• **معيار ISO 27002:2005**: وهو معيار اخر من معايير ISO الخاصة بأمن المعلومات وتقانات الأمن - الشفرة التنفيذية، والذي يتكون من افضل الممارسات العالمية لحماية النظم. (JACKSON,2010:77).

• **معيار GRAMM-LEACH-BLILEY ACT**: وهو يعد من اهم المعايير التي غزت بها الحكومة الامريكية مجال معايير أمن المعلومات مما تطلب انشاء وسائل الوقاية المناسبة التي تتضمن، التأكد من موثوقية وأمن سجلات ومعلومات الزبائن، الحماية من التهديدات والمخاطر (CUNNINGHAM ET.AL ,2007 :289)

• **المعيار البريطاني BS 7799**: تم نشره في بريطانيا عام 1995 والهدف منه السماح للشركات التي تخضع لهذا المعيار باظهار قدرتها على التأكيد على عدم قدرة انتهاك الموثوقية والتكاملية والتوافرية للبيانات باي طريقة من الطرق (KRITZINGER,2006:46).

• **معيار معالجة المعلومات الفيدرالية FIPS 140-2**: وهو معيار يصف متطلبات تشفير البيانات الغير المصنفة وقد تم نشره من قبل المؤسسة القومية للمعايير والتكنولوجيا (NIST) وتم اعتماده بعد ذلك كاحد المعايير الفعلية، ويعرف هذا المعيار المستويات الأمنية الى المستوى الاول الاقل الى المستوى الرابع. (OSBORNE ,2006:102).

• والثقة تمثل واحدة من المقاييس التي تحدد العلاقة ما بين الجودة، والتي من المعتقد انها تزيد من شعور الامان لدى الزبون وتقلل من مستويات عدم التأكد لديه، وبالتالي تساهم في بناء بيئة داعمة لكافة الاطراف سواءاً الزبون او المنظمة (BALLA ET.AL, 2015: 4). من جانب آخر تمثل الثقة النية الكاملة للاعتماد على اطراف اخرى في مرحلة الخطر وهذا يأتي من الفهم الكامل للطرف الآخر والذي يكون مبنياً على خبرات سابقة (UPAMANNYU ET.AL, 2015: 4). بينما اوضح (NGUYEN, 2013: 99) ان الثقة تمثل مستوى الاعتمادية والذي يقدم من قبل طرف معين الى الطرف الآخر على اساس العلاقة التبادلية التي تربط بينهما.

• وصف مجال تطبيق البحث :تضمنت عينة الدراسة مجموعة من الموظفين العاملين في مجال تكنولوجيا المعلومات في شركات نوروز تيليكوم وشركة كورك تيليكوم وشركة اسياسيل في مدينة اربيل وكان عدد الاستثمارات الموزعة على الشركات الثلاث بشكل عام (61) استمارة ، اذ بلغ عدد الاستثمارات الموزعة في شركة كورك 32 استمارة في حين تم توزيع 10 استمارات في شركة نوروز و19 استمارة في شركة اسياسيل ،اذ تم توزيع الاستثمارات بشكل عام على كافة الموظفين العاملين في اقسام تكنولوجيا المعلومات.

3.6.1 الارتباط: تم استخدام اختبار بيرسون لقياس مدى الارتباط ما بين متغيري البحث وكما هو موضح في الجدول الآتي:

الجدول (3)

ارتباط بيرسون ما بين أمن المعلومات وثقة الزبون



		أمن المعلومات	ثقة الزبون
أمن المعلومات	Pearson Correlation	1	.516**
	Sig. (2-tailed)		.000
	N	61	61
ثقة الزبون	Pearson Correlation	.516**	1
	Sig. (2-tailed)	.000	
	N	61	61

- وبالاعتماد على فرضيات البحث فان نتائج التحليل الاحصائي التي تم الحصول عليها من برنامج SPSS اظهرت ان قيمة P بلغت (0.000) وهي اقل من (0.05)، سنرفض فرضية العدم ونقبل الفرضية البديلة مما يعني انه توجد علاقة ارتباط طردية متوسطة القوة ما بين متغيري أمن المعلومات وثقة الزبون ، اذا بلغت قيمة ارتباط بيرسون 0.51% عند مستوى معنوية (0.000) والذي يعني وجود علاقة ارتباط ذات دلالة معنوية ما بين متغيرات البحث.

الأنحدار

تم استخدام معامل الانحدار الخطي البسيط ما بين متغيري البحث (أمن المعلومات، وثقة الزبون) والذي يتضمن تحليل ANOVA الضروري لحساب مدى معنوية وتأثير المتغير المستقل (أمن المعلومات) على المتغير المعتمد (ثقة الزبون).

الجدول (4)

الانحدار الخطي البسيط

Model	Sum of Squares	<u>df</u>	Mean Square	F	Sig.
1 Regression	4.033	1	4.033	21.376	.000 ^a
Residual	11.131	59	.189		
Total	15.163	60			

الاستنتاجات

- تبين ان الشركات المبحوثة تمتلك السياسات الأمنية الملائمة والتي تجعل المعلومات المنقولة بشكل الكتروني عبر انظمتها تتمتع بالموثوقية والتكاملية والتوافرية.
- أمن المعلومات يتضمن توفير الحماية الكافية للمعلومات وعناصرها الحساسة والمتضمنة النظم والمكونات المادية، التي تستخدم لخرن ونقل المعلومات.
- ثقة الزبون تعد من اساسيات بقاء الزبون واستمراريته في التعامل مع الشركة، والتي تنبع من رضاه الدائم عن الخدمات التي يحصل عليها، اذ تبين ان ادارة الشركات المبحوثة تتعامل مع جميع العاملين والزبائن بصدق ونزاهة، وتحاول ايفاء جميع وعودها المقدمة للزبائن.

- توجد علاقة ارتباط طردية ومعنوية ما بين متغيري أمن المعلومات و ثقة الزبون مما يدل على اهمية الاهتمام بهذين العاملين داخل المنظمة سوياً .
- يوجد تأثير معنوي لأمن المعلومات على ثقة الزبون فكلما زاد مستوى أمان المعلومات المنقولة كلما ادى ذلك الى زيادة ثقة الزبون اكثر بالتعامل مع شركات الاتصال خصوصا في العصر الحالي الذي تكثر فيه حالات القرصنة .

التوصيات

• زيادة الوعي بأهمية استخدام التقانات الحديثة للحفاظ على أمن المعلومات كاستخدام معدات شركة سيسكو التي تعد الاقوى في مجال حماية المعلومات الأمر الذي يساهم في رفع مستوى ثقة الزبون .

• اهمية اعطاء الزبون الخصوصية الكافية من خلال استخدام انظمة ادارة ذاتية لخدمات الانترنت من دون اطلاع شركات الاتصالات على محتوى المعلومات والبيانات المنقولة من والى الزبون.

• ضرورة استخدام الشركات لشبكات داخلية تغنيها عن استخدام الانترنت العام والذي قد يتعرض للقطع في حال حدوث اي مشاكل داخلية او خارجية بالاضافة الى استخدام تقنية الشبكة الافتراضية الخاصة التي تجعل عملية نقل البيانات الشخصية تتم بشكل سري وآمن.