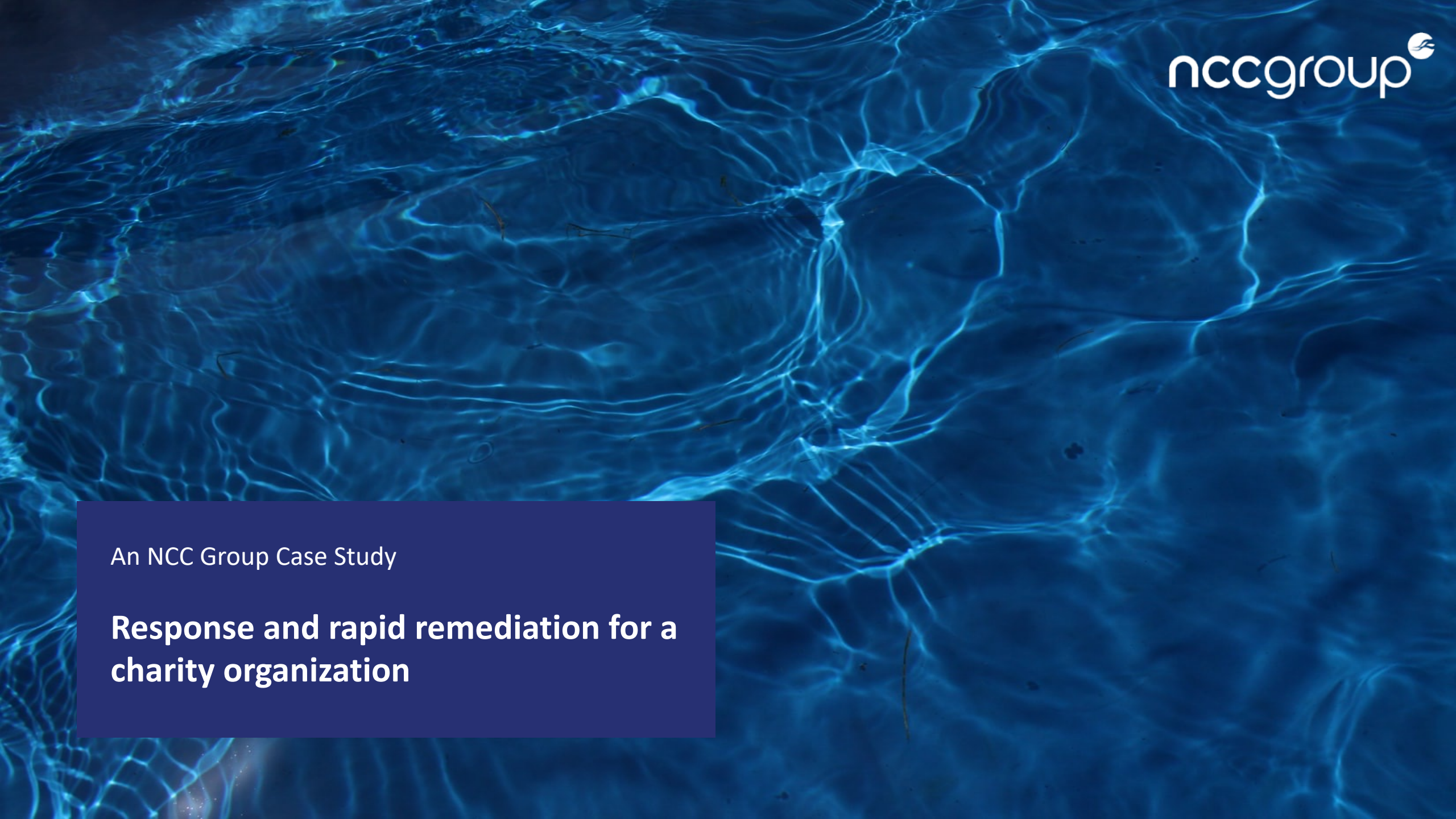

An NCC Group Case Study

Response and rapid remediation for a charity organization

Response and rapid remediation for a charity organization

At a glance

Organization:
Charity organization

Industry:
Charity

Challenge:
Providing support for a charity after it fell victim to a ransomware attack

Solution:
The extent of the attack was ascertained, with key information identified and systems rebuilt to ensure service could be resumed

Results:
Vulnerabilities were rectified, saving the organization resources and time in the process

Short Summary

NCC Group provided extensive support to a charity organization after they had fallen victim to a ransomware attack. The support consisted of both a full investigation into the root cause of the attack, as well as a remediation service from NCC Group's Security Improvement and Remediation (SIR) team to fix any potential vulnerabilities and protect the organization against similar attacks going forward. Thanks to the support, guidance and expertise of the teams, vulnerabilities were able to be rectified, saving the organization valuable time and resources in the process.

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.

Summary

NCC Group supported a charity after they had fallen victim to a ransomware attack. The support consisted of both a full investigation into the root cause of the attack, as well as a remediation service from NCC Group's Security Improvement and Remediation (SIR) team to fix any potential vulnerabilities and protect the organization against similar attacks going forward.

Challenge

After falling victim to a ransomware attack, a charity contacted NCC Group to enlist its support in investigating the incident, assistance in reasserting control of the estate and to stand up critical services. The organization also wanted to strengthen its security capabilities to protect itself against similar attacks going forward.

The organization had a severe lack of resources when it came to cyber security, and its small IT team had been primarily focusing on patching any vulnerabilities as and when they occurred; this combined with a move to some cloud services meant the charity had not had the time or the opportunity to perform necessary upgrades or invest in putting further protections in place.

Solution

NCC Group performed two workstreams in parallel, with the CIRT team establishing the extent of the attack. The SIR team, meanwhile, liaised with key stakeholders at the organization to identify exactly what information was held on the estate, what systems were currently in place and what assets were critical to stand up as soon as possible.

This helped the team to understand how to rebuild the security infrastructure for the organization to operate and to ensure it could handle any potential breaches. One of the vulnerabilities identified during this scoping exercise was the fact that the organization currently utilized single-factor authentication for external services. Collaboration with the CIRT team investigation showed credential stuffing from public breach data to be the successful attack vector.

To allow the client to operate, the team rapidly rebuilt the finance system onto a cloud-based platform based in Microsoft Azure, and secured it with multi-factor authentication and conditional access.

The team also helped the charity rebuild its on-premise Domain Controllers to operate wider services, as well as implementing group policy server hardening to further bolster its security controls. This was combined with a full password reset program with proactive auditing and filtering against known breached accounts.

Finally, the NCC Group SIR team also assisted the charity with getting its network set up to operate via a cloud-based platform and through ExpressRoute, allowing its users to seamlessly access their internal networks.

Results

In addition to the ransomware attack being fully investigated and handled by NCC Group's CIRT, the SIR team was able to rectify many of the vulnerabilities that were illuminated by the attack in the first place.

The project also saved the organization a considerable amount of expenditure in both resources and time. This was particularly notable as the charity was initially considering outsourcing to one of its suppliers. It transpired that this supplier would have continued to use SFA as a security measure, which would not have resolved one of the major vulnerabilities which led to the ransomware attack in the first place.

NCC Group has become a trusted advisor to the organization and continues to work with it, having recently rolled out an Endpoint Detection and Response capability across its estate.