GUIDANCE

10 Steps to Cyber Security

Guidance on how organisations can protect themselves in cyberspace.

IN THIS GUIDANCE

PUBLISHED

11 May 2021

REVIEWED

11 May 2021

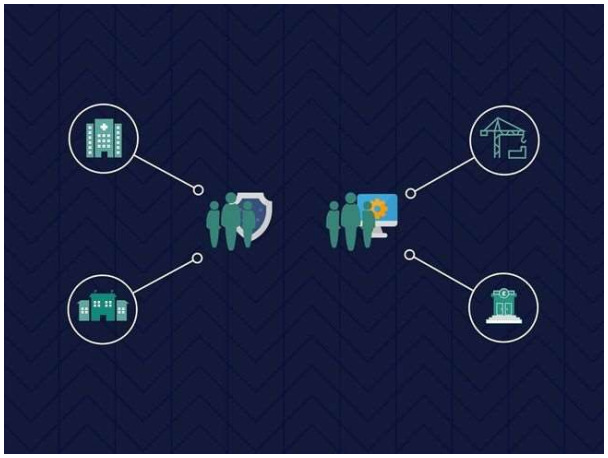
VERSION

1.0

WRITTEN FOR

Cyber security professionals

Architecture and configuration



Design, build, maintain and manage systems securely.

The technology and cyber security landscape is constantly evolving. To address this, organisations need to ensure that good cyber security is baked into their systems and services from the outset, and that those systems and services can be maintained and updated to adapt effectively to emerging threats and risks.

What are the benefits?

- **Getting security right at the start of any development helps to create systems that are easier to keep secure, and can reduce the need for any costly rework in the future**
- **A well architected and configured system or service will help you gain confidence that your security controls are mitigating the risks that your organisation cares about**
- **Being able to manage your systems securely, and maintain their security over time**

What should you do?

Understand what you are building and why

- Understand the context before designing a system, including the risks your organisation are, and are not, willing to accept, and the threat model for your system. Identifying the most critical systems and components in relation to your organisational objectives will help you focus your effort in the right places. Choose security controls based on the risks identified, and how effective they are at mitigating the types of attacks you expect, based on that threat model
- Consider the expected lifetime of your systems, and how they can adapt to an evolving context. The cyber security landscape changes rapidly, so systems will need to adapt to new and emerging threats to remain secure. Ensure that your approach to system development and delivery can help you evolve your security controls to keep pace.

Make systems easy to maintain and update

- Before designing a system, consider if there are existing, securely designed products or services that you can make use of (instead of investing in the resource and expertise necessary to implement it all yourself). For example, consider how to benefit from the shared responsibility model of cloud services. Using concepts such as Platform as a Service

(PaaS) and Software as a Service (SaaS) allows you to shift some of the responsibility for the management of the underlying technology and its security to the service provider, allowing you to focus more of your effort on the applications and services that are bespoke to you. You will also benefit from the vendor's investment and expertise in security. You should still seek assurance that the service delivered by the cloud provider meets your needs.

- Design systems so that security updates can be applied as soon as they become available, in ways that minimise your exposure to vulnerabilities without adversely affecting the availability of your system.
- Use configuration management technologies such as Mobile Device Management systems and use Infrastructure as Code to formalise system deployments so that it is easier to track, update and re-deploy systems over time.

Make compromise and disruption difficult

- Make compromise harder by adopting a layered approach to security so that an attacker would have to get through multiple controls to be successful. Consider using a framework such as MITRE ATT&CK to help identify possible ways of disrupting an attacker at different stages of an attack.
- Reduce the attack surface by protecting external interfaces and removing or disabling configurations and features that aren't required such as accounts, software and demo capabilities. This should include:
    - applying secure configurations to servers and end user devices to restrict the options available to an attacker
    - not trusting data from external sources; where required, transform, validate or safely render data from external or less trusted sources (so that it can't be used to craft an attack against your systems)
    - making it harder for email from your domains to be spoofed to make convincing phishing emails by employing anti-spoofing controls, including DMARC, SPF and DKIM

- Choose products and services that are designed to be secure by default. This reduces the effort required to deploy products in a secure manner, and gives greater confidence that they will remain secure over time.
- Make it easy for users to do the right thing. Security breaches often occur because users have developed workarounds for system inadequacies. Be sure to consider the potential for this and identify any methods users might resort to when circumventing security features.
- Understand the limitations of your systems and consider how you will deal with Denial of Service attacks, whether or not they are malicious. This could include upstream defences via your service providers, options for scaling your systems, and what response planning and testing should cover. Ensure you consider cost protections (for example to limit spending when enabling auto-scaling cloud resources).
- Prefer tried and tested approaches to security and ensure you have the right expertise when building a bespoke solution. Avoid commonly used architectural anti-patterns which can reduce system security.
- Gain confidence that the security controls chosen are genuine and effective at mitigating your risks, and seek independent validation for the most critical controls.

Reduce the impact of compromise

- Reduce the impact of compromise by preventing lateral movement and making it easier to recover. After an initial compromise, attackers will typically attempt to gain access to other systems and data. Make it harder for an attacker to reach their target once in the network by protecting your data and communications, and ensuring critical components are more isolated using segregated networks or adopting a zero trust architecture.
- Prevent malware from running on devices if it does reach you. Use antivirus applications that can detect threats based on known signatures and behavioural analysis to increase the chance of spotting emerging threats. Configure application controls to only allow authorised executables to run and

disable macros for users and applications if they are not required.

- Plan for backup and recovery. Ensure that your plans include data and services, such as relevant configurations and accounts, and that you have tested your plans so that you are able to respond effectively in the event of a major incident such as a ransomware attack. You should have backups that remain protected and can be accessed in the event of a significant incident.

Make it easy to detect and investigate compromises

- Design your communication flows so that it is easier for you to detect a compromise. Use clearly defined and tightly constrained communication methods between components and restrict flows using allow and deny lists so that malicious behaviour is more likely to stand out from normal operations.
- Collect logs and monitor your systems to help you detect and investigate possible compromises. Ensure that your logging and monitoring systems are sufficiently separated so that it is hard for an attacker to hide their tracks by deleting or altering logs.

Safely develop and manage systems

- Control and manage the way changes to your systems and services are made. Use a combination of technical and policy controls to ensure that all changes are authorised and have undergone appropriate checks to gain confidence that they will not adversely affect live services. Design these controls to make it easy and quick to apply security updates and fix vulnerabilities, so that exposure to known vulnerabilities can be minimised.
- Secure your development and deployment processes. Make it hard for accidental or malicious changes to impact your systems by protecting your code repositories and your pipelines for build and deployment. You should include human and machine-based checks (such as code review and automated code analysis) to detect unauthorised changes and help prevent vulnerabilities from being introduced. Ensure credentials and secrets are protected and separated from source code.

- Gain trust in the devices used to manage your systems. If an attacker compromises one of these devices (for example through a phishing attack), they could inherit the same level of access. Use Privileged Access Workstations for managing any systems you deem critical for your organisation.
- Protect your management interfaces to make it harder for an attacker to access critical functions. Restrict access to administrative interfaces, including SSH, RDP and web consoles, to trusted locations or devices and ensure multi-factor authentication is enabled for administrative accounts. Ensure you can still gain access in an emergency by having a 'break-glass' procedure in the event of a system or device failure.

Learn more

Mobile device guidance
Help for organisations from choosing and purchasing devices to the advice you give the end users.

Secure system administration guidance
Explains how to develop and implement your own secure system administration strategy.

Secure design principles
Guides for the design of cyber secure systems.

Cloud security guidance
Guidance on how to configure, deploy and use cloud services securely.

Denial of service (DoS) Guidance
Guidance to help organisations understand and mitigate DoS attacks.

Mitigating malware and ransomware attacks
How to defend organisations against malware or ransomware attacks.

Phishing attacks: defending your organisation
How to defend your organisation from email phishing attacks.

Preventing lateral movement
Guidance for preventing lateral movement in enterprise networks.

Application development

Recommendations for the secure development, procurement and deployment of generic and platform-specific applications.

← Asset management

Vulnerability management →

Topics

Operational security

Risk management

Configuration management

Security architecture

PUBLISHED

11 May 2021

REVIEWED

11 May 2021

VERSION

1.0

WRITTEN FOR

Cyber security professionals

Also see

Weekly Threat Report 23rd July 2021

The NCSC's weekly threat report is drawn from recent open source...

Report
23 July 2021

The first Certified Cyber Professional (CCP) Specialism is now live!

'Risk Management' is the first certifiable specialism under the...

Blog Post
8 July 2021

NCSC statement on Kaseya incident

The NCSC's official statement on the Kaseya cyber incident.

News
5 July 2021