Prism Infosec: Driving PCI Compliance Through Innovative Security Testing

Using an innovative advanced red teaming approach to identify risks associated with a retail client's PCI Cardholder Data Environment (CDE).

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.

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. Furthermore, Prism Infosec learned more about how the organisation wanted to test the effectiveness of an outsourced Security Operations Centre (SOC) and Security Information and Event Management (SIEM) service.

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, these were:

- **Objectives** – the key objectives of the planned exercise, which included whether it would be possible to exfiltrate sample records of PCI and/or personal data stored internally, either within the Cardholder Data Environment or otherwise;
- **Agreed Attack Types** – including internal and external (to the organisation) network- based attacks, application layer attacks, social engineering (including phishing and spear-phishing) and physical break-ins. Additionally, other innovative break-in methods were agreed, such as leaving potentially malware laden USB sticks in the vicinity of the reception area to determine whether a member of staff placed them in their laptops;
- **Scope and Initial Information** – to satisfy the clients expectation but without constraining the teams creativity, a minimal scope and set of boundaries were agreed. This included restricting the test to the client's UK operations and excluding certain subsidiaries;
- **Out of Scope Attacks** – given the organisation and its payment handling was in a productive state, a purposeful Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks on both perimeter, internal systems and networks needed to be out of scope. To minimise disruption, test to the limit of the organisations appetite for risk and best focus resources, both parties agreed and documented out of scope test types;
- **Communication Channels** – given the client wanted to test the effectiveness of the monitoring and response teams to identifying attack methods, Prism Infosec established clear communication channels and escalation routes. These were documented and agreed in the statement of work such that any communication (including emergency escalations, general test progress updates and incident response handling) points within both the client and Prism Infosec were established;
- **Time, Coverage and Budget** – the length of the project and consultant's time assigned to it, this had to strike an effective balance between ensuring enough time to cover the proposed testing, as well as the client's budget. Prism Infosec produced a clear timetable of events and associated costs for each phase based on extensive experience of bringing greatest value to the client. The timetable helped the client determine the types of attacks that would occur

and when, and assist the CISO and Security Manager understand whether the attacks during the project window were malicious or simulated exercises by the authorised attack team;
- **Agreed Output** – specifying and agreeing the format of the report, the client appreciated the format of our sample report format but also wanted the ability to quickly include risks in their risk register. Prism Infosec agreed the fields that should be included and understood the organisational risk scoring methodology to ensure the statement of work made it clear what information was to be captured.

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.

Knowledge is the Key to Success
The test began by conducting a significant period of surveillance on the organisation, both electronically and physically.

This included:
- Assimilating information about the target company, its structure and key locations from its own corporate website as well as online resources. Prism Infosec identified locations for the head office and contact centre;
- Identifying people and email addresses within the organisation using common popular social networking sites such as LinkedIn, Facebook, Twitter and other online forums;
- Finding networks and key systems associated with the target based upon Internet registration records;
- Looking for case studies that could assist with identifying key technologies and security controls that might be in place;
- Searching darknet forums and cracked password/hash dumps for information and organisational email addresses that have been previously compromised;
- Finding key resources such as network, system and security administrators and personnel from freely available Internet resources;
- Using mapping and satellite views to observe the layout and geography of locations and searching for floorplans;
- Visiting sites to survey ingress points such as reception areas, loading bays, fire escapes and secondary entrances. Additionally, busy periods (such as morning arrival, lunchtimes and staff departure times) or shift change patterns were identified as these can often be the opportunities that attackers can exploit. Furthermore, it was possible to identify physical security controls, such as barriers, CCTV, access pass layouts and associated lanyard colours and logos.

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.

Attack Scenarios
Following the period of surveillance, a number of attack scenarios were established which could lead to success:
- **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. The transient nature of staff within the contact centre and their casual dress presented an informal environment which could potentially be exploited. It was also possible to identify lanyard colours and photo badge formats used by the organisation. The contact centre access facility also seemed to be weak, with a clear entry route into the rest of the building past the reception area;

- **Head Office** – security seemed tight in the head office location with airport style barriers in reception restricting unauthorised access to the rest of the building. However, it was theorised that leaving USB sticks branded with the organisation's logo on the tables in the waiting area may be successful;
- **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.

Standard Internet-based penetration test attempts were ruled out, as online searches showed they had engaged the services of other approved security vendors and were conducting Approved Scanning Vendor (ASV) scans on a quarterly basis. It was felt that this route could use too much time, and that the chance of success was low and could trigger intrusion detection.

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. This allowed access through the RFID access control, as well as intended staff held the door open allowing the team to follow them into the main office. 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.

Manual low volume probing of the networks over a further three weeks identified that a single server was missing a critical Microsoft patch, that had a public exploit that been successfully tested by Prism Infosec.

Exploitation of the server allowed the team to gain a high level of privileges and using attack chaining techniques, it was quickly possible to escalate from a local user on the system to an administrative account with access to many other systems in the client's internal domain.

Prism Infosec managed to establish

an ongoing remote graphical user interface into the client environment and gain access to many other servers within a short space of time. Through investigation of the local and remote network maps, it was possible to locate servers that were accessible from the contact centre environment that had hostnames associated with PCI systems as well as SQL databases. This allowed the team to quickly home in on target servers associated with the target data. Connections to the databases and manual analysis of the contents using SQL statements allowed the team to quickly identify and locate the target objectives.

Given that Prism Infosec had established a covert channel into the environment, it was straightforward to exfiltrate sample records, which were anonymised to ensure the client's customer data was not fully exposed, yet would demonstrate to the client that the targets had been achieved. It would have been possible to transmit this in a relatively straightforward manner using the client's own Internet connection.

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. This was on a different network to the contact centre, but within a short amount of time access to the same servers within the PCI and database environments was possible.

Prism Infosec had identified and successfully demonstrated two separate attack vectors that would achieve the same goals.

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.

The client was delighted with the results as it had demonstrated a simulated cyber-attack on the organisation and identified real methods that could be used to compromise payment and customer data. It was thought that previous assessments that had been conducted had been too narrowly scoped and whilst they had satisfied PCI requirements for conducting annual segmentation testing, they would not identify a number of critical risks associated with the environment.

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) sduring 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.

The client was not only able to satisfy PCI DSS and Information Commissioner's Office (ICO) requirements but also take away some key core issues that could drive security improvements moving forward:

- **Think about the physical** – how small weaknesses in location, access controls, could be exploited by an attacker;
- **Implementing a polite but firm challenge culture** – how if something does not look quite right it should be challenged, otherwise an attacker will exploit familiarity and trust;
- **Protecting against the "plug-in"** – how the organisation can "buy" valuable time when an attacker is trying to locate an area to host command and control boxes;
- **Network Segmentation** – Defence-in-depth and supporting the organisation with a strong network architecture and segregating key data;
- **[Active] Monitoring** – Ensuring that anomalous activity was identified and responded to;
- **Licensing and Patching** – how all systems are important and to minimise attacker lateral movement;
- **Password Security** –Local admin passwords and privilege escalation;
- **Data Management –** domain access privileges, bulk data access, database encryption; and
- **Internet Communications and Egress Filtering** – the dangers of allowing Internet access on server desktops and ease of exfiltration of data and facilitating C2 connections. ●