Insight Space

cyber insights programme

nccgroup

Case Study

Response, rapid remediation and solution implementation for a charity organisation

NCC Group provided extensive support to a charity organisation after it fell victim to a ransomware attack.

The support consisted of a full investigation into the root cause of the attack and remediation of the organisation's vulnerabilities to protect the organisation against attacks in the future. NCC Group's support, guidance and expertise enabled the organisation to strengthen its security posture and save valuable time and resources in the process.

AT A GLANCE

Industry/Sector
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 services could be resumed

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

CHALLENGE

After falling victim to the ransomware attack, the charity enlisted NCC Group to investigate the incident, assist it in reasserting control of its estate and restore its critical services. The organisation also wanted to strengthen its security capabilities to protect itself against similar attacks going forward.

The organisation severely lacked resources that it could allocate to cyber security, and its small IT team was primarily focused on patching vulnerabilities as and when they occurred. This shortage, combined with an ongoing move to the cloud, meant that the charity did not have the time or the opportunity to perform or invest in necessary security upgrades and protections.

RESULTS

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

The project also saved the organisation 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 have exacerbated one of the major vulnerabilities which led to the ransomware attack in the first place.

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

SOLUTION

NCC Group performed two workstreams in parallel, with its Cyber Incident Response Team (CIRT) establishing the extent of the attack. Meanwhile, its Remediate team liaised with key stakeholders at the organisation to identify the information that was held on its estate, what systems were currently in place and which assets were mission critical.

The team used this information to rebuild the charity's security infrastructure, enabling it to resume operations and ensuring that it could handle any potential breaches in the future. During the scoping exercise, NCC Group identified that the organisation was using single-factor authentication (SFA) for external services.

By collaborating with the CIRT team's investigation, it identified that the successful attack vector originated from credential stuffing from public breach data. As such, the team rapidly rebuilt the charity's 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 to rebuild its on-premise domain controllers to operate wider services and implement group policy server hardening to further bolster its security controls. This was combined with a full password reset programme with proactive auditing and filtering against known breached accounts.

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

Insight Space

cyber insights programme

nccgroup

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses assess, develop and manage the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

To discuss how you can reduce your ransomware risk, speak to our team today.

+44 (0)161 209 5111

response@nccgroup.com

www.nccgroup.com