PCI compliance by creating network segmentation across 3500 stores nationwide

At a glance

> **Customer name:** The Co-operative Group

> **Industry:** Retail

Challenge
In order to satisfy PCI compliance regulations the company needed to segment store systems in order to isolate and protect cardholder data.

Solution
Kerv Connect achieved network segmentation by implementing a firewall appliance with security zones in each of the 3500 stores. This isolated cardholder data without the need to reconfigure every in-store system and device.

Benefits
> The simplicity of Kerv Connect's solution meant an extensive VLAN deployment was not necessary to segment various store systems.

> The cost of deploying a firewall in each store was significantly less than having to reconfigure every in-store system and device, which would have included approximately 210,000 devices.

Overview

The Co-operative Group is the UK's largest mutual retailer. It is the fifth largest food retailer, the third largest retail pharmacy chain, the number one provider of funeral services, and the largest independent travel business. It also has strong market positions in banking and insurance. The Group employs 110,000 people and has around 4,900 retail outlets. In March 2009 Somerfield joined The Co-operative Group. Somerfield was a high street supermarket with 900 stores in many high street locations throughout the UK.

The Challenge:

The Co-operative Group (including the TCG Food stores, Somerfield stores, and Pharmacy business) processes almost 200 million credit and debit card transactions per year, from a store estate of almost 3,500 stores.

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. The standard also required retailers that process large volumes of credit/debit cardholder data to be PCI DSS compliant. The Co-operative Group therefore deemed it necessary to review its store environment with regard to how store devices are segmented as a means of protecting cardholder data in order to work towards PCI compliance.

Segmenting store systems such as tills and guest wireless onto functional VLAN's to protect cardholder data would require all endpoints to be re-assigned an IP address. The financial implications of achieving this across the 2800 food stores alone was almost cost prohibitive.

In fact the PCI compliance requirement would encompass some 3500 stores across the Co-Operative Group including Food, Pharmacy and Funeral business units which would have dramatically increased the financial burden of achieving PCI compliance.

The Solution:

Kerv Connect's experience in understanding the business needs and processes required at the infrastructure layer to achieve PCI compliance had been through working with other customers in the retail sector. In particular Kerv Connect was familiar with the challenges, complexity and cost when network segmentation was introduced into a store environment.

Although network segmentation is not a PCI requirement, it is deemed a mechanism to reduce the scope, cost and difficulty of implementing and maintaining PCI DSS controls. Without network segmentation the entire network would fall in scope of the assessment.

Kerv Connect's solution to achieve network segmentation and consequently isolate cardholder data was to implement a small firewall with security zones. The stateful firewall that was implemented would filter traffic flows in transparent mode, that is, it would be able to restrict access between defined security zones based on specifically defined policy information without the need to re-address endpoints. The security zones and policy definition was specifically designed to align to the requirements of the PCI DSS standard by de-scoping a large part of the store environment including the wireless infrastructure.

The implementation phase was scoped for twelve months that included:

› Pre-staging of all firewall devices, checking for DOA's and applying a base configlet to each firewall to enable centralised configuration and policy provisioning.

› Managing and co-ordinating a third party in-store implementation team with centralised Kerv Connect Engineering resources provisioning configurations and policies as well as troubleshooting.

› Managing and co-ordinating firewall licensing and RMA processes as well as weekly management reporting updates.

› Streamlined processes enabled the project to be completed three months ahead of schedule and well within budget.

Benefits

This solution had a number of significant benefits:

- The solution maintained a level of simplicity within the store environment in that extensive VLAN deployment was not necessary to segment the various store systems and devices including servers, tills, wireless access points and wireless handheld devices.

- All store systems and devices would not need to be reconfigured with new IP addressing details, which would have been the case if VLANs had been deployed.

- Traffic flows were centrally controlled through template policy definitions that could be quickly deployed across all 3500 stores

- Although a firewall appliance was needed in every store, the cost for deployment was significantly less than having to reconfigure every in-store system and device, which would have included approximately 210,000 devices.

- Deploying the firewall appliance rather than re-addressing every in-store system and device also greatly reduced PCI project timescales
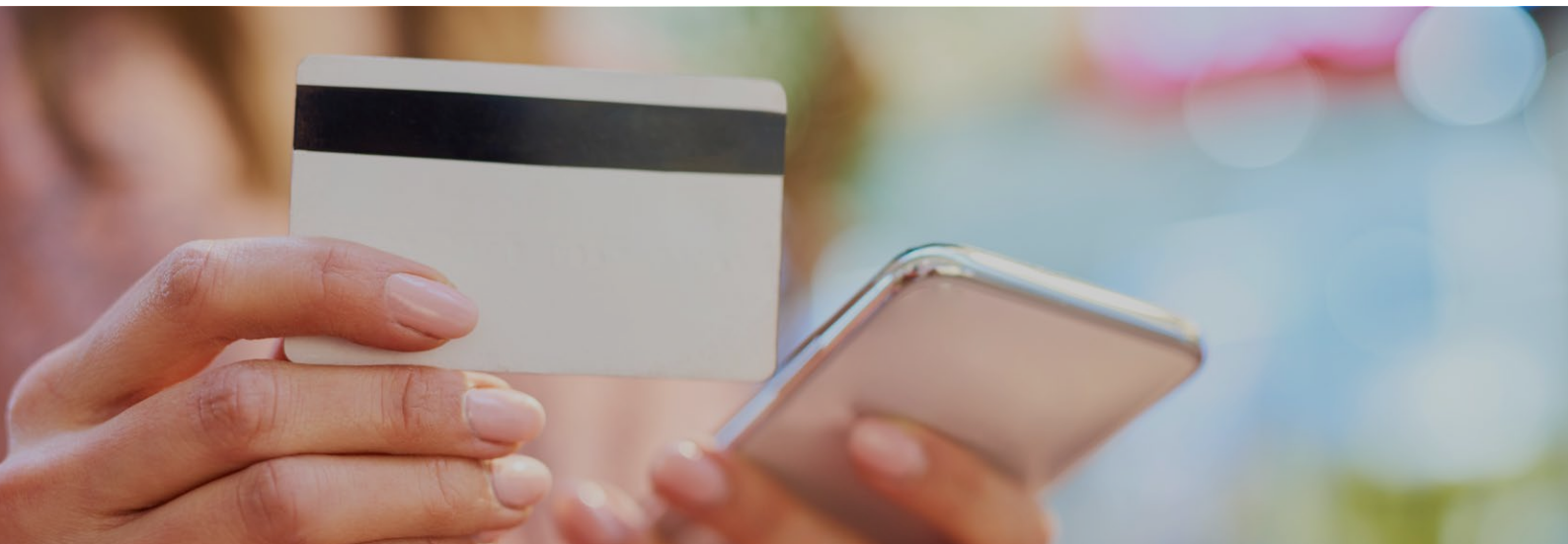
Get in touch with us

For general enquiries please contact
hello@kervgroup.com

Kerv Group, Unit 1B, 1 Finsbury Avenue, London, EC2M 2PP

kerv