TRANSATLANTIC CYBER SECURITY BUSINESS NETWORK

NCSC Annual Review 2021- Key findings

The National Cyber Security Centre (NCSC) published their fifth Annual Review on Wednesday 17th November. The review sets out the NCSC's key achievements and activities between 1st September 2020 and 31st August 2021. These cover a wide range of areas including improving the UK cyber resilience via Active Cyber Defence, actively supporting technology development and research, collaborating with industry, sharing best practice and growing talent.

Below is a selection of the key findings from the review.

The sector

The latest figures on the UK cyber security show the sector is continuing to go from strength to strength with 1,483 companies (up 21%) and 46,683 employees (up 9%). Overall the industry is valued at £8.9bn (up 7% on last year).

The pandemic

Cyber criminals continued to exploit the pandemic as an opportunity with a record year for incidents (777 overall). 20% of these were linked to health care workers and vaccines. The NCSC Takedown Service removed a total of 2.3 million cyber enabled commodity campaigns, including: 442 phishing campaigns which used NHS branding, compared to 105 in the same period in last year's report.

The threats

The cyber threat to the UK and its allies continued to grow and evolve with a range of attacks including indiscriminate phishing scams, ransomware attacks and targeted hostile acts against critical national infrastructure and government. Russia and China are highlighted as producing the majority of global cyber threats while Iran and North Korea are also mentioned.

Ransomware

The NCSC warned that ransomware has become the most significant cyber threat facing the UK this year with attacks across the economy. In the first four months of 2021, the NCSC handled the same number of ransomware incidents as for the whole of 2020 – which was itself a number more than three times greater than in 2019.

Although ransomware attacks gained increased public attention following attacks on Colonial Pipeline in the US early this year, the nature of them has developed further into what is termed Ransomware as a Service, (RaaS). This is where off-the-shelf malware variants and online credentials are available to other criminals for a one-off payment or a share of profits. The NCSC also warn of the now routine "double extortion" where criminals infiltrate data before encrypting victim networks and then threaten to leak this information unless paid.

Supply chain attacks

The SolarWinds attacks and exploitation of Microsoft Exchange Servers have highlighted the threat and impact of sophisticated supply chain attacks. Both of these events which saw actors target managed service providers or commercial software platforms in supply chains are included as case studies within the review. The NCSC warn that similar supply chain incidents are "almost certain over the next 12 months".

Global Leadership

The NCSC describe cyber security as a "global challenge which demands an international response." The review outlines the ongoing efforts of the NCSC and global partners to work together to detect and disrupt shared threats including actively participating in multilateral organisations and standards development organisations and partnering with industry and academia.

Informing Policy

The NCSC provided technical advice to DCMS on the development of the Telecommunications (Security) Bill which proposes new powers for the Secretary of State to remove high risk vendors from the UK's telecoms networks. The NCSC advised on roughly 200 recommendations which a variety of operators will need to follow to ensure the security and resilience of their networks.

The NCSC also helped develop the National Security and Investment Act which will take effect in full from January 2022. The Act covers 17 sensitive sectors of the UK economy such as artificial intelligence to Communications where companies may need to notify Government of an acquisition.

Next steps

The review gives a taste of what the next National Cyber Strategy (NCS) is likely to cover. The Ministerial Forward by Cabinet Office Minister the Rt Hon Steve Barclay MP describes the new NCS as "broadening the scope beyond cyber security to consider the full range of our cyber capabilities and our approach to cyberspace and giving greater weight to the underpinning technologies and the international environment." As well as focussing on the importance of international collaboration and emerging threats, the NCS is also expected to take a "whole of society" approach with important roles for each part of the value chain to play in making the UK resilient to cyber threats.