Risk Control Bulletin: Cyber Security - Point of Sale

CNA
We can show you more.®

RISK CONTROL

Credit card information has always been a target for attackers, and historically it has been attacked in a number of ways; terminal skimming and server/database attacks being two of the main vectors. Terminal skimming was generally confined to ATMs and gasoline pumps with "pay at the pump" functionality. The second method of server and database attackers would leverage website vulnerability such as SQL Injection to gain unauthorized access to a database, granting the attacker the potential to access a much larger amount of data.

There are steps that a company can take to protect their data:

- Properly segment the point of sale (POS) network from other parts of the corporate network.
- POS devices can be "hardened" by ensuring that security patches are regularly installed; application whitelisting and automatic device reimaging is used to prevent unauthorized applications or malware from being installed.
  - o Whitelisting is designed to prevent the execution of unauthorized and malicious programs. With the ever increasing number of viruses and malware some companies find it easier to define what "can" run on their computers instead of defining what "cannot" run.
- Intrusion detection can be installed on the network to detect unauthorized access.
- Connectivity restrictions can be used to disallow internet access from POS devices.
- End-to-end encryption can be utilized to encrypt credit card information from the moment it is read into the POS device, thwarting memory-scraping malware.
- Tokenization removes the actual credit card number from the transaction, replacing it with a randomly generated token. This token can be set to expire after one transaction or after a set period of time. This reduces or eliminates the usefulness of stolen transaction data.

PCI-DSS is the payment card industry data security standard. Its purpose is to provide an information security standard for organizations that handle branded credit cards from the major card brands (i.e., Visa, MasterCard and American Express). While it is a good basis for protecting payment card data, it is not all inclusive and in many cases only provides general guidance (not technology specific). It is also important to note that PCI compliance is a point in time designation. PCI is also in process of rolling out the new 3.0 standard, which took effect July 1, 2015. Areas that it will be focusing on are:

- Evaluating malware threats for systems not commonly affected by malware.
- Two-factor authentication for sensitive systems.
- Implementing a methodology for penetration testing.
- Maintaining information about which PCI DSS requirements are managed by service providers and which are managed by the entity.

Payment card security is a complex and ever changing landscape. As consumers continue to favor cashless transactions, both in person and online security for these systems will need to adapt to continue to provide adequate protection. To put it simply, there is no silver bullet. As new security technologies are devised and deployed, attackers will continue to adapt their methodologies to find new ways to compromise the information they seek.

To learn more about how CNA's Risk Control services can help you manage your risks and increase efficiencies, please contact CNA Risk Control at 866-262-0540, or visit www.cna.com/riskcontrol.

Bulletin Location: www.cna.com > Find Resources to Manage & Reduce Risks > Property, Assets & Products > Cyber Liability > Articles & Guides.

CYBER SS 110215