Case study on the best alternatives to sony corp to resolve their security crisis...

Business, Company

In 2011 Sony corporation suffered several major attacks by hackers angered over Sony’s prosecution of people who had illegally modified Sony PlayStations. These attacks exposed several weaknesses in Sony security. The purpose of this article is to address each of these weaknesses in turn and to attempt to suggest the best solution for each.

In recent years, one of the most exciting new ideas in IT has been cloud computing based on Web 2. 0 technologies that foster greater user interaction and sharing. For businesses, this often refers to the process in which they make use or one or more virtual servers instead of having one on site, which saves a great deal in overhead expenses. However, use of cloud computing can be seen in game consoles that connect to the Internet for online gaming. Sony’s PlayStation is an example of this kind of cloud computing (Rudman 2010). Unfortunately for Sony, their system has proven to be very vulnerable to attack by hackers. Several attacks at last forced Sony to temporarily shut down the entire system while they searched for a solution to the problem.

The several attacks that took place against Sony were of different types that targeted different weaknesses in Sony security. What this indicates is that Sony, and may other corporations, need to take a broader approach than just addressing these particular failures. They should look at several areas. These include deleting or destroying old data, ensuring that all important data in encrypted, ensuring that the data has full backups, setting up a protocol for checkout of materials, establishing a web browsing policy, creating a security

conscious culture in the company and setting up an approach to be used for DOS and DDOS attacks (Howell 2011).

The attacks on Sony took two primary forms. The first was a DOS or denial of service attack. DOS attacks can be carried out from a single computer, but they are more effective when done from multiple computers at the same time. The hacker usually accomplishes this by infecting other computers with a virus so that he can use them for the attack. Denial of service works by overwhelming the server with requests, which blocks legitimate users from getting access (Howell 2011).

The other way that Sony was attacked was with the theft of data related to clients credit cards. This information was obtained from 2007 data files on the server that were no longer being used. In addition, the files were in simple text format, rather than being encrypted (Mills 2011).

The first issue that Sony needs to address is that of deleting data that it no longer needs, such as the 2007 credit card data. However, the principle involved applies to other aspects of any business’s operations. The company should have in place mechanisms for destroying by incineration or other means any documents that are being discarded that might contain important information. In addition, they should erased and crush any discs or other storage media that might contain data (Microsoft 2005).

It is rather surprising that Sony stored client data in a completely unprotected text file. This is a major mistake that risks major financial liability on the company’s part. A simple solution that will avoid this kind of

exposure is to fully encrypt all important data, or even all data period (Stross 2011).

In addition to preventing the files from being read, any company like Sony should have full backups on separate servers for all their data. While this is an additional expense, it is far less expensive than the costs that a company might face should it lose huge amounts of valuable data.

Another way that a company can lose valuable data is by theft of papers, laptops, CD-ROMs or other storage media. Employees often take their work home with them, and this work can easily be lost or stolen. There are also employees who steal information from the company for the purpose of selling it. To combat this, companies should have a strictly enforced checkout policy. Any digital information or paper that leaves with an employee should have to be logged out when it goes and logged in when it returns. This might seem like an arduous process, but hopefully it will encourage employees to take home only what they really need.

Companies that want to protect themselves from outside hackers also need to establish rules regarding Internet use at work. While it is often a necessary part of work to go on the Internet during the day, many sites or activities can risk downloading viruses to the company computers. This is why employees should only be allowed to visit safe, work related sites. They should be informed that their activity will be monitored to ensure compliance with policy (Schirick 2012).

These last two issues revolve around creating a conscious awareness among the employees about security. Many employees underestimate how great an impact security lapses on their part can have on the company. Even managers sometimes are ill-informed. For example, while the weakness that led to the break-ins at Sony will well understand by lower level employees, upper management was unaware of them. The solution is an ongoing effort to keep all employees aware of security issues (Microsoft 2005).

The final point that Sony and other companies have to address is that of denial of service attacks. The primary method for stopping a denial of service attack is to block the ISP of the computer that is attacking. However, in the cases of multiple computers, this is made more problematical.

While it is true that often the attacking computers will have the same range of ISPs, blocking all of the ones from the area will also cut off many legitimate users. However, there is really no other open if service is going to be restored. Companies should have this policy in place and ready to go in the event of a DDOS attack. It is even a good idea to practice an attack so employees can be prepared.

The multiple attacks that were made on Sony last year show that it has become a primary target for hackers, if for no other reason because they all want to say they have done it. Given this, it would be wise for Sony (and any other corporation) to carry out the previous suggestions for tightening their online and internal security. This will protect both their customers as well as their bottom line.

References:

Howell, Donna. (2011) Security, Outages Gray Areas For Cloud Computing 'Significant Challenges' Still Sony PlayStation hack, Amazon Web Services issues cast black clouds. Investor's Business Daily, A05.

Microsoft. (2005) Security Guide for Small Business. Microsoft. Retrieved April 27, 2012, from http://www. google. com/url? sa= t&rct= j&q=&esrc= s&source= web&cd= 1&ved= 0CG0QFjAA&url= http%3A%2F%2Fdownload. microsoft. com%2Fdownload%2F3%2Fa%2F2%2F3a208c3c-f355-43ce-bab4-890db267899b%2FSecurity_Guide_for_Small_Business. pdf&ei= 98KcT-PCLaaaiALdqrRy&usg= AFQjCNEmSNiQ4okOiXj8xWokgByuqHLAMg&sig2= viZsazC_yzYv7x3Q39CGew

Mills, E. (2011) Attacks on Sony, others show it's open hacking season. CNET News. Retrieved April 27, 2012, from http://news. cnet. com/8301-27080_3-20069995-245/attacks-on-sony-others-show-its-open-hacking-season/ #ixzz1PHwIH7dt

Rudman, Riaan J. (2010) Incremental Risks in Web 2. 0 Applications. The Electronic Library 28. 2 (2010): 210-230.

Schirick, Edward A, CPCU, CIC, CRM. (2012) Computer Network Security - Evolving Risks. The Camping Magazine 85. 2 (Mar/Apr 2012): 16, 18-19.

Stross, Randall. (2011) Guard That Password (and Make Sure It's Encrypted). New York Times, BU. 3.