سلوكية قواعد البيانات في الحفاظ على امنية البيانات المخزنة

صباح محمد فياض

المعهد التقني في الناصرية

المستخلص

ان الحفاظ والسيطرة على أمنية وسرية معلومات قواعد البيانات من الإجراءات المهمة جدا في العصر الحديث طالما أن هنالك الكثير من وسائل الاختراق والتجسس والدخول على البيانات في شبكات الانترنيت .

وتزداد أهمية امن قواعد البيانات بزيادة أهمية البيانات المراد حمايتها. ويتوفر العديد من الطرق والوسائل الأمنية التي تساعد المحافظة على امن المعلومات وتشفيرها بالمستوى الذي يحقق متطلبات امن قواعد البيانات. ومن المعروف إن لكل منشأة او دائرة معينة توجد سياسة خاصة بها لحماية بياناتها من السرقة أو التلف بما يتناسب وحجم ونوع تلك البيانات بالإضافة إلى اليد التي تعمل على تلك البيانات وان وضع امن المعلومات يكون متماشيا مع إنشاء قاعدة البيانات .

Abstract

Obviously, For control and protect Database, security and confidential its an important procedures in the new century life whenever there is more hackers media for entering on the data in the network .

And the security increase when important data increase , and there are more methods and security medias helps to keep confidential Data and coding it in an method that verify Database security confidential .

As we Know for each company there is an special policy to protect it from destroying it associated with type and size the data .

Adding to the hand that its work on that data and the information state associated with Database building .

المقدمة

إن اغلب المنشآت والمؤسسات تعتمد في الوقت الحاضر على نظم إدارة قواعد البيانات لتسيير نشاطاتها وبرامجها اليومية ونتيجة للتطور الحاصل في العلم والتكنولوجيا الحديثة وسرعة الاتصال ونقل البيانات والتأكد من صحة صدورها والخزن والاسترجاع فقد ساعدت قواعد البيانات على إتمام كل هذه الأمور وبالسرعة الممكنة مع تقليص عدد الكوادر اللذين يعملون على إدارة قواعد البيانات هذه فعلى سبيل المثال , عند قيامك بحجز مقعد سفر بالطائرة ذهابا وإيابا إلى دولة معينة عن طريق مكتب حجز للطيران فعند وصولك إلى تلك الدولة والذهاب إلى مكتب الحجز والسفر لغرض العودة فانك بالتأكيد ستجد اسمك ورقم المقعد وتاريخ الذهاب والإياب وبعض المعلومات متوفرة هناك لدى تلك الدولة في قاعدة بيانات أي مكتب للحجز ولا يمكن التلاعب بهذه البيانات مهما كان الأمر إلا بموافقات وصلاحيات معينة وعند تغيير تاريخ الإياب مثلا فان المكتب يقوم بتغيير البيانات في جميع قواعد البيانات المرتبطة بقاعدة البيانات تلك , ويعتبر هذا التطور مهم جدا وذلك لسرعة نقل وتبادل البيانات المطلوبة وموثوقية تلك البيانات. ومن الممكن الرجوع إلى هذه البيانات والبحث عن أي سجل من سجلات قاعدة البيانات في أي وقت آخر دون الحاجة إلى تدوين تلك البيانات في أوراق أو اراشيف خاصة بذلك .

وأضاف الباحث بان قاعدة البيانات يجب إن لاتكون سهلة الوصول من قبل أي شخص اخر وان الكثير من قواعد البيانات تتطلب كلمة مرور أو طلب لوصول المعلومات بينما يوجد العديد من قواعد البيانات يمكن الوصول اليها بسهولة عن طريق الانترنيت .

مشكلة البحث :بالنظر لوجود الاهمية القصوى للحفاظ على سرية البيانات المخزنة من التلف او التلاعب ومن اجل تعزيز دور قواعد البيانات في الحفاظ على المعلومات المخزنة ولما لهذه الامنية من دور فعال لمنع محاولات الاختراق والسرقة لوجود العديد من المخترقين والمبرمجين على كافة الاصعدة البرمجية لذا ارتأى الباحث ان تكون الاستفادة من الشفرات البرمجية وطريقة عملها للحفاظ على تلك البيانات من الامور المهمة جدا لتكامل سرية البيانات .

أهمية البحث:تتبع أهمية البحث من خلال مايوفره من طرق جديدة لحماية البيانات المخزنة في جداول قاعدة البيانات من التلف والتلاعب والاطلاع على طرق وأنواع الاختراقات التي تمت بالسابق ومالها من تأثير على المصلحة الخاصة والعامة لأي منشاة أو مؤسسة .وماهي اهمية قواعد البيانات لما لها من دور فعال في خزن واسترجاع الكم الهائل من البيانات وبسرعة عالية بما يتناسب مع متطلبات الوقت الحاضر إضافة إلى التعرف على سلوك وعمل بعض الشفرات البرمجية إثناء التغيير والتلاعب بها . ويعتبر كوسيلة من وسائل التطور الحديث لحماية البيانات من العبث والتغيير والاطلاع عليها من قبل الأشخاص غير المخولين بالدخول الشرعي على البيانات ويعتبر من المواضيع المهمة جدا لأي منشأة أو دائرة أو شركة أو مؤسسة معينة

هدف البحث : يهدف البحث إلى التعرف على سلوكية امن قواعد البيانات وكيفية حماية البيانات المخزنة في جداول قاعدة البيانات. واشار الباحث الى كتابة بعض الشفرات البرمجية بلغة الاستفسارالمهيكل وتغيير بعض سلوكيات واجراءات هذه الشفرات وما لها من تأثير على امن قواعد البيانات . واكد الباحث على ان وسائل الاختراق هذه تعتبر بمثابة الاحتيال على الدخول الى قواعد البيانات على الرغم من ان اللغة البرمبية المكتوبة بها قواعدالبيانات تلك رصينة .

تحديد المصطلحات :قاعدة البيانات : هي عبارة عن تجميع من البيانات المترابطة فيما بينها ومجموعة من البرامج التي تسمح للمستخدمين للوصول الى هذه البيانات وتحديثها [1] .

ويرى الباحث انه في الحقيقة يوجد تعريفان أساسيان لقواعد البيانات :

1-من وجهة نظر المستخدم : هي عبارة عن مكان مخصص لخزن كم هائل من البيانات واسترجاعها من الذاكرة لغرض التعديل والتحديث أو طباعتها أو البحث عن بيانات معينة وبالسرعة الممكنة بدون أي تغيير أو تلاعب بها.

2- وجهة نظر المبرمج: هي على الاقل جدول او مجموعة جداول المترابطة فيما بينها بعلاقة معينة (من علاقات قواعد البيانات) لمنع التكرار ودقة عملية الخزن وسرعة الاسترجاع والحفاظ على امنية البيانات المخزونة من التلاعب او السرقة والاختراق .

سلوكية قواعد البيانات: وهي الاداء المتبع لنقل وتبادل البيانات والمعلومات المخزنة في جداول خاصة او تحديثها من قبل الاشخاص المخولين للدخول على هذه البيانات فقط في .

امن البيانات : هو السرية التامة للحفاظ على البيانات المخزنة من الاطلاع والسرقة والتلاعب .

الجانب النظري :سوف يقوم الباحث بعرض بعض المعلومات النظرية المتعلقة بالبحث ومنها :-

مدير قاعدة البيانات database Administrator:واحدة من الأسباب المهمة لاستخدام نظم إدارة قواعد البيانات هو وجود سيطرة مركزية لكلا من البيانات والبرامج التي يراد الوصول إليها . وان الشخص الذي يمتلك تلك الصلاحيات على ذلك النظام يسمى مدير قاعدة البيانات "Database administrator" (DBA) . [2]

ويرى الباحث ما إذا كان الطرف غير المصرح به قد حصل على رقم البطاقة بأي شكل من الأشكال ،وبذلك فقد تم انتهاك مبدأ السرية في حفظ وتخزين البيانات.

وظائف مدير قاعدة البيانات وتتضمن:-

1- تعريف المخططات : يقوم بإنشاء المخطط الأولي الأصلي بواسطة تنفيذ مجموعة من عبارات تعريف البيانات في لغة تعريف البيانات Data Definition language (DDL) .

2- هيكل التخزين وتعريف طريقة الوصول للبيانات Storage structure &access-method definition

3- المخططات و تعديل التنظيم الفيزيائي: Schema and physical-organization modification

3-يحمل التغيرات الى المخطط والتنظيم الفيزيائي ليعكس حاجة التغيرات في التنظيم .

4-ان مدير قاعدة البيانات هو الشخص المسؤول عن تخويل اشخاص ومنع اخرين ايضا بالدخول الى قواعد البيانات .

5- منح التفويض للدخول للبيانات: granting of authorization for data access:يقوم بمنح انواع من المفوظين للدخول على البيانات وكذلك ينظم أي جزء من قاعدة البيانات يمكن لمستخدمين مختلفين من الوصول للبيانات,والمعلومات الموثقة تحفظ في هيكل نظام خاص وبدوره يقوم بالاستشارة (consult) عندما يقوم شخص ما بمحاولة الوصول للبيانات في النظام .

6- إدامة وصيانة الإجراءات Routine maintenance:ويرى الباحث من الأمثلة المهمة لإدامة الإجراءات الفعالة لمدير قاعدة البيانات هي :-

1- إسناد قاعدة البيانات بشكل دوري periodically backing up the database إما بواسطة الأشرطة أو الأقراص أو بواسطة الخوادم البعيدة لتجنب فقدان البيانات في حالة فائضية البيانات .

2- التأكد من وجود مساحة كافية متوفرة على القرص للعمليات الاعتيادية وترقية وتحديث حجم القرص المطلوب دون فقدان أو تلف البيانات .

3- مراقبة الوظائف التي تجري على قاعدة البيانات وتضمن الأداء الجيد بالمهام العالية جدا والتي تقدم لبعض المستخدمين

نقاط ضعف أمن قواعد البيانات :يوجد العديد من الأخطاء التي تؤدي إلى ضعف الأمن في قواعد البيانات منها:

1) الأخطاء البرمجية إثناء كتابة البرامج .
2) خلل في تصميم هيكل النظام .
3) عدم الاستعداد التام والأخذ بنظر الاعتبار قواعد البيانات البديلة .

1) الأخطاء البرمجية إثناء كتابة البرامج :

غالبا مايو جد أخطاء برمجية و ثغرات في أي نظام حاسوبي، فمن الصعب على الشركات المنتجة لهذه الأنظمة التأكد من خلو المنتج من هذه الأخطاء لأنها غالبا ماتظهر بعد الاستخدام العملي لهذه الأنظمة من قبل

المنشات الأخرى. وللحماية من هذه الثغرات يجب تحديث النظام باستمرار و ذلك بتحميل و تنصيب آخر التحديثات الموجودة لنظام قواعد البيانات المستخدم في المنشأة و يمكن متابعة التحديثات و الحصول عليها من قبل منتج النظام .

2) خلل في تصميم هيكل النظام .

يعتبرالتصميم الهيكلي لأي نظام من الأمور الهامة جدا و التي يجب أن تأخذ جزء كبير من الإعداد و التصميم الجيد لها. فبعض أنظمة قواعد البيانات تستخدم هيكلية لاتوظف حلول جيدة للناحية الأمنية في النظام [3] .

3) عدم توافق نظام التشغيل مع نوع تلك التطبيقات يؤدي في بعض الاحيان الى اجبار قاعدة البيانات على العمل مع نظام غير متوافق وهذا يودي الى ضعف الامان فيها.

واضاف الباحث :

أ)إن التصميم الصحيح لأي نظام قاعدة بيانات يجب دراسته مليا وفق ما يتناسب مع متطلبات المنشاة ووضع إجراءات أمنية لغرض الدخول على البيانات فبمجرد ما أن يتم التعرف على هيكل قاعدة البيانات من قبل المخترقين يصبح من السهل التعرف والدخول على البيانات .

ب) عدم الاستعداد التام والأخذ بنظر الاعتبار قواعد البيانات البديلة :

عدم الاستعداد التام واستلال واستخدام بعض الإجراءات الفرعية لبرامج قواعد بيانات أخرى قد يكون ذات تأثير مباشر على أمن قاعدة البيانات.

فيوجد الكثير من الخيارات التي يمكن أن تضبط بشكل يجعل النظام عرضة للإختراق. و كمثال على هذه الخيارات يوجد في نظام قواعد البيانات المعروف أوراكل (Oracle) خيار يسمى ب 'REMOTE_OS_AUTHENT'. [4]

العواقب الأساسية المترتبة من قبل الهجمات على قواعد البيانات:

لاستيعاب حجم هذه المخاطر سوف يذكرالباحث حسب علمه بعض من الأمثلة الواقعية لمواقع وأنظمة تعرضت إلى اختراقات لقواعد البيانات وتم الاعلان عنها في شبكة الانترنيت العالمية . في أكتوبر من عام 2007، تعرض 3000 سجل من سجلات عملاء بنك التجارة الأمريكي (Commerce Bank)إلى الخطر والكشف عن معلوماتها من قبل المخترقين ، وقد تمت فعليا سرقة 20 سجل من هذه السجلات.تعرضت معلومات 570 عميل من عملاء متجر لبيع الهدايا الكترونيا (Scarborough & Tweed)إلى السرقة من قبل المهاجمين فقد تمكنوا من سرقة معلوماتهم الخاصة وكذلك سرقة معلومات بطاقاتهم الائتمانية.تعرض موقع الأمم المتحدة إلى تغيير في مظهر وشكل صفحة الموقع (Website defacement)من قبل مجموعة من المهاجمين المناهضين للحروب وذلك في شهر أغسطس من عام 2007.كذلك في عام 2007 تعرضت صفحة موقع أخبار ميكروسوفت البريطاني إلى تغيير في مظهر وشكل الصفحة من قبل مجموعة من المهاجمين [9] .هذه كانت بعض من الأمثلة على أنظمة تعرضت لهجمات حقن لغة الاستعلام وغيرها الكثير. وجميعها تجعلنا ندرك الخطر الكبير المترتب من هذه الهجمات – هجمات حقن لغة الاستعلام – وتجعلنا نتساءل كيف يمكن لنا أن نحمي النظام وقواعد المعلومات من مثل هذه الهجمات .

كيف يقوم المخترق باختراق قاعدة البيانات :

إن أي مبرمج يبدأ بتصميم قاعدة بيانات يقوم بوضع اسم للمستخدم كلمة مرور الى قاعدة بياناته وحسب علم الباحث انه في واقع الامر توجد للمخترق محاولات كثيرة للدخول على قاعدة البيانات والجانب

المهم هو كيفية الحصول على اسم المستخدم وكلمة السر , وان هذة العملية تسمى بالاختراق بالمفهوم العام وطالما إن قاعدة البيانات تستخدم في المنشات والمؤسسات والمصارف وما لها من أهمية عظيمة ولوجود شبكات الانترنيت اصبح الخطر جسيم نظرا لارتباط قاعدة البيانات بخادم الشبكة (server) لكي يتمكن مستخدم الانترنيت من الوصول لتقديم الخدمات المختلفة لزائر معين حسب صلاحياته المخولة له على ذلك الموقع ولان الخادم من الممكن اختراقه وهو مرتبط بخادم الشبكة , اذن اصبح من السهل اختراق قاعدة البيانات ولحل هذه المشكلة أو تخفيف المخاطر على الاقل فقد تم تزويد قاعدة البيانات بنظام تشفير قد لايكون صالحا دائما .

وبالطبع هناك عدة انواع من قواعد البيانات اشهرها Oracle وMysql وبالتحديد فان لغة الاستعلام البنيوية Mysql تعتمد عملية اختراقها على مايسمى بالحقن Injections والذي بدوره طريقة لاختراق قواعد البيانات ويعتمد على مبدا ارسال استعلام خاطئ للطرف الاخر بغية الحصول على منفذ للدخول فعند القيام بارسال معلومات يقوم باستقبالها مايعرف بخادم قواعد البيانات وهو يعلن عن اسمه وعمله فخادم قواعد البيانات لا يحتوي على قاعدة بيانات واحدة بل على عدة قواعد وبالتالي فمهمته تتلخص في توجيهك نحو القاعدة المناسبة وهنا تبدا المشكلة .

فعبارة لغة الاستعلام التالية توجة المستخدم نحو القاعدة المناسبة في حالة معرفته لاسم المستخدم وكلمة السر [5].

Select user WHERE name = '(name)' AND password = '(pass hashed)';

فلو فرضنا إن شخصا اخر يحمل الاسم xxxxوله كلمة سر هي abcd فعند تسجيل الدخول فان الطلب يرسل بالصيغة التالية :

SELECT user WHERE name = 'abcd' AND password = '900163f7d28e17f72';

وطالما ان المستخدم متوفر في قاعدة البيانات سوف يتمكن من الدخول الى البرنامج الجانب العملي: قام الباحث بتصميم الشفرة البرمجية اللازمة لحماية قاعدة البيانات من الاختراق كيف يحاول المخترق اختراق قاعدة البيانات.ان من لديه خبره في اختراق قواعد البيانات والدخول الشرعي او غير الشرعي القيام بالاتي حسب علم الباحث :

1- القيام بكتابة اسم المستخدم كما حصل عليه .

2- يقوم بكتابة كلمة السر كلاتي في حقل خانة password " or 1=1" فيصبح لدينا العبارة التالية :

SELECT user WHERE name = 'xxxx' AND password = ' ' OR 1=1 --

وذلك يعني بان المستخدم ذو الاسم xxxx ليس له كلمة سر أو كلمة سر فارغة لان 1=1 فلذلك نلاحظ بان المستخدم سوف ينفذ ويقوم بتغير كلمة السر الى كلمة فارغة وبالتالي تفتح قاعدة البيانات وتتم العملية بنجاح وقد تم اختراق العملية رهينه باحداهما اما الباسورد منعدم او 1=1 وبما ان 1=1 فانه سيرد علينا كما لو اننا قمنا بتسجيل الدخول

ولربما يتسائل البعض عن فقدان التشفير في الاستعلام ؟

والجواب هو لوجود علامتي التنصيص والتي تفيد بان مابعدهما هو تعليق , فعلامتا الناقص -- تفيدان في جعل ما بعدهما تعليق فقط وبالتالي فان الاستعلام التالي :

SELECT user WHERE name = 'xxxx' AND password = ' ' OR 1=1 --

يكون مكافئ للاستعلام التالي :

SELECT user WHERE name = 'xxxx' AND password = ' ' OR 1=1

وبالتالي فان عملية الاختراق تتم بنجاح إلا اذا اتخذت الاجراءات الامنية الصحيحة لمنع عملية الاختراق .

تعليق:ان ما حصل في الشفرة البرمجية اعلاه هو توجيه سؤال من قبل المستخدم بلغة الاستفسار المهيكل وهو هل ان (1=1) فكان الجواب نعم وكلمة نعم ادت الى قبول كلمة السر .

وقد قام الباحث بتجربة على قاعدة بيانات مشروع تخرج لطلبة المعهد التقني في الناصرية ووضع كلمة سر لهذه القاعدة محاولا لاختراقها وتم اتباع خطوات الاختراق اعلاه وبذلك تم فتح قاعدة البيانات المطلوبة . الامر الذي ادى الى ظهور سلبيات قاعدة البيانات الغير مرتبطة بامنية الدخول .

الأمور الواجب إتباعها لضمان أمن قواعد البيانات:الاطلاع على المعلومات المخزنة من خلال شاشة الكومبيوتر او سرقة كلمات السر بدون علم المقابل او إرسال رسائل البريد الالكتروني من أشخاص غير معروفين يعتبر نوعا من أنواع الاختراق والتجسس وبمثابة كشف لسرية المعلومات المخزنة . خرق السرية يتخذ أشكالا عديدة [10]. تجسس شخص ما على شاشة الكمبيوتر لسرقة كلمات سر الدخول لقاعد البيانات،أو رؤية بيانات سرية لديك بدون علم منك يمكن أن يكون خرقا للسرية. إذا الكمبيوتر المحمول يحتوي على معلومات حساسة عن موظفي الشركة قد يكون سرقة أو بيع، يمكن أن يسفر عن انتهاك لمبدأ السرية. إعطاء معلومات سرية عبر الهاتف هو انتهاك لمبدأ السرية ايضا إذا كان الطالب غير مخول أن يحصل على المعلومات.

السرية أمر ضروري (لكنها غير كافية) للحفاظ على الخصوصية من الناس الذين يخترقون الأنظمة لسرقة المعلومات الشخصية في النظام .

وفيما يأتي اهم الامور الواجب اتباعها لضمان امن قواعد البيانات:-

1- **التكامل او سلامة البيانات(data Integrity):** يعني تكامل البيانات هو عملية المحافظة على البيانات الموجودة في قاعدة البيانات من التغيير المتعمد او التحريف او التحديث عليها او حذفها وتدميرها بالكامل ويعتبر بمثابة انتهاك لتكامل البيانات المخزنة في قاعدة البيانات .ويرى الباحث بانه قد يكون الدخول على البيانات غير مقصود فيعتبر ايضا انتهاك لتكامل وسلامة البيانات .

2- **توفر البيانات :(data Availability):** والمقصود بهذا المصطلح هو استمرارية تواجد وتدفق البيانات إلى الأشخاص المخولين بالدخول الى بيانات قاعدة البيانات بصورة مستمرة و عند الحاجة لتلك البيانات ويجب الأخذ بنظر الاعتبار عدم منع الاشخاص المخولين من الدخول والاطلاع على قاعدة البيانات .

3- تحديد عدد محاولات الدخول الى قاعدة البيانات ولتكل ثلاث محاولات كحد أقصى.

4- تعطيل إذا أمكن الأمر الشبكي Ping والذي يوجد في برتوكل رسالة التحكم بالإنترنت (ICMP) و ذلك بعدم السماح للجهاز الخادم الذي يحتوي على نظام قواعد البيانات من الرد لطلبات هذا الأمر. فانه من الممكن الدخول الى قاعدة البيانات من خلال البروتوكول الخاص بالجهاز او خادم الجهاز .

ويرى الباحث الغاء امر فتح قاعدة البيانات وخصوصا قاعدة بيانات اكسس" Access" بأمر المفتاح .Shift ضروري جدا.

ويؤكد الباحث على عدم الاستجابة لطلبات الجهات الغير معروفة او الغير موثوقه .والتحديث المستمر للنظام بالتنسيق مع مبرمج قاعدة البيانات لانه يعرف مداخل ونقاط ضعف قاعدة بياناته.

وسائل الحماية من اختراق قواعد البيانات:

يمكن لمبرمجي قواعد البيانات الحماية من الاختراقات بتغييرات برمجية بسيطة مثل:

1- التحقق دائما من مدخلات المستخدم وذلك باختبار نوع المدخل ، طوله ، شكله ومدى الاحتمالات التي يأخذها هذا المدخل [6]

2- عدم استخدام مدخلات المستخدم مباشرة في شفرة ال SQL ، حيث يفضل فصلها واستخدام المتغيرات (Parameterized Input) .

3- على قدر الإمكان يفضّل عدم قبول المدخلات التي تحتوي على العلامات التالية:

الفاصلة المنقوطة التي تعني نهاية الشفرة،الواصلة المزدوجة (- -) التي تشير إلى أن ما تبقى من الشفرة هو تعليق وينبغي تجاهله، (/* ... */) [7] . والتي تعني أن ما بينها هو تعليق ينبغي تجاهله من قبل الخادم..

3- تنقيح المدخلات وإزالة بعض العلامات منها كالفاصلة المنقوطة و الواصلة المزدوجة وغيرها من العلامات التي قد تسهل على المخترق الوصول إلى قاعدة البيانات.

4- بعض وظائف قاعدة البيانات الأساسية والمخصصة يمكن استغلالها في الاختراق فالبرنامج قد يحتوي على مهام إضافية يمكن استغلالها مثل تغيير كلمة المرور وإنشاء مستخدمين جدد؛ لذلك جميع الوظائف والدوال الغير ضرورية في البرنامج يجب منعها من الاستخدام.

5- تعطيل خاصية الاستعلامات المتداخلة (Nested Queries) في نظام قواعد البيانات.

6- عدم عرض رسائل خطأ تفصيلية، بعض المبرمجين يقوم بعرض رسائل خطأ تبين أين كانت المشكلة، و في أي جدول من قواعد البيانات، هذه التفاصيل تعتبر تفاصيل ثمينة جدا للمخترقين ، حيث يتمكنون من خلالها تكوين صورة كاملة عن بنية قاعدة البيانات الخاصة بالنظام.

7- يفضل استخدام حسابات بأقل صلاحيات ضرورية للبرنامج وعدم استخدام حساب المدير وما يشابهه [8]

مراجعة الشفرة واختبارها ضد حقن لغة الاستعلام البنيوية ، وإيجاد الثغرات التي يمكن الاستفادة منها بواسطة هذه الحقن من قبل المخترق ثم تعديل الشفرة بما يلزم.

واضلف الباحث بأنه :

توجد طرق عديدة لتشفير قواعد البيانات [9]:

أ- تشفير على مستوى ملفات قواعد البيانات:في هذه الطريقة يتم تشفير ملفات قواعد البيانات بشكل كامل على مستوى التخزين، وذلك بإستخدام برمجيات أو ملحقات وحدات مادية خاصة لذلك ويفضل دائما استخدام برامج الضغط والتشفير الملحقة ببرامج قواعد البيانات المعمول عليها .

ب- تشفير على مستوى أعمدة الجداول في قواعد البيانات:في هذه الطريقة يتم تشفير الحقول في جداول البيانات بناء على الأعمدة التي تنتمي إليها مع الاخذ بنظر الاعتبار وجود المفتاح الأساسي لتلك الحقول .

ت- تشفيرعلى مستوى البرنامج التطبيقي الذي يستخدم قواعدالبيانات:في هذه الطريقة يتم تشفير البيانات بواسطة البرنامج التطبيقي و ليس عن طريق نظام قواعد البيانات، فقبل تخزين البيانات يقوم البرنامج بنفسه بتشفير البيانات ويكون البرنامج التطبيقي ملحق ببرنامج ومحرك قواعد البيانات .

عملية تشفير البيانات ليس حل أساسي أو مطلق و إنما يجب استخدامه في الحالات التالية :

1- منع الوصول الغير شرعي للبيانات أو تخفيف مخاطر سرقة الملفات التي تحتوي هذه البيانات.

2- حماية أرقام البطاقات الإئتمانية .

3- منع المستخدمين المصرح لهم من عرض البيانات الخاصة غير المخولين برؤيتها.

4- إستيفاء المعاهدات التنظيمية أو الشروط التعاقدية.

المناقشـــــة :

ان امنية قواعد البيانات تهدف الى المحافظة على جميع البيانات والمعلومات مــن التلــف او التلاعــب او الاطلاع عليها لذلك يجب ان تكون المعلومات المدخلة الى قاعدة البيانات معلومات صحيحة ودقيقة ومتكاملة ومتوفرة على الدوام لدى مستخدمي قواعد البيانات هذه والجانب المهم في امنية قواعد البيانات هو الموثوقية فعندما يقوم شخص معين بإيداع مبالغ خاصة به لدى احد المصارف ويقوم باسترجاعها بعد حين فيجــب ان يحصل ذلك الشخص على المبلغ الذي تم ايداعه من دون أي تلاعب او الاطلاع على البلغ المودع من قبــل اشخاص اخرين والجانب المهم الاخر هو ان انقطاع التيار الكهربائي يجب ان لا يؤثر على قاعدة البيانات او الاجهزة الملحقة الاخرى وذلك لضمان استمرارية تدفق البيانات وان ابسط انواع حماية البيانات هو استخدام نظام التعريف الشخصي الخاص وذلك يتمثل بكلمات سرية وارقام خاصة للمستخدم تضمن الدخول الشرعي لذلك الشخص المخول فقط .

الاستنتاجات:

نستنتج مما سبق بانه لا امان للبيانات بدون وضع امنية لقواعد البيانات وذلــك لان اختــراق قواعــد البيانات ليس بلغة برمجية وهذه اللغة تدرس وتعرف نقاط الضعف فيها وانما هو بمثابة معرفة لنقاط ضـــعف قاعدة بيانات معينة والدخول عليها .

تمكن البحث من تحقيق تنمية ذهنية من خلال تقديم اساليب الاختراق ووسائل الحماية منها بالكامل اذن نستنتج مما سبق بانه لا امان للبيانات بدون وضع امنية لقواعد البيانات وذلك لان اختراق قواعد البيانات ليس بلغة برمجية وهذه اللغة تدرس وتعرف نقاط الضعف فيها وانما دخول غير شرعي على قواعد البيانـــات او عن طريق كتابة شفرات خاصة للاختراق او اجراءات يقوم بها اشخاص محترفون او ضعف في وسائل امن قواعد البيانات

ولغرض التاكد من سلامة وكفاءة الخطوات البرمجية المصممة فقد قمنا بتشغيل حاسوب اخر والدخول على قاعدة بيانات مصممة في جهاز اخر مرتبط بشبكة الانترنيت فحين الاتصال بقاعدة البيانات الضحية تــم طلب كتابة اسم المستخدم وكلمة السر وبالفعل ادخلنا الشفرة البرمجية اعلاه وعلى الفور تم فتح قاعدة البيانات .وبعدها وجدنا بان الخطوات البرمجية ناجحة ومعالة .

التوصيات

– اختيار الاشخاص الموثوق بهم للعمل على ادخال البيانات واستخدام الحاسوب بالشكل المثالي لكي لانسمح بتسرب البيانات الى جهات اخرى او الاطلاع عليها من قبل الاخرين .

– تخصيص جهاز كومبيوتر خاص للقيام بمهام ادخال واخراج البيانات من والى قاعدة البيانات فقط . وعدم استغلال هذا الجهاز للعمل لاداء أي مهمة اخرى .

– تكامل البيانات المدخلة الى قاعدة البيانات والتأكد من صحة المحتوى والنص المدخل ولا يتم التغيير فيه إلا من قبل اشخاص مخولين بذلك . (أي انه بعد ادخال البيانات لايمكن تغييرها او العبث بها)

–عدم فتح قاعدة البيانات في الحواسيب التي لاتحتوي على جدار ناري (Fire wall)

– إستمرارية توفر البيانات (Availability): ان توفر البيانات على الدوام للاشخاص المخولين من الامــور المهمة جدا لان عدم توفرها في اوقات الحاجة قد يخلق نوع من العبث او العمل على الحصول عليها بطــرق عديدة قد تساعد الاشخاص الغير مخولين من الدخول على البيانات والاطلاع عليها او العبث بها

كما يجدر بنا الى الإشارة إلى أنه من المهم جدا أخذ قضية أمن البيانات عند وضع السياســات و الإجــراءت الأمنية الخاصة بمنشأة او مؤسسة معينة التأكد من تنفيذ هذه الإجراءت وفقا لما هو مطلوب.

خاتمة :

ان مشروع امنية قواعد البيانات من الامور المهمة جدا في الوقت الحاضر وتم الاخذ بنظر الاعتبــار هذا الموضوع حين البدء بتصميم قاعدة البيانات وتزايد هذا الامر مع ظهور وانتشار شبكات الانترنيت وطرق الاختراق والتلاعب بالبيانات والمعلومات المراد الحفاظ عليها والعبث بها أو تدميرها.

المصادر

[1] Kevin. Loney and George Koch, "Oracle 9i The Complete Reference", 16th reprint 2005, Tata McGraw-Hill Edition, 2002.

[2] Abraham Silberschatz and Henry F . Korth and S.sudarshan "Database Syatem Concepts" , Fifth Edition 2006.

[3] Nick Snowdon ,"Oracle Programming With Visual Basic ", First Indian Edition Reprinted 2002.

[4] E. Bertino and R. Sandhu, "Database Security—Concepts, Approaches, and Challenges", IEEE Transactions on Dependable and Secure Computing, vol. 2, No. 1, Jan 2005.

[5] E. Bertino and R. Sandhu, "Database Security—Concepts, Approaches, and Challenges", IEEE Transactions on Dependable and Secure Computing, vol. 2, No. 1, Jan 2005.

[6] 2004 آندي اوبل "كشف ارار قواعد البيانات

[7] " c++ " الدكتور العجيلي ذياب وآخرون البرمجة بلغة

[8] Halferson. Mikel , “Visual basic Data base concepts “ 1999

[9]. شبكة المعلومات الدولية الانترنيت

[10] www.IVSL \\ “computer databases security “2010.