Internet payment security review

7 Elements was engaged to perform a comprehensive security review for a leading internet payment services provider as part of its annual Payment Card Industry Data Security Standard (PCI DSS) assessment. The scope of the engagement included an infrastructure assessment, web application assessment and a multiple scenario, remote social engineering assessment. Our client's business leadership approach to information security requires that the organisational approach to security management should exceed its external compliance requirements, including that set out by PCI DSS. With that in mind, we were challenged to find innovative ways in which to assess its resilience to attack.

Throughout the engagement, we hosted daily conference calls in order to update on progress. The dialogue we maintained with the client, from pre-assessment through to report delivery and wash-up, was well received and enabled them to react to technical exposures as we identified them.

The infrastructure assessment was completed quickly with a small attack surface and good controls in place. Due to the information security management system in place and strong secure-coding ethos, the web application employed an excellent suite of security defences with validation and encoding at its very core.

Common vulnerabilities were not evident in our assessment, so we quickly moved to a deeper technical level of interaction with the application. Using our experience of working in other payment service providers and the wider financial services industry, we built a complete service to integrate with the client's payment gateway in a matter of hours. This allowed us to interact with the full end-to-end application as one of their customers would, exposing APIs and parts of the code that an automated test would not be able to do.

Through the methodical, manual analysis of the application, we identified a series of security issues that had not previously been discovered through annual assessments, prior to 7 Elements engagement with the client. One vulnerability in particular, though technically difficult to exploit, could have led to the capture of customer payment card details and thus removed the client from being PCI DSS compliant. Software fixes for the issues identified were developed prior to the completion of testing due to the open communication channel we kept with our client, allowing the immediate mitigation of risk.