Identity And Access Management In Healthcare Hospital

Posted on March 14, 2019

Abstract

The paper discusses in detail the function of the IAM in Healthcare hospital. The introduction gives a detailed concept of the hospital and the departments involved in systems security. The body contains four parts. The first part explains the description of the IAM. The second part shows the importance of IAM. The third part describes the developments within the IAM department. The last part deals with recommendations. The paper winds to a conclusion which summarizes all the points.

Identity and Access Management

One of the most critical and sensitive industries in the world is the health sector. It is a sector that involves a lot of confidentiality between the patients and the medical experts. Some systems are used in hospitals and are controlled by a computer. Some data are kept in the hospital database that should be protected. Healthcare is a private hospital in Australia with over 46 hospitals, and 52 branches should have computerized infrastructures that help treatment activities. With all these branches, the hospital has many patients; hence, millions of patients' lives are always in their hands. It also indicates that they contain a lot of patient data in their database. The systems and the data should be protected at all costs. That's why the identity and access management department is crucial.

Technology keeps on changing every second (Gupta, 2018). If a company does not advance according to the growing technology, then attacks will be a common thing in the hospital systems. Malware keeps advancing, too; old methods can rarely protect against new malware in information technology. That's why the IAM is very important in the Healthcare hospital. Currently, surgeries and other departments use software developed by people. It means that if such software fails in the treatment process, then serious implications can be witnessed, which include the death of a patient. ISIA is a very important department and, hence, should be managed accordingly.

Description of IAM

As the name suggests, the IAM department is responsible for identifying threats related to the hospital systems, neutralizing the threats, and coming up with new advanced systems (Garcia et al. 2017). The primary aim of the department is to make sure the organization is secure. There are

different ways the IAM makes sure the hospital is secured. When a patient is admitted to a hospital, either an inpatient or an outpatient, some records are kept in the database using the computers. The data is very important to the organization. There are rules that patient's data should not be known to other third parties unless authorized. If such things happen, the organization can be sued in court. That's why the database should be protected from SQL injections and other threats. If measures are not kept in place, the database can be attacked and data leaked. Such a hospital contains the data of even popular people like a politician who have lots of secrets, leakage of such data can lead to hospital closure, bad image and be sued by people affected.

Various ways are met to ensure that the information is secured (Joharapurkar, 2016). One of the common methods is by only allowing authorized individuals to access the data in the database. In case that is not effective, there is the changing of password after a time interval, and if that's not fully secure, there is the use of decrypted passwords, which other intruders can't just guess. Some of these methods don't fully secure the data since they are hackers who can inject the data into the database from their comfort. The ISIA department contains security engineers who are experts in the Python programming language, relational databases, NoSQL databases and other specialities. They are fully equipped to make sure that when hackers try to attack organizational databases, they are ready to protect them using very powerful firewalls and strong codes, which are unknown and rare in other organizations.

The ISIA contain all kinds of developers; the IAM ensures that they develop real-time software. The developers in this field are website developers, mobile application developers (Android and iPhone), backend developers and other software developers. The Healthcare Hospital has a website where people can register, log in, and get directions. Websites are the easiest targets if not well protected. The front and back engineers make sure the website is secure. The community in Australia can use mobile applications to ask doctors questions and advice on different conditions. The data the applications correct is a secret. If such an app is bypassed, then data can be leaked. All the developers need to come together to make sure they all play their roles and that the organizational security is at its best.

Importance of IAM

IAM, as explained earlier, ensures that the organization is secure (Villa-Real, 2014). The department is very important to the organisation. An attack on the organizational database can lead to illegal data loss. It's IAM work to make sure the data is secure. The hardware and the software used in surgery are developed by the engineers. IAM makes sure such software meets all the requirements to be sure it can be responsible for a personal life. IAM ensures organization security.

Developments

As indicated, technology keeps on changing; hence, developers should be up to date at all times. The IAM is making sure that the developers are well-trained and ready for any attack. They also make sure they employ qualified candidates who are up to date on the new technologies. The IAM is trying its best to provide favourable working conditions for the engineers.

The IAM has a project to develop its own software, which should only be used in the organisation. It is a very wise move since hackers can find it hard to enter into their systems. It is very simple for a hacker to crack a system which is used in almost all hospitals. The software cannot be sold to the market.

Recommendation

There are certain technologies developed by the engineers that the management should implement to supplement organization safety. The organization uses the WAN, which is prone to attacks. The network should be destroyed, and the management should provide capital to facilitate the LAN network, which is secure but costly to set up in such an organization.

The databases used by the organisation are relational databases. The world is changing towards the NoSQL databases like the Mongo DB (Garcia et al. 2015). Upgrading the new database will require resources that can only be authorized by management.

In conclusion, information and systems security is a requirement in all organizational hospitals. The IAM has a unique responsibility in regard to the healthcare hospital for setting aside such a department. The IAM is there to ensure organizational security. The engineers are highly qualified and make sure their developments are secure. The management should provide all resources so that all implementations are made to ensure security is guaranteed.

References

Garcia, D. J. P., Ouye, M. M., Rossmann, A., Crocker, S. T., Gilbertson, E., Huang, W., ... & Ryan, N. M. (2015). *U.S. Patent No. 9,129,120*. Washington, DC: U.S. Patent and Trademark Office.

Garcia, D. J. P., Ouye, M. M., Rossmann, A., Crocker, S. T., Gilbertson, E., Huang, W., ... & Ryan, N. M. (2017). *U.S. Patent No. 9,542,560*. Washington, DC: U.S. Patent and Trademark Office.

Gupta, A. (2018). *U.S. Patent No. 9,860,224*. Washington, DC: U.S. Patent and Trademark Office.

Joharapurkar, A. R., & Kwak, S. U. (2016). *U.S. Patent Application No. 14/717,705*.

Villa-Real, A. E. C. (2014). *U.S. Patent No. 8,831,677*. Washington, DC: U.S. Patent and Trademark Office.