Quarterly Security Statistics Review

Consumer Security and Online Threats

RSA 2010 Global Online Consumer Security Survey

Threat awareness

- 76% of consumers are aware of the threat of phishing. This number has doubled compared to the 38% that responded in 2007.
- 81% of consumers are aware of Trojans. This is an increase from the 63% that responded similarly in 2007.
- Consumers are not as aware of newer threats such as vishing, smishing and botnets. Survey participants that expressed awareness of these threats are as follows:
    - Vishing – 26%
    - Smishing – 33%
    - Botnets – 14%

Security concerns among consumers

- 90% of consumers expressed concern with phishing
- Three out of ten consumers have been the victim of a phishing attack (29%)
- 93% of consumers expressed concern with Trojans or spyware being installed on their computer

Online banking

- 86% of consumers stated they were concerned with their personal information being accessed or stolen at an online banking site
- 80% of consumers stated that banks should implement a stronger form of security to identify users when logging in
- 90% of consumers stated they expect their banks to monitor their online banking transactions
- 98% of consumers stated they would be willing to use stronger security if it was offered by their bank

Social networking

- 81% of consumers stated they were concerned with their personal information being accessed or stolen on a social networking site
- 65% of consumers stated their concerns with their personal information being stolen makes them less likely to submit personal information to a social networking site
- 59% of consumers stated that social networking sites should implement a stronger form of security to identify users when logging in
- 90% of consumers stated they would be willing to use stronger security if it was offered at the social networking site(s) they regularly visit

Healthcare

- 64% of consumers stated they were concerned with their personal information being accessed or stolen on a healthcare site
- 59% of consumers stated their concerns with their personal information being stolen makes them less likely to submit personal information to a healthcare site
- 64% of consumers stated that healthcare sites should implement a stronger form of security to identify users when logging in
- 95% of consumers stated they would be willing to use stronger security if it was offered at the healthcare site(s) they regularly visit

Government

- 68% of consumers stated they were concerned with their personal information being accessed or stolen on a government site
- 60% of consumers stated their concerns with their personal information being stolen makes them less likely to submit personal information to a government site
- 70% of consumers stated that government sites should implement a stronger form of security to identify users when logging in
- 95% of consumers stated they would be willing to use stronger security if it was offered at the government site(s) they regularly visit

Data Breaches, Data Loss and Encryption and Tokenization

Open Security Foundation, DataLossDB

The following statistics are based on the data breaches reported in 2009:

Data breach incidents by sector
46% business (including financial services)
18% education
21% government
14% medical/healthcare

Data breach incidents by attack vector
51% external sources
32% insider (accidental)
8% insider (malicious)

US Cost of a Data Breach Report[1] (Ponemon Institute)

- The average cost per compromised record is $204.
- The average cost of a data breach to an organization is $6.75 million.
- 67% of those affected by a breach stated **training and awareness programs** would lead their efforts to prevent future data breaches.
- The cost of a data breach as a result of malicious attacks and botnets were more costly and severe.

2009 Identity Theft Resource Center Breach Report

- *Only one percent* of organizations that experienced a data breach in 2009 stated they had encryption or some other form of security mechanism in place to protect the exposed data.

2009 Data Breach Investigations Report (Verizon Business)[2]

- 74% of data breaches resulted from external sources; 20% were caused by insiders.
- 38% of data breaches involved the installation of malware on a system or network.
- Cardholder data was compromised in 81% of breaches; personally identifiable information was compromised in 36%; and intellectual property in 13%.

Gartner

- More than 80 percent of companies use live data for non-production purposes (this makes the case for tokenization).

[1] This study was commissioned by PGP Corporation.

[2] The study is an analysis of 4 years of data security breaches from 2005 through 2008. There were 500+ cases that were analyzed.

Quarterly Security Statistics Review

Identity Theft and Money Mules

Javelin 2010 Identity Fraud Survey Report *(*Consumer Reports National Research Center)

- The number of identity theft victims in 2009 in the U.S. was 11.1 million, an increase of 12% from 2008.
- Total losses from identity fraud in 2009 were $54 billion.

APACS (UK Payment Card Association)

- Phony job ads have increased 345 percent over the past three years.
- Online banking fraud losses in the UK totaled £39m in the first six months of 2009 – a 55% increase from the same period the previous year.

RSA Anti-Fraud Command Center

- According to the AFCC, the average selling price for a U.S. credit card in the fraud underground is $1USD. But when that single card is sold with a full identity profile, which includes information such as the customer's billing address, Social Security number, mother's maiden name and date of birth, the price is inflated to as much as $20USD.

GetSafeOnline.org

- In the UK, it is estimated that at any given time, there are about 100 known mule recruitment sites in operation, each of which may have about 50 active mules.

Phishing and Malware

RSA Anti-Fraud Command Center

- The volume of phishing attacks addressed by RSA during 2009 increased 17% over those detected in 2008.
- Over the past year, the five countries that have consistently suffered the largest portion of phishing attacks have been the US, the UK, Italy, Canada, and South Africa.
- The number of Trojan communication resources (including infection and update points and drop zones) that RSA has addressed has increased over 300% in the last year.

Gartner, The War on Phishing is Far from Over Report

- 40% increase in the number of U.S. consumers that lost money to phishing attacks in 2008.
- The average consumer loss in 2008 per phishing incident was $351.

Federal Bureau of Investigation (FBI)

- Spear phishing attacks cost U.S. businesses $100 million in losses in 2009.

The Intrepidus Group

- 23% of people worldwide will fall for spear phishing attacks.
- 60% of corporate employees who were susceptible to targeted spear phishing responded to the phishing emails within three hours on average.

Australian Institute of Criminology

- Fraud accounts for the largest percentage of crime costs in Australia, at an estimated A$8.5b.
- Cybercrime is costing Australian businesses more than A$600 million per year.

ScanSafe Annual Global Threat Report

- Data theft Trojans have increased significantly across many industries in the last year:
    - Energy and oil – 356% increase
    - Pharmaceutical and chemical – 322% increase
    - Government – 252% increase

Authentication and Password Management

Trusteer

- 73% of bank customers use their online bank account password to access other sites.

Forrester Research, Best Practices: Implementing Strong Authentication in Your Enterprise

- 44 percent of organizations use just a password to secure remote access to their intranet

Insider Threat

Association of Certified Fraud Examiners, 2008 Report to the Nation on Occupational Fraud & Abuse

- U.S. organizations lost 7 percent of their annual revenues to fraud committed by employees between 2006 and 2008, for an estimated total cost of $994 billion in losses.

Social Networking

Breach Security Labs, Web hacking Incidents Database 2009 Bi-Annual Report

- Nearly 20% of online attacks are targeted at social networking sites.

Nielsen, Global Faces and Networked Places (August 2009)

- Two-thirds of the world's Internet users visit a social networking or blogging site.
- 17% of all time spent on the Internet is on a social networking site.

Compliance

12th Annual Ernst & Young Global Information Security Survey

- 55% of organizations indicated moderate to significant increases in compliance-related cots as part of overall security costs.

Medical/Healthcare

Federal Trade Commission

- According to the FTC, a medical ID card can fetch between $25 to $50 compared to a Social Security card which is only worth $1.

Critical Infrastructure and Government

Center for Strategic and International Studies[3]

- The cost of downtime resulting from a cyber attack costs $6.3 million on average per day. For the oil and gas industry that number was much higher at $8 million per day.
- 89 percent of organizations had experienced a cyber attack as a result of a malware or virus infection.

[3] This study was commissioned by McAfee.