ISE West Executive Forum
Moving from Reactive to Proactive

Bryan Vargo
Sr. Manager, Information Security and Risk Management
McKesson Corporation

August 10, 2011

Question

- How big of a threat or breach is needed to get your company's attention?

  - "We've been reminded that no one is immune to a cyberattack. We believe the attack on us was unprecedented in size and scope," said Tim Schaaff, president of Sony Network Entertainment International, a division of Sony. "We look forward to a national initiative that protects consumers."

  - The Sony hack, discovered April 19, is believed to have affected at least 77 million online PlayStation Network gamers. An additional 8,500 user accounts, part of Sony Music Entertainment, were later reported by Sony to be impacted as well.

Source: SC Magazine

Top Data Loss Breaches

Name	Type of Breach	Number of records, tokens, or code
Sony PlayStation Network (PSN) (New York)	• Sony discovered an external intrusion on PSN and its Qriocity music service around April 19. • As of today they have been hacked 19 times	• 77 Million records
WordPress (San Francisco)	• Hackers accessed several of WordPress's servers.	• 18 Million records
Texas Comptroller's Office (Austin, Texas)	• The information from three Texas agencies was discovered to be accessible on a public server.	• 3.5 Million records
RSA	• Attackers may have stolen the source code, or private cryptographic keys to trick RSA servers or tokens.	• Unclear of amounts of information compromised
Lockheed Martin	• It is not known what information the alleged hackers were after, but it is believed the breach could have been an attempt to exploit Lockheed's customers	• Unclear of amounts of information compromised • Possible link to RSA breach

Source: SC Magazine, EWEEK, and others

Was your data included?

McKESSON
Empowering Healthcare

534,801,553

- Total number of records involved in security breaches containing sensitive, personal information, since January 2005, in the U.S.
- How would you feel if your information was breached and what actions will you take to prevent this from happening?
- Do you trust that your information assets are secure and accessed properly?

Ensure a secure environment

McKESSON
Empowering Healthcare

- As security practitioners we must be as agile as attackers
- Want to hear the answers to the tough questions
- Reduce the vulnerability noise by continually testing potential attack paths. Narrow down vulnerabilities and focus on actual risks.
- Establish effective lifecycle principles within your security programs, policies and processes. Be iterative.
- Build metrics that matter not what you can cobble together. Measure effectiveness and make modifications as needed
- Understand that hackers don't have 'start and finish' concepts like projects or longer-term program efforts

Ensure a secure environment

(continued)

- Have an accurate inventory of top critical business systems and environments. Know the connected systems and their potential impact to critical business systems.
- Increase the frequency of your security awareness education. Test your users for susceptibility to phishing
- Company's and their service provider should be proactive on security programs and remediation efforts. If you wait too long, business impact could occur.
- Get personally involved to show executive level sponsorship of enhancing your company's security posture. Challenge IT resources and security teams to update threats frequently and remediation strategies.

Advantages of Continuous Testing

- Proactive vs. reactive posture when it comes to security decisions
- Efficient, precise and cost-effective remediation priorities = Accurate information and corrective actions with minimum business disruptions
- See business information systems and networks **through the eyes of attackers** to prevent various forms of an breaches
- Expose vulnerabilities – systems and information assets that are at risk
- Routinely test your current security posture! Data and the systems that house information are in constant changing states. Continuously monitor your:
  - Remediation activities, Patch Mgt, AV Solutions, Firewalls, and IDS/IPS systems

Summary

- Penetration tests, CEH, etc. are proactive and authorized attempts to compromise network entry points and access sensitive information by exploiting vulnerabilities.
- Conducting reoccurring risk assessments can mature your companies security posture and helps avoid a breach
- If your company has reoccurring tests preformed by a external vendor, your company could have funded a internal Red team and save money in the long-term.
- Don’t wait before it’s your own company's wake up call via a breach

Contact Info. and Appendix

- Contact Information:

Bryan T. Vargo, CRISC, CCM, CICP
Sr. Manager, Enterprise Product Security Office
Information Security and Risk Management
McKesson Corporation
(608) 348-8087 Direct
(563) 213-0456 Mobile
Bryan.Vargo@McKesson.com
http://www.linkedin.com/in/bryantvargo

- Appendix
  - Additional Notable Breaches
  - What is Penetration Test?
  - Notable References

Additional Notable Breaches

January 2005	George Mason University	32,000 records exposed
March 2005	DSW, Retail Ventures	1.4 million records affected
December 2006	University of California Los Angeles	800,000 records exposed
January 2007	TJX	100 million records exposed
September 2007	TD Ameritrade Holding Corp.	6.3 million records exposed
August 2008	Countrywide Financial Corp.	17 million records exposed
November 2008	University of Florida College of Dentistry	330,000 records exposed
January 2009	Heartland Payment Systems	130+ million records affected
January 2009	CheckFree Corp.	5 million records affected
May 2009	Virginia Dept of Health Professions	530,000 records affected
May 2009	Kaiser Permanente Bellflower Medical Center	1 records affected
May 2009	Aetna	65,000 records affected
July 2009	Network Solutions	573,000 records affected
September 2009	UNC Chapel Hill	236,000 records affected
December 2009	RockYou	32 million records affected
December 2009	Penn State University	30,000 records affected
December 2009	Eastern Washington University	130,000 records affected

Additional Notable Breaches

January 2010	Lincoln National Corp.	1.2 million records affected
March 2010	Educational Credit Management Corporation	3.3 million records affected
November 2010	Desert Rose Resort	UNKNOWN
December 2010	Stony Brook University	61,001 records affected
December 2010	deviantART, SilverPop Systems, Inc	13 million records affected
December 2010	Ohio State University	750,000 records affected
December 2010	Social Security Administration	15,000 records affected
December 2010	Home Depot	UNKNOWN
December 2010	Department of Education – Federal Student Aid	UNKNOWN
December 2010	McDonalds, Arc Worldwide, SilverPop Systems	UNKNOWN
December 2010	Gawker	1.3 million records affected
January 2011	South Carolina State Employee Insurance Program	5,600 records exposed
January 2011	Seacoast Radiology	231,400 records exposed
January 2011	University of Connecticut, HuskyDirect.com	18,000 records exposed
January 2011	Pentagon Federal Credit Union	514 known records exposed

What is Penetration Test?

- A **penetration test** is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source. The process involves an active analysis of the system for any potential vulnerabilities that could result from poor or improper system configuration, both known and unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures.

This analysis is carried out from the position of a potential attacker and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner, together with an assessment of their impact, and often with a proposal for mitigation or a technical solution. The intent of a penetration test is to determine the feasibility of an attack and the amount of business impact of a successful exploit, if discovered. It is a component of a full security audit.

References

- http://www.scmagazineus.com/
- http://www.eweek.com/c/a/Security/RSA-Warns-SecurID-Customers-of-Data-Breach-395221/
- http://gamutnews.com/20110528/11525/data-breach-affects-lockheed-martin.html
- www.DataLossDB.org
- http://www.wikipedia.org/