National Cyber Security Centre
a part of GCHQ

Guidance ()

10 Steps: Executive Summary

Created: 29 Sep 2015
Updated: 08 Aug 2016
Part of: 10 Steps to Cyber Security (/guidance/10-steps-cyber-security)

Guidance on how organisations can protect themselves in cyberspace, including the 10 steps to cyber security.

Introduction

This guidance is designed for organisations looking to protect themselves in cyberspace. The 10 Steps to Cyber Security was originally published in 2012 and is now used by a majority of the FTSE350. The 10 steps guidance is complemented by the paper Common Cyber Attacks: Reducing The Impact(/white-papers/common-cyber-attacks-reducing-impact). This paper sets out what a common cyber attack looks like and how attackers typically undertake them. We believe that understanding the cyber environment and adopting an approach aligned with the 10 Steps is an effective means to help protect your organisation from attacks.

10 Steps To Cyber Security: At-a-glance

An effective approach to cyber security starts with establishing an effective organisational risk management regime (shown at the centre of the following diagram). This regime and the 9 steps that surround it are described below.

Download the NCSC 10 Steps To Cyber Security infographic (PDF)(/file/1473/download?token=eLNoAX4O)

Risk Management Regime

Embed an appropriate risk management regime across the organisation. This should be supported by an empowered governance structure, which is actively supported by the board and senior managers. Clearly communicate your approach to risk management with the development of applicable policies and practices. These should aim to ensure that all employees, contractors and suppliers are aware of the approach, how decisions are made, and any applicable risk boundaries.

Secure configuration

Having an approach to identify baseline technology builds and processes for ensuring configuration management can greatly improve the security of systems. You should develop a strategy to remove or disable unnecessary functionality from systems, and to quickly fix known vulnerabilities, usually via patching. Failure to do so is likely to result in increased risk of compromise of systems and information.

Network security

The connections from your networks to the Internet, and other partner networks, expose your systems and technologies to attack. By creating and implementing some simple policies and appropriate architectural and technical responses, you can reduce the chances of these attacks succeeding (or causing harm to your organisation). Your organisation's networks almost certainly span many sites and the use of mobile or remote working, and cloud services, makes defining a fixed network boundary difficult. Rather than focusing purely on physical connections, think about where your data is stored and processed, and where an attacker would have the opportunity to interfere with it.

Managing user privileges

If users are provided with unnecessary system privileges or data access rights, then the impact of misuse or compromise of that users account will be more severe than it need be. All users should be provided with a reasonable (but minimal) level of system privileges and rights needed for their role. The granting of highly elevated system privileges should be carefully controlled and managed. This principle is sometimes referred to as ‘least privilege’.

User education and awareness

Users have a critical role to play in their organisation’s security and so it's important that security rules and the technology provided enable users to do their job as well as help keep the organisation secure. This can be supported by a systematic delivery of awareness programmes and training that deliver security expertise as well as helping to establish a security-conscious culture.

Incident management

All organisations will experience security incidents at some point. Investment in establishing effective incident management policies and processes will help to improve resilience, support business continuity, improve customer and stakeholder confidence and potentially reduce any impact. You should identify recognised sources (internal or external) of specialist incident management expertise.

Malware prevention

Malicious software, or malware is an umbrella term to cover any code or content that could have a malicious, undesirable impact on systems. Any exchange of information carries with it a degree of risk that malware might be exchanged, which could seriously impact your systems and services. The risk may be reduced by developing and implementing appropriate anti-malware policies as part of an overall 'defence in depth' approach.

Monitoring

System monitoring provides a capability that aims to detect actual or attempted attacks on systems and business services. Good monitoring is essential in order to effectively respond to attacks. In addition, monitoring allows you to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is often a key capability needed to comply with legal or regulatory requirements.

Removable media controls

Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. You should be clear about the business need to use removable media and apply appropriate security controls to its use.

Home and mobile working

Mobile working and remote system access offers great benefits, but exposes new risks that need to be managed. You should establish risk based policies and procedures that support mobile working or remote access to systems that are applicable to users, as well as service providers. Train users on the secure use of their mobile devices in the environments they are likely to be working in.

NCSC 10 Steps to Cyber Security Infographic.pdf
(https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/NCSC%2010%20Steps%20To%20Cyber%20Security%20NCSC.pdf)

PDF, 399.05KB

This file may not be suitable for users of assistive technology.

Topics

Risk management(/topics/risk-management)
Cyber attacks(/topics/cyber-attacks)

Was this guidance helpful?

We need your feedback to improve this content.

Yes No