White Paper

6 MOST COMMON INSIDER THREATS - HOW TO STAY PROTECTED

Prepared by
BSC Systems Incorporated
14340 Sullyfield Circle, Suite 250
Chantilly, Virginia 20151

18 February 2016

Cyber attacks are growing at an exponential rate, and many businesses are not prepared for security breaches. Once hackers are able to gain access to sensitive company information, they can quickly inflict damage that may cause long-term consequences to business operations. Implementing simple best practices, and properly managing internal controls, can prevent most security breaches. Here is a list of the top six insider security threats, and how to stay protected.

EXCESSIVE PRIVILEGED ACCESS

One of the most common and easily preventable risks is granting employees privileges that go beyond their job role. The database administrator having undefined job requirements or unclear directions often causes this. If an employee leaves a company on bad terms and has excessive database rights, he or she may abuse these privileges to inflict damage to the company. A way to prevent this is to manually assign privileges to individual users depending on what they need to do their job, rather than granting wide sets of default privileges to large groups of users.

PRIVILEGE ABUSE

Privilege abuse includes employees using database privileges for unauthorized purposes. This can result in employees being able to access confidential information or manipulate existing data files. Often employees store confidential files on their personal computer for easier accessibility. Once this information has been transferred out of the database, it is outside of the organization’s control, and therefore likely vulnerable. A way to prevent this is to put in place database controls that record the context of access. This includes details like time of access and location, so any suspicious activity can be tracked.

SQL INJECTION

SQL injections are popular with hackers and can cause devastating threats to a company database. Applications are attacked by injections, which leave behind malicious code which is passed through the SQL server. This can result in the hacker having access to the entire database. A way to prevent these attacks is to use firewalls to protect web-facing databases, as well as perform extensive testing to input variables for SQL during development.

WEAK AUDIT TRAIL

All organizations should have an automated recording of database transactions, especially when dealing with sensitive information. Companies with weak database auditing systems will often find that they are at odds with government regulatory requirements such as HIPAA. Having proper auditing systems in place is the best way for an organization to make sure they remain government compliant. This is also more likely to deter attackers that do not want to leave behind forensic evidence. A high-quality network based audit program can help keep your database protected.

DATABASE INCONSISTENCES

All of the previously mentioned threats can be caused by a lack of consistency with database administration. Companies should have solid policies to ensure system administrators are staying aware of the latest threats, and looking after databases on a regular basis. Database developers should be aware of the system's vulnerabilities that may have potential to compromise the database. Creating proper documentation can help to ensure software updates are made, sensitive data is inventoried, and critical patch updates have been completed. By having organized database policies in place, companies can help prevent inconsistencies that may lead to a compromised database.

PHISHING ATTACKS

Phishing is a type of Internet fraud that seeks to acquire a user's credentials by deception. It can result in theft of passwords, credit card numbers, bank account details and other confidential information. Since this type of attack seems to come in waves, as soon as an organization gets wind of the latest attack, this information should be shared with employees immediately. Phishing attacks usually take the form of fake notifications from banks, service providers, package delivery companies, etc. Most of these appear as time sensitive threats that give the user less time to think so they feel they have to move fast. For example, they often claim your account has been compromised, and provide instructions to rectify the problem, where in reality your account is safe unless you follow the attacker's instructions. The only way to control phishing is through awareness training and regular emails to keep employees abreast of the latest scams. As soon as the IT department is aware of a current phishing approach being used, a high priority email should be sent to the entire staff alerting them. If they are expecting a phishing attempt, the probability of success goes down drastically. Punishing employees does not work as it is not their fault, and it creates an environment where people will be hesitant to tell IT if a security breach occurs. Therefore, keep your staff informed, and be sure they are aware that reporting is a good thing.

HOW BSC CAN HELP

At BSC Systems, we go beyond merely checking the box — we work to improve your actual security. We assist in improving your security posture while achieving compliance with regulatory requirements. Our assessment approach is structured to minimize interference to reduce impact on your operations. Contact us today for a free consultation about your security and compliance needs.