NCSC

NATIONAL CYBER SECURITY CENTRE

Cyber Vitals Checklist V1.0

Background

In today's fast-paced and dynamic digital environment we can expect to see regular fluctuations in the cyber threat landscape. Organisations should be aware of these changes so that at times of heightened cyber threat they can ensure their key security controls are operating effectively.

All organisations can be potential targets for a cyber-attack and by recognising an increased threat and reacting to it, organisations can bolster their defences, accentuate key cyber security tasks and help to reduce your vulnerability to an attack or the impact on your organisation should an attack occur.

There are many factors that may influence an increased change in the threat level. These can include a deteriorating geopolitical situation, the widespread exploitation of discovered vulnerabilities, cybercriminal operations increasing their capabilities or an uplift in malicious cyber-attacks. Organisations need to know what actions they can take during a heightened threat to reduce any vulnerabilities they may have to an attack.

The cyber vitals checklist has been produced by the NCSC to ensure that organisations can check their critical cyber controls are implemented and working correctly. In order to ensure that efforts are prioritised to the most important areas during a heightened threat level, consider delaying significant system changes which are not security related.

Actions to Take

1	**Review Access Control**
a	Check have you enabled multi-factor authentication (MFA) across the network, particularly for privileged accounts or those using remote access. Always use MFA when authenticating to services that hold sensitive or private data.
b	Check have old accounts been disabled, particularly privileged accounts. Confirm that you have implemented role-based access control (RBAC) and the principle of least privilege on all users/services.
c	Check that you have enforced strong and complex passwords for all users. Remind users that passwords should be unique to your business systems and should never be shared across other personal accounts.
d	Check existing privileges for external contractors, ensuring it is the minimum level required, and update/remove where necessary.
2	**Review Your Network Defences**
a	Make sure you have implemented appropriate segregation in your network.[1] Check your firewall rules are up to date and working effectively to prevent unauthorised access and malicious content to your networks.

[1] Layering Network Security Through Segmentation Infographic (cisa.gov)

b	Check that you have anti-virus installed and signatures are up to date. Consider a more comprehensive endpoint detection and response (EDR) solution for larger organisations.
c	Check does your organisation ensure all sensitive data is encrypted in transit and at rest.
d	Confirm if your Intrusion Detection System (IDS) and/or Intrusion Protection System (IPS) are operating effectively, and alerts are being reviewed.
e	Check are you are protected from fraudulent email by implementing Domain-based Message Authentication Reporting and Conformance (DMARC),[2] Domain Keys Identified Mail (DKIM)[3] and Sender Policy Framework (SPF).[4]
3	**Review Vulnerability Management**
a	Check that your organisation has a comprehensive inventory of your assets, particularly of internet facing applications.
b	Confirm the last time a vulnerability scan occurred and make sure all of your hardware and software, particularly edge devices, are kept up to date with the latest security patches. Prioritise patching known exploited vulnerabilities.[5]
c	Turn on automatic updates if possible.
4	**Review Backups**
a	Confirm that your organisation is backing up critical systems and data (such as Active Directory), and that the backup process is operating effectively.
b	Check are you following the 3-2-1 rule – 3 copies, on 2 separate systems, with 1 being 'offline'.
c	Confirm the last time that your organisation tested restoring from backup, and that the test was successful.
5	**Incident Response Plan [6]**
a	Confirm that you have an up-to-date incident response plan which includes the key actions to take, escalation paths and the contact details of external people who can help during an incident, including the NCSC.
b	Check the last time the plan was reviewed and tested.
c	Ensure that the incident response plan and its communication mechanisms will be available, even if systems are not.

[2] dmarc.org – Domain Message Authentication Reporting & Conformance
[3] How to use DKIM for email in your custom domain - Office 365 | Microsoft Docs
[4] Set up SPF to help prevent spoofing - Office 365 | Microsoft Docs
[5] https://www.cisa.gov/known-exploited-vulnerabilities-catalog
[6] Annex 3 of the NCSC Cyber Security Baseline Standard contains a Cyber Incident Response Plan Checklist

6	**Monitoring and Logging**
a	Review your logging and monitoring tools and ensure the coverage and retention is sufficient.
b	Confirm that important logs, such as anti-virus, are monitored and alerts are actioned.
7	**Raise Awareness Among Employees**
a	Brief key staff to raise vigilance of any heightened threats.
b	Confirm that staff have received sufficient training and awareness to spot phishing e-mails and to reduce the chances of them visiting malicious websites or opening unusual e-mails.
c	Remind staff on how to report activity they deem suspicious.
d	Circulate password policies around the organisation to promote the use of strong passwords and improve account security.
8	**NCSC Services**
a	Operators of Essential Services (OES) and Government agencies should ensure they have subscribed to the NCSC's Alerts & Advisories service.
b	Check if your organisation has set up a Malware Information Sharing Platform (MISP) to allow sharing of threat information.
c	Confirm that your incident response plan includes reporting to NCSC, who can provide assistance in investigating and resolving the issue.

Reporting

If you are the victim of a crime, it should be reported to your local Garda station. You may also report cybersecurity incidents to the NCSC at **certreport@decc.gov.ie** or **info@ncsc.gov.ie**.

Further Information

Additional guidance resources can be found on the NCSC website using the following links:

NCSC Guidance

https://twitter.com/ncsc_gov_ie

https://www.ncsc.gov.ie/