nccgroup

An NCC Group case study

Financial Services Organisation

At a glance

Organisation:
Financial services organisation

Industry:
Finance

Challenge:
Testing of security posture to ensure that customer's information was protected

Solution:
Thorough and comprehensive testing of all aspects of the organisation's security posture

Results:
Collaboration between NCC Group and the organisation ensure fully integrated cyber security knowledge and provided greater visibility of potential vulnerabilities

Summary

NCC Group worked with a large international financial services organisation with a large portfolio of digital offerings, ranging from customer facing banking related applications, commercially orientated applications as well as the exposure of financially related APIs to be consumed by third-parties.

Challenge

Given the high value of the information on which the applications operate, the client required the integration of security testing at various points within a rapidly moving development lifecycle. Traditional, periodic, security assessment and penetration testing was identifying security vulnerabilities at a sub-optimal part of the development process and the client was seeking greater assurance of end-to-end security throughout their development processes.

A breach in any of the applications would likely attract large regulatory fines and infringements, and reputational damage to the brand through loss of customer trust due to the sensitive financial information accessible by the applications.

NCC Group provided the necessary expertise at the optimum parts of the development processes to provide high value assurance activities on critical applications.

Solution

Consultants from NCC Group were integrated into the development lifecycle of the applications, providing consultation to the different teams as various points. This included:

- Review of design patterns and architectural collateral in order to identify any logic based vulnerabilities, and to highlight any improvements to security mechanisms related to the design.
- Assessment of the implementation, firstly to confirm that intended security was functioning as expected, followed by fuzzing of the implementation in order to identify any unexpected error conditions that could then be exploited.
- Consultation with developers at an early stage of the development process to ensure security requirements were captured and documented.
- Working with the development teams to ensure in-life application development activities had a greater focus on security use and abuse cases within the applications.
- Provide security assurance and penetration testing on new and existing assets.
- Working in line with the client's rapid deployment model meant that cutting-edge developments of functionality could have security implications on legacy or pre-existing solutions. NCC Group consultants helped the client understand these risks, assess their feasibility and impact and provide remedial advice to improve the security posture.

As the applications offered banking functionality, it was vital that NCC Group tailored our test cases to focus on the specific threats targeting financial institutions in real life. For example, the possibility of fraud and scenarios in which non-technical customers could potentially allow compromise of their account despite the security controls implemented, as well as typical vulnerabilities commonly observed within web applications such as those described within the OWASP top ten. Due to the sensitive nature of the applications and their data, NCC Group's attack scenarios covered broader tradecraft that also included wider threat actors such as nation state attackers and organised criminal groups.

Throughout this process, NCC Group remained in constant communication with the development teams in order to allow quick insight into any potential vulnerability, as well as to provide consultation on relevant fixes.

Due to the large amount of development work ongoing at any one time, solutions were devised to allow accurate and rapid reporting of any potential issues to the relevant stakeholders. A ticketing style system was agreed upon which different development teams would request testing or consultation, and decisions were then made with the client regarding the priority assigned. This was based on the potential impact of a vulnerability within the feature or functionality, and the likelihood of the functionality being targeted (such as required privileges, open sign ups to access the feature etc.). This supplemented the presence of NCC Group security consultants on daily scrum calls, where new functionality and release candidates were identified.

Existing assets were also continually assessed against emerging threats, novel or newly discovered attack techniques and zero-day vulnerabilities. Due to the embedded nature of the consultants, details within public disclosure of a newly identified vulnerability could be adapted into current and future assessments against the application estates rapidly, and techniques in which to negate or monitor the applications for attempted exploitation, or potential fixes proposed.

Additionally, NCC Group supported the client through COVID-19 remote working implications through deployment of our remote assessment capability, NCC Group Firebase. This enabled us to provide a seamless transition from onsite to remote working and security assessment, whilst adhering to all security related policy and procedures required to operate remote connectivity within a banking environment.

Results

NCC Group integrated our deep cyber security expertise into the client's development teams and processes to provide a rapid acceleration on cyber security knowledge. As a result, the client gained greater visibility of security related vulnerabilities and issues at an earlier stage of the development process, making remediation more effective and reducing the overall risk to the organisations brand and clients. NCC Group worked collaboratively with the client to provide the necessary skills and expertise at the optimum point so that the client's risk was significantly reduced.

About NCC Group

NCC Group is a global expert in cyber security and risk mitigation, working with businesses to protect their brand, value and reputation against the ever-evolving threat landscape.

With our knowledge, experience and global footprint, we are best placed to help businesses identify, assess, mitigate & respond to the risks they face.