LANCOM Whitepaper
PCI Compliance

With the PCI DSS (Payment Card Industry Data Security Standard), the leading providers of electronic payment systems (card operators) agreed in 2005 on a binding minimum standard for the data security of their customers. This standard is intended to ensure that card payers' customer data is not stolen, altered or otherwise misused. The reason for introducing this standard is the rapid increase in cases of card fraud. According to industry reports, attacks on retailers who accept card payments increased by more than 50% between 2003 and 2006. Companies that accept card payments are required by the credit card companies to have their installations tested and certified for PCI DSS compliance. If they do not adhere to this requirement, the credit card company can extraordinarily terminate the contract and also refuse to accept liability for damages incurred. The certification audits are conducted by companies that have been declared 'Security Assessors' by both Mastercard and Visa.

Economic damage and loss of image

The economic damage caused by inadequate protective measures against card fraud usually affects the retailers themselves - the card operators often reject liability with reference to existing security gaps. In addition, the loss of customer confidence is a realistic threat if a retailer becomes the victim of an attack due to inadequate protection measures. The standard makes life much easier for card operators and retailers, as they can now demand or meet a fixed set of requirements and thus gain legal certainty. The merchant can communicate a comprehensive security strategy to the end customer and thus guarantee data security and the associated trust. All companies and merchants that accept card payments must meet the conditions of the standard. Otherwise, there is the threat of severe penalties and the dealers themselves are liable in the event of an attack.

The PCI standard in detail

Card-related data is processed via various components in the networks of retail companies – from card readers and cash registers to central servers and ERP systems. These networks are realized with the help of routers and switches, which establish the connection between the individual components and control the data transmission in the local and to remote networks (up to the accounting server of the card operators). In particular, the PCI standard defines what the credit card industry expects of the IT infrastructure used in retail companies. Only an entire system can meet the standard, not individual devices or detailed areas. Even if a large part of the network would technically comply with PCI DSS, a single vulnerability or a single protection measure not activated is enough to compromise the entire system. Nevertheless, all components used must have PCI compatibility in order to be used within a PCI-compliant network. The desired goal is PCI conformity in a so-called 'end-to-end' form, i.e. along the entire data path between the point of sale and the card operator.

Planning of PCI compliant IT systems

Even if various sub-components of an infrastructure seemingly have nothing to do with card payments, any unprotected location is sufficient for attackers to break into the entire system. When planning the computer networks used, it is therefore necessary to aim for a long-term and

scalable solution in which individual components remain interchangeable without endangering the overall system. Furthermore, compliance with the standard only plays a role at the time of an attack, not afterwards or before. It is therefore necessary to choose a permanent solution with appropriate measures and to make them comprehensible. After an attack, companies must themselves prove that they have met the standard. This results in a set of requirements for the implementation of PCI DSS: The intended solution should have a modular structure and be centrally managed, maintained and monitored. Furthermore, it must also be possible to investigate events that occurred in the past, i.e. there must be complete logging.

The 12 requirements of the PCI standard

The PCI DSS specifically covers 12 requirements:

- Setting up a firewall
- Immediate change of all factory passwords and other safety-relevant parameters to your own safe values
- Protection of stored data
- Encryption of data transmission via open networks
- Virus protection
- The maintenance and development of secure systems and applications
- Only necessary data access should take place, 'need-to-know' basis
- Each user of the network must be clearly identifiable
- A physical access protection
- A comprehensive logging of all accesses to card data
- A regular inspection of all safety equipment
- The creation of an IT security strategy (policy) and its compliance

The last requirement has a special meaning, since all other points can be derived directly from it. The IT security strategy required here must affect the entire system and cover all remaining points. It is not enough to use PCI-compatible hardware and software, the IT security policy must also include the behavior of employees, cover all remaining requirements of PCI DSS and thus close every possible point of attack in the system. Although individual devices and software must meet the requirements of the PCI DSS, they can only contribute to the desired PCI compliance within an overall system that meets the requirements.

Network components must support PCI conformity

Some of the requirements of the PCI standard must be met by the network components used (e.g. routers and switches), e.g. by setting up suitable firewalls and encrypting data (e.g. VPN in the WAN). With these functions, however, the network components only provide certain security functions for other services of the network structure.

An essential aspect of meeting PCI requirements is control over access to the network components themselves: if an attacker gains access to a router or switch, he may be able to switch off the other security measures by changing the configuration, thus compromising the entire IT system. In order to protect the network hardware from unauthorized access and thus achieve PCI compliance, the components used must support a 'Triple-A' procedure. 'Triple A' stands for authentication, authorization and accounting.

- With the authentication the user is recognized. This ensures that only uniquely identified users are granted access to network components (point 8 of the PCI requirements).
- Via the authorization function the user is assigned his special rights.
- With accounting, all actions of the user are recorded. This means that it is possible to check at any time afterwards whether the IT system was PCI-compliant at any given time.

Only if the network components used support the authentication, authorization and accounting functions can they be used in a PCI-compliant network. One possible

Triple-A system is 'TACACS+'. Compared to the widely used RADIUS, TACACS+ has the advantage that the three separate areas of authentication, authorization and accounting can be executed on separate components. For example, the administration of user accounts for authentication can be done on one server, but the logging of activities (accounting) on another server. TACACS+ also provides better encryption of the transmitted information.

LANCOM devices enable system-wide PCI compliance

With the support of TACACS+, LANCOM devices ensure that only uniquely authenticated users have access to the configuration of the devices. An appropriate setting of user rights (authorization) ensures that users are only allowed to make traceable changes that can be logged by the accounting server. Specifically, this means, for example, that the functions with which a complete device configuration can be written to the device are blocked, as is usual when using LANconfig. As long as this function is allowed, a non-loggable change of the configuration would otherwise be possible, which would contradict PCI compliance. Routers and switches from LANCOM Systems also provide additional security functions to protect the configuration in the event of theft of the devices, helping to establish a PCI-compliant IT infrastructure.