



Deedoc Managed Security Services

William Harbert
Chief Information Officer (CIO)
Deedoc Managed Security Services

Need for Third Party Vulnerability Assessments

On April 19, 2011 Sony's Play Station Network suffered one of the largest and most severe financial information breaches in history. An estimated 102 million accounts were compromised. The data stolen includes credit card information, email addresses, passwords and other personal information. As of May 4, 2011 the PSN is still shutdown. Sony has lost the trust of its customers as well as being the subject of a class action lawsuit. The true cost to Sony may be millions of dollars. At this point, Sony has tough questions to answer.



PLAYSTATION®Network

How did this breach occur? Were they aware they had such a severe vulnerability? What was done to mitigate their vulnerabilities? Did they have a process in place to find and manage these vulnerabilities?

More alarming than the headlining compromise stories are the attacks that are never reported. While some attacks go unreported to limit loss of reputation, Ted DeZabala, principal, Deloitte & Touche LLP and national leader of Deloitte's Security & Privacy services, states, "We believe that most cybercrimes go unreported, not because they are handled internally, but rather because they are never detected in the first place. This is a proverbial 'tip-of-the-iceberg' situation, and the implications are significant."

The world is changing. The complexity of modern information systems continues to increase. More and more, these systems rely on services on the public internet. This increases both the number of vulnerabilities and paths to exploit those weaknesses. In such a complex environment even a small change or software patch can cause a significant security gap. Such complexity can quickly overwhelm system administrators and provide the perfect setting for attacks to go unnoticed for months.

While in the past cyber criminals have primarily targeted individuals, increasingly organizations are the new focus of attacks. From organized criminals committing acts of fraud or extortion to the increasingly popular use of cyber crime as a form of political expression, these crimes are causing increasing amounts of damage. Several high profile attacks in 2010 and 2011 were committed by groups with political motivation. In December of 2010



group known as Anonymous launched denial or service attacks against the websites of MasterCard Inc and Visa Inc. These issues come at a time when organizations are being held increasingly responsible for the security of their customers' information.

In order to mitigate potential vulnerabilities, they need to be discovered first. This is where the expertise of an outside penetration testing firm becomes invaluable. Such firms use the same tools, techniques and methods as an actual attacker. There are several different ways in which a penetration test can be implemented. The most basic plan would be to run a vulnerability assessment against a specific service or device. In this way the security of a single system could be quickly determined. A comprehensive scan of system- wide vulnerability will give a much better picture of overall security, so that any compromise, loopholes or exposure on the system or networks that have no legitimate use, can be closed. The most comprehensive assessment would be to play the role of the attacker and use publicly available information to mount an attack and try to breach the system.

Modern information systems are constantly changing and adding new services. This is why it is important to have regularly scheduled vulnerability assessments. A single assessment is only a snapshot of the system at a specific time. When patches are deployed as part of regular maintenance, they may create unexpected vulnerabilities. The ongoing adding or removing systems and services changes the system and calls for reassessment. Regularly scheduled assessments will ensure that new vulnerabilities are discovered and mitigated quickly and responsibly

Beyond discovering vulnerabilities, there are many benefits to regular assessments. Such assessments can create performance data that can be used to measure the effectiveness of new policies or procedures. Internal IT staff and systems administrators can also gain valuable information on how to distinguish attacks from normal operations. Management will gain insight on how their departments and policies handle a real attack. Regular vulnerability assessments are also an important part of many regulatory compliance procedures as well as establishing due diligence in legal matters.

Every organization that uses the internet today is a potential target for financially or politically motivated attackers. There is also an increasing expectation from the public, as well as regulatory bodies that organizations must keep personal information well secured and confidential. As more services and data are pushed out on to the internet, IT departments are finding themselves overwhelmed by the scope and complexity of properly securing sensitive information.



The trend today is to hire a third party vulnerability assessment firm to significantly reduce this burden by regularly scanning for weaknesses as well as providing policy recommendations and security awareness training. In addition to the direct benefits, these assessments test the effectiveness of an organizations risk management and response policies, as well as demonstrates to regulators and the public a strong commitment to information security and confidentiality.