JUNE 8, 2020

CS3052 – COMPUTER SECURITY

SECURITY PLANNING FOR A SECURITY DESIGNING PROJECT

H.A.A.S. HALLAWAARACHCHI
170203P

System Environment

1. A web application written using PHP need to be customized and installed in a server running RedHat Enterprise Linux
2. Back end is implemented using Oracle DBMS
3. Perimeter protection comes through firewalls, DMZ configurations and use of appropriate VLAN implementations
4. A mobile App is also developed to facilitate customer interactions
5. Most of the management functions are carried out by the staff using MS-Windows based workstations and laptops

Proposed Plan

According to the security plan, which is going to be implemented, there will be five major roles. They are,

I. CISO (Chief Information Security Officer)
II. DB admin
III. Security architect
IV. Security analyst
V. Security incident manager

Other than these five roles, the organization may want to hire a penetration tester to find out whether there are any security breaches in the system. They can do this quarterly, by six month or according to the situation.

The tasks and responsibilities of each position is as follows.

CISO

The CISO is the head of the security team. He has the responsibility of managing the others in the team to make sure that the system is protected well. He should have a great understanding about the security concepts, various types of attacks and security policies and regulations. Furthermore, he should have an idea about the latest techniques and strategies used by the attackers to attack the systems.

And according to our system, since it is served in server which runs on Red Hat Enterprise Linux, the CISO should have the expertise on the Red Hat Enterprise Linux. He should know how to configure the OS to protect the system against any incoming attacks. And he should make sure that the system meets all the necessary security requirements and regulations

imposed by the authorities. Moreover, it is his responsibility to maintain the system with the latest technologies in the world according to the budget of the company.

DB admin

Database admin is responsible for maintaining the database of the system securely. In our system since the database is implemented using Oracle DBMS, the DB admin should have the expertise on Oracle DBMS. And he should have a great understanding about the security features of the Oracle DBMS. He should maintain the database according to security requirements and regulations imposed by the authorities. And the various access privileges to the database should be given to the system users accordingly. More or less he is the person responsible for maintaining the database securely.

Security Architect

Security architect should have the understanding about the security concepts and the technologies used to develop the system. Then according to our system, we may need to security architects. One is expert in PHP based app development and another one which is an expert in mobile app development.

The major responsibility of the security architect is to make sure that the system which is going to be developed is up to the security standards. Then he may need to work corporately with the software architects to make sure the system architecture is up to the security standards. And he should have a great understanding about the techniques used to implement the security requirements the system needed, in his specialized system development technology stack (PHP, Android etc).

Security Analyst

He is the person who is the expert about the security concepts and the networking features used to secure the system. Our system is protected from attacks using firewalls and DMZs. The security analyst should have the expertise in configuring those firewalls and DMZ to protect our system from outside attackers. Furthermore, he may use VLAN configurations to increase the security of our system.

Security Incident Manager

Security Incident Manger looks at the traffic comes to our system and try to find out if there is any attack is coming to our system. This should be done through the twenty-four hours of the day. Hence, we may need more than one security incident manager according to capabilities of the company. He may use logs and other technologies to find out the attacks coming to our system.

Those are the five major positions in our security team. But when the company want the asses the security of the system, they may hire an outside penetration tester to check for any security breaches in our system.