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

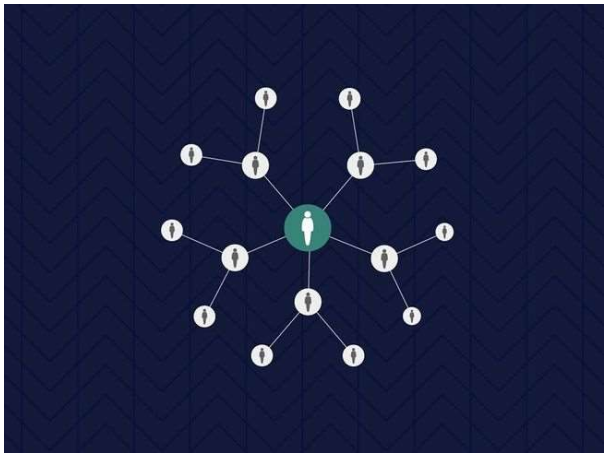
VERSION

1.0

WRITTEN FOR

Cyber security professionals

Identity and access management



Control who and what can access your systems and data.

Access to data, systems and services need to be protected. Understanding who or what needs access, and under what conditions, is just as important as knowing who needs to be kept out. You must choose appropriate methods to establish and prove the identity of users, devices,

or systems, with enough confidence to make access control decisions. A good approach to identity and access management will make it hard for attackers to pretend they are legitimate, whilst keeping it as simple as possible for legitimate users to access what they need.

What are the benefits?

- **Only individuals and systems that are authorised to have access to data or services are allowed to do so**
- **Less impact on staff's workday by getting identity and access management right across an organisation**
- **Smoother collaboration with customers, suppliers, and partners**
- **More effective security monitoring and other controls that require identity and access management to function effectively**

What should you do?

Develop appropriate identity and access management policies and processes

- In the first place, consider how you establish identity. Ensure you have an identity and access management policy that covers **who** should have access to which systems, data or functionality, **why**, and under **what** circumstances. Make sure you consider all potential types of user including full and part-time staff, contractors, volunteers, students and visitors.
- Ensure the policy covers what and how audit records are acquired, and how they are safeguarded against tampering, and an identification of which actions or processes, if any, should require more than one person to perform or authorise them.
- Policies should not just cover systems you control, but also wherever your organisational identities can be used (for example, what websites or online services can staff create an account by using their work email address). Single sign-on (SSO)

may be available using your organisational identity for some online services to help you control access to those services (and revoke access along with someone's work account when they leave your organisation).

- Ensure your account management processes includes a 'joiners, movers and leavers' policy, so access can be revoked when no longer needed, or changed for movers. Temporary accounts (perhaps created to test processes) should also be removed or suspended when no longer required.
- If third parties require access to your systems, make sure that you have non-disclosure agreements in place and can revoke any accesses when necessary.

Consider multi-factor authentication for all user accounts

- Choose authentication methods that are proportionate to the risk and support the ways in which people naturally work. Ensure you consider user-to-service, user-to-device, and device-to-service authentication.
- Implement multi-factor authentication (MFA) - also known as or two-factor authentication - on any accounts for online services to protect against password guessing and theft. Where appropriate, offer people a choice of factors to self authenticate, as no single method will suit everyone (or all environments or devices). These may include SMS or email messages, biometrics or physical tokens.
- Where passwords are required, implement a password policy that appropriately balances usability and security. You should aim to minimise the number and complexity of passwords that your users need to remember, for example, by using single sign-on or allowing password managers. This will help to discourage insecure practices (such as reusing passwords, choosing easy-to-guess passwords, or writing them down). Implement technical controls such as MFA, account throttling or lockouts, monitoring for suspicious behaviour, and preventing the use of weak or exposed passwords to help prevent and detect password-based attacks.
- Ensure credentials are adequately protected both at rest and in transit.

Use MFA and other mitigations for privileged accounts

- Use a tiered model for administrative accounts and only use accounts with full privileges (like domain admin, global admin, or cloud admin accounts) when absolutely necessary.
- Ensure multi-factor authentication is enabled for administrative accounts and consider the use of strong authentication methods such as hardware security tokens and factors such as location or time for making a risk-based decision to allow access, depending on the circumstances and attempted activity.
- Ensure admins have separate user accounts for day-to-day business (such as email and internet browsing) and another for activities requiring their administrative privileges. These accounts should adequately separated, for example by using separate devices or a browse-down approach, and consider blocking any unnecessary web and email access on those devices. This limits exposure to spear phishing, and makes it harder to achieve wide system access through a single vulnerability. These considerations may also apply to other users with greater accesses, for example those approving financial payments or developers who can commit changes to any software your organisation relies on.
- Review user accounts and systems for unnecessary privileges on a regular basis, and ensure privileged accesses are revoked when no longer required.

Employ security monitoring to detect potential malicious behaviour

- Ensure authentication and authorisation events are logged and monitored for suspicious behaviour that may indicate a potential compromise. Indicators of malicious behaviour could include login attempts that fail the second step of MFA, attempts from unexpected geographical areas, brute-forcing of account passwords (including password spraying), or reports of unexpected account throttling or lockouts.
- Design your access control systems to allow for easy monitoring of account usage and accesses, and ensure you can associate all

actions in the system to the person or account that performed them (for example, in a web service all API calls performed might be linked to access tokens).

Learn more

Introduction to identity and access management
This guidance provides a primer on the essential techniques, technologies and uses of access management.

Multi-factor authentication for online services
Advice for organisations on implementing multi-factor authentication (or two-factor authentication) to protect against password guessing and theft on online services.

Password administration for system owners
Password strategies that can help your organisation remain secure.

Biometric recognition and authentication systems
Understanding biometric recognition technologies, and how to build secure authentication systems.

Protecting SMS messages used in critical business processes
Security advice for organisations using text messages to communicate with end users.

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

← Vulnerability management

Data security →

Topics

Authentication
Operational security
Risk management

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