North East Regional Cyber Crime Unit

Business Cyber Summary

JULY, 2019

The North East Regional Special Operations Unit (NERSOU) is a collaboration between the three forces of Northumbria, Durham and Cleveland. The unit creates additional specialist capacity to deliver an increased response to tackling serious and organised crime that transcends Force borders in the region.

The North East Regional Cyber Crime Unit (NERCCU) is a specialist police unit working within NERSOU to tackle Cyber Crime in line with the national serious and organised crime strategy.

What We Offer

Vulnerability Assessment

Scan your public facing online services for vulnerabilities and find where your business' IT defences are weak

User Awareness Sessions

Staff training for phishing, passwords, securing devices & incident reporting

Cyber Exercising

Simulating cyber attacks to test and improve response plans

Data Leak Searches

Identify any compromised email addresses linked to your organsation from leaked data sets

Cyber Basic Review

A self-assessment set of questions based on Cyber Essentials aimed at securing your business

And more...

To discuss any of the above free services or other services we can offer, please contact us using the details below...

This Edition

Welcome to this introductory newsletter produced by the North East Regional Cyber Crime Unit (NERCCU), we hope for this to be the first of many. The purpose of the newsletter is to continuously engage with those in the North East with the latest information, advice and guidance from the National Cyber Security Centre (NCSC)

June 2019 has seen the NCSC release Top tips for Staff and Small Business Guide: Response & Recovery. Top tips for staff is a new e-learning package which can be completed online, or built into your own training platform. Small Business Guide: Response & Recovery is guidance that helps small to medium sized organisations prepare their response to and plan their recovery from a cyber incident.

@NERCCU

nerccuprotect@durham.pnn.police.uk

www.nersou.org.uk

NCSC News & Blogs

Small businesses given support to bounce back from cyber attacks
The NCSC has published guidance for small businesses looking to prepare their response to and plan their recovery from a cyber incident.
https://www.ncsc.gov.uk/news/small-businesses-given-support-to-bounce-back-from-cyber-attacks

Ryuk ransomware targeting organisations globally
The NCSC is investigating current Ryuk ransomware campaigns targeting organisations globally, including in the UK. In some cases, Emotet and Trickbot infections have also been identified on networks targeted by Ryuk
https://www.ncsc.gov.uk/news/ryuk-advisory

Getting back to business
An easy-to-use guide that helps small businesses prepare their response to (and plan their recovery from) a cyber incident
https://www.ncsc.gov.uk/blog-post/getting-back-to-business

NCSC's new cyber security training for staff now available
The NCSC's new e-learning package 'Top Tips For Staff' can be completed online, or built into your own training platform.
https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available

The bare Essentials
Cyber Essentials is evolving to meet the cyber security challenges of the future
https://www.ncsc.gov.uk/blog-post/bare-essential

For more news and blogs, visit

https://www.ncsc.gov.uk/section/keep-up-to-date/all-blogs

NCSC Weekly Threat Reports

Unsecured database exposes security logs of major hotel chains
Security researchers have discovered an unsecured database that exposed the security logs - and therefore potential cyber security weaknesses - of major hotels managed by the Pyramid Hotel Group
https://www.ncsc.gov.uk/report/weekly-threat-report-7th-june-2019

Organisations still struggle to manage vulnerability patching
Almost 27% of organisations globally have suffered a breach as a result of vulnerabilities that have remained unpatched, according to Tripwire's 2019 Vulnerability Management Survey.
https://www.ncsc.gov.uk/report/weekly-threat-report-7th-june-2019

Microsoft drop password expiration policies
Microsoft has acted to change its security rules meaning users will no longer have to reset credentials periodically
https://www.ncsc.gov.uk/report/weekly-threat-report-7th-june-2019

FBI warns users to be wary of phishing sites abusing HTTPS
This week the FBI issued a warning that too many web users view the padlock symbol and the 'S' on the end of HTTP as a guarantee that a site is trustworthy
https://www.ncsc.gov.uk/report/weekly-threat-report-14th-june-2019

Free decryption tool for GandCrab ransomware
A new decryption tool that counters GandCrab ransomware by allowing victims to retrieve their files for free has been launched. The tool is a collaborative effort by Europol, the UK's National Crime Agency and Met Police, the FBI, cybersecurity company Bitdefender, and others
https://www.ncsc.gov.uk/report/weekly-threat-report-21st-june-2019