System forensics: external intrusion of the playstation network case study sample...

Technology, Internet

There was an external intrusion into the Sony PlayStation Network (PSN) in 2011 April 20th. There was a data breach on Qriocity music and video service because of this instance. Soy server which was located in San Diego data center was remotely accessed by the hackers. The systems users were informed of the instance after the network was shut down.

There were unusual activities of the servers in San Diego where the servers were re-booting when they were not scheduled to reboot on 19th April. This resulted into an internal forensic investigation on the servers after putting offline four of the servers. On 20th April there was an expansion of the forensic team and the network servers that were being assessed. It was identified that there were unauthorized access to the data on the network server. The internal forensic team also established that there was transfer of information from the data servers without authorization. The internal investigation team required that all the servers be mirrored by an external forensic firm (Leick, 2011).

There was a second forensic team that was invited to assist in the investigation process on 22nd April. It was established the following day that hackers obtained an authorized access and hidden their activities from the administrators. The intruders were able to give themselves more privileges and deleted log files so that their activities cannot be easily established. It was on 25th that Sony had a forensic report which outlined the damage done by the intruders (Leick, 2011).

The public announcement from the company came out on 26th with a warning on credit card compromise. There was a communication on the official play station blog. In the post Patrick SeyBold the senior director of

corporate communication stated that:

“ An external intrusion on our system has affected our PlayStation Network and Qriocity services. In order to conduct a thorough investigation and to verify the smooth and secure operation of our network services going forward, we turned off PlayStation Network & Qriocity services on the evening of Wednesday, April 20th. Providing quality entertainment services to our customers and partners is our utmost priority. We are doing all we can to resolve this situation quickly, and we once again thank you for your patience. We will continue to update you promptly as we have additional information to share.” (Roberts, 2011).

The news about hacking started between April 17th until the company went public on 20th about the external intrusion. The reason why the company took a long time to go public was because they had not established the damage to the customers from the external intrusion. They were able to determine that their network had been illegally accessed but they were not aware of the extend of the damage the intruders had on the site. The impact of the attack was that about 77 million user data was compromised. The information that was stolen include personal identification information such as the names, billing addresses, email addresses, username, passwords, date of birth among other personal details (Leick, S. (2011).

The reason why the internal forensic team took a long time before telling the users the extent of damage done by intruders was because they did not have enough capacity to manage the process. The fact that the intruders were able to remove log files was challenging for the Sony forensic team to establish the damage. They were not able to tell the public immediately to

avoid panic and anxiety because they were not able to give the extent of the damage. It could not have been possible to provide a quick report from the forensic team because of the nature of the hackers. The hackers were able to delete their activities hence it should have taken the time to actually establish. The team was very small and did not have enough capacity to have all the servers mirrored in a short time to give a report.

References

Detected, I., & Down, N. S. Sony PlayStation Network Attacked.

Leick, S. (2011). NTS201-SP11169.

Roberts, P. (2011). Many Stuxnet Vulnerabilities Still Unpatched. Threatpost. com.