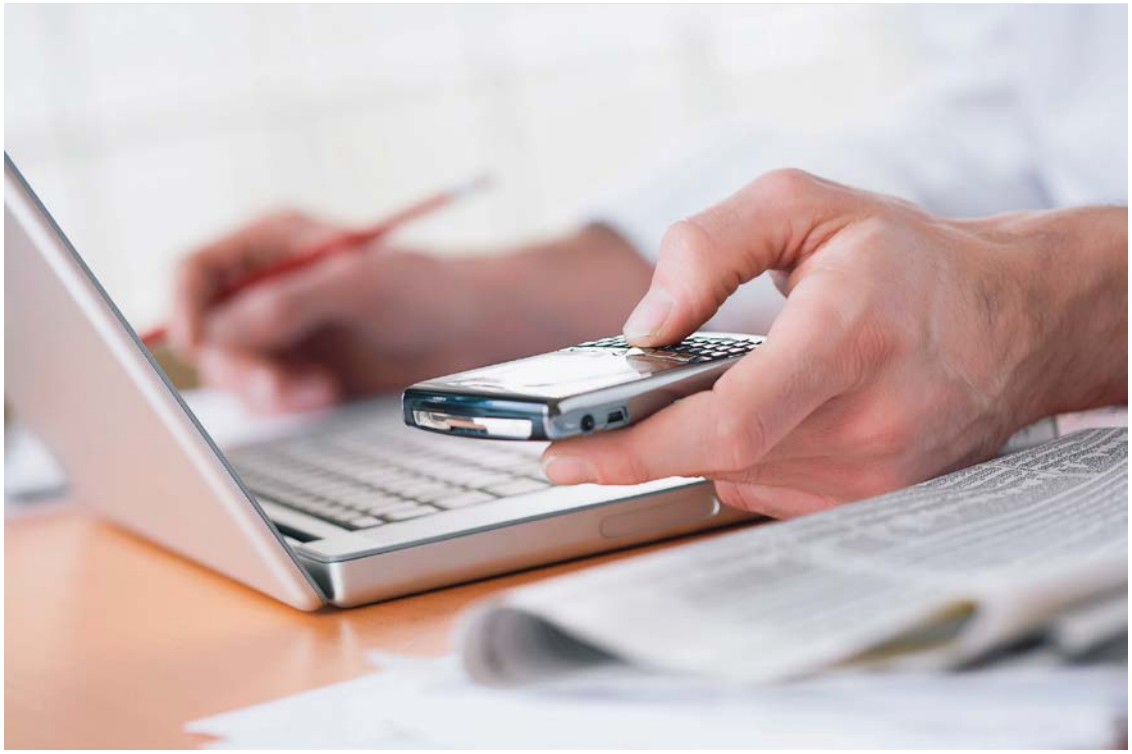
Remote Access Technology

PCI Best Practices



HACKERS ARE NOT TARGETING A SPECIFIC MERCHANT, RATHER, THE HACKER WILL SCAN THE INTERNET FOR VULNERABLE REMOTE ACCESS SYSTEMS AND ATTEMPT TO COMPROMISE THEM, REGARDLESS OF THE MERCHANT SIZE OR TYPE.

Remote access technology is an incredibly valuable tool to a small business as it allows merchant employees to connect to the office from anywhere in the world, as long as they have an internet connection. However, remote access technology also has the potential to be used by an attacker to compromise the merchant's network.

Recent attack trends have shown that hackers are beginning to increase their focus on smaller merchants with improperly configured remote access systems. Generally, hackers are not targeting a specific merchant; rather, the hacker will scan the internet for vulnerable remote access systems and attempt to compromise them, regardless of the merchant size or type.

MasterCard analysis of Account Data Compromise Events has shown that insecure remote access is the #1 point of entry for attacks against brick-and-mortar merchants.

All merchants, regardless of size, level or transaction volume that store, transmit or process payment card account data are required to comply with the Payment Card Industry Data Security Standard or PCI DSS. The PCI DSS identifies specific requirements for managing remote access technology. By securing remote access systems in accordance with PCI DSS requirements, merchants can reduce the likelihood of an attacker compromising the merchant network and stealing valuable payment card account data.

Merchants should be aware of five primary security concepts that the PCI DSS calls out for remote access:

Lock user accounts after 6 failed login attempts

Risk: Allowing an unlimited number of failed login attempts allows an attacker to perform a "Brute Force" attack, in which the attacker attempts to guess an account password. By locking the account for 30 minutes after 6 attempts, an attacker is more likely move on to another target, rather than wait for the 30 minutes to guess another 6 passwords.

PCI DSS Requirements 8.1.6&8.1.7: Most common operating systems have built in functionality to allow for accounts to be locked after 6 failed login attempts. Accounts should be locked for at least 30 minutes or until manually reset by an administrator.

CONTINUED FROM COVER

Change default passwords

Risk: Many vendors utilize common default passwords. These default passwords are often documented in user manuals or technical articles. Attackers make lists of these common default passwords and will attempt to guess an account password by using a default password, such as “password123”. By changing a weak default password to a strong default password, the attacker will have more difficulty in guessing the password.

Requirements 2.1, 8.2.3& 8.2.5: All default or “out of the box” passwords should be changed to unique, complex passwords prior to the system being put in place. Passwords should be at least seven characters long and made up of both numbers and letters. Ideally, passwords should not be “reflective”. For example, The Administrator password should not be “Administrator123” as it is very easy to guess.

Enabling vendor remote access only when needed

Risk: If remote access is enabled all of the time, it provides an attacker an ever-present window in which to attempt to break in to your environment. Limiting the time that remote access is enabled reduces the opportunity for intrusion.

Requirement 8.1.5: Remote access for any vendors, such as your POS vendor, should only be enabled when actually needed. It is not acceptable to leave the remote access “always on”.

Service Providers must use unique credentials for each customer

Risk: To prevent the compromise of multiple customers through the use of a single set of credentials, vendors with remote access accounts to customer environments should use a different authentication credential for each customer.

Requirement 8.5.1: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.

Ensuring that two-factor authentication is enabled for remote access

Risk: Utilizing only a single authentication factor, such as a password, makes it easier for attackers to gain access to your systems. Two-factor authentication greatly reduces the risk of a brute force attack in which an attacker attempts to guess a password.

Requirement 8.3: Incorporate two-factor authentication for remote network access originating from outside of the network by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance).

Two-factor authentication includes any two of: something you know, something you have, or something you are. A common example of two-factor authentication for remote access is the use of a password in conjunction with a security token that generates a new access code on a regular basis (commonly every 30 or 60 seconds). Another common form of two factor authentication is use of a password and a certificate. UserIDs are not considered a factor of authentication.

For questions on how to properly secure your remote access system, please refer to your Acquirer or a Qualified Security Assessor (QSA). A list of QSAs can be found at the PCI Security Standards Council web site at: https://www.pcisecuritystandards.org/approved_companies_providers/qualified_security_assessors.php

The entire PCI DSS is made up of over 300 sub-requirements. While meeting the requirements listed in this fact sheet can significantly help reduce an entity’s risk of compromise, it does not mean that an entity is fully PCI DSS compliant. MasterCard requires all entities that store, transmit or process cardholder data to be fully compliant with the PCI DSS. For questions on compliance and your merchant environment, please contact your acquiring bank.

MasterCard