بسم الله الرحمن الرحيم

الاسم: ماجد فالح راكان العتيبي الرقم الجامعي:423100759

Paper 2

DataBase Security
حماية قواعد البيانات

محتويات هذه الورقة العلمية:

1. ما معنى قاعدة البيانات وأنواعها (مقدمة بسيطة).
2. معنى أمن قاعدة البيانات.
3. توضيح أهمية أمن قاعدة البيانات.
4. بعض القضايا في أمن قواعد البيانات.
5. الخسائر التي قد تنتج من إهمال أمن قواعد البيانات أو التقصير فيها.
6. الخاتمة.

1. معنى قاعدة البيانات وأنواعها:

مقدمة عن قاعدة البيانات:

قاعدة البيانات هي عبارة عن قاعدة و ملجأ و مكان تتجمع فيها مجموعة من البيانات يتم تجميعها من مصادر معينة.
إذا قاعدة البيانات تحتوي على بيانات أو مجموعة كبيرة جدا من البيانات التي ينشأ بين هذه البيانات علاقة معينة مما ينتج من هذه العلاقات معلومة معينة ، إذا هذه القاعدة قد تحتوي على بيانات شخصية وسرية لأشخاص معينين (معلومات عن العملاء وبياناتهم الخاصة والمبيعات الخاصة بهم) مما يستلزم حماية هذه البيانات والتي بذاتها تستلزم حماية قاعدة البيانات وهذا هو الموضوع الذي نحن بصدد التكلم عنه.

أنواعها:

هنا سوف نتكلم عن أنواع قاعدة البيانات ولكن هنا يجب التفريق بين أنواع قاعدة البيانات ومصنع هذه القاعدة.
أنواع قاعدة البيانات:

1. قاعدة البيانات العلائقية (Relational Data Bases): وهي عبارة عن قاعدة بيانات تنشأ عن طريق علاقات بين الجداول المتكونة منها.
2. قاعدة البيانات الوراثية(Object Oriented Data Bases): وهي عبارة عن قاعدة بيانات تنشأ عن طريق الوراثة بين الجداول
3. قاعدة البيانات الشبكة(Network Data Bases): هي قاعدة بيانات تنشأ عن طريق شبكات فيما بينها.

هذه بعض أنواع قواعد البيانات والتي تبين العلاقة والتركيبة التي تتكون منها الجداول المكونة لهذه القاعدة.

مصنع قاعدة البيانات:

1. أوراكل ORACLE
2. مايكروسوفت Microsoft (SQL Server, Access)
3. Sybase

2. معنى أمن قاعدة البيانات:

المعنى المفهوم من أمن قاعدة البيانات هو الحفاظ على البيانات والمعلومات التي تتكون منها قاعدة البيانات أي الحفاظ عليها وحمايتها من الاختراق والحصول على البيانات التي تحتويها ولبيان معنى أمن قاعدة البيانات بشكل أوضح نورد مثال يبينها بشكل أوضح فلنفرض أن لدينا قاعدة بيانات تحتوي على بيانات العملاء في بنك معين هنا أمن هذه القاعدة هو حماية بيانات العملاء (رقم البطاقة ، رقم الحساب ، عدد الحسابات) فهنا أمن قاعدة البيانات هو حماية هذه المعلومات من التسريب والاختراق من قبل أناس آخرون قد يستفيدون منها بطريقة ما.

3. توضيح أهمية أمن قاعدة البيانات:

هنا سوف نوضح لماذا حماية قاعدة البيانات مهمة في هذه النقاط:

1. لحماية الوصول إلى معلومات المنظمة الحساسة والأصول الرقمية:
المنظمات الحكومية والتجارية تستخدم قواعد البيانات لتخزين المعلومات الشخصية للموظفين كذلك البيانات الطبية والتي تتطلب الحماية والسرية التامة كذلك قواعد البيانات تحتوي معلومات مالية حساسة للماضي والحاضر والمستقبل(المتوقع) مثل السجلات التجارية والسجلات المحاسبية وخطط التسويق وغيرها من البيانات الإستراتيجية التي تتطلب الحماية والسرية من المنافسين في نفس الصناعة، كذلك تحتوي قواعد البيانات عن معلومات مفصلة جدا عن العملاء بما يتضمن معلوماتهم المالية والبطاقات الائتمانية ومعلومات شركاء العمل.

2. قواعد البيانات أنظمة معقّدةَ جداً وصعبة التَشكيل والضمان بشكل صحيح وينتج من ذلك التعقيد وجود ثغرات قد تستغل والتي نستنتج من خلالها ضرورة حماية هذه القواعد ومعرفة جميع مشاكلها الأمنية أي نقوم ببناء قاعدة البيانات بطريقة مفهومة وسهلة مما تمكننا من حمايتها ومعرفة الثغرات التي قد تنتج منها وهذا من احد طرق الحماية وهو تبسيطها من الداخل وإظهار أنها معقدة من الخارج.

3.ضعف أمن قاعدة البيانات لا يؤثر على قاعدة البيانات فقط ولكن أيضا يؤثر على الأنظمة الأخرى المتصلة بها .
مثال على ذلك نفترض أن شركة لديها قاعدة بيانات تحتوي على معلومات غير مهمة مثال على معلومات للأوراق المستخدمة والأقلام وغير ذلك من الوهلة الأولى نستطيع أن نجزم عدم أهمية أمن هذه القاعدة ولكن هذه القاعدة من الأصل مرتبطة بنظام تشغيل ، وفي هذه الحالة حماية هذه القاعدة ضرورة لحماية نظام التشغيل لأنها تعتبر (ثغرة) فبدخوله لقاعدة البيانات (اختراقه) يكون بذلك أمامه فرصة الدخول على نظام التشغيل واختراقه.

4.قواعد البيانات تعتبر الآن حجر الأساس في أنظمة التجارة الإلكترونية وأنظمة دعم القرارات ونظم إدارة الموارد لذلك عند بناء هذه الأنظمة يتم التأكد من سلامة كتابة البرمجة في هذه الأنظمة وعمل الاختبارات لها وغير ذلك من الإجراءات في حين انه يجب التأكد من حماية قاعدة البيانات التي تعتبر المحرك الرئيسي لهذه الأنظمة ، نلاحظ هنا أنهم يقومون بالتأكد من سلامة البرامج نفسها والتطبيقات وغير ذلك ومثال على ذلك التأكد من سلامة الأنظمة الجديدة وملائمتها للمنظمة والتأكد من حمايتها وعدم وجود ثغرات فيها مع عدم الاهتمام بقاعدة البيانات المرتبطة فيها والتي تعتبر الأساس ولكن عند نقوم بالتفكير قليلا نلاحظ أن قاعدة البيانات تعتبر ثغرة لهذه الأنظمة وذلك عند القيام بإهمالها.

4. بعض القضايا في أمن قواعد البيانات:

هنا سوف أتكلم عن بعض القضايا العامة في قواعد البيانات أو التهديدات التي قد تتعرض لها قواعد البيانات.

أول قضية سوف أتكلم عنها هي حقن ال اس كيو ال (SQL Injection)
هذه الكلمة تعني محاولة حقن قاعدة البيانات بحيث يتمكن المستخدم من الدخول لها وهنا يستعمل لحقن قاعدة البيانات التطبيقات التي تعتمد على قاعدة البيانات.
فكل تطبيق يكون له عدد من المستخدمين مثل(المستخدم ذو الصلاحيات الكاملة (admin).....)
وعند بداية تشغيل التطبيق يحتاج المستخدم لإدخال اسم المستخدم وكلمة المرور وفي هذه الحالة يحاول المخترق حقن قاعدة البيانات وذلك بإرسال أوامر تجعل قاعدة البيانات أو التطبيق يقبل هذا المخترق
وهناك مثال على ذلك :
يدخل المخترق في خانة كلمة السر `Aa' OR 'A'='A`
وبذلك تكون لغة الاستعلام (SQL) مطابقة ل

```
SELECT * FROM users WHERE
username='Mike' AND password='Aa'
OR 'A'='A'
```

وهنا قاعدة البيانات سوف تقبل المستخدم وترجع جميع البيانات في جدول الصلاحيات مما يكون قد أسندنا للمخترق إحدى الصلاحيات وقد تكون صلاحية الadmin

القضية الثانية: ديدان قواعد البيانات:
منذ إصابة دودة سلامر قاعدة بيانات SQL Server 2003 بدأ الإدراك العام لأهمية موضوع الديدان وإصابتها لقواعد البيانات مع ذلك فإن التركيز العام القائم الآن يركز على القضايا الأخرى مثل قضية SQL Injection

القضية الثالثة: إيقاف الخدمة أو نكران الخدمة (Denial Of Service)
إيقاف الخدمة هي محاولة ضرب السير فرات أو الخوادم التي تكون مخصصة لقواعد البيانات أو غيرها وذلك بإرسال طلبات كثيرة جدا جدا مما يؤدي إلى توقف الخادم أو إدخالها في دوامة من الأوامر المتكررة infinite loop مما يؤدي إلى توقف الخادم عن العمل.

5.الخسائر التي قد تنتج من إهمال أمن قواعد البيانات أو التقصير فيها:

هناك خسائر كثيرة وكبيرة تنتج من اختراق قواعد البيانات أو إهمالها تأمينها مثل:

1. المعلومات المخترقة قد تكون سرية جدا جدا مما يؤدي إلى نشرها إلى أناس قد تكون من المحضور عليهم معرفتها.
2. معلومات العملاء لدى المنظمات سرية واختراق هذه المعلومات يعرض المنظمات إلى عقوبات كبيرة.
3. الوقت الذي تفقده المنظمة عند التعرض للهجوم والاختراق وما يتسبب له من تأخير للعمليات والعملاء.
4. الوقت المستغرق للقيام بإصلاح الأجهزة المتضررة من الهجوم وقواعد البيانات.
5. قد تحتاج المنظمة إلى الرجوع إلى السجلات القديمة في حالة ضياع السجلات الموجودة في قاعدة البيانات المخترق واستخدامها وذلك لإرجاع النظام إلى آخر حالة له قبل الاختراق, كذلك قد تستخدم المنظمة العملاء والموردين لمساعدتهم في ذلك في حالة ضياع السجلات أو عدم وجودها مما يضعها في موقف محرج.

6.الخاتمة:

في النهاية أتمنى أن يكون القارئ قد استفاد بعد قراءة هذه الورقة.
سوف أتكلم عن بعض الأمور المهمة والتي يجب أن تكون في الاعتبار:
1. وضع الخادم الخاص بقاعدة البيانات داخل حرم المنظمة (داخل الشبكة الداخلية للمنظمة).
2. حماية قاعدة البيانات من الناحية المادية ولا نقوم بإغفالها وذلك بحماية الخادم من الناحية المادية وليست من الناحية البرمجة فقط.
3. تثقيف مستخدمو قواعد البيانات بأهمية حمايتها.
4. وجود جدار ناري قبل الدخول إلى قاعدة البيانات.

REFERENCES:

1. http://www.db2mag.com/story/showArticle.jhtml?articleID=17602334

2. http://www.ecominfo.net/arts/015_ISS_database.htm

3.http://www.stanford.edu/dept/itss/docs/oracle/10g/server.101/b10743/security.htm

4.http://msdn2.microsoft.com/en-US/library/ms181061.aspx

5.http://www.oracle.com/technology/pub/articles/jucan_security.html

6.http://www.sitepoint.com/blogs/2005/06/28/securing-mysql-and-other-databases/