Cis 333 discussions

Technology, Information Technology

Computer Sciences & IT Question Providing Security over Data Data confidentiality within a work place ensures that data is not disclosed to unauthorized persons. In my place of employment, encryption is used. This ensures that only those with the right key can have access to the data. Access control lists and implementing and enforcing file access permissions. Data integrity ensures that the data cannot be modified by unauthorized persons. Our I. T department makes use of cryptography to ensure data integrity. Data hashing guarantees that the original data is received securely. Finally, the I. T department makes off-site data backups and employs redundancy to ensure that data is readily available to authorized persons when required.

e-Activity

One of the biggest attacks on mobile operating systems today as noted by researchers at Silicon Valley Security Company is the malware called WireLurker (Perlroth, 2014). It targets the Apple mobile and desktop users. The malware is designed in a way that unauthorized people can access the data from the devices. The security company confirmed that this is a malware affecting the Apple iOS mobile users in China (Perlroth, 2014). The devices become infected with the malware if they connect their devices to Macs through the USB wires and in cases where mobile users have altered their devices and installed software that Apple has not authorized.

The problem can be solved by informing mobile users in China to install software from trusted sources, to avoid jailbreaking their devices and keeping the iOS software up to date.

Question 2: Risk Management and Malicious Attacks

In china’s case of malware attack on Apple mobile devices it is important for the device users to avoid the risk by not using unauthorized software applications. Users should also prevent the transfer of the malware from the Macs to the mobile devices which occurs when using the USB wire. Users who have altered their devices by jailbreaking or those updating their devices from unknown sites should accept that it is a risk and the consequence is stolen information. Users of Apple mobiles can mitigate this risk by using the mentioned preventative measures.

e-Activity

After the attack on Sony in November last year, the company had to face new attacks in December after the company computer systems were breached (Barnes & Perlroth, 2014). The latest breach exposed the company’s executive compensation documents and had more movies pirated (Barnes & Perlroth, 2014).

If I was an IT security professional at Sony, I would join a team of other IT engineers at Sony to work with security encryption companies to ensure that more is done beyond having everyone with the same VPN passwords.

Question 3: Security Administration and Access Control

e-Activity

Tang Yan, a former employee at NetEase and now the founder of Momo, a dating application in China was accused of lack of professional ethics in December 2014 (Clover, 2011). Tang violated the labor contract and according to the officials at NetEase, he took advantage of his position at work to gain the data and resources to come up with the application.

References

Clover, C. (2011, December 11). China dating app founder accused of stealing technology. The Financial Times. Retrieved from http://www. ft. com/cms/s/0/9a91e0a6-8121-11e4-896c-00144feabdc0. html

Perlroth, N. (2014, November 5). Malicious software campaign targets apple users in china. The New York Times. Retrieved from http://bits. blogs. nytimes. com/2014/11/05/malicious-software-campaign-targets-apple-users-in-china/? _r= 0

Barnes, B., & Perlroth, N. (2014, December 2). Sony films are pirated, and hackers leak studio salaries. The New York Times. Retrieved from http://www. nytimes. com/2014/12/03/business/media/sony-is-again-target-of-hackers. html