Identifying potential risk response and recovery critical thinking sample

Business, Strategy

The following threats and vulnerabilities were identified as specific to the organization developing videogames. Attacks include malwares, worms, viruses Trojans/rootkits, spyware and adware in one category, phishing and spam messages in another category, Denial of service (DOS), web exploiting-Structured Query Injection (SQL) injection, Cross-Site Scripting (XSS)-XSS attacks uses non-sanitized or non-validated parameters to inject javascript or html codes into a running program. Vulnerabilities include accessibility of the database to the wrong persons through Data sniffing, leaked passwords, login details, security questions or personal data that is being used by developers (Weiss, 2010). The following are potential strategies for the identification of risks, responses and the recovery plans for each category of threats and risks.

Dealing with malwares, viruses, worms, Trojans and Rootkits

- The best strategy (risk mitigation) for dealing with the risks posed by malwares is to install programs called antiviruses. The antivirus used should be updated to enable it detect and neutralize all malwares, viruses and unwarranted programs.
- Mitigation strategies can also include isolating infected computers from the network and disinfecting them appropriately.
- It is appropriate for developers to disable System Restore before they start running any antivirus software.
- Risk acceptance strategies include identifying the differences between malwares, worms, viruses, Trojans, adwares among other related threats and then applying the relevant treatment measures effectively.

- Risk assignment strategies include designating and knowing the types of potential malwares, viruses and Trojans in order to select an antivirus that can handle all potential threats.

- Risk avoidance strategies include scanning and disinfecting storage devices before inserting them to computers that are being used to develop the videogames (Marty, 2009).

Phishing and Spam messages

- The best risk mitigation measure is installing programs that prevent or detect phishing and spam messages.

- Risk assignment in this case could entail ensuring that the staff is able to distinguish risky and genuine messages and how to respond appropriately in case of they receive risky messages.

- At all times, staff and developers should never open a message s/he is suspicious about

- Developers should not open suspicious links sent through email as they could activate malwares.

- The videogame developers should customize the firewalls of all the computers on which they develop videogames to minimize chances of an attack or vulnerability.

Spyware and adware

- When a computer is infected with spywares and adwares, it should be disconnected from the internet

- The best mitigation measure against spywares and adwares is for developers to avoid downloading “ free” screensavers or programs.

- They should also not click on pop-up adverstisements which mostly entise peole that that stand to win some money or a reward.

Data Sniffing

- The developers should regularly change the passwords to the databases of the programs that they develop.
- In case they are developing several videogames at once they should not reuse the same passwords to all the programs or use passwords that they have used elsewhere such as in emails.
- The developers should also use strong passwords that cannot be easily guessed by hackers.
- In order to increase security, the developers can use multi-factor authentication methods.
- It is advisable for developers to store backup information in case attackers or hackers destroy all the data or programs
- Training of employees especially the programmers on how to use different programming languages enables them to develop programs that are able to resist different kinds of threats and attacks.
- The company should also set policies that govern online behaviors of employees or program developers.

Controls to mitigate against risks

- The most effective administrative strategy to use in preventing computers against malwares, viruses, worms, Trojans among others is to install an antivirus. The administrative rights of the antivirus should be limited to specific program developers. This ensures that no unauthorized persons tampers with the antivirus for instance by uninstalling it.

- The antivirus should also be updated regularly to ensure that it can prevent against viruses causing damage to stored data. Updating an antivirus also enables it to detect unwanted programs.
- Once a computer is infected the necessary corrective measure entails disconnecting it from the internet, scanning it and then disinfecting or deleting infected files and programs. If need be, the storage devices bearing the infected files and programs can be formatted to as to remove the unwanted programs in their entirety. (Kim & Solomon, 2011).

Phishing and spam messages

- The administrative strategy for handling phishings and spam messages is to install a firewall blocker and antiphishing software.
- The use of emails that detect and place spam messages in a secluded folder is a proper preventative and detective control

Data Sniffing

- The best administrative control against data sniffing is setting up login and personalized details that are difficult o hack
- Prevention control could entail changing the passwords regularly
- The detection controls put in place could entail tracing the internet protocol access of the hackers to nab and deter them from accessing the computers used for development of the video games

References

Kim, D., & Solomon, M. (2011). Fundamentals of information systems security. Sudbury, MA: Jones & Bartlett Learning.

Marty, R. (2009). Applied security visualization. Upper Saddle River, NJ: Addison-Wesley.

Weiss, J. (2010). Protecting industrial control systems from electronic threats. New York: Momentum Press.