Database security pdf

Most IT security pros believe that continuous monitoring of the database network is the best approach to prevent large-scale violations like those by retailers Target, Michaels and Neiman Marcus, a study has shown. [Organizations suffer SQL injection attacks, but do little to prevent them] Nearly two-thirds of the 595 U.S. experts interviewed by the Ponemon Institute cited monitoring as the best form of database protection, a situation other security experts questioned. Constant monitoring, looking for unusual or abnormal types of behavior, becomes very important, Larry Ponemon, president of the Ponemon Institute, said. The more you watch, the more things you see, and the more things you can stop. The tools described as database activities typically record and record activities related to structured query language (SQL) that database administrators and others use to perform different tasks. Alerts are generated when the activity violates policies. While the devices have been in use for years, many were too expensive and delivered too many false positives, which makes them difficult to use, Ponemon said. Today, the assets are more mature and will not bankrupt the company. For example, the devices are better positioned in active databases that the company has many not known were in use, Ponemon said. They are also right on the contagious software that might have been installed by a picker to store stolen data before it is sent to a remote server. Some technologies also monitor unusual human activity on the network, as well as unauthorized applications connected to a database. Database watchdog vendor DB Networks sponsored the Ponemon study, which a security consultant said made the conclusions suspicious. Database monitoring does not detect SQL injections (attacks), Kevin Johnson, CEO of Secure Ideas, which does penetration testing, said. By the time the attack gets to where monitoring can see, it looks like just another query from the app. It's a typical supplier solution. Penetration testing of all business applications has been more effective in preventing violations because if you don't know the fault you have, you can't prevent it from happening, Johnson said. Paul Henry, senior lecturer at the SANS Institute, believed that much more was needed beyond database verification for good security. I believe in a layered approach that perhaps should include a database firewall to reduce the risk of SQL injection, along with continuous monitoring of the database in addition to continuous monitoring of normalized network traffic flows, said Henry. The study also found that respondents were close to believing that attacks on retailers included SQL injections. Such an attack would include the insertion of malicious SQL statements into an execution input box. Box. successful, the technique may result in the database throwing its contents at the attacker. Retailers have not disclosed whether the SQL injection was involved in the attacks reported in the past eight months. Respondents' opinions were based on their own experience. Nearly seven participants worked for organizations that must comply with the Payment Card Industry Data Security Standard (PCI DSS). The standard is what retailers must follow in order to get approval to accept payment cards issued by banks. I agree that SQL injections are probably involved because of their occurrence today, but I also have yet to draw a conclusion as there are still not enough details, said Henry. [Data breaches are 9% more costly in 2013 than a year earlier] Target, for example, admitted that the credentials of a subcontractor with access to the retailer's network had been stolen. In addition, malware used to steal 40 million credit card numbers grabbed data from memory at the retailer's electronic cash register. Target also had personal information from 70 million customer accounts. This story, Why Database Monitoring may or may not, Secure Your Data was originally published by CSO. Copyright © 2014 IDG Communications, Inc. January 14, 2008 8 min read reviews expressed by contractor contributors on their own. Mathew SchwartzA common trait of recently well-publicized data breaches? For lost laptops, purloined handheld devices, dumpsters or someone physically reaching down from the office, each breach involves a common entity: the database. At least a third of the more than 200 million personal data hacked in the past two years have been taken from a database, says Ted Julian, Vice President of Marketing and Strategy for App Security, citing data breach statistics from the Privacy Rights Clearing House. Furthermore, the frequency and severity of infringements are increasing. According to the Identity Theft Resource Center in San Diego, nearly four times as many Americans had their personal information stolen in 2007 as in 2006. Don't let databases fool you. Of course, their names sound imposing (Oracle, Ingres) or innocent (MySQL, SQL Server, Sleepycat). But there's no database, just out of the box, it's safe. Moreover, because databases are concentrated in one place, these are the primary targets. The databases are indeed where the store's crown jewels are stored, notes Mark Bowker, an analyst at Enterprise Strategy Group. This applies regardless of the size of the company. However, due to the scale of the operations, larger organizations are in the spotlight for more data leaks. In September, for example, Ameritrade disclosed a breach affecting the data of more than 6.3 million customers. Meanwhile, TJX Companies - T.J. Maxx and retail store owners - have recently offered to a massive class action lawsuit stemming from improper storage and unsecured 45.7 million customers' credit card details. While storing sensitive or regulated information puts any company at risk, smaller businesses may have more to lose. For small businesses, the impact of data loss is much greater because they have less infrastructure, says Mark Kraynak, Director of Strategic Marketing at Imperva. They probably don't have backups, and they don't have the organizational and response team to handle a major public wrongdoing or sue them. So how can small and medium-sized enterprises ensure that their databases are not broken in the business? Experts offer 10 tips for protecting databases:1. You know you're in danger, don't you have a database that contains sensitive information for the Internet? You're still in danger. Forrester Research estimates that 70% of database breaks occur internally -- no Internet connection required. Unfortunately, detecting internal attackers can be quite difficult, especially since the person who poses the greatest threat is the actual database manager (DBA). DBs are allowed a certain amount of freedom from their jobs, which is a bad DBA hard to catch, notes Noel Yuhanna, an analyst at Forrester Research. In particular, since the budget system has full access to all data within the database, it can potentially change or delete the data without anyone knowing. Thus, DBA's, and all other users' privileged access, ideally should be a safe way to capture what they have done because they want to make sure they are not doing things that they shouldn't be doing, says Kraynak. Still, most database experts recognize that database management tools are largely the domain of larger businesses; small and medium-sized enterprises must first focus on fundamental issues.2. Security is prioritize: If you pose a security risk for security reasons, you may need to examine their security habits. Yuhanna estimates that the budget system spends on average only 7% of their time late with the security of the database. The scarce attention paid to database security is not so surprising. In an SMB, it's all about getting that application out, getting that database out, making sure it stays online and available, and maintains proper performance notes ESG's Bowker. Unfortunately, security usually falls towards the bottom of the list. Add the security of the database to the DBA job description.3. By default, enabling security capabilities to ship databases is virtually not enabled without protection controls. Moreover, most databases have poor authentication and has well-known default passwords for both user and administrator accounts. This is a step forward: some older databases - namely Sybase and SQL Server - by default do not require a password for full database access, says Yuhanna. Today's databases, however, are natively managed by what he terms the A: authentication, authorization, and access control. Enable such capabilities.4. Repair the database Before you place any data in a database, check the level of repair, see how it is set, and see which default values are potentially vulnerable - from default users to features turned on by default, says Krayak. So you want to assess the database and correct them, which is not as easy as it sounds. If you need help, visit the commercial database for vulnerabilities in tools or free options such as Imperva's Scuba.5. Restrict database access Then restrict database access to both the production database and the underlying hardware based on the knowledge you need. Too often, administrator passwords are an open IT secret, says Bowker, who pleads guilty when he previously ran a medium-sized company IT shop. Even something as simple as the HR database, to be honest, all the IT guys had access to it and could search for payments and this type of information just because there were no prior checks, such as access restrictions on the machine the database had. Who gets administrative access rights? An organization with at least a few IT employees, says typically one of them is responsible for the database and copies, and you just need to have restrictions on the other actors, so you won't be able to go there and do nothing. Also, make sure that database backups are stored in encrypted format only so that no one can secretly access the data.6. Do not copy a wholesale database: The production database usually has a designated owner or gatekeeper. Who's going to look at the database after it's been copied? Simply put, each copy of a database is probably unsafe and therefore it is an internal threat, says Bowker. The DBA, for these types of people, we all root access at this point and essentially read anything. Do not allow unverified double-checking of databases.7. Inventory of existing databases Locking databases out of the box and prohibiting wholesale parallel sounds fine, but what about providing databases and copies that are already large? Companies must regularly find and inventory all existing databases. You know that a production database can hide a lot of copies. Usually, many businesses have production databases, but you know what, the database usually contains a lot of copies - for example, developers have copies - and many databases match each other and make calls to each other, says Bowker.Large organizations often use automated discovery tools to to ensure that sensitive data is not stored in an unenen encrypted format. However, experts say smaller organizations are likely to already know which databases contain confidential information.8. Secure existing databases: Database inventory helps you to take the riskiest First. With this information in hand, most SMEs will find that they can eliminate some [data], mask some, and thus on, thus minimizing their exposure and at the same time simplifieing the security improvements they need to do, says Julian of Application Security.Also, appraisal databases for known vulnerabilities and patch levels. Once you've done that assessment, do it again quarterly or regularly make sure you have a process to check this stuff because things are changing, says Imperva to Kraynak.Finally, study user accounts; Forrester estimates that 30% of database accounts are duplicate or inactive. To protect against disgruntled former employees, regularly empty inactive and duplicate accounts.9. How to get the data developers need to develop and test new applications If companies restrict the creation of copies of databases? How can sales managers train new managers for the customer relationship management system? In such cases, Bowker recommends using tools from companies such as Applimation, HP OuterBay, IBM Princeton Softech, and Solix Technologies, a subset of the database. The subset allows the DBA, or the designated gatekeeper of sensitive data, to selectively share parts of the database after the first deletion, conversion, or circumvention of the subset of the database, based on how the subset of the database is used. For example, developers and testers need fake data (such as credit card and Social Security numbers) that is still good enough (in terms of app logic) to do the real thing.10. Plan database extraction Finally, keep in mind that databases don't live forever. Databases are withdrawn - or sunset if you want to use that term, says Bowker. This usually means that the database must be written in XML format with tags to facilitate subsequent search or to meet retention requirements. Like all sensitive data, restrict access to these XML files. The New Breakage Equation For Getting Business Leaders to Sign The Above Tips May Require a Change in Attitude. Budget files are usually authorized to work and operate quickly, he tells Kray. If it breaks, the deal breaks, and if it doesn't go fast enough, essentially the deal still breaks. Now, just factor in data breaches to the breaking equation. Mathew Schwartz has been involved in IT and business topics as a journalist, researcher and editor for more than 10 years. His work has been published in a number of publications, including the Boston Globe, Computerworld, Information Security Magazine, the London Times, IT Compliance Institute and Wired News. News. News.