New dimensions in SNMP Protocol in Romania

Alice Nastovici

In this year 2009, after e-finance shock made in each banks who worked with Simple Network Management Protocol (SNMP) default community string and vulnerability:

- If you do not absolutely require SNMP, disable it
- If you must use SNMP, use the same policy for community names as used for passwords. Make sure that they are difficult to guess or crack and that they are chanced periodically
- Validate and check community names using SNMPwalk. Additional information can be found at http://www.2nd.com/functionSNMPwalk.php
- Filter SNMP (port 161/udp) at the border-router or firewall unless it is absolutely necessary to pool or manage devices from outside of the local network, where possible read-only

2008 crisis in establishing a benchmark to actuarially measure the cyber-risk of hack attacks electronic identity theft, and other forms of related e-risk, banks combined information security standards with principals of risk management that include e-system analyses, avoidance, control and e-risks transfer.

Certification authorities are in 2008 seven global financial institutions that are ABN, Bank of America, Deutsche Bank, Barclays, Chase, Citigroup and Hypoverens Bank. Technology must offer unique ways of authenticating such digital time stamps that utilise satellite with GPS must identify position of losses adding value to a contract documents.

Procedures are the documented intimacies of how the systems work. Six nations had Standards Setting as Canada, United Kingdom, United States, Netherlands, Germany and France.

German Information Security Agency (GISA) with internal corporate standards translates policy into action in National Bank of Romania using vulnerability tests of network and encryption.

The various losses sustained because of the intrusion into the financial entity's networks.

Date of Attack	E-commerce entities	Losses
1. July 26,27 2005	Italian Bank Romania	Hackers made illegal charges on customer accounts by attacking the VISA check card program. Investigation ongoing
2. August 2005	Bank of Spain	Hackers send spam stating they were bank representatives informing customers of a chance to win 500$. A link was placed within the email to take customers to a false Bank of Spain site in which customers had to enter bank information and PIN numbers. The link also contained the Trojan horse virus. Investigation ongoing
3. September 2005	Paypal, Ebay	Utilised a spoofed Paypal email address liking to www.paypalwarning.org, a site unrelated to the official Payal website
4. July 2006	ABN Amro Romania bank	With the help of computer spyware hackers stole approximately 500.000 RON from customer accounts in the bank. Investigation ongoing

5. July 2006	Wells Fargo USA	Contained a spoofed email with an attachment caring the Trojan horse virus. The virus collected passwords and send them to a third party. Investigation offgoing
6. September 2007	Barclays	False emails concerning Barclays new security policy were sent to random customers directing them to a Barclays link which would then take them to one of eight spoofed Barclays websites where customers were prompted to input bank and credit information
7. September 2007	Stock Market Romintrade Brasov Romania	Romintrade used key stoke logger to steal Romania brokerage firm customer accounts and then used a victim's account identity as a means to unload falling stokes.

Bibliography

John Leyden "Trojan Infection linked to SA Net thefts", The World Bank Report Review 7/21/2003
http://www.wellsfargo.com/jump/fraud_prevention.jhtml
http://www.usatoday.com/tech/news/computesecurity2007
Ebay / Paypal hit again, http://www.internetnews.com/iar/article.php
Bank of Spain, http://www.workopolis.sp/servlet
Barcalys http://www.guardian.co.uk/business
BBC News October 2008, US Hacker accused of massive fraud, http://news.bbc.co.uk/1/hi/business