DRIVING PCI COMPLIANCE THROUGH INNOVATIVE SECURITY TESTING

Prism Infosec, a Payment Card Industry (PCI) Qualified Security Assessor (QSA) and European CREST member company, used an innovative advanced red teaming approach to identify risks associated with a retail client's PCI Cardholder Data Environment (CDE). The delivery of an extensive red team engagement meant that the retailer could comply with multiple requirements of the Data Security Standard (DSS), whilst raising the level of information security associated with the protection of cardholder data and personal information. The combination of Prism Infosec's technical expertise, along with significant experience with PCI compliance, delivered a truly unique client engagement.

Client Requirement for Innovation

Prism Infosec's client, a major UK retailer wished to comply with the PCI DSS for the protection of its cardholder data, but also wanted more than just a "tick box exercise". The client was very clear that simply meeting the bare minimum of PCI DSS penetration testing through segmentation and web application testing would fall short of their requirements - they wanted their partner to add greater value and identify gaps in the control framework across the organisation and identify whether their critical data assets (cardholder data and personal information) were adequately protected from advanced threats.

Prism Infosec delivered a red teaming exercise to establish whether the organisation's security controls could be circumvented, thereby allowing unauthorised access to customer details and cardholder data. The Prism Infosec team adopted the mindset of a tenacious attack team who would use multiple exploit and compromise routes, including phishing and spear-phishing attempts, social engineering and physical break-ins.

Defining the Engagement

Prism Infosec engaged with the client's Chief Information Security Officer (CISO) and the Security Manager to define the projects objectives. It was important to define these early in the engagement to ensure key stakeholders had a clear expectation of the required goals and outcomes.

During this initial pre-engagement phase of the project, Prism Infosec worked with the client to agree a clear and unambiguous statement of work that detailed the essential success elements, including objectives, agreed attacks, time, coverage and budget.

Clear definition of the approach, communication channels, timescales and budget boundaries meant that the client was assured the project was properly planned and would be executed in a formal and structured way.

Attack Scenarios

Following the period of surveillance, a number of attack scenarios were established which could lead to success, including:

- **Contact Centre** – this was located in a shared business campus and used by people who were not associated with the organisation making it easier for the team to be less conspicuous;
- **Spear Phishing** – a significant online recruitment strategy was identified and known to be in operation. Using this knowledge, a plan was formed to compromise security through a CV that included a macro, that if run by a less security aware worker in the Human Resources team, could introduce a malicious payload.

Attack Execution

The attacks were executed and success was achieved via two of the planned scenarios. The Prism Infosec team managed to gain unauthorised access into the contact centre by tailgating members of staff into the building during the busy lunch period and showing a fake pass to the security personnel. Once in the building it was possible to connect a micro custom-made backdoor device to an unused network port under a desk and establish a bridge to the corporate network over both Wi-Fi and 4G.

Once the team back at the Prism Infosec offices had observed that the connection was successfully established, it was possible for the red team to exit the organisation without any further confrontation and the attack continued remotely with a reduced risk of physical challenge. This also gave the team time to conduct "under the radar" network enumeration and location of potential weaknesses. Furthermore, as the device was located within the contact centre network, it was thought that there would be an increased opportunity for success to compromise either desktops or services processing payments or personal details. Vulnerable IT assets were identified and compromised with exfiltration of data demonstrated.

The spear phishing attack was also successful, for which Prism Infosec's technical team crafted an email and macro-enabled a Word document purporting to be a CV. The macro within the email was crafted to avoid the AV technology that had been identified from the open source surveillance and establish a command and control (C2) connection to our servers. After an initial enquiry to ask whether a specific role we had found on the Internet was still open to applications (essentially to identify active monitoring of the mailbox and "warm" the recipient), the document was transmitted into the HR team. Within minutes the control channel was established and Prism Infosec's team had control of the desktop within the client environment.

Results and Benefits

Following the exercise Prism Infosec produced the report and risk register entries for the client and formally presented them to the organisation's CISO. The report described in detail how the attacks were planned and executed, including those attacks that were unsuccessful. The output from the exercise clearly identified flaws in people, process, policy and technology (P3T) and provided clear, actionable and pragmatic recommendations on how to address individual issues as well as root causes. The report also satisfied a number of the PCI DSS requirements for conducting penetration tests and segmentation assessments bringing real value to the client.

Furthermore, the testing had been delivered on schedule, within budget and had highlighted gaps in the monitoring and incident handling that was supposedly in place to identify ongoing attacks against the client. Essentially, the client had not received any reports of our activity (or identified the physical backdoor placed within the network) during the entire attack simulation. It was then possible to use the Prism Infosec report, output and conduct a period of risk management and a programme of improvements.

To learn more, call:
+44 (0) 1242 652100

To send us an enquiry:
contact@prisminfosec.com

Visit our website:
https://prisminfosec.com