International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 1, January-2014, pp: (498-501), Impact Factor: 1.252, Available online at: www.erpublications.com

Reducing Database Security Implementation Gaps

Dr. Mohammad Iqbal[1], Dr. Farid Ahmad[2], Dr. Manoj Kumar Singh[3]
[123]Computing Department, Adama Science & Technology University, Adama, Ethiopia

Abstract: The proposed strategy borrows from risk analysis methods and consists of nine elements. The first step is system characterization. This should be followed by identification of threats, gap identification, control analysis, determination of the likelihood of occurrence, an impact analysis, risk determination, recommendations for control and finally documentation of results. System characterization involves determining the level of risk in each aspect of the system. After characterizing, the organization needs to identify threats. Gap identification is done by detecting whether a control exists in the system. A control analysis involves the examination of the controls put in place to guard against threats. Thereafter, the organization ought to determine the likelihood of occurrence of a threat. Impact analysis involves examining the effects of the threat once gaps are exploited. Risk determination is a ranking process that will affect resource allocation in the organization based on the threats with the highest chance of occurrence. Recommendations and documentation are the last phase.

Keywords: Database security, risk analysis, threat likelihood, impact analysis and system characterization.

Introduction

Several organizations lack database security strategies, which explain why they are likely to experience gaps during the implementation process. Most firms will dwell on network security or middle ware and leave their databases exposed. Basic approaches in implementation leave gaps that could harm an organization. Failure to prioritize this matter through resources and budgetary allocations could cause dire consequences. The proposed strategy marks a shift away from controls to preventive measures.

The strategy

Database security approaches are needed in order to protect data from attacks, which may either be internal or external. Furthermore, one does it in order to reduce exposure of data to unauthorized users. The entire database must be kept secure regardless of whether it contains non production or production information. Literature indicates that an effective database security strategy ought to consist of certain features.
First, the concerned company needs to have an understanding of all that needs protection. This may involve health information, customer data, and personal identification information among others. After establishing what needs protection, one should know the regulatory compliance conditions associated with each type of information. Sometimes this could be Payment Card Industry or Sarbanes Oxley compliance. An effective database security approach needs to have ways of performing an inventory of the database. Classification and discovery of databases are critical especially with regard to sensitive data, [1].

Once classification occurs, an organization needs to determine security policies for its databases. These must then be converted into actionable policies across all the databases. The firm needs to take security measures in accordance to the needs of the organization. Sometimes, this may entail encryption, monitoring, data masking, access control and auditing. Finally an effective approach is one that employs a database security solution with low costs. The proposed strategy will consist of the above elements. It will emanate from the HIPP risk assessment method. Gaps in database security occur across the whole continuum of implementation. This is the reason why one must start at the beginning. The first step is system characterization. This should be followed by identification of threats, gap identification, control analysis, determination of the likelihood of occurrence, an impact analysis, risk determination, recommendations for control and finally documentation of results, [6].

As the name suggests, system characterization involves determining the level of risk in each aspect of the system. The purpose of doing this is to establish the elements that need protecting. Sometimes these components could be crucial to

business or may store sensitive information. Companies can characterize the information in their databases in order of risk factors. It is these areas that expose the company to certain threats. If systems have a high user number, or if the information is easily available on the internet and the information moves from party to party, then it could have a potential security gap. Additionally, the type of information found on the system may also determine its susceptibility to risk. Ranking should occur on the basis of the above factors or any others that are relevant to the organization, [3].

After characterizing the system, the organization needs to identify threats. This will determine how the security gaps will compromise the database. Threats may be any items that can affect information, confidentiality or integrity of the system. Usually, threats can be environmental or man-made. Environmental threats to database security include power outages, network cable breakdowns, water leakages, hardware failures among others. Database security may also be compromised by man made errors. This may involve hacking, unauthorized access, unintended errors, loss of equipment due to theft and tampering of data. It should be noted that an organization need not identify all its threats as these may be overwhelming. It only needs to concentrate on those threats that are likely to occur. To achieve this, the company may need to look at previous factors, industry trends as well as statistics on the same. Once this is done, it needs to be linked to the support system in respective order. Networks, laptops and tablets as well as workstations are all examples that may be linked to each threat, [7].

Gap identification is the next step of the process. However, because the subsequent step is closely associated with it, then one may combine this component with control analysis. Gaps may also be perceived as vulnerabilities. These are weaknesses that could be acted on by the threats. Gap identification is done by detecting whether a control exists in the system. If this is absent, then a gap exists. When a database security system lacks an antivirus, then malicious code could threaten it. Absence of the software is the gap. Alternatively, a company may have instated a control but this may not work sufficiently. In the case of an antivirus that has not been updated, a gap may exist in the system.

Usually, organizations attempt to put threats and gaps together although this is not a requirement. For instance, malicious code like Trojans and spyware may be classified as threats and the corresponding gap could be failure to update the antivirus software. A control analysis involves the examination of the controls put in place to guard against threats. Companies may rely on websites that are designed for this purpose. Alternatively, they may do a security assessment. Internal auditors could also be another way of controlling analyses. Past incidences either in the organization or in similar environments may also help. Work inspection to determine if workstations have firewalls or may be done. Scanning of networking efforts is also another way of looking at the environment for controls.

These controls could be preventive in nature and typical examples include encryptions, authentication or access controls. They may also take the form of deterrents. These refer to measures put in place to deal with casual threats like internet policies or passwords. Detective controls include those ones that have been put in place in order to identify when a threat is about to take place. They also involve intrusion tests as well as audit trials. Reactive controls come after a gap has already manifested as a threat, and their purpose is to alert the organization that a threat is now in existence. Finally, a control could take the form of a corrective action after the threat is in place. This is done in order to retrieve data or at least recreate it, [9]. Once a control analysis is complete, the organization ought to determine the likelihood of occurrence of a threat. This needs to keep in mind the security safeguards that the firm has already put in place. A company could have high, medium or low likelihood ratings. When no controls exist or the ones in place are insufficient to guard against threats, or, when the source of the threat is quite able and motivated, then the threat is of a high likelihood level. Conversely, when the threat is able and highly motivated but a firm already has sufficient controls to deal with it, then it will have medium likelihood levels. Lastly, when the source of the threat is not highly motivated and it does not have the ability to execute or the controls put in place can prevent the threat from exploiting the gap, then the threat has low likelihood definition.

An impact analysis should be the next phase of the project. This involves examining the effects of the threat once gaps are exploited. Companies ought to rate impacts based on their magnitude. If the threat takes advantages of database gaps and causes a huge loss to the assets of the corporation, then ratings will be high. This category should also consist of those database harms that could cause human death or ruin the organization's reputation. Medium ratings consist of those threats that may cause injury, lead to sufficient loss of assets to the organization and harm the company under consideration. If the threat exploits a security gap and leads to loss of assets as well as tarnishes the company's mission, then this impact is of a low rating, [8]. Companies are supposed to use the following criteria for impact analysis as a guide. They must have a strong awareness of what constitutes loss in their own organization. This means giving precedence to the possible impacts that could arise out of the threat. Confidentiality, opportunity, integrity, litigation, reputation and availability are potential risk impacts. If a threat has an impact that will impinge on confidential data, then it needs to be categorized as such. For

instance, personal identification numbers could cause identity theft. Financial fraud may emanate from the theft of a debit or credit card data. Research information may make a company lose its competitive edge.

Opportunity refers to those threats that lead to lost opportunities within the business. This may refer to loss of the entire business or an advantage that the organization had. It may also refer to impacts related to equipment loss or damage and even increases in insurance payments. An impact that falls in the 'integrity' category is one that compromises data as it is in the system. This means that it may affect data entry; it may alter the nature of data or change the degree of error synchronization for data, [2].

Threats whose impact falls under litigation are those ones that may lead to civil or criminal liability. They may also cause fines and punishment designed for criminal behavior. On the other hand, the availability category refers to those threats which will damage data availability. This may cause the organization to deny its customers service or temporarily close operations. Conversely, lost data may necessitate replacement or delays in operation. Reputation threats are those ones whose impact will undermine customer confidence in the system. They also demoralize employees and could make administrators lose faith in the institution, [5].

Once the likelihood of the threat has been determined as well as its impact, then a risk determination needs to occur. This is a ranking process that will affect resource allocation in the organization based on the threats with the highest chance of occurrence. Classification enables the firm to prioritize risk intervention. Businesses have the choice of using qualitative or quantitative approaches. The qualitative approach combines the ratings from the likelihood analysis as well as the impact analysis to find the appropriate score as shown in the table below.

		Effect		
Likelihood		**High**	**Medium**	**Low**
	High	9	6	3
	Medium	6	4	2
	Low	3	2	1

Source: (National institute of Standards and Technology, 2011)

The scale above utilizes arbitrary values of 1 for low ratings, 2 and 3 for medium and high ratings. When combined, the threat with maximum likelihood and impact would have a value of 9 while the ones with least likelihood and impact would have a value of 1.Conversely, companies may take the quantitative approach which involves allocation of a definite financial approximation on the losses. This may be tricky because not all effects can be quantified, such as loss of brand image. Regardless, firms using this approach will base it on the asset under consideration and its value. Sometimes, a business can consider the frequency of the threat when assessing its monetary impact,[4]. After this process, the organization must then make control recommendations. These are the actions that will counteract the security facts. For instance, if a gap involves poor review of audit logs, then the control recommendation would be to instate procedures where users have formal log responsibilities. Finally, a documentation of the results is critical in order to develop a risk profile. This will enable the company to decide if it needs to mitigate, transfer or accept the risk, [10].

Conclusion

The above approach considers all elements of the organization that depend on its database. A systematic risk approach will trace the source of each security gap and quantify its likelihood as well as impact. Companies can effectively close these gaps if they stick to the procedure religiously and carry out follow-up of the risk reduction process. Full commitment is essential to the success of this strategy.

References

[1]. Basharat, I, Azam, F. and Muzaffar, A. (2012). Database security and encryption: A survey study. International Journal of Computer Applications, 47(12), 28-35.
[2]. Burns, R., Sack, P. and Pesati, V. (2012). Techniques for adding multiple security policies to a database system. Retrieved from www.freepatentsonline.com/8316051.html.
[3]. Gollmann, D. (2010). Computer security. Wiley interdisciplinary Reviews, 2(5), 544-554.
[4]. Herzig, T. (2010). Information security in healthcare: managing risk. Chicago: HIMSS
[5]. Kroenke, D. and Auer, D. (2010). Database concepts. UpperSaddleRiver, NJ: Pearson Education Inc.

[6]. National institute of Standards and Technology (2011). Recommended security controls for federal information systems and organizations. NIST Special publication, 3, 800-853.
[7]. Summers, G. (2007). Data and databases. Melbourne: Nelson Australia Pty Limited.
[8]. Taitsman, J., Grimm, C. and Agrawal, S. (2013). Protecting patient privacy and data security. New England Journal of Medicine, 368, 977-979.
[9]. Waksman, A. & Simha, S. (2011). Silencing hardware backdoors. Oakland California: Routledge.
[10]. Wang, O., Xing, L., Gu, X. and Zhu, C. (2013). Design and implementation of security enhanced module in database. Internet Computing for Engineering and Science, 5, 60-62.