Corporate Point-of-Sale (POS) Systems
Prevention of Breaches/Hacks/Malware

Team 2 - Anthony McNeil and John Curry | Business Advisor: Wendy A. Matthews | Professor: Dr. Yair Levy

Introduction

For this project, a family member and her partner have started up a small business. The business name is Sandy Toes & Sally Kisses, LLC. This is a small local spa business in downtown Jacksonville, Florida (Duval County) operating in Bayard. Their website is located at http://www.bayardantiquiquilages.net. The business is a small retail shop/target with two managers handling retail, jewelry and prepared nourishment and, in-store bakery. The shop is open seven days a week, from Monday to Sunday. For credit card processing, Wendy and Matthew’s partner will utilize two Square. Inc. mobile credit card readers attached to Apple, Inc. mobile devices. Apple, Inc. iOS system software will be installed on all Apple, Inc. mobile devices. The two Square. Inc. mobile credit card readers will process payments directly to a business checking account located at a major US-based bank.

The hacking industry brought in $2.5 billion between mid-2013 and mid-2014 (Peters, S., n.d.). This is due in part to a breach that happened with Target in 2013. Point-of-Sale (POS) system hacking attacks are projected to intensify and are more sophisticated because they can convery data that is ten times more lucrative than your customary plastic card credit card numbers (Peters, S., n.d.). There is a great deal of nefarious hackers, indiscriminate infections, target attacks and unethicalness of operators to provide the needed level of protection, which result in enormous leaks. In addition, the size and the evolution of the booming fraudulent credit card market has greatly improved. There is new professional that deal in stolen credit card data. It is a very lucrative market as seen by millions of dollars made by a supplier of stolen credit card data named “Reseller” (Peters, S., n.d.). Recruiters must be paid by selling over 150,000,000 credit cards to an online trading platform called “SMWED”. This online trading platform made $85 million in one year alone.

The market value of a credit card dump is ten times more valuable than the cost of the credit card details itself (Peters, S., n.d.). Credit card dumps offer a much greater opportunity for banked transactions. An attacker can make a physical replica of the credit card with the dump of the credit card’s data and conduct operations in off-line points of sale, buying expensive electronics, luxury goods and other goods to be sold in the secondary market. These credit card dumps are stolen using skimming hardware or stolen by infecting POS terminals with special Trojans.

Recognizing the Problems

- Credit card fraud prevention
- Physical security - theft protection of company merchandise and cash during business and after hours
  - Safety linking Square. Inc. mobile credit card readers to a mobile device with device connection to in-store Wi-Fi and/or wireless AT&T networks
  - Security of Square. Inc. mobile credit card readers’ hardware, software and information
  - Non-sufficient funds (NFS) check protection
  - Protection of customer information gathered during transactions
  - Mobile tracking of receipts to customers
  - Protection of paper cash register receipts
  - Ability to upgrade POS system to Europay, MasterCard and Visa (EMV) credit cards

Gather Facts

- Consultations with Business Advisor
- Research the project, which includes Internet searches and previous course tests.

Project Scope, Goals, and Objectives

- Train all customer service representatives (CSR’s) on ways to prevent credit card fraud within 6 weeks of go-live date
- Integrate sales training with functional training on new POS system
- Update all sales team members, Square. Inc. mobile card credit readers to business checking account
- Train all CSR’s on ways to protect customer information gathered during transactions
- Discuss safeguards to prevent NFS as it pertains to checks used for purchasing
- Train all staff on use of firewalls and other safeguards of networks.

Identify Costs

One-Time Costs:

<table>
<thead>
<tr>
<th>Hardware Acquisition</th>
<th>Quantity</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Square. Inc. Mobile Credit Card Reader Terminal</td>
<td>2</td>
<td>Free</td>
</tr>
<tr>
<td>Apple, Inc. iPhone 6 Plus</td>
<td>2</td>
<td>$200.00</td>
</tr>
<tr>
<td>Apple, Inc. iPad Air</td>
<td>1</td>
<td>$650.00</td>
</tr>
<tr>
<td>Panasonic KX-TGD12 Expandable Digital Cordless Phone</td>
<td>1</td>
<td>$85.00</td>
</tr>
</tbody>
</table>

Software Acquisition:

| Square. Inc. POS App | 2 | Free          |
| Apple, Inc. iOS X iPhone Operating System | 2 | Free          |
| Apple, Inc. iOS X iPad Operating System | 1 | Free          |

Testing:

| Testing of Apple. Inc. Mobile Devices on Wi-Fi and Wireless Networks (Provide Written Results). | $250.00 |
| Testing of Square. Inc. Mobile Credit Card Reader Terminals, POS-Apple and Apple. Inc. Mobile Devices (Provide Written Results). | $350.00 |
| Testing of Panasonic KX-TGD12 Expandable Digital Cordless Phone on Wireless Networks. | $75.00 |

Project Consultation & Personnel Training:

| Project Consultation | $250.00 |
| Introduction of Apple. Inc. Mobile Devices and Apple. Inc. iOS Operating Systems. | $50.00 |
| Introduction of Square. Inc. Mobile Credit Card Reader Terminals and Square. Inc. POS App. | $75.00 |
| How to Prevent Credit Card Fraud and how to Protect Customer Information Gathered During Transactions. | $25.00 |
| Training on the use of Firewalls and Other Network Safeguards. | $100.00 |

Recurring Costs:

| Wireless Network & Credit Card Fees: | Cost          |
| AT&T Mobile Share™ Value Plan With Unlimited Talk & Text, 30 GB of data for (2) -iPhone 6 Plus | $130.00/month |
| AT&T DataConnect™ for Apple, Inc. iPad Air | $30.00/month |
| Apple. Inc. iPad Plan for Parlay KX-TGD12 Expandable Digital Cordless Phone | $30.00/month |
| Square. Inc. Mobile Credit Reader (Swiped Transactions). | $25.00/month |
| Square. Inc. Mobile Credit Reader (Manually Entered Transactions). | $5.00/month |

Hardware and Software Resources

Resources in place at Sandy Toes & Sally Kisses, LLC:

| Two Square. Inc. mobile credit card readers |
| Apple. Inc. mobile devices including: (1) -iPad Air with Wi-Fi and wireless connections and (2) -iPhone 6 Plus with Wi-Fi and wireless connections |
| Apple. Inc. devices are on the current version of Apple iOS system software |

Resources Sandy Toes & Sally Kisses, LLC are planning to acquire:

| AT&T high speed Internet Modem |
| Royal 24x24 Cash Management System |
| 2 Square. Inc. mobile credit card readers for EMV credit cards |
| Bank of America Small Business Checking – Business Fundamentals |

Risk Management Analysis Outline

- PROJECT - The project manager working with the management team will ensure that risks are activity identified, analyzed, and managed throughout the entire life of the project. Risks will be identified as early as possible in the project to minimize their impact.
- The steps for accomplishing this are outlined in the following sections. Curry & McNeil Information Security will serve as the Risk Manager for this project.

- RISK IDENTIFICATION - Risks identification will involve the management team and will include an evaluation of environmental factors, organizational culture, project management plan, and project scope. Careful attention will be given to the project environment. Risks identification will be a continuing process.
- Elaborate updates will be generated and updated as needed and will be shared electronically in the project library located at the site of business.

- RISK ANALYSIS & RESPONSE - All risks identified will be assessed to identify the range of potential project outcomes. Qualification will be used to determine which risks are the top risks to pursue and respond to and which risks can be ignored.

- QUALITATIVE RISK ANALYSIS - The probability and impact of occurrence for each identified risk will be assessed by the project manager with input from the project team.

- Mitigation STRATEGIES - Mitigation strategies and detailed implement and frequent communications and confirm that only allowed ports, services and Internet Protocol (IP) addresses are communicating with the network.
- Apply hardware based post-project expectation.
- Use EMV enabled PIN entry devices or other credit-card accepting devices with secure networking and data exchange (SDRE) capabilities.
- Insist that merchants examine their payment application to make sure that it is not configured in a debugging/tunneling mode.
- Ensure that the Square. Inc. merchant is using the pay-together encryption.
- Make sure that there are regular administrative permissions on users and applications.
- Provide reports to the merchant and Square. Inc. on request or demand user.
- Develop and implement a comprehensive, third-party, post-project process by establishing policies and procedures to manage and measure the efficiency of security controls.
- Consider using strong administrative services that provide secure access, maintaining stateless perimeter and keeping compliant status.
- Implement Web application security vulnerability assessment and testing to help identify critical security vulnerabilities.
- Sandy Toes and Sally Kisses, LLC should institute thorough go live procedures and communicate to all the management teams, review the current levels of authentication and authorization, update software patches and install any missing security and usability controls.

Anticipated Results

- Successfully train CSR’s on ways to prevent credit card fraud within 6 weeks of go-live date.
- Successfully integrate sales training with functional training on new POS system.
- Safety link the Square. Inc. mobile credit card reader to business checking account.
- Successfully train CSR’s on ways to protect customer information gathered during transactions.
- Discuss safeguards to prevent NFS as it pertains to checks used for purchasing.
- Train all staff on use of firewalls and other safeguards of networks.

Conclusion

In conclusion, the project titled “Corporate Point-of-Sale (POS) Systems Prevention of Breaches/Hacks/Malware” was written and compiled by Curry & McNeil Information Security for Sandy Toes & Sally Kisses, LLC. The scope, goals and objectives of this project include: training of CSR’s on prevention of credit card fraud; integration of sales and functional training of POS system; safely linking POS device to business checking account; training CSR’s on ways to prevent customer information theft; training CSR’s on prevention of theft of merchandise; discuss safeguards to prevent NFS of personal check payments; train on safeguards to prevent theft of cash and in-store; and train staff on using firewalls. The anticipated results are based on this project’s scope, goals and objectives. Curry & McNeil Information Security hope this poster provides Sandy Toes & Sally Kisses, LLC with an appropriate overview of information with an underlying goal of making sure customer and company information and devices are as secure as possible.

Reference List


Center for Information Protection, Education, and Research (CIPHER)
Graduate School of Computer and Information Sciences (GCSIS)