Data Security Alert

Retail Data Security Breaches

November 11, 2014

Data Security is a top priority for Discover Network. We periodically publish Data Security Alerts regarding emergency security threats and best practices to help protect payment card data. Data Security Alerts may be useful in assisting stakeholders with valuable information for mitigating security risks. Please provide this alert to your IT or security personnel.

Retail Point-of-Sale Breaches

Remote Access is being exploited at Payment Integrators, Third Party Service Providers and Franchises where remote access is left enabled. Discover/ Diners Club International highly recommends that merchants with multiple locations review the security of their payment environment with specific attention to remote access and network traffic into and out of the payment environments, and their Point of Sale (POS) Systems.

The results of recent forensic investigations revealed that the use of default/weak passwords without two factor authentication in conjunction with remote access are significant contributing factors in these data breaches. Merchants should work with their Information Technology (IT) staff and/or payment system service providers to verify that remote access to the payment environment is configured in a secure manner in accordance with PCI Data Security Standard guidelines including password complexity requirements.

A new family of malware known as 'Backoff' with multiple variants has been identified in several recent investigations. Keep all anti-virus software, operating systems and web browsers up to date to prevent against known vulnerabilities.

Hackers targeting the Big Box and Holding Companies' payment environments have installed malicious executables on the point-of-sale servers and terminals with the purpose of scanning for additional network systems, searching for non-compliant storage of track data, setting up services that parse volatile memory for track data, and installing back doors. Please see the attached list of malicious files which have been detected.

Recommendations

Discover/ Diners Club International requires entities that process, store and transmit cardholder data to comply with all PCI DSS requirements and we recommend the following actions to address these recent trends:

- Use complex passwords and two factor authentications when accessing the payment environment. Remote Access should be disabled when not in use.
- Merchants should install new software patches as they are released by the software vendors.
- Install and keep anti-virus and anti-spyware up to date.
- Implement file integrity monitoring to identify when files or logs are maliciously modified.
- Install and maintain firewalls to protect unauthorized access into the cardholder data environment from untrusted networks.
- Ensure your network environment is segmented and processing cardholder data separately from other areas of the network.
- Reboot point-of-sale systems daily to clear volatile memory.
- Additional guidance on preventing skimming and POS tampering can be found at https://www.pcisecuritystandards.org/documents/skimming_prevention_IS.pdf

If you detect or suspect a security breach, promptly contact your Acquirer. You may contact Discover Network Data Security at (800) 347-3083 to report a breach. For more information on how to handle a data security breach, visit the Discover Network Data Security page at http://www.DiscoverNetwork.com/merchants/fraud-protection