Cyber Security
A NSS Centre of Excellence

NHS
National
Services
Scotland

NHS National Services Scotland
Gyle Square
1 South Gyle Crescent
Edinburgh
EH12 9EB
01698 794578

CyberQuarter
Dundee
csoc@nhs.scot

Dear Head of IT Security,

NHS National Services Scotland (NSS) 3rd Party Supplier Assurance Guidance

Assurance of Cyber Security Resilience

This communication is being issued to all 3rd party suppliers contracted by NSS. This guidance is intended to be proportionate in balancing the current threat against the burden of organisations to be appropriately prepared.

Security Problem Statement

Due to events within Ukraine, the National Cyber Security Centre (NCSC) issued guidance to all public sector bodies including the NHS in Scotland. If we are advised by NCSC about a specific increase in threat, such as hostile cyber activity affecting the UK, NSS may seek further assurance from organisations about some or all of the recommended actions. We will also consider mandating action through the NHS high-severity cyber alert process, Network and Information Systems (NIS) Regulations or other means, therefore organisations that supply goods and services to the NHS in Scotland should be prepared to provide rapid assurance.

Immediate Action

We would ask all 3rd party suppliers to complete the following actions as soon as possible. These actions should be straightforward to complete, and provide assurance on critical controls that reduce the risks of ransomware and denial-of-service attacks being carried out either to the organisation in question or NHS NSS.

Patching

Check your patching approach is working as intended, consider if you can apply security updates more quickly. Review all exceptions to you patching polices, including any temporary changes made during the COVIS-19 pandemic response.

Access Control

Implement multi-factor authentication or conditional access policies on privileged accounts, especially Active Directory and Remote Access, wherever possible. Check that passwords are strong, unique and not shared.

Attack Surface

Review your internet facing attack surface as well as leveraging the NCSC https://www.ncsc.gov.uk/information/mailcheck#main Service. Close all unnecessary inbound access routes, particularly https://en.wikipedia.org/wiki/Remote_Desktop_Protocol and https://www.ssh.com/academy/ssh and review justification and risk appetite for those that remain open.

Monitoring

Register with the NCSC https://www.ncsc.gov.uk/information/early-warning-service and regularly review device and system logs for anomalous or unusual activity.

Backups

Ensure backups are in place. Perform test restorations from your last backup, guidance on backups https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world Consider whether you can backup data more frequently without compromising your long-term backups or indeed network performance.

Incident Response and Business Continuity Planning

Check your BCP arrangements are up to date and available to all relevant staff even in the event of a IT systems failure. Consider and agree alternative methods of communication in the event of day to day communication capability becomes unavailable due to system failure or in the event of being under attack.

Awareness

Remind all staff how to spot and report social engineering calls, phishing emails and Smishing texts, and consider a broader https://digital.nhs.uk/keep-it-confidential.

Priority Improvements to Consider

Unsupported Systems

Accelerate migration away from unsupported systems, ensuring you have good processes and effective controls to remain on supported versions.

Incident Exercise

Run an incident response exercise, such as using the scenarios and tools available from https://www.ncsc.gov.uk/information/exercise-in-a-box.

Additional Resource

For further information visit: https://www.ncsc.gov.uk/guidance/actions-to-take-when-the-cyber-threat-is-heightened where you will find the relevant advice, actions and resources.

A link to this document can be found at: https://www.nss.nhs.scot/procurement-and-logistics/existing-suppliers/assurance-of-cyber-security-resilience/

We would also encourage you to follow the NCSC's social media channels: LinkedIn and Twitter for further alerts and updates.

Regards,

Scot Barnett
Head of Cyber
Digital and Security NSS

CC Cyber Centre of Excellence communications