Interested in learning more about security?

SANS Institute InfoSec Reading Room

Information Security Issues in E-Commerce

A discussion on some of the issues in the state of information security as it pertains to e-commerce. Topics include the neglect for information security in the heads of e-commerce pioneers, intrusions and consequences that have been revealed to the general public, and a few notes about the future. It is perhaps those who consider security as a core function of e-business that will be the long-term beneficiaries of this revolution.

Information Security Issues in E-Commerce

by

David J. Olkowski, Jr.

for

SANS GIAC
Security Essentials

March 26, 2001

Information Security Issues in E-Commerce

Introduction

The Internet has evolved far beyond a collection of research and government technology labs and communications centers for which it was founded. The opening of access points on this global collection of local networks to commercial enterprises in the early 1990's spurned numerous innovations to produce immense increases in speed of transfer and quantity of storage of data capital. The means of competing in a free market economy adapted, and productivity increased at a much faster pace in the last decade than the century and a half since the dawn of the Industrial Revolution. The manipulation of digital capital shaping the progress of the Information Age must be secured in order for massive change in marketspace and transaction processes to become accepted and cost-effective for producers, sellers, and buyers. What has transpired in commerce in the last ten years may send armed guards at physical bank buildings toward extinction. Some of these armed guards might just find new employment at massive secure data centers. However, their importance will diminish as more and more data is stored behind the gates of these data centers where the most lethal of firearms and high voltage chain link fences will not stop the growing class of electronic thieves, terrorists, and vandals.

Dreams of being the next Jeff Bezos of Amazon.com, have inspired many hot-shot e-commerce entrepreneurs to rush their ideas to market in "Internet-time." Lately, we have witnessed the mass failures and layoffs at many dot-coms. Perhaps it is fortunate though that some of them failed because of market forces. I say this because if anything, there are an alarming amount of these digital capital moguls that would rather show massive sales growth to their investors than concern themselves of potential devastation by theft of data from an intruder months down the road. In writing on this subject, my goal was to bring to light the dire need for improvements from a business perspective for information security as transactions of money shift between businesses and individuals. There are many great success stories in the works. However, the state of security in e-commerce I believe is far behind the great economic efficiencies that these processes are intended to create. Information security in many factions of this new economy ranges from an "afterthought" to "never a thought." I will focus on some of the issues in the state of information security as it pertains to e-commerce. Areas that will be covered include the neglect for information security in the heads of e-commerce pioneers, intrusions and consequences that have been revealed to the general public, and a few notes about the future. It is perhaps those who consider security as a core function of e-business that will be the long-term beneficiaries of this revolution.

The Business of E-Commerce

E-commerce can be simply defined as conducting business over a data network that in some logical way has access to the all-encompassing Internet. The major market researchers have weighed in with revenue projections to push the fervor higher to new extremes. Gartner Group predicted in August 2000 that the year would end with an

Internet retail revenue tally in North America up 75% of 1999's figure of $16.8 billion and 157% from 1998.[1] Taking into consideration e-commerce in the much larger Business-to-Business (B2B) realm, the forecast by e-commerce statistical firm eMarketer is for the current $226 billion global revenue of 2000 to approach $2.7 trillion by 2004.[2] Thus the wealth being moved on electrons over wires and in the air is indeed a tempting pot-of-gold for thieves.

Response at the Corporate Level

We all know the stereotype round-the-clock on-call system and network administrator who receives at most a pat on the back in lieu of fair monetary or career reward. Organizational IT budgets in the traditional economy often fall short of what is necessary for positive return on investment in the form of profit or cost savings. However with money up for grabs in e-commerce space, the corporate stakeholders have loosened the purse strings for IT. If you take security as a well defined portion of that IT budget, spending by many companies for network security is not keeping up with production nor is it being strategically spent.

A recent report from Forrester Research titled "Sizing the Security Market," predicted spending on IT security at $19.7 billion by 2004. What matters little though are not the amounts and increased figures, but the reality that businesses will continue to pour this money into external security spending rather than key business assets. Resource shortages and time constraints are forcing firms to direct what funds they can allocate at outsourced services. It also instills the trend of scrambling to hold on to customers rather than looking at internal security threats. This criticism comes in terms of a perceived negligence over control by business managers as they predict outsourcing spending will increase into 2002 while internal funding for planning and management or core system security remains stagnant.[3] I do not totally agree with Forrester's rationale for misallocation of security funds to outsourced services. This is because outsourcing and consulting can return value when the alternative is to overtax an internal staff that is not full time security. However, I do think Forrester's recommendation to put business management in full charge of security has strong merits. In this way a security framework can be built into processes that will function whether the near future in security staffing can be met internally or externally.

A widely publicized survey effort was undertaken by *Information Security* magazine in June and July 2000 to assess the state of the information security in the opinion of 1,897 IT managers. The number of companies spending more than $1 million annually on network security doubled over 1999. This ranged from consulting companies having a median of $2 million to post-secondary education institutions reaching a median of just $100,000. At first glance this may be impressive. However,

[1] "E-Commerce Growth Predicted for North America," *CyberAtlas*, August 8, 2000, URL: http://cyberatlas.internet.com/markets/retailing/article/0,,6061_408451,00.html

[2] "New Report Reveals: Global B2B eCommerce to Reach $2.7 Trillion by 2004," ebizChronicle.com February 1, 2001, URL: http://www.ebizchronicle.com/backgrounders01/feb/eCommerce_b2b.pdf

[3] Michael Mahoney, "Report: IT Security Spending Missing Mark," *E-Commerce Times*, October 30, 2000, URL: http://www.ecommercetimes.com/perl/story/?id=4677

the gist of this survey is that security spending is not keeping pace with the crime that is being perpetrated against all parties from producers to brokers to buyers moving toward greater reliance on e-commerce.[4]

To put this in perspective, the survey report indicates that "security is riding the coattails of business initiatives that involve security, but aren't necessarily security driven." A Forrester Research survey conducted in May 2000 found that only half of managers are actively involved in risk management. The *Information Security* report makes an important note that even though security spending has risen, the distribution of security is misplaced. Management has a tendency to direct security spending at a directed area for a specific service or venture. Thus throwing money at problems is rarely spent to build a security culture and architecture that is company wide and is easily integrated with temporary B2B partner engagements. Global Integrity's Dan Woolley brings this down from the higher authorities by stating, "For the most part, information security is still funded as a necessary evil, and as a result security isn't even the first or second or third most critical issue in getting a product or service to market." The *Information Security* survey report gives a quick hypothetical remark that "management probably won't want to hear about how complicated it is to update and enforce certificate policies for different levels of users in a 200-member extranet."[5]

News Flash: E-Commerce Sites Attacked

Just a few years ago, even the casual office worker did not have e-mail accessibility over the Internet. However, the massive worm/virus attacks of recent months such as the "I Love You" vbs attachment virus have brought a sense of reality in destructive computing power to the simple desktop PC office user. Major broadcast television networks now commonly dedicate a segment to report on an attention grabbing hack whether it be defacing government web sites or credit card database compromise. Though this is just the tip of the iceberg, it is a good start at making the knowledge society cognizant of threats to information. Other factors which are relevant including exposing the concern over business-to-consumer credit card databases and the significant increase in stock ownership of the average individual in recent times.

Now that news of hackers breaking into e-commerce data, what exactly is behind the sensationalism? A high profile distributed denial of service (DDoS) attack made big headlines when web sites including CNN.com, Yahoo!, e-Bay, and Amazon.com were put out of commission in February 2000. A few months later a teenager known by his cyberspace alias of "Mafiaboy" was arrested for carrying out this attack. Though this attack hit some of the more established on-line retailers, its financial damage was estimated at $1.5 billion as it interrupted the initial public offering of Buy.com and stopped securities trading at E*trade and Datek. At the time of the indictment of MafiaBoy, Robert Harvey of Validity Systems, was interviewed by NewsFactor in which he said, "this guy's a dumb punk looking for some glory," and "these are the same kids

[4] Andy Briney, "Security Focused," *Information Security*, September 2000, URL: http://www.infosecuritymag.com/articles/september00/pdfs/Survey1_9.00.pdf
[5] Ibid.

that spray paint walls."[6] It is true that the form of this criminal activity is that of vandals, but the cost to stakeholders is far beyond that of simply rolling fresh paint on a wall to cover up graffiti. In addition to the immediate loss of business activity before these sites could restore order processing, the customer retention factor is so volatile in e-commerce that such attacks could kill a merchant just by the fear and mistrust instilled in customers.

More alarming to the wired public is when the 16 digit numbers that tie the world together in the exchange of goods and services are taken deep inside data centers with no personal means for maintaining confidentiality. This year began with the disclosure of the outsider breach of Travelocity's customer's names, addresses, phone numbers, and e-mail addresses.[7] Barnesandnoble.com had a report from a thankfully honest user that was redirected into another user's account with plenty of their personal information available.[8] In early 2000, the hacker who conceals his identity with the alias "Curador" seemed to bask in the publicity as he revealed his theft of 2,000 records including credit card numbers from e-commerce broker SalesGate. Curador also hit shoppingthailand.com, promobility.net, and LTAmedia.com to become privy to over 5,000 credit card numbers which he posted to a publicly accessible web site until the host removed it. Somewhat amusing though controversial is how Curador has left his mark by thanking Bill Gates for creating "SQL servers with default world readable permissions."[9]

One common trend is the use of application service providers (ASPs) for hosting of e-commerce sites. This is especially prevalent among small- and medium-sized businesses which could suffer terminal consequences on compromise of their systems. A Russian web programming company called Strategy LLC, demonstrated this for the on-line press in early 2000.[10] Anatoliy Prokharov, a programmer at Strategy LLC, demonstrated for an MSNBC reporter how easy he could look into 20 Web Sites to access as many as 25,000 credit card numbers as well as employee data. Prokharov pointed out that many of these flaws happen when 3rd party developers turn over systems to a company with no liability for the open holes that they leave. It is then the merchant's responsibility to cover any information obtained through an attack.

Besides the obvious critical blame on Microsoft with its history of neglect for security in its applications, there are many other vulnerabilities that expose the e-commerce world to attack. CGI-bin vulnerabilities are a classic example as the outsider can flood or manipulate an entry box when making a web transaction. Cross-site scripting has come to light where the end user web browser unknowingly hits a hyperlink that inserts malicious code enabling the intruder the chance to intercept credit card

---

[6] Jay Lyman, "Teenage Hacker Mafiaboy Pleads Guilty," January 19, 2001, URL: http://www.newsfactor.com/perl/story/?id=6836

[7] Paul A. Greenberg, "In E-Commerce We Trust…Not," *E-Commerce Times*, February 2, 2001, URL: http://www.ecommercetimes.com/perl/story/?id=7194

[8] Ibid.

[9] Brian McWilliams and Clint Boulton, "Another E-Commerce Site Suffers Hack Attack," internetnews.com, March 2, 2000, URL: http://www.internetnews.com/ec-news/article/0,,4_314341,00.html

[10] Rob Spiegel, "Security Leaks Found at Dozens of E-Commerce Sites," *E-Commerce Times*, January 17, 2000 URL: http://www.ecommercetimes.com/perl/story/?id=2227

numbers. Key-finding attacks where cryptographic private keys are compromised are also a looming threat, though quite often this is perpetrated by insiders.[11] Thus exploitable holes are numerous for the conniving intruder, and it will take a stronger drive in the e-commerce industry to reduce the threats to financial necessities of business, while keeping pace with the vulnerabilities introduced by new applications and technologies.

Where is E-Commerce Security Heading?

Much as there are winners and losers in e-commerce when it comes to the bottom-line results, there will continue to be those who operate a tight ship fending off the sophisticated and random attacks and also those who fall victim from their lack of planning and implementation of defenses. Access to wealth electronically will continue to expand at a frantic pace in electronic transactions over wires and through the air and the applications that store and process the digital codification of information. It is therefore in the interests of the enablers of these payments to educate their customers to set priorities and methodologies for practicing the best techniques for electronic security.

Recently the Worldwide E-Commerce Fraud Prevention Network was formed by American Express and e-tailers such as Amazon.com and Buy.com to establish common grounds for reducing the threats created by increasing reliance on the Internet for commerce. Membership has expanded swiftly to now include 375 large and small players united to promote the growth of e-commerce in large part by keeping fraud to a minimum. Some of the recommended strategies for merchants advocated by this group include: obtaining real-time information from a credit card company, use of address verification systems, use of credit card verification codes, purchase of rule-based detection systems, and purchase of predictive statistical models.[12]

Visa has stepped up a campaign to establish high standards of security for its merchants and cardholders. This was launched in June 2000 as the Global Secure E-Commerce Initiative. Visa has been actively pursuing the production of smart cards which have a logical chip component to provide enhanced authentication for electronic transactions. Visa uses third-party security assessments to build its own evaluation and weigh these against benchmarks of competitors to develop compliance standards. Visa has also recently launched Global Security Web to serve as an information resource for merchants. This site includes a program for a security self-assessment to help merchants find out what the weak and strong points in preventing unauthorized access to their information.[13] This is a component that will include seminars and training for merchants to establish compliance in the standards that Visa establishes. By organizing a formal set

[11] Matthew W. Beale, "Security Firm Warns of New E-Commerce Threat," *E-Commerce Times,* January 7, 2000, URL: http://www.ecommercetimes.com/perl/story/?id=2244

[12] Mark Merkow, "Worldwide E-Commerce Fraud Prevention Network Launches," Ecommerce-Guide.com, January 26, 2001,
URL: http://ecommerce.internet.com/outlook/article/0,,7761_572111,00.html

[13] James Christiansen, "Visa/Secure, Everywhere You Want to Be," *Information Security,* November 2000, URL: http://www.infosecuritymag.com/articles/november00/coverb.shtml

of rules for compliance, Visa is raising the bar to a level that will benefit all parties in the electronic transaction process.

Great success is possible for those businesses which implement e-commerce. However, throughout this paper I have tried to expose the warning signs for these e-commerce entities from being a few nodes away from the professional or amateur intruder. Just as there are legitimate opportunists who play fair, there are opportunists in the criminal element hoping to seek small fortune or destroy someone else's dream. The scary part is that at the speed of light an e-commerce star can go from the accolades on the cover of the financial press to an irrecoverable death spiral. My hope is that a greater awareness of this problem will further the security culture necessary in the innovative ideas that are being brought to market now and in the future on the great information superhighway.

Bibliography

"E-Commerce Growth Predicted for North America," *CyberAtlas*, August 8, 2000, URL: http://cyberatlas.internet.com/markets/retailing/article/0,,6061_408451,00.html

"New Report Reveals: Global B2B eCommerce to Reach $2.7 Trillion by 2004,"ebizChronicle.com February 1, 2001, URL: http://www.ebizchronicle.com/backgrounders01/feb/eCommerce_b2b.pdf

Michael Mahoney, "Report: IT Security Spending Missing Mark," *E-Commerce Times*, October 30, 2000, URL: http://www.ecommercetimes.com/perl/story/?id=4677

Andy Briney, "Security Focused," *Information Security*, September 2000, URL: http://www.infosecuritymag.com/articles/september00/pdfs/Survey1_9.00.pdf

Jay Lyman, "Teenage Hacker Mafiaboy Pleads Guilty," January 19, 2001, URL: http://www.newsfactor.com/perl/story/?id=6836

Paul A. Greenberg, "In E-Commerce We Trust…Not," *E-Commerce Times*, February 2, 2001, URL: http://www.ecommercetimes.com/perl/story/?id=7194

Brian McWilliams and Clint Boulton, "Another E-Commerce Site Suffers Hack Attack," internetnews.com, March 2, 2000, URL: http://www.internetnews.com/ec-news/article/0,,4_314341,00.html

Rob Spiegel, "Security Leaks Found at Dozens of E-Commerce Sites," *E-Commerce Times*, January 17, 2000 URL: http://www.ecommercetimes.com/perl/story/?id=2227

Matthew W. Beale, "Security Firm Warns of New E-Commerce Threat," *E-Commerce Times*, January 7, 2000, URL: http://www.ecommercetimes.com/perl/story/?id=2244

Mark Merkow, "Worldwide E-Commerce Fraud Prevention Network Launches," Ecommerce-Guide.com, January 26, 2001, URL: http://ecommerce.internet.com/outlook/article/0,,7761_572111,00.html

James Christiansen, "Visa/Secure, Everywhere You Want to Be," *Information Security*, November 2000, URL: http://www.infosecuritymag.com/articles/november00/coverb.shtml

Last Updated: October 2nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Seattle 2013	Seattle, WAUS	Oct 07, 2013 - Oct 14, 2013	Live Event
SANS Baltimore 2013	Baltimore, MDUS	Oct 14, 2013 - Oct 19, 2013	Live Event
SEC760 Advanced Exploit Development for Penetration Testers	Baltimore, MDUS	Oct 14, 2013 - Oct 19, 2013	Live Event
SANS Bangalore 2013	Bangalore, IN	Oct 14, 2013 - Oct 26, 2013	Live Event
GridSecCon 2013	Jacksonville, FLUS	Oct 15, 2013 - Oct 17, 2013	Live Event
Healthcare Cyber Security Summit	San Francisco, CAUS	Oct 17, 2013 - Oct 24, 2013	Live Event
Securing the Internet of Things Summit	San Francisco, CAUS	Oct 17, 2013 - Oct 22, 2013	Live Event
SANS Tokyo Autumn 2013	Tokyo, JP	Oct 21, 2013 - Oct 26, 2013	Live Event
ICS410	Sterling, VAUS	Oct 21, 2013 - Oct 25, 2013	Live Event
October Singapore 2013	Singapore, SG	Oct 21, 2013 - Nov 02, 2013	Live Event
SANS Dubai 2013	Dubai, AE	Oct 26, 2013 - Nov 07, 2013	Live Event
FOR572 Advanced Network Forensics and Analysis	Washington, DCUS	Oct 28, 2013 - Nov 02, 2013	Live Event
SANS Chicago 2013	Chicago, ILUS	Oct 28, 2013 - Nov 02, 2013	Live Event
MGT415 at (ISC)2 SecureSoCal 2013	Manhattan Beach, CAUS	Oct 31, 2013 - Oct 31, 2013	Live Event
SANS South Florida 2013	Fort Lauderdale, FLUS	Nov 04, 2013 - Nov 09, 2013	Live Event
SANS DHS Continuous Diagnostics & Mitigation Award (CDM) Workshop	Washington, DCUS	Nov 06, 2013 - Nov 06, 2013	Live Event
MGT415 at (ISC)2 SecureDallas 2013	Dallas, TXUS	Nov 06, 2013 - Nov 06, 2013	Live Event
SANS Pen Test Hackfest Training Event and Summit	Washington, DCUS	Nov 07, 2013 - Nov 14, 2013	Live Event
SANS Sydney 2013	Sydney, AU	Nov 11, 2013 - Nov 23, 2013	Live Event
SANS Korea 2013	Seoul, KR	Nov 11, 2013 - Nov 23, 2013	Live Event
Cloud Security @ CLOUD Expo Asia	Singapore, SG	Nov 13, 2013 - Nov 15, 2013	Live Event
SANS London 2013	London, GB	Nov 16, 2013 - Nov 25, 2013	Live Event
SANS San Diego 2013	San Diego, CAUS	Nov 18, 2013 - Nov 23, 2013	Live Event
FOR585 Adv Mobile Device Forensics	Vienna, VAUS	Nov 18, 2013 - Nov 23, 2013	Live Event
Asia Pacific ICS Security Summit & Training	Singapore, SG	Dec 02, 2013 - Dec 08, 2013	Live Event
SANS San Antonio 2013	San Antonio, TXUS	Dec 03, 2013 - Dec 08, 2013	Live Event
SANS Cyber Defense Initiative 2013	Washington, DCUS	Dec 12, 2013 - Dec 19, 2013	Live Event
SANS Oman 2013	Muscat, OM	Dec 14, 2013 - Dec 19, 2013	Live Event
SANS Golden Gate 2013	San Francisco, CAUS	Dec 16, 2013 - Dec 21, 2013	Live Event
SANS Forensics Prague 2013	OnlineCZ	Oct 06, 2013 - Oct 13, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced