Chorzowskie Studia Polityczne
Nr 8 rok 2014

Teresa Pereira

Polytechnic Institute of Viana do Castelo
School of Business Science
Valença, Portugal
e-mail: tpereira@esce.ipvc.pt
tel. +351 258 809 679

Henrique Santos

Universityof Minho
Guimarães, Portugal
e-mail: hsantos@dsi.uminho.pt
tel. +351 253 510 319

A Framework to Mitigate Security Risks in Online Transactions

Summary. The growth of the Internet-based services and applications has caused unprecedented changes in our lives, in economies, in social relations, and technological systems. These evolvements promote new business opportunities, but also bring severe security risks. Attackers are constantly seeking vulnerable systems to compromise, disable, or deface. The speed with which attackers adopt the latest exploit techniques, means that companies should adopt adequate security practises on a regular basis, in order to enable organizations in maintaining a secure posture. This paper considers the issue of online transaction security and the implications for the parties involved. It begins by highlighting a variety of vulnerabilities commonly exploited in online systems, delivering actionable information for the implementation of good practises in security, in order to mitigate or reduce the impact of a security incident.

Key words: security, information security, information security management, online transaction; online operations

Introduction

The popularity of online shopping is growing exponentially. Innovations such as the Internet and mobile businesses have promoted productivity, created new opportunities, and enhanced access to information. Companies use the Web to promote their products and services, while consumers are demanding new and innovative products, as well as, faster and more efficient communication systems. This increases the opportunity for online fraud and stolen sensitive data.

Almost every day, there are notices on the news about data breaches experienced by well-known companies. An example of this was reported in the news recently, about the attacks performed to the iCloud, where private photos from celebrities were accessed and published. Another example would be the alleged Russian attack to Wall Street businesses noticed last August, in retaliation for US sanctions imposed on Ukraine. The Russian hackers allegedly stole large amounts of sensitive data from JP Morgan Chase[1]. In fact, a cyber attack may cause critical impacts and is much less expensive than a military offensive. The Edward Snowden disclosures and new forms of espionage created geopolitical tensions that may have far reaching implications in years to come. These events have painfully emphasized that the online sphere is an enabling environment to exploit, and organizations need to be prepared and equipped to deal with global security risks.

In this article, some information regarding the vulnerabilities commonly exploited in online systems is highlighted, and based on identified vulnerabilities and their security risks, the article delivers actionable information for the implementation of good security practices, in order to mitigate online fraud. This paper is divided into sections; section 2 introduces the current models of online transactions; section 3 presents an overview of the commercial activities most affected by online fraud; in section 4 an overview of security risks is presented; and section 5 introduces some considerations regarding good security practices to adopt in order to mitigate online fraud. Finally, conclusions are drawn in section 6.

1. An Overview of Online Transaction Models

The widespread adoption of information and communication technology has promoted the appearance of new models of online commerce, namely B2B (Business-to-Business), B2C (Business-to-Consumer), and C2C (Consumer-to--Consumer). B2B applies to transactions between manufacturers and suppliers or distributors. This commerce model has been widely used between organizations to perform orders and delivering the goods or services. The increasing use of the Web and innovative products, with high levels of quality required by the customers, contributes to the evolvement of the B2C commerce model with retail selling their products/services exclusively on-line. In fact, it is in this commerce model that a higher volume of transactions occurs. Findings published by

[1] P. Sherwell, *FBI investigates alleged Russian cyber attack on Wall Street*, "The Telegraph", 27 August 2014, http://www.telegraph.co.uk/news/worldnews/northamerica/usa/11060338/FBI-investigates-alleged-Russian-cyber-attack-on-Wall-Street.html [18.09.2014].

Forrester Research and other analysts indicated that online sales have experienced double-digit growth rates over the past decade. The business-to-consumer (B2C) online sales worldwide exceeded $1 trillion for the first time in 2012. They are predicting a continued growth in 2014, forecasting U.S. e-commerce spending of nearly $250 billion for the current year. In the U.S. alone, Forrester predicts that online sales will account for 10% of retail sales by 2017[2]. However, the US is by no means alone here, and the signs point toward continued growth in other regions as well[3].

In the beginning, B2C transactions started with companies selling on-line products such as music, software applications et cetera, but soon the banks and brokerage services enabled their clients to retrieve bank statements online, transfer funds, pay credit card bills, apply for and receive approval for a new mortgage, buy and sell securities, and get financial guidance and information. Currently, almost all retail brands have an online presence, which allows their customers to search for products that they can purchase later in the physical store. Recently, there has been a trend towards multi-channel retail, allowing for new models such as purchasing online and picking up in the store. In fact, this is a mechanism adopted by stores to promote confidence in the online services they provide, since one fear of the customers is to not receiving the expected product they actually bought.

Lastly, the C2C model applies to transactions performed between individuals, and involves forms of cash commerce generally used for low-cost services or goods[4]. A classic example of this commerce model is eBay, with individuals typically trading low-cost items using its on-line auctions. The value of eBay lies in its ability to connect millions of sellers with millions of possible buyers worldwide. More recently, there has been a growing interest in the potential of social networking sites, such as Facebook, for having commercial activity.

Many benefits have been claimed from the adoption of online transactions, generally related to improving network activities and/or relationships, such as[5]:

1. Reduced costs; when sales and after-sales service operations replace paper-based communications with electronic communication, it makes their processes more efficient.
2. Enabling a company to manage its inventory better, in addition to being able to capture and process orders more quickly.

---

[2] S. Mulpuru, C. Johnson, D. Roberge, *US Cross-Channel Retail Forecast, 2012 To 2017*, "Forrester. For ebusiness & Channel Strategy Professionals", 29 October 2013, https://www.forrester.com/US+CrossChannel+Retail+Forecast+2012+To+2017/fulltext/-/E-RES105461 [15.07.2014].

[3] Ibidem.

[4] P. Beynon-Davies, *Business Information Systems*, 1st edition, Palgrave Macmillan, UK 2009, pp. 227-246.

[5] Ibidem.

3. Closer integration of suppliers and consumers, enabling just-in-time manufacturing.
4. Innovative ways of marketing new products and services, leading to a general improvement in customer relations. This might allow companies that traditionally traded on a local scale to do business on a global scale.

Additionally, there are also a number of limitations associated with online transactions, such as[6]:

1. Technology developing fast in support of electronic trade and sometimes not being particularly secure or not easily integrated with technologies in other areas.
2. It being difficult to find particular suppliers of goods and services on the Internet.
3. Security issues; this is considered the primarily problem related to online transactions. Many people still do not trust electronic transactions enough to use the Web to buy high-value goods or services. Users are still reluctant to release personal information over the Internet. The first reason is related to information security, while the second is an issue of information privacy.

It is recognized that issues related to information security and information privacy are the main constraints in online transactions. Thereby, it is noticed that when online security is discussed, the privacy and anonymity concepts are frequently misunderstood. Privacy is the protection of information about oneself from others without one's knowledge or consent, in order to allow the selection of which aspects should have protection (e.g. defence against unauthorized disclosure of information about an individual). In fact, privacy is granted by law (even if with different assumptions in different countries). Anonymity is being able to communicate without revealing an identity. Another way to look at these two terms is[7]:

1. With privacy, others cannot see what you are doing or what you are communicating, but they can know who you are.
2. With anonymity, others can see what you are doing or what are you communicating, but they do not know who you are.

Often, one or the other is assumed to be assured by a solution when, in fact, it is protecting one of these and not the other. Usually consumers want both privacy and anonymity. Unfortunately, they typically have neither concerning online activities[8].

This highlights the importance of being aware of the concepts related to security, and then following adequate security guidelines and good practices in

[6] Ibidem.

[7] J.M. Stewart, *White Paper: How To Secure Online Activities*, Global Knowledge Training LIC, 2013, www.globalknowledge.nl/Knowledge-Centre/white-papers/security-white-papers/WP--How-To-Secure-Online-Activities [10.07.2014].

[8] Ibidem.

order to have a more secure behaviour. In the following section, an overview of the most common vulnerabilities in online transactions will be presented. It starts with an introduction of the concept of vulnerability, since an attack may occur through the exploitation of such vulnerabilities. Thus it is very important to know the most common vulnerabilities and then follow adequate, good security practices.

2. Common Security Vulnerabilities in Online Transactions

According to the international security standard ISO/IEC JTC1[9] a vulnerability represents any weakness of the system[10]. It is a flaw in an organizational asset that may be exploited by an attacker and result in a security incident[11]. The vulnerabilities all have a different nature. They are present in user practices, flaws in the technology, or even in the online platform or system. As illustrated in Figure 1, most of the web application developers are often not very well aware about secure programming practices. As a result, the security of an application is not necessarily one of the design goals. This is aggravated when developers are forced to meet deadlines in the fast-moving online sphere. In practice, a one day delay in publishing a brand new feature on its website could allow a competitor to gain an advantage. The online environment is under countless fast changes, and businesses need to stay ahead of the competition. In such scenario, the goal is to get the functionality online, disregarding security issues to a later phase. Another reason for the appearance of security vulnerabilities is due to the inherent complexity in most online systems. Nowadays, users are demanding diverse requirements of their online providers, and this requires complex design and programming logic. Other vulnerabilities are linked to users. In 2013, Symantec published a report (2013 Internet Security Threat), which states that one of the exposed security breaches among other things, occur from users inside of the organizations[12]. Take for instance, in the case of a well-meaning employee simply willing to work from home by sending a spreadsheet through a third-party web-based email, a cloud service, or by simply copying the files to a USB drive.

---

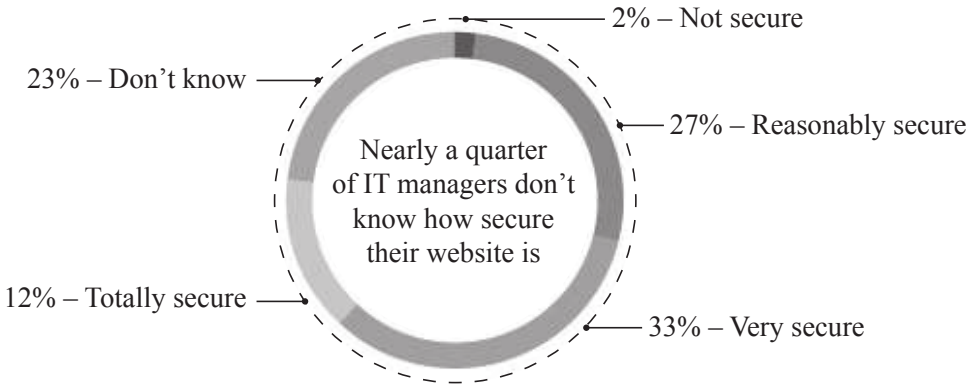
[9] International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), Joint Technical Committee (JTC1).

[10] ISO/IEC FDIS 27001 Information technology – Security techniques – Information security management systems – Requirements, ISO copyright office, Geneva, Switzerland 2005.

[11] T. Pereira, "Conceptual Framework to Support Information Security Risk Management", Ph.D thesis, University of Minho 2012.

[12] *Vulnerability Assessment 2013*, "Symantec. Website Security solutions", 2013, https://www.cherryorange.co.uk/Media/Default/PDF/Symantec_Feeling_Vulnerable_UK.pdf [18.09.2014].

Figure 1. Symantec Threat Report



Source: *Vulnerability Assessment 2013*, "Symantec. Website Security solutions", 2013, https://www.cherryorange.co.uk/Media/Default/PDF/Symantec_Feeling_Vulnerable_UK.pdf [18.09.2014].

Moreover, findings published by Symantec Research show that organizations' confidence in their websites is higher among those who perform vulnerabilities assessments every month. In general, larger companies are more aware of the risks and more likely to conduct and regularly repeat vulnerability assessments. However, according to Symantec's 2013 Website Security Threat Report[13], it is a mistake to assume that only large companies are targeted by attacks. The report shows a significant number of smaller companies (31%) that are being pursued. Larger companies will naturally gravitate towards more in-depth assessments, but smaller companies also clearly need to get a better picture of not only what their overall exposure is, but also, what specific risks they may face[14].

In the following section, a list of the top commercial categories traded online will be presented, indicating the categories affected by fraud.

3. Top Commercial Categories Affected by Fraud

The RSA anti-fraud command center provides a report with a list of the commercial activities widely traded on-line and affected by fraud. The following list is the top ten commercial activities sought for electronic transactions[15]:

– Airlines,
– General Retail,

[13] *Website Security Threat Report 2013*, "Symantec. Website Security solutions", 2013, https://www.symantec-wss.com/campaigns/14385/uk2/social/assets/symantec-WSTR1-UK.pdf [18.09.2014].

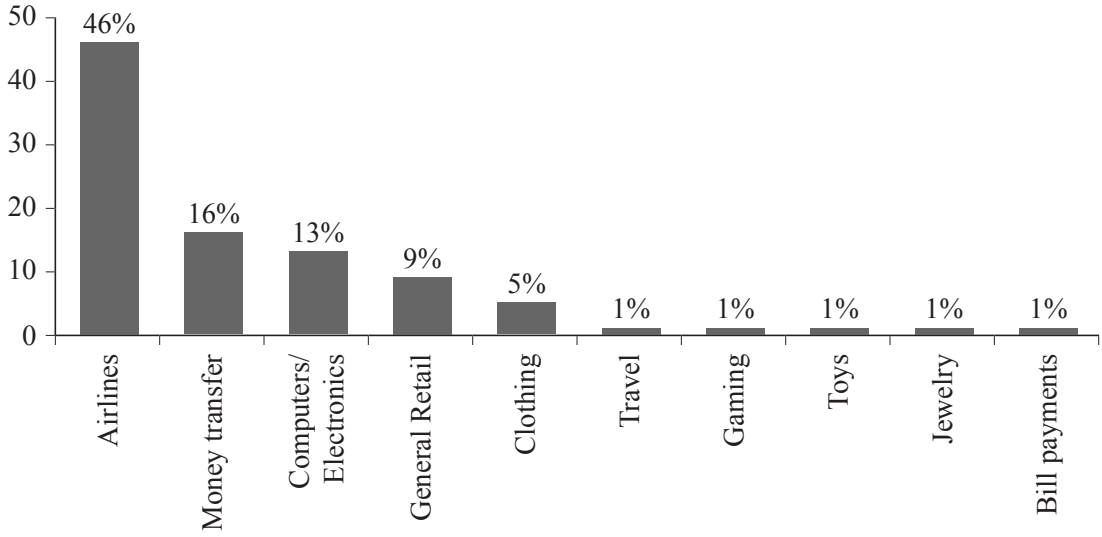
[14] *Vulnerability Assessment 2013*, op. cit.

[15] *E-commerce Fraud Trends 2014: Securing the Online Shopping Cart*, RSA-online-fraud, "EMC.com", July 2014, https://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-0714.pdf [18.09.2014].

– Computers/Electronics,
– Ticketing,
– Telecommunications,
– Money transfer,
– Automotive,
– Toys,
– Clothing,
– Restaurants and dinning.

These commercial activities are the most sought on the Web and, unsurprisingly, the subjects of fraud most often. Figure 2 illustrates that reality.

Figure 2. Top commercial categories affected by fraud



Source: *E-commerce Fraud Trends 2014: Securing the Online Shopping Cart*, RSA-online-fraud, "EMC.com", July 2014, https://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-0714.pdf [18.09.2014].

According to the Discover Financial Services Pulse ATM Network, in 2013 one out of every seven payments by card were exposed by a data breach. A security breach can result in the loss of intellectual property, a theft of identity, the loss of confidentiality, the disruption of critical operations, as well as, damage to an organization's image, brand, and public reputation[16]. Rapid changes are taking place and will certainly modify the liability rules concerning card purchases for both issuers and commercial entities. This is going to be conducive to rapid changes in the card payment landscape, so financial institutions and retailers must be prepared to make investments in technology to manage fraud and risk in online transactions.

[16] *Managing security risks and vulnerabilities*, IBM Corporation, "IBM Software Thought Leadership White Paper", January 2014.

3.1. Some Values of Fraud in Online Transactions

A growing proliferation of Web attacks drove a 93% increase from 2009 to 2010. The trend is ongoing escalation. In fact, the RSA anti-fraud command center identified 55.8 phishing attacks in June of 2014, marking an impressive 43% increase from May – this in just one month. Based on this information, the RSA estimated phishing costs for global organizations as $476 million in losses, for the month of June[17]. In general, organizations do not inform that they were victim of a security incident, as it will affect their reputation and compromise their customer's confidence. In June, the most targeted country was the United States with 57% of phishing volume, followed by the Netherlands, the United Kingdom, Malaysia and South Africa[18].

4. Security Risks

An organization has a security risk condition when there is a possibility of a vulnerability to be exploited and/or threats that can compromise the normal functioning of an organizational asset/resource. When there is a possibility of the vulnerability being exploited, the impact can be the loss of confidentiality, integrity, or availability of computer services[19]. According to the security standard ISO/IEC 27000 a threat can be a potential cause of an unwanted incident, which may result in harm to a system or organization. Generally, a risk may have its source in nature, like power surges, floods, fires, hurricanes, and others, or it may even be of man-made origin. The man-made risk can be both intentional and performed by hackers, thieves, and spammers, and/or unintentional, such as coding mistakes, mistyping, and loss of data storage media[20]. In online transactions one of the main security risks is linked to the authentication control; once in the online context, the operations are performed without knowing the stakeholders. Those who buy do not know who sells, and this fact contributes to a main constraint on online transactions. Usually, consumers are suspicious about sellers, whom they do not know or do not have human contact with. Additionally, the security issues related to online payments and identity frauds are also limitations to online businesses. Consumers are often hesitant to share their credit card details online. On the other hand, sellers are also vulnerable to several attacks and other forms of security fraud. This scenario is aggravated by a constant change in the environment (conditions, opportunity, and motivation to perform attacks) and a technological advancement that allows exploits to become available at an increasing ratio.

---

[17] *E-commerce Fraud Trends 2014...*

[18] Ibidem.

[19] T. Pereira, op. cit.

[20] Ibidem.

In this context, information security risk management should be an integral part of information security management activities, and it should be applied in the implementation and continuous improvement of an Information Security Management System (ISMS)[21]. This fact is especially important when the organization strongly depends on IT-based systems to remain viable. These decisions are based on the balance between the costs of applying information system controls and the benefits realized from the operation of secured systems. Moreover, the benefits should be viewed not only in the context of the activity itself, but in relation to many and varied stakeholders who can be affected. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization.

To address the security risk management process, the execution of the following actions is required[22]:

1. Identify assets and estimate their value. In the context of online transactions, assets include: clients, image and reputation of the company, software applications, online infrastructure, and digital data. In general, everything that has value for the organization to develop their online activity.
2. Conduct a threat assessment. This includes: malicious acts originating from inside or outside the organization; messaging and email threats like malicious links and attachments;
3. Conduct a vulnerability assessment. Cloud computing, Bring Your Own Device (BYOD), and other trends bringing new vulnerabilities. One example is the latest attack performed on private photos of celebrities stored in the iCloud (Apple).
4. Calculate the impact that each threat would have on assets. An impact might be a loss of availability, integrity, and confidentiality, and result in possible losses (lost income, loss of real property, a penalty imposed by regulation, damage of image and reputation, et cetera). For example, assess the impact when an online site is unavailable, or even worse, when shopper's personal and financial data have been compromised.
5. Identify, select, and implement the appropriate controls. Productivity, cost effectiveness, and asset value should be considered when a control is selected to be implemented.
6. Evaluate the effectiveness of the control implemented. Ensure the controls provide the required cost effective protection without perceptible loss of productivity – principles of efficiency and efficacy[23].

---

[21] ISO/IEC_JTC1, 2008. ISO/IEC FDIS 27005 Information Technology – Security Techniques – Information Security Risk Management. ISO copyright office, Geneva, Switzerland.

[22] K.K. Mookhey, *Common Security Vulnerabilities in e-commerce Systems*, 2014, www.symantec.com/connect/articles/common-security-vulnerabilities-e-commerce-systems [17.04. 2014].

[23] Ch.P. Pfleeger, S.L. Pfleeger, *Security in Computing*, Prentice Hall PTR 2002.

The information collected about identified risks can be valuable to manage security and may help to reduce or mitigate potential harm. Manager and staff awareness of the risks and knowledge about the nature of controls used to mitigate the risks can assist the organizations in how to deal with security incidents and unexpected events in the most effective manner. The choice of the controls should be based on a risk analysis process.

The following section makes an approach to some security controls that might be used in the scope of online transactions.

5. Good Practises to Mitigate Online Frauds

Security is not a singular concept, solution, or state, it is rather a combination of numerous aspects, implementations, and perspectives. Security is usually a relative term with graded levels, rather than an end state that can be successfully achieved[24]. In fact, there is no such thing as "100 percent safe". A system is not secure; it is always in a state of being secured.

In the scope of online activities, confidentiality is an issue that concerns consumers when they have to provide unknown vendors with personal, sometimes sensitive, information. Moreover, the medium of the Internet is a broadcast network; whatever is placed on it is routed over wide-ranging and essentially uncontrolled paths. Additionally, there is concern about the integrity of information for much the same reason. On the other hand, vendors are particularly focused on availability. If their online infrastructures are not operating, they cannot do business and lose on potential revenues. In addition to the CIA, some further issues are increasingly required in dealing with online transactions: authentication, accountability, and non-repudiation. These three are closely linked. Individuals using online applications must be identified and in some manner must prove that they are who they say they are before the transaction is entered into, or at least, before it is completed. Then, there must be some manner of ensuring that the individuals cannot deny that the transaction had been entered into, or at least that they had performed the transaction, as it is supposed to happen.

In this context, several organizations came up with recommendations, models, or even standards, including controls, tools, mechanisms, and supervision necessary to respond to the challenge. One example is the following set of defence vectors[25]:

– strong authentication of all parties to the application or communication,

[24] J.M. Stewart, op. cit.

[25] *e-Commerce Security: Enterprise Best Practices*, 2014, ISACA – Information Systems Audit and Control Association, https://www.isaca.org/bookstore/extras/Pages/e-Commerce-Security-Enterprise-Best-Practices-Introduction.aspx [15.07.2014].

- protect the online traffic from modification, destruction, interference, or contamination,
- protect the online traffic from inappropriate or unnecessary disclosure,
- ensure that the business can continue to operate in the case of technology failures,
- recognize variances from the intended use, operation, or behaviour of systems and take timely and effective corrective action.

In order to ensure the previous requirements, vendors can consider the following good practices on data security when building their websites[26]:

1. Creation of a page with information on an organization's security practices and controls. In particular, it should inform consumers how their card account information is protected within the organizational website's server.
2. Ensure the organization is PCI (Payment Card Industry) compliant. Being PCI compliant means that a set of security standards were developed to protect card information during and after a financial transaction. A secure connection through the SSL (Secure Sockets Layer) or the integration of a stronger EV SSL (Extended Validation Secure Sockets Layer). The use of these certificates enables authentication of the identity of the business company and encrypts the data in transit.
3. Sensitive data should not be stored. In fact, there is no reason to store thousands of records of all customers, especially credit card numbers, expiration dates, and CVV (card verification value) codes. This is strictly forbidden by the PCI standard. In practice, the risk of a security breach outweighs the convenience for the customers at checkout. The main idea is if the company does not have information to steal, then it will not be stolen.
4. Employ an address and card verification system. This will enable an address verification system (AVS) and require the card verification value (CVV) for credit card transactions in order to reduce fraudulent charges.
5. Require strong passwords. It is the responsibility of the retailer to keep customer information safe on the back-end. However, requiring a minimum number of characters and the use of symbols or numbers will certainly help customers to protect themselves. Longer, more complex logins will make it harder for criminals to breach the online site.
6. Set up system alerts for suspicious activity. It is advisable to set an alert notice for multiple and suspicious transactions coming from the same IP address. Similarly, it is also prudent to set up system alerts for multiple orders placed by the same person using different credit cards, phone numbers that are from markedly different areas than the billing address, and orders where the recipient name is different from the card holder name.

[26] J.L. Schiff, *15 Ways to Protect Your Ecommerce Site From Hacking and Fraud*, 2013, www.cio.com/article/2384809/e-commerce/15-ways-to-protect-your-ecommerce-site-from-hacking-and-fraud.html [15.07.2014].

7. Provide security training to employees. Employees need to know they should never email or text sensitive data or reveal private customer information in chat sessions, since none of these communication methods is secure. Employees also need to be trained on the laws and policies that affect customer data and be trained on the actions required to keep it safe. Finally, the use of strict written protocols and policies to reinforce and encourage employees to adhere to mandated security practices should be implemented.
8. Monitor the website on a continual basis. It is recommended to have a real--time analytics tool. In the real world, it is equivalent to the installation of security cameras in the online shop. Tools like Woopra[27] or Clicky[28] allow to observe how visitors are navigating and interacting with the website in real time, allowing to detect fraudulent or suspicious behaviour. When any suspicious activity is detected, it enables acting more quickly and prevents suspicious behaviour from causing harm. It is also important to regularly monitor the organization servers for malware, viruses, and other harmful software.
9. Patch the systems. When a new release is available it is very important to patch everything immediately. Usually, this includes the Web server, as well as, other third-party codes like Java, Python, and Perl, which are favourite targets for attackers. Outdated sites are constantly found running with more than a three-year-old version. It is critical to install patches on all software. For example, Web applications widely used in the implementation of online transaction applications, such as Xcart, OSCommerce, ZenCart, Joomla, and many others, all need to be patched regularly.
10. Ensure DOS (Denial of Service) and DDOS (Distributed Denial of Service) protection and mitigation service. DOS and DDOS attacks are increasing in frequency, sophistication, and the range of targets, in particular, on online platforms. A Denial of Service attack impacts the availability of a service. It involves getting the server to perform a large number of tasks, exceeding the server's capacity to handle any other task.
11. Implement a proper data back up, and a disaster recovery plan. A recent study by Carbonite revealed that businesses have big gaps in their data backup plans, putting them at risk for losing valuable information in the instance of a power outage, hard drive failure, or even a virus[29]. Therefore, to make sure the site is properly protected, it is essential to back it up regularly, or make sure the hosting service is doing so.

---

[27] https://www.woopra.com

[28] http://clicky.com

[29] E. Delaney, *New Study From Carbonite Finds Big Gaps in Small Businesses' Backup Plans*, "Carbonite", 13 March 2012, http://investor.carbonite.com/releasedetail.cfm?ReleaseID=656831 [22.08.2014].

12. Creation of a "Frequently Asked Questions" (FAQ) page that provides detailed information on how consumers can protect themselves when shopping online. It is important to be specific in the suggestions and do not assume that some information is too obvious to warrant mentioning. For example, tell visitors how to identify whether or not a checkout page is SSL-secured or not, what it means, and why it is important. A system is only as secure as the people who use it.
13. Awareness regarding the use of emails to share private information. The costumer should be advised against using emails for communicating transaction information or any other sensitive data. Some customers may wrongly believe that email is a secure way for transmitting personal account information, when this is actually a non-secure way of doing business. In order to protect consumers, an organization should highlight its best practices for data security on their website and in all email replies. In particular, the consumers should be informed that email is a non-secure way for transmitting information and should never be used to transmit card account numbers or other sensitive information. Additionally, the customers should be informed that the online website incorporates information encryption capabilities that offer reliable protection from unauthorized access and provides cardholders with the safest way to shop online.

Implementing as many of the above recommendations as possible will promote organization security, make it harder for someone to exploit it, and inspire trust and confidence in customers.

On the customer side, there are a set of good practises to follow in order to reduce or mitigate fraud. Some of them are described as follows:

1. Never automatically save access credentials. In general, online stores demand to create an account with a login and password. Clients should never save this data on their computer.
2. Strong Passwords. A strong password must be used for shopping and for email address that the shop is connected to. The same password for a shop, an email address, or any other online matters must not be used.
3. Individuals should never respond to emails that request personal financial information. This request is usually the result of a phishing attack, whos aim is to steal access credentials.
4. Banks or online companies generally personalize emails, as they know the user. In a phishing attack, the attacker does not know the victim and often includes false but sensational messages, such as "urgent – your account details may have been stolen", in order to get an immediate reaction. Reputable companies do not ask their customers for passwords or account details in an email. Even if the email seems legitimate, users should not respond. The best practice is to contact the company by phone or by visiting their website.

5. Special caution must be taken in opening attachments and downloading files from emails, no matter whom they are from.
6. It is very important to check the web address bar. If the website is on a secure server it should start with https:// rather than the usual http://.
7. It is mandatory to keep the computer secure. Some emails or other spam may contain software that can record information on Internet activities (spyware) or open a 'backdoor' to allow hackers access to the users personnel computer (Trojans). Installing anti-virus software and keeping it updated will help detect and disable malicious software, while using anti-spam software will, for example, block phishing emails. It is also important, particularly for users with a broadband connection, to install a firewall. This will help them to keep the information on their computer secure while blocking communication from unwanted sources. It is important to maintain updated and download the latest security patches of the used browser. If patches are not installed, the user should visit the browser's website.

These are by no means the only steps the users should take to make their online transactions more secure. However, they do offer a baseline to help users reduce the risk of fraud. It is also very important to be alert of any changes that might happen in the online company services and always be suspicious about those changes.

The above-mentioned good practices should enable managers of online companies to gain a better awareness of competitive benchmarks that are driving current online activities. Moreover, consumers should be aware of the security risks in online transactions and have adequate behaviour in order to not suffer a fraud incident or at least minimize the impact when a security incident occurs.

Conclusions

The growth of popularity of online transactions has brought new and, most of the time, underestimated security risks. This demands better awareness about security issues by managers and businesses in order to ensure the confidentiality, integrity, and availability of information. In the online sphere, the asset exchange is information and therefore, companies should conduct their businesses adequately to ensure the CIA properties of information. There are countless methods that attackers and cybercriminals use to compromise the integrity, availability, and confidentiality of information or services. Many attacks rely on common flaws in computer software that create weaknesses in the overall security of computer networks. Others exploit vulnerabilities created by improper computer or security configurations, or users' illiteracy.

In this paper the main threats that can compromise the operability of online applications were presented and based on the identified threats, good practises were described to guide vendors when building their web applications, and to guide consumers that use these applications as well, in order to mitigate frauds and reduce the impact when a security incident occurs.

We realize that new services and application functionalities are emerging everyday to respond to globalized competition, since consumption on the web is growing, as well as, consumer demand for new and innovative products and services. This brings new vulnerabilities that inevitably will be exploited by sophisticated attackers.

The identified good practices should enable managers of online companies to gain a better awareness of competitive benchmarks that are driving current online activities and to take steps to affect improvements in client trust and confidence in the services provided. Finally, consumers should be aware of the security risks in online transactions and have adequate behaviour in order not to suffer a fraud incident, or at least minimize the impact when a security incident occurs.

References

Beynon-Davies P., *Business Information Systems*, 1st edition, Palgrave Macmillan, UK 2009.

Delaney E., *New Study From Carbonite Finds Big Gaps in Small Businesses' Backup Plans*, "Carbonite", 13 March 2012, http://investor.carbonite.com/releasedetail.cfm?ReleaseID=656831 [22.08.2014].

E-commerce Fraud Trends 2014: Securing the Online Shopping Cart, RSA-online-fraud, "EMC.com", July 2014, https://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-0714.pdf [18.09.2014].

e-Commerce Security: Enterprise Best Practices, 2014, ISACA – Information Systems Audit and Control Association, https://www.isaca.org/bookstore/extras/Pages/e-Commerce-Security-Enterprise-Best-Practices-Introduction.aspx [15.07.2014].

ISO/IEC FDIS 27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary, ISO copyright office, Geneva, Switzerland 2009.

ISO/IEC FDIS 27001 Information technology – Security techniques – Information security management systems – Requirements, ISO copyright office, Geneva, Switzerland 2005.

ISO/IEC_JTC1, 2008. ISO/IEC FDIS 27005 Information Technology – Security Techniques – Information Security Risk Management. ISO copyright office, Geneva, Switzerland.

Managing security risks and vulnerabilities, IBM Corporation, "IBM Software Thought Leadership White Paper", January 2014.

Mookhey K.K., *Common Security Vulnerabilities in e-commerce Systems*, 2014, www.symantec.com/connect/articles/common-security-vulnerabilities-e-commerce-systems [17.04. 2014].

Mulpuru S., Johnson C., Roberge D., *US Cross-Channel Retail Forecast, 2012 To 2017*, "Forrester. For ebusiness & Channel Strategy Professionals", 29 October 2013, https://www.forrester.com/US+CrossChannel+Retail+Forecast+2012+To+2017/fulltext/-/E-RES105461 [15.07.2014].

Pereira T., "Conceptual Framework to Support Information Security Risk Management", Ph.D thesis, University of Minho 2012.

Pfleeger Ch.P., Pfleeger S.L., *Security in Computing*, Prentice Hall PTR 2002.

Schiff J.L., *15 Ways to Protect Your Ecommerce Site From Hacking and Fraud*, 2013, www.cio.com/article/2384809/e-commerce/15-ways-to-protect-your-ecommerce-site-from-hacking-and-fraud.html [15.07.2014].

Sherwell P., *FBI investigates alleged Russian cyber attack on Wall Street*, "The Telegraph", 27 August 2014, http://www.telegraph.co.uk/news/worldnews/northamerica/usa/11060338/FBI-investigates-alleged-Russian-cyber-attack-on-Wall-Street.html [18.09.2014].

Stewart J.M., *White Paper: How To Secure Online Activities*, Global Knowledge Training LIC, 2013, www.globalknowledge.nl/Knowledge-Centre/white-papers/security-white-papers/WP--How-To-Secure-Online-Activities [10.07.2014].

Vulnerability Assessment 2013, "Symantec. Website Security solutions", 2013, https://www.cherry-orange.co.uk/Media/Default/PDF/Symantec_Feeling_Vulnerable_UK.pdf [18.09.2014].

Website Security Threat Report 2013, "Symantec. Website Security solutions", 2013, https://www.symantec-wss.com/campaigns/14385/uk2/social/assets/symantec-WSTR1-UK.pdf [18.09.2014].

Ogólne wytyczne dla obniżenia ryzyka w transakcjach online

Streszczenie. Nieustanny rozwój usług i aplikacji internetowych spowodował bezprecedensowe zmiany w naszym życiu, w gospodarce, w relacjach społecznych oraz w systemach technicznych. Postęp z jednej strony otwiera nowe możliwości biznesowe, z drugiej zaś tworzy poważne zagrożenia. Napastnicy nieustannie poszukują wrażliwych na ataki systemów i próbują zakłócić ich działanie, unieruchomić je lub wyrządzić w nich określone szkody. Tempo, w jakim sieciowi przestępcy absorbują najnowsze technologiczne osiągnięcia, oznacza, że przedsiębiorcy powinni stale i regularnie stosować adekwatne praktyki w zakresie bezpieczeństwa, które pozwolą im bezpiecznie funkcjonować. W artykule podejmuje się dociekania na temat bezpieczeństwa transakcji w sieci oraz jego implikacji dla zainteresowanych stron. Wylicza się w nim słabe punkty internetowych systemów, które są często wykorzystywane do nadużyć, a tym samym dostarcza się informacji użytecznych z punktu widzenia wdrażania dobrych praktyk, które pozwolą złagodzić lub zmniejszyć siłę oddziaływania incydentów z zakresu bezpieczeństwa.

Słowa kluczowe: bezpieczeństwo, bezpieczeństwo informacji, zarządzanie bezpieczeństwem informacji, transakcje online, działalność w sieci