CASE STUDY — Security Remediation

Privileged access woes addressed using a structured remediation approach

Problem statement

One of the UK's largest retail banks required a review of its production IT systems to ensure access rights were appropriate and to identify privileged access ownership. Any inappropriate access had to be addressed urgently. Thereafter, the bank wanted to establish an additional layer of security in a new access validation process.

Privileged account credentials provide people with elevated systems access. This allows them to perform otherwise restricted tasks such as installing software, altering IT configuration settings, accessing sensitive data, and even controlling access rights for others.

Privileged user access needs be closely managed to ensure that only those with a justified business need can have it. This mitigates the threat from compromise to an organisation's most sensitive systems and information.

Our approach

We were able to help the client using our Security Remediation offering, an end-to-end methodology for resolving security control problems. Security Remediation was developed based on our experience of resolving cyber weaknesses across many of the UK's largest financial services companies.

> "The client's privileged application access was reduced by 80% - significantly improving its risk position."

After initial data collection and validation, work moved on to remediation using our structured prioritisation approach. In driving the remediation activity, we worked closely with the relevant application and platform support teams across the organisation.

A key feature of Security Remediation is the ability to quickly establish and track activities against a defined set of priorities. This meant the business executive received effective, timely progress reporting, and could provide additional management support where required.

Inappropriate user access compromises security

Our approach supports high-volume, asset-based remediation exercises. In this instance, the scope included 23,000 accounts and 700 applications.

Action was taken in several ways: deleting redundant accounts, removing inappropriate entitlements, and restricting data access to read-only. Finally, accounts which did require elevated rights were configured to be managed within a privileged access management tool.

The outcome

By using Security Remediation, our privileged access management programme reduced the risk of unauthorised data access throughout the client organisation. Redundant and inappropriate user access rights were removed or restricted, and the new access management tool controlled the granting of valid elevated privileges in the future.

The client's privileged application access was reduced by 80% - significantly improving its risk position. Steps were also put in place at this stage for ongoing remediation to be transitioned to a business as usual activity.

i-confidential
Cyber Security & Information Risk Specialists ®