National Cyber Security Centre
a part of GCHQ

NIS Guidance Collection

v1.0 [29 May 2018]

Introduction to the NIS Directive

Details on who is affected, the role of the NCSC, and how to comply. Start here if you are in any doubt.

1. General introduction

The UK is implementing the EU directive on the security of Networks and Information Systems (known as the NIS Directive). Network and information systems and the essential services they support play a vital role in society, from ensuring the supply of electricity and water, to the provision of healthcare and passenger and freight transport. Their reliability and security are essential to everyday activities.

The EU recognised that any cyber security incident could affect a number of Member States and in 2013 put forward a proposal to improve the EU's preparedness for a cyber attack. This proposal became a directive in August 2016, giving Member States 21 months to embed the Directive into their respective national laws.

As we have seen from numerous cyber security incidents these systems can be an attractive target for malicious actors, and they can also be susceptible to disruption through single points of failure. Incidents affecting any of these systems could cause significant damage to the UK's infrastructure, economy, or result in substantial financial losses. The magnitude, frequency and impact of network and information system security incidents is increasing. Events such as the 2017 WannaCry ransomware attack, the 2016 attacks on US water utilities, and the 2015 attack on Ukraine's electricity network clearly highlight the impact that incidents can have.

There is therefore a need to improve the security of network and information systems across the UK, with a particular focus on essential services which if disrupted, could potentially cause significant damage to the economy, society and individuals' welfare.

2. What does the NIS Directive cover and when will it be implemented into UK law?

The NIS Directive aims to raise levels of the overall security and resilience of network and information systems across the EU. The Directive provides the legal footing to:
The deadline for member states transposing the Directive into domestic legislation is **9 May 2018**.

The UK government undertook a Public Consultation during the summer of 2017 to seek views from industry, regulators and other interested parties on the government's plans to transpose the Directive into UK legislation. It set out the government's proposed transposition approach and asked a series of questions on a range of detailed policy issues relating to transposition.

The government's Response to the Consultation provides more detail on the revised approach to implementation and what can be expected during the initial phases.

- Ensure that Member States have in place a national framework so that they are equipped to manage cyber security incidents and oversee the application of the Directive. This includes a National Cyber Security Strategy, a Computer Security Incident Response Team (CSIRT), and a national NIS competent authority, or competent authorities.
- Set up a Cooperation Group among Member States to support and facilitate strategic cooperation and the exchange of information. The Member States will also need to participate in a CSIRT Network to promote

swift and effective operational cooperation on specific network and information system security incidents as well as sharing information about risks.

- Ensure that organisations within vital sectors which rely heavily on information networks, for example utilities, healthcare, transport, and digital infrastructure sectors, are identified by each Member State as "operators of essential services" (OES). Those OES will have to take appropriate and proportionate security measures to manage risks to their network and information systems, and they will be required to notify serious incidents to the relevant national authority. The participation of industry is therefore crucial in the implementation of the directive.

3. Essential Services: Who does the NIS Directive apply to?

Companies and organisations identified as either operators of essential services (OES) or Competent Authorities (CAs) are primarily involved. The criteria for identifying OES and the list of CAs in the UK can be found within the **government response to the consultation**.

Some sectors are exempt from some aspects of the Directive where there are provisions within their existing regulations which are, or will be, at least equivalent to those the NIS Directive specifies (eg finance and civil nuclear sectors). The technical guidance we produce will be widely applicable, and all sectors should take note of it.

4. The NCSC role in the implementation of the NIS Directive

The NCSC is providing technical support and guidance to other government departments, Devolved Adminstrations, CAs and OES through:

- a set of cyber security principles for securing essential services
- a collection of supporting guidance
- a Cyber Assessment Framework (CAF) incorporating indicators of good practice
- implementation guidance and support to CAs to enable them to:
- adapt the NCSC NIS principles for use in their sectors
- plan and undertake assessments using the CAF and interpret the results

The NCSC has the following three roles in support of the NIS Directive:

- Single Point of Contact (SPOC) - we'll act as the contact point for engagement with EU partners on NIS, coordinating requests for action or information and submitting annual incident statistics.
- CSIRT (Computer Security Incident Response Team) - incidents that are believed to be reportable under the NIS Directive MUST be reported to the appropriate Competent Authority. Where they are identified or suspected of having a cyber security aspect the operator is also strongly encouraged to contact NCSC for advice and support as appropriate.
- Technical Authority on Cyber Security - the NCSC will support OES and CAs with cyber security advice and guidance and act as a source of technical expertise. We may work with OES and CAs to tailor some generic guidance to individual sectors if necessary.

The NCSC will have no regulatory role in NIS.

5. How our guidance is intended to be used - the outcome-based approach

The implementation of the NIS Directive is an opportunity to put mechanisms in place that drive real improvements to national cyber security. NCSC is committed to working constructively with CAs and OES to help ensure that NIS regulatory requirements are defined and used to promote and support effective cyber risk management. This objective has shaped the NCSC approach throughout.

While recognising the risk of over-simplifying a complex subject, there are two basic approaches available when aiming to drive change towards a recognised desirable end-state. The first approach is to create a set of prescriptive rules that, if closely followed, will result in achieving the desirable end-state.

The second approach is to define a set of principles that, if consistently used to guide decision-making, will collectively result in the desirable end-state. Much has been written about the advantages and disadvantages of the two approaches, but it is the NCSC view that the principles-based approach is more effective as a way of driving improvements to cyber security in the context of the NIS Directive.

To work well, a set of prescriptive rules needs to cater for all eventualities. When this is possible, and the rules are followed, the approach can deliver what is required. However, in complex topic areas and rapidly changing circumstances, it may be impossible to cater for all eventualities. In such cases, which include cyber security, all attempts to devise and apply a set of prescriptive rules is almost certain to lead to unintended consequences, resources being badly misallocated, and limited benefit.

While it is not possible to devise an effective set of prescriptive rules for good cyber security, it is possible to state a set of principles as a guide to cyber security decision-making. NCSC has developed such a set of principles for the implementation of the NIS Directive.

The NIS cyber security principles define a set of top-level outcomes that, collectively, describes good cyber security for operators of essential services. Each principle is accompanied by a narrative which provides more detail, including why the principle is important.

Additionally, each principle is supported by a collection of relevant guidance which both highlights some of the relevant factors that an organisation will usually need to take into account when deciding how to achieve the outcome, and recommends some ways to tackle common cyber security challenges.

Some organisations may be concerned that the principles and guidance are too vague. It is important to recognise that the NCSC intent is not to produce an all-encompassing cyber security "to do" list – an unachievable goal in any case. Organisations understand their own business better than any external entity, and should be capable of taking informed, balanced decisions about how they achieve the outcomes specified by the principles. NCSC expects the principles and guidance to be used in the following way by operators of essential services:

- Understand the principles and why they are important. Interpret the principles for the organisation.
- Compare the outcomes described in the principles to the organisation's current practices. Use the guidance to inform the comparison.
- Identify shortcomings. Understand the seriousness of shortcomings using organisational context and prioritise.
- Implement prioritised remediation. Use the guidance to inform remediation activities.

6. The relationship between NCSC, Competent Authorities and Operators of Essential Services

While the implementation of the NIS Directive will significantly expand the scope of cyber security regulation in the UK, it will not fundamentally alter the role of NCSC (although we will be taking

on the formal roles of CSIRT and Single Point of Contact within the national framework). The key point is that regulatory responsibilities under NIS will be carried out by the new Competent Authorities (CAs), not NCSC. Within the general UK cyber security regulatory environment, including NIS, NCSC's aim is to operate (as now) as a trusted, expert and impartial advisor to all interested parties.

To help ensure that the Directive delivers the intended improvements in cyber security, NCSC will be supporting the NIS CAs in a number of specific ways. For example, we will assist NIS CAs by developing cyber security standards and guidance, and by helping them build their internal cyber security expertise through accessing suitable training.

However, some important constraints will govern how NCSC works with CAs, in order to maintain the benefits that result from the open and collaborative relationship NCSC enjoys with most of the organisations that fall under the scope of NIS.

There will be strong restrictions on the type of cyber security information that NCSC shares with the CAs, and those restrictions will be designed to address concerns about how information considered sensitive by industry and other organisations is handled in the NIS regulatory environment. And, while NCSC will be advising the CAs on how to do cyber security assessments against the NIS standards, we will not be undertaking regulatory assessments on behalf of the CAs.

More detail about how the NCSC works with NIS CAs will be made available when the CAs have been fully established.

Objective A. Managing security risk

Appropriate organisational structures, policies, and processes are in place to understand, assess and systematically manage security risks to the network and information systems supporting essential services.

Principles under this Objective

A1. Governance

Putting in place the policies and processes which govern your organisation's approach to the security of network and information systems.

A2. Risk Management

Identification, assessment and understanding of security risks. And the establishment of an overall organisational approach to risk management.

A3. Asset management

Determining and understanding all systems and/or services required to maintain or support essential services.

A4. Supply chain

Understanding and managing the security risks to networks and information systems which arise from dependencies on external suppliers.

A1. Governance

Principle

The organisation has appropriate management policies and processes in place to govern its approach to the security of network and information systems.

Description

Effective security of network and information systems should be driven by organisational management and corresponding policies and practices. There should be clear governance structures in place with well-defined lines of responsibility and accountability for the security of network and information systems.

Senior management should clearly articulate unacceptable impacts to the business (often called *risk appetite*), which should take into account the organisation’s role in the delivery of essential services, so decision makers at all levels can make informed decisions about risk without constantly referring decisions up the governance chain.

There should be an individual(s) who holds overall responsibility and is accountable for security. This individual is empowered and accountable for decisions regarding how services are protected. For small organisations, the governance structure can be very simple.

Guidance

NCSC Introduction to Security Governance

Your organisation's approach to security governance needs to be an appropriate fit for your organisation. Good security governance is integrated with your business's usual decision making structures and processes.

Decisions about risk can be made at all levels of your organisation when delegated effectively to people with the right security, business and technical knowledge, skills and experience. Clear lines of communication are also necessary.

Risk management standards

Following a standardised risk management approach can help in achieving good cyber security governance. There are many such standards to choose from. Some of the most well-known for NIS sectors are:

ISO 27001

An Information Security Management System can aid governance of cyber security risk

An Information Security Management System (ISMS) is a set of policies, procedures, and roles designed to ensure cyber security risks are identified and managed. Traditionally an ISMS is considered to be an information risk management system, however it can be used to manage cyber security risks to essential services.

A properly scoped and implemented ISMS can help your organisation to meet the requirements of the NIS Directive by putting in place policies, procedures, and roles which govern the organisational approach to managing cyber security risks to essential services.

ISO 27001 is one of many standards you can use to implement an ISMS. If your organisation is intending to use ISO 27001, you should consider which elements will help achieve your organisational objectives - full compliance and certification may be unnecessary.

Your organisation must incorporate into the ISMS any relevant external requirements, for example direction from the competent authority. You should also set appropriate cyber security requirements for your supply chain to ensure their support in achieving your NIS objectives (see A4 Supply Chain Security).

IEC 62443-2-1:2010

An industrial automation and control system (IACS) cyber security management system (CSMS) that is relevant to particular essential service sectors.

The CSMS defined in IEC 62443-2-1 is designed to build on ISO 27001 & 27002 for IACS environments, with the aim of aligning cyber security risk management with existing safety risk management practices. A management system framework is provided as a baseline, which organisations are encouraged to tailor for their own context.

References

NCSC Introduction to Security Governance
ISO 27001
IEC 62443-2-1:2010

A2. Risk management

Principle

The organisation takes appropriate steps to identify, assess and understand security risks to the network and information systems supporting the delivery of essential services. This includes an overall organisational approach to risk management.

Description

There is no single blueprint for cyber security and therefore organisations need to take steps to determine security risks that could affect the delivery of essential services and take measures to appropriately manage those risks.

Threats can come from many sources, in and outside the organisation. A good understanding of the threat landscape and the vulnerabilities that may be exploited is essential to effectively identify and manage risks.
Such information may come from sources including NCSC, information exchanges relevant to the organisation's sector, and reputable government, commercial, and open sources, all of which can inform the organisation's own risk assessment process.

Organisations may contribute to the understanding of threats and vulnerabilities in their sector by participating in relevant information exchanges and liaising with authorities as appropriate.

There should be a systematic process in place to ensure that identified risks are managed and the organisation has confidence mitigations are working effectively. Confidence can be gained through, for example, product assurance, monitoring, vulnerability testing, auditing and supply chain security.

Guidance

NCSC Risk Management Guidance

Our Risk Management guidance aims to help you to choose an approach that's right for your organisation.

Operators of essential services are likely to benefit from a combination of a system-based approach, which looks at the interactions between components of the service, and a component-driven analysis, which considers the threats, vulnerabilities, and impacts relevant to particular critical components.

Risk methods and frameworks

Your organisation should choose a method or framework for managing risk that fits with the organisation's business and technology needs. The NCSC has summarised some commonly used risk methods and frameworks as a starting point.

Whichever approach you choose, the scope of your programme must include all systems relevant to the operation of essential services. Simply following the minimum requirements of a standard or applying blanket controls across the organisation is unlikely to adequately manage risks to critical systems.

Where industrial control and automation systems are in scope of the essential service, you should keep in mind that controls suitable for managing risks on the corporate IT network may be inappropriate or damaging in an operational technology environment.

These systems will likely require a more tailored approach, and some frameworks and standards address specific concerns relating to such systems.

Cyber security assurance

Various means are available to gain confidence in the effectiveness of the security of technologies, processes and people.

The NCSC assurance blog provides some examples that may be useful to understand cyber security confidence in your organisation and there are some specific technical NCSC guides:

NCSC Penetration Testing Guidance
This guidance will help you understand the proper use and commissioning of penetration tests to gain assurance in the security of an IT system.
NCSC Cloud Security Collection: Having confidence in cyber security
Our Cloud Security Collection provides guidance on managing the risks involved with using cloud services, and some of the principles and guidance are more broadly applicable.

The cloud guidance for having confidence in cyber security provides principles that are useful for assuring cyber security effectiveness of essential services. The collection will be of particular interest if your organisation hosts any part of your essential service infrastructure on a cloud service.

References

NCSC Risk Management Guidance
NCSC Assurance Blog
NCSC Penetration Testing Guidance
NCSC Cloud Security Collection: Having confidence in cyber security
Risk frameworks and methods

A3. Asset management

Principle

Everything required to deliver, maintain or support networks and information systems for essential services is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).

Description

In order to manage security risks to the network and information systems of essential services, organisations require a clear understanding of service dependencies.

This understanding might include physical assets, software, data, essential staff and utilities. These should all be clearly identified and recorded so that it is possible to understand what things are important to the delivery of the essential service and why.

Guidance

Whichever risk management method your organisation uses, asset management will play a key role as you cannot effectively manage risks without understanding what assets are part of the essential service.

Your asset management regime should consider all relevant assets, and dependencies between them. Dependencies may be identified between assets under your organisation's control (including IT and OT domains), elements of the supply chain (including power), and key staff who are critical to operations.

Assets in an operational technology environment may need a more tailored approach than the corporate IT assets.

For asset management to be effective, up to date knowledge of your assets must be maintained throughout their lifecycle.

ISO 27001/2

Asset management is part of an ISO 27001 ISMS, but management of critical assets may require a tailored approach

An Information Security Management System (ISMS) is a set of policies, procedures, and roles designed to ensure cyber security risks are identified and managed. Traditionally an ISMS is considered to be an information risk management system, however it can be used to manage cyber security risks to essential services.

If your organisation is using an ISMS as a tool for compliance with the NIS Directive, you must ensure the scope includes all systems relevant to the operation of essential services. Asset management is a key part of an ISMS, although critical services may need more attention than the minimum requirements of the standard. Further guidance is detailed in ISO 27002.

ISO 55001 - Asset Management

This standard aligns with ISO 27001 and can be used in conjunction with it or independent of it. It outlines requirements for a generic asset management system. An organisation following this standard as a tool for NIS compliance must ensure the scope encompasses critical

systems. Section 4.2 covers needs and expectations of stakeholders, which must include any requirements from competent authorities.

ITIL
ITIL best practice recommends a staged approach to IT asset management. You may find this useful for improving management of your IT assets, but must keep in mind that there may be assets and dependencies beyond the corporate IT domain as outlined above.

References
ISO 27001/2
ISO 55001 - Asset Management
ITIL

A4. Supply chain

Principle
The organisation understands and manages security risks to networks and information systems supporting the delivery of essential services that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.

Description
If an organisation relies on third parties (such as outsourced or cloud based technology services) it remains accountable for the protection of any essential service. This means that there should be confidence that all relevant security requirements are met regardless of whether the organisation or a third party delivers the service.

For many organisations, it will make good sense to use third party technology services. Where these are used, it is important that contractual agreements provide provisions for the protection of things upon which the essential service depends.

Guidance
Operators of essential services need to ensure that when third party suppliers are used, all relevant security requirements are met. This means that a number of specific supply chain related security considerations should be addressed where relevant to the provision of the essential service. This might include:

- Ensuring the protection of data shared with a third party. This includes protecting data from actions such as unauthorised access, modification, or deletion that may cause disruption to the essential services (see Principle B3).
- Effective specification of the security properties of products or services procured from a third party that are important for the protection of the essential service. This should include the security requirements derived from the rest of these Principles.
- Ensure that any network connections or data sharing with third parties do not introduce unmanaged vulnerabilities that have the potential to affect the security of the essential service.

- Confidence that third party suppliers are trustworthy such that malicious attempts to subvert the security of products or systems that could affect the essential service are managed.

NCSC Supply Chain Security

Our guidance on supply chain security gives an overview of supply chain risks and indicators of good practice. It also provides references to further reading and guidance.

Cloud service security

Where your organisation relies upon a cloud service, you should have confidence in the cyber security measures in place.

Consider cloud-specific supply chain assurance guidance in NCSC cloud security principle 8: supply chain together with many cloud security assurance resources, including industry schemes such as the Cloud Security Alliance (CSA) Security, Trust & Assurance Registry (STAR) academic research and cloud provider information.

References

NCSC Supply Chain Security
NCSC Cloud Security Principle 8: Supply Chain Security
Cloud Security Alliance (CSA) Security, Trust & Assurance Registry (STAR)

Objective B: Protecting against cyber attack

Proportionate security measures are in place to protect essential services and systems from cyber attack.

Principles under this Objective

B1. Service protection policies and processes

Defining and communicating appropriate organisational policies and processes to secure systems and data that support the delivery of essential services.

B2. Identity and access control

Understanding, documenting and controlling access to essential services systems and functions.

B3. Data Security

Protecting stored or electronically transmitted data from actions that may cause disruption to essential services.

B4. System security

Protecting critical network and information systems and technology from cyber attack.

B5. Resilient networks and systems

Building resilience against cyber attack.

B6. Staff awareness and training

Appropriately supporting staff to ensure they can support essential services' network and information system security.

B1. Service protection policies and processes

Principle

The organisation defines, implements, communicates and enforces appropriate policies and processes that direct its overall approach to securing systems and data that support delivery of essential services.

Description

The organisation's approach to securing network and information systems that support essential services should be defined in a set of comprehensive security policies with associated processes. It is essential that these policies and processes are more than just a paper exercise and steps must be taken to ensure that the policies and processes are well described, communicated and effectively implemented.

Policies and processes should be written with the intended recipient community in mind. For example, the message or direction communicated to IT staff will be different from that communicated to senior managers.

There should be mechanisms in place to validate the implementation and effectiveness of policies and processes where these are relied upon for the security of the essential service. Such mechanisms should also support an organisational ability to enforce compliance with policies and processes when necessary.

To be effective, service protection policies and processes need to be realistic, i.e. based on a clear understanding of the way people act and make decisions in the workplace, particularly in relation to security.

If they are developed without this understanding there is a significant risk that service protection policies and processes will be routinely circumvented as people use work-arounds and shortcuts to achieve their work objectives.

Guidance

Developing policies and processes

The policies and processes needed by an organisation depend upon its function and should integrate with the organisation's approach to governance and risk management. Operators of essential services should have a range of policies and processes, including:

- **An organisational security or service protection policy**: endorsed by senior management, this high-level policy should include the organisation's overarching approach to governing security and managing risks, the organisation's aims and intents for security and what is of key concern.
- **Supporting policies and processes**: contextual lower-level definitions controlling, directing and communicating organisational security practice.
- **Compliance policies and processes for sector regulations, standards, etc**.: specific policies and processes appropriate to the compliance regime; these may be defined by the regulation, standard, etc. For example, to comply with ISO/IEC 27001, organisations should have in place certain security policies and procedures relevant to what the organisation does, how it does it, and what their ISO/IEC 27001 information security management system covers (see ISO/IEC 27002 for detail).

People-focussed practical approach

There is a growing body of evidence that people have a limit to the effort available to comply with security and there are recognisable costs to security behaviours. Exceeding human limits of compliance is likely to result in non-compliance, such as workarounds or circumventing controls.

Organisations should understand how people work with the systems and data they use to support the delivery of essential services to ensure security and people work together. Discover how people and security really need to work together to achieve the organisation's objectives and desired productivity.

Engage in and continue security conversations with staff, partners, contractors, any other system users, security and technical experts, plus organisational representatives such as HR, change and communications experts.

These conversations can be enabled through, for example:

- personal interviews,
- staff security attitude surveys,
- promoting security reporting culture without fear of blame or recrimination,
- engaging people in the design of processes and policies

Use your understanding of how people work to develop practical security policies and processes and, wherever possible, reduce the human effort required to comply.
There are many resources available intended to help organisations decide what their service protection policies should look like; for example, SANS provide various information security policy templates.

Personnel security

You should ensure that individuals authorised to access networks and information systems supporting the delivery of essential services are trustworthy. To be fully effective, link personnel security with identity and access control. Further information can be found in CPNI's Personnel and People Security and ISO/IEC 27002.

Implementing and communicating service protection policies and processes

Implementation of a new or improved service protection policy or process requires communication to those under its scope and evaluation of its effectiveness.

Effectively communicate the policies and information on how service protection processes work to everyone who can affect the security of the system, so that they can readily understand the contribution they make and their responsibilities to essential service security.

Communication can be achieved through continued security conversations and staff awareness and training programmes. However, it should be noted that having a staff awareness and training programme alone, without an understanding of how people work with security, is unlikely to result in improved compliance with service protection policies and processes. Refer to B6. Staff Awareness & Training for further information on effective staff awareness and training programmes.

Suitable data and metrics should be defined prior to implementation to evaluate the previous condition and assess the impact of the new or updated policy or process. Information may be drawn from security incidents, technical measurements, surveys, customer feedback, etc.

Improving policies and processes

Service protection policies and processes should be designed to be adaptable, to fit the needs of the changing environment. Organisations should regularly review their service protection policies and processes in light of any recorded security breaches so that these documents and the organisation's security can be continually improved.

References

HP & University College London whitepaper *The Compliance Budget*
SANS blog on security costs to people
SANS information security policy templates
ISO/IEC 27001 & 27002
IEC TS 62443-1-1 & 62443-2-1
CPNI's Personnel and People Security

B2. Identity and access control

Principle

The organisation understands, documents and manages access to systems and functions supporting the delivery of essential services. Users (or automated functions) that can access data or services are appropriately verified, authenticated and authorised.

Description

It is important that the organisation is clear about who (or what in the case of automated functions) has authorisation to interact with the network and information system of an essential service in any way or access associated sensitive data.

Rights granted should be carefully controlled, especially where those rights provide an ability to materially affect the delivery of the essential service. Rights granted should be periodically reviewed and technically removed when no longer required such as when an individual changes role or perhaps leaves the organisation.

Users, devices and systems should be appropriately verified, authenticated and authorised before access to data or services is granted. Verification of a user's identity (they are who they say they are) is a prerequisite for issuing credentials, authentication and access management. For highly privileged access it might be appropriate to include approaches such as two-factor or hardware authentication.

Unauthorised individuals should be prevented from accessing data or services at all points within the system. This includes system users without the appropriate permissions, unauthorised individuals attempting to interact with any online service presentation or individuals with unauthorised access to user devices (for example if a user device were lost or stolen).

Guidance

Identity and access management

The Introduction to identity and access management sets out security fundamentals that operators should consider in designing and managing identity and access management systems. Identity and access control should be robust enough that essential services are not disrupted by unauthorised access.

Physical security

In addition to technical security, operators should protect physical access to networks and information systems supporting the essential service, to prevent unauthorised access, tampering or data deletion. Some operators may already have physical security measures in place to comply with other regulatory frameworks. See CPNI guidance for further information.

References

NCSC Introduction to identity and access management
CPNI Physical Security guidance
BS ISO/IEC 27002
IEC 62443-2-1
NIST Identity and Access Management publications, e.g. SP 800-63 suite "Digital Identity Guidelines"

B3. Data security

Principle

Data stored or transmitted electronically is protected from actions such as unauthorised access, modification, or deletion that may cause disruption to essential services. Such protection extends to the means by which authorised users, devices and systems access critical data necessary for the delivery of essential services. It also covers information that would assist an attacker, such as design details of networks and information systems.

Description

The protection in place for data that supports the delivery of essential services must be matched to the risks associated with that data.

As a minimum, unauthorised access to sensitive information should be prevented (protecting data confidentiality). This may mean, for example, protecting data stored on mobile devices which could be lost or stolen.

Data protection may also need to include measures such as the sanitisation of data storage devices and/or media before sending for maintenance or disposal.
Protect data in accordance with the risks to essential services posed by compromises of data integrity and/or availability.

In addition to effective data access control measures, other relevant security measures might include maintaining up-to-date, isolated (e.g. offline) back-up copies of data, combined with the

ability to detect data integrity failures where necessary. Software and/or hardware used to access critical data may also require protection.

It is important to ensure that data supporting the delivery of essential services is protected in transit. This could be by physically protecting the network infrastructure, or using cryptographic means to ensure data is not inappropriately viewed or interfered with. Duplicating network infrastructure to prevent data flows being easily blocked provides data availability.

Some types of information managed by an OES would, if acquired by an attacker, significantly assist in the planning and execution of a disruptive attack. Such information could be, for example, detailed network and system designs, security measures, or certain staff details. These should be identified and appropriately protected.

(**Note**: data supporting the delivery of essential services must be identified in accordance with Principle A3 Asset Management. Important data to protect may include operational data, network traffic, configurations, as well as data that could provide an insight or advantage to an attacker, such as network and information system designs)

Guidance

Design to protect data

Networks and information systems should be designed to protect important data, for example:

- protecting the confidentiality of sensitive data by minimising the number of copies of data, the detail these include and by retaining operationally sensitive data on segregated systems (this includes design documentation)
- removing functionality that could allow greater access than has been authorised
- protecting the integrity of data essential to the operation of the service by providing a read-only copy (e.g. through a DMZ) for non-essential business system consumption
- only deploying well-tested cryptographic suites in common use by your chosen software stack
- protecting availability through resilience measures such as multiple network paths and tested automatic backup systems
- consider suitable means to retain access to essential information in the event of an incident. For example network diagrams needed for restoration, safety-critical information or essential forecasting data

Consider applying the NCSC principles of protecting bulk personal data to data supporting the delivery of essential services.

Protecting data in transit

Data in transit may be at risk of attacks such as interception, traffic replay, manipulation or jamming. VPNs are one of the most common and effective cryptographic methods used to assure the confidentiality and integrity of data transmitted over an untrusted network, such as remote access or between two sites.

TLS is often used to protect external data connections such as web browser traffic and IPSec is a well-known encryption technology for individual communication links. Where cryptography is deployed to protect communication links, you should protect cryptographic material such as certificates and keys from external or unauthorised access.

Alternative communications links or network paths are recommended for critical data paths.

For cloud services, see our guidance on protecting data in transit.

Protecting data at rest

Wherever data is stored, even temporarily, it may be vulnerable to unauthorised access, tampering or deletion.

You should identify where data supporting the delivery of essential services is stored, including:

- exports from core operational systems to other business systems
- on mobile devices
- removable media
- in temporary caches
- in systems used for remote access.

You should reduce these unauthorised access, tampering and deletion risks to stored data by limiting the quantity and detail of data held to the minimum necessary for business purposes, especially on devices and media that are more vulnerable to unauthorised access or that could be stolen.

Where dedicated systems and removable media are used, the storage devices can be hardware or software encrypted. You should take suitable measures to physically protect devices and media containing data supporting the delivery of essential services.
Backups remain an essential part of resilience measures and should be appropriately secured.

For cloud services, refer to NCSC cloud security principle 2 on asset protection and resilience.

Protecting data on mobile devices

Mobile devices may be used by the operator of essential services, a partner or third-party supplier. Whether owned and managed by the operator or not, these devices are likely to contain business data. Potentially, data important to the delivery of the essential service could be on these devices.

Well-configured and managed, business-owned, devices are preferred to personal or external organisation equipment: refer to the NCSC End User Device Security Collection for security principles and platform-specific guidance.

It may be possible to gain sufficient assurance that a partner or supplier applies security controls to the same rigour (or better).

In addition to good mobile device management, ensure that mobile devices accessing data supporting service delivery are well monitored.

Secure disposal

Data important to the delivery of the essential service is likely to be found on network and information system media and operational equipment, including IT and operational technology (OT) assets. Service management systems, along with network and mobile devices are familiar targets for secure sanitisation. Some essential services may also need to consider the data stored on defunct OT and safety systems.

References

NCSC 10 Steps: Home and Mobile Working
NCSC End User Device Security Collection
ISO/IEC 27002
IEC 62443-2-1
ENISA Big Data Security (2016)

B4. System security

Principle

Network and information systems and technology critical for the delivery of essential services are protected from cyber attack. An organisational understanding of risk to essential services informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.

Description

There is a range of protective security measures that an organisation can use to minimise the opportunities for an attacker to compromise the security of networks and information systems supporting the delivery of essential services.

Not all such measures will necessarily be applicable in all circumstances – each organisation should determine and implement the protective security measures that are most effective in limiting those opportunities for attackers associated with the greatest risks to essential services.

Opportunities for attackers to compromise networks and information systems, also known as vulnerabilities, arise through flaws, features and user error. Organisations should ensure that all three types of vulnerability are considered when selecting and implementing protective security measures.

Organisations should protect networks and information systems from attacks that seek to exploit software vulnerabilities (flaws in software). For example, software should be supported and up-to-date with security patches applied.

Where this is not possible, other security measures should be in place to fully mitigate the software vulnerability risk. Limiting functionality (e.g. disabling services that are not required) and careful configuration will contribute to managing potential vulnerabilities arising from features in hardware and software.

Some common user errors, such as leaving an organisation-issued laptop unattended in a public place, inadvertently revealing security-related information to an attacker (possibly as a result of social engineering) etc. can provide opportunities for attackers. Staff training and awareness on cyber security should be designed to minimise such occurrences (see B.6 Staff Training & Awareness).

Guidance

The majority of cyber security incidents can be traced to common cyber attack vectors. The opportunity for successful attack can be minimised by managing the known vulnerabilities which these attacks exploit. Many opportunities for user error can be reduced by technical means.

Attempts to circumvent the measures described below should be detected by security monitoring. Together with data security and resilience measures, the impact of any attempts to circumvent security on the operation of the essential serviceshould be limited.

System design

You should design the systems and networks operating or supporting the delivery of essential services to make compromise difficult, avoid disruption and reduce the impact of compromise. Where the design also makes compromise easy to detect, this will help achieve effective monitoring.

Stronger security architectures usually include:
0

- the most critical services and systems segregated into a higher security zone. This corresponds with the concept of *zones and conduits* described in the IEC 62443 reference model.
- at boundaries with higher security zones where it's necessary to import and trust data from a lower security zone, where possible:
- in a DMZ convert the data into the simplest appropriate alternate protocol, to create a "break" that makes protocol based attacks more difficult;
- perform validation of both message format and content.
- where messaging received from outside the organisation is used to control the essential service (e.g. customer or supplier system messages or critical telemetry), prefer a simple messaging format that can be validated and authenticated, or consider additional monitoring.
- reduced attack surface by limiting software, network data flows, system access, etc. to only those essential and necessary
- secured platform by default, with a system design that enables application of system updates without interrupting business, wherever possible
- a separate management layer, preferably using dedicated equipment and a separate network
- resilience and recovery features

Configuration

Well-configured networks and information systems reduce unauthorised access to technologies and simplify security management across hardware, firmware, software and configuration data. This should include:

- A baseline build (also known as a “gold build”) is recommended to apply a well-understood, consistent and secured platform across the organisation, and can also apply system hardening techniques to minimise the

attack surface. Gold build images should be appropriately protected from interference and be available for use in the event of system recovery.

- Configuration management policies or software should be used to ensure that only permitted software is installed and authorised devices, e.g. mobile devices and removable media, are permitted to connect. An asset management inventory could be used to manage authorised devices.
- In addition to the gold build and permitted software installed, maintain a record of the current "known good" configuration (including, for example, patch levels, OT ladder logic) and the resources, such as patch and configuration files, required to create this environment. It should be possible to revert or rebuild to this known good baseline.
- Systems, software or devices that are not actively supported by the developers should be identified, with appropriate additional security measures in place until they can be retired and removed.
- Users should not be able to change settings affecting the security of the service.
- Network devices should be configured to limit access to the minimum required for business operation. It may also be possible to apply standardised network device builds.

Some operators of essential services may use automated decision making technologies, for example safety systems or machine learning in smart transport technologies. Where such automated decision making has the ability to affect an essential service, it must be possible to understand the data, process and thresholds used to make automated decisions so that it can be reproduced, audited and malicious changes detected.

- For decisions based on pre-determined, unchanging behaviour this would entail knowing the exact hardware, firmware, software, and configuration of individual systems (this may be achieved with detailed configuration and asset management) and monitoring for any unplanned changes.
- Where systems use some element of machine learning and the decision making process changes over time. The model used should be auditable, so that malicious changes can be detected. This should identify cases where changes have been made directly, or where malicious or misleading data has been used for learning.
-

System management

Routine system management should support and maintain security. Technical documentation of the networks and information systems should be up to date.
Access to the essential service's facilities and systems should be managed and monitored to restrict to authorised personnel, in line with guidance in B2 Identity and Access Control.

As described in B2 Identity and Access Control Privileged User Management, technical means for access should separate essential services from other activities, for example using dedicated separate systems or sandboxed email and Internet access.

Further protection from physical interference can be afforded through tamper protection, such as port locks and tamper evident tape. Such physical tamper protections should be regularly checked.

Vulnerability management

Flaws, features and user errors that impact the security of the essential service may be known to the organisation, or not yet discovered. System design, configuration and system management

can reduce the likelihood of a vulnerability being accessed or exploited. New vulnerabilities need to be managed to maintain network and system security.

Effective risk management should ensure that appropriate measures are taken to maintain awareness of and address known vulnerabilities. The organisation endeavours to detect when changes to internally managed settings and configurations introduce vulnerabilities.
The latest mitigated vulnerabilities are often published by vendors, some providing automatic update functionality. Other vulnerabilities can be discovered through threat intelligence sources.

You should prevent the exploitation of known vulnerabilities in networks and information systems supporting essential services. Many of the most effective methods are well-known, including:

- removing vulnerabilities by maintaining systems to the latest patch level and only applying authentic, vendor-sourced and validated updates.
- removing access to vulnerabilities by segregation, or ensuring the vulnerable system only receives trusted data.
- preventing, detecting and removing malware or unauthorised software.
- verification of imported data and software. Where possible this should be automatic.
- regular vulnerability and security assessments, e.g. penetration tests and vulnerability scans. NCSC guidance on penetration testing provides further detail. Operators should carefully consider their approach to the testing of live Operational Technology, as system operation or availability could be affected. Assurance could be gained without this additional risk by testing against non-operational environments or by testing individual components in a laboratory environment.
- software that the essential service relies upon should be in active support, so vulnerabilities will be patched. You should provide additional protection where obsolete platforms cannot be easily replaced.

References

NCSC Common Cyber Attacks: Reducing the Impact
NCSC Mitigating malware
NCSC Obsolete platforms security guidance
NCSC Penetration testing
NCSC Secure by default platforms
IEC TS 62443-1-1
ISO/IEC 27002

B5. Resilient networks and systems

Principle

The organisation builds resilience against cyber attack into the design, implementation, operation and management of systems that support the delivery of essential services.

Description

The services delivered by an organisation should be resilient to cyber attack. Building upon B.4 (the technical protection of systems), organisations should ensure that not only is technology well built and maintained, but consideration is also given to how delivery of the essential service can continue in the event of technology failure or compromise. In addition to

technical means, this might include additional contingency capability such as manual processes to ensure services can continue.

Organisations should ensure that systems are well maintained and administered through life. The devices and interfaces that are used for administration are frequently targeted, so should be well protected. Spear phishing remains a common method used to compromise accounts with privileged access. Preventing the use of these accounts for routine activities such as email and web browsing significantly limits the ability for a hacker to compromise them.

Guidance

Preparation

It's important to be prepared to respond to significant disruption by having business continuity and disaster recovery planning in place. This should include a definition of your most critical resources and an understanding of the order of actions needed to restore service. Test that these plans work, for example through manually triggering failover testing, carrying out table-top scenario walk-throughs or red-teaming.

You should be ready to adjust the security measures in place in response to changes in risk. For example, if threat intelligence indicates an increased likelihood of your organisation or sector being targeted you may decide to isolate operational networks until the threat has decreased.

Alternatively, in the event of public disclosure of an unpatched vulnerability in equipment that you use, with reported use of exploits targeting the vulnerability, you may respond by elevating your protective monitoring, changing your configuration to avoid being susceptible, or taking other mitigating action in the period until a patch is made available and can be deployed.

Maintenance and repair

You should reduce the likelihood of failure or attack by taking all reasonable measures to maintain networks, information systems and necessary technologies in good working order. Exceptions should be appropriately managed.

Segregation

In the event of an incident, it is more likely that an essential service will be able to continue where the networks and information systems that support it are segregated from other business and external systems. Separation of system architecture, remote access and privileged access are some key principles that can protect more critical systems from external disruption.

Some essential service sectors may apply the industrial automation and control system security standard IEC 62443, which applies a reference model that separates systems into different logical layers. The standard's architecture model segregates equipment into security zones.

Capacity

Limitations of networks and information systems, or external services or resources, such as network bandwidth, processing capability, or data storage capacity, should be understood and managed with suitable mitigations to avoid disruption through resource overload.

Diversity and dependencies
Make appropriate use of diverse technologies, geographic locations and so on, to provide resilience. You should understand and manage external or lower-priority dependencies to ensure that alternative means are suitable for continuation of the essential service.

Working backups
In the event of a disruptive event, you should be able to revert to backups of hardware and data that are known to be functioning and accessible. Operators should maintain secured offline, potentially off-site, backups of the operational data, equipment configurations, gold builds, etc. needed to recover from an extreme event.

Suitable alternative backups may include paper-based information and manual processes. Other essential backups may include personnel with appropriate knowledge and access to up-to-date documentation. Consider how to make it easy to recover following an incident or compromise.

References
NCSC Denial of Service (DoS) guidance
IEC TS 62443-1-1
IEC 62443-2-1
HMG Emergency preparedness
HMG Emergency Response and Recovery: Non statutory guidance accompanying the Civil Contingencies Act 2004
The Business Continuity Institute has some freely available introductory business continuity guidance and members can access more detailed resources

B6. Staff awareness and training

Principle
Staff have appropriate awareness, knowledge and skills to carry out their organisational roles effectively in relation to the security of network and information systems supporting the delivery of essential services.

Description
Staff are central to any organisation's ability to operate securely. Therefore, operators of essential services should ensure that their employees have the information, knowledge, and skills they need to support the security of networks and information systems.

To be effective any security awareness and training programme needs to recognise and be tailored to reflect the way people really work with security in an organisation, as part of creating a positive security culture.

Guidance

The people who operate and support essential services should be provided with all they need to carry out their job while supporting the organisation's cyber security. In line with the design of service protection policies and processes, you should apply the same people-focussed approach to staff awareness and training.

Training and awareness activities should provide appropriate cyber security skills for the job role based on an understanding of how people *really* work with the systems, with ongoing reminders and top-up training to maintain skills.

Using a range of approaches to training and awareness can improve understanding and information retention, from briefings, online courses and blogs to simulated cyber attack. You may achieve the widest uptake of training and awareness by accommodating different learning preferences and using various delivery methods.

Operators may find the GCHQ certified training scheme useful when considering commercial offerings.

Security culture

Operators of essential services should aim to create a positive security culture, where people are aware of their role in maintaining security and actively take part and contribute to improving security.

This is particularly important where a technical solution is not possible, so security relies on people making the right cyber security decisions. Developing a positive security culture is likely to take some time, with some changes possibly taking years to become established and is unlikely to be achieved simply through written guidance or training events.

Communications

These outcomes are best achieved when organisations actively engage with staff and communicate effectively with them about network and information system security and how it relates to their jobs.

This should be more easily achieved where organisations create and promote a long-term security culture vision that is endorsed and supported by senior management, then make incremental, focused changes to address specific business issues.

Some essential service sectors may be able to draw on activities supporting positive safety culture to build up the organisation's cyber security culture.

References

NCSC 10 Steps: User Education and Awareness
CPNI's guidance on developing a security culture
GCHQ certified training scheme

Objective C: Detecting cyber security events

Capabilities to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential services.

Principles under this Objective

C1. Security Monitoring
Monitoring to detect potential security problems and track the effectiveness of existing security measures.

C2. Proactive Security Event Discovery
Detecting anomalous events in relevant network and information systems.

C1. Security monitoring

Principle

The organisation monitors the security status of the networks and systems supporting the delivery of essential services in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.

Description

An effective monitoring strategy is required so that actual or attempted security breaches are discovered and there are appropriate processes in place to respond. Good monitoring is more than simply the collection of logs. It is also the use of appropriate tools and skilled analysis to identify indicators of compromise in a timely manner so that corrective action can be taken.

This principle also indicates the need to provide effective and ongoing operational security. As time goes on new vulnerabilities are discovered, support arrangements for software and services change and functional needs and uses for technology change. Security is a continuous activity and the effectiveness of the security measures in place should be reviewed and maintained throughout the delivery and operational lifecycle of a system or service.

Guidance

In order to comply with NIS Directive requirements, your security monitoring should focus on detecting incidents or activity that impact on the protection and resilience of essential services and the network assets and systems that underpin them. Log and network data collection, analysis tools and threat intelligence should prioritise these assets and systems.

Of course, your monitoring should also address other security and resilience requirements that are outside the scope of the NIS Directive e.g. the protection of personal data, or general network performance and service quality.

Known and unknown threats

An organisation's monitoring capability should be able to find known threats on their network, for example detecting when known command and control traffic is communicating to the Internet, or an AV signature is present in a file.

Organisations should endeavour to understand what automated tools do and how best to use them, in order to ensure they are getting value for money from them.
Organisations should also have the capability to find previously unknown threats, by looking for indicators of attack combined with local system knowledge and sector threat information.

C1 focuses on known threats, where as C2 covers unknown threats.

Log collection and aggregation

Having the correct visibility of your systems is critical to detect potentially malicious activities. It is possible to detect cyber-attacks at an early stage by collecting and aggregating the following non-exhaustive list of log sources and then comparing them against known indicators of compromise:

- **Web site traffic going to the Internet**. As a minimum this should include domain names and URL's, but if possible, stretch to the full HTTP header information. This is because the initial infection and persistent connections are often made through HTTP(S) traffic and could appear to come from user devices (most likely) or servers. HTTP headers often provide clues to malicious activity.
- **Email traffic.** As a minimum, the metadata about what is sent and received, but if it is possible to capture both headers and contents then consider doing so. Phishing attacks, delivered over email, often tempt the user to click links, so getting visibility of these links in combination with web traffic helps detection and subsequent analysis.
- **IP connections between your network and the Internet.** It is useful to capture 5-tuple metadata of accepted connections on the edge of your network. This would show any raw connections coming out of your network, such as HTTP traffic not going through a proxy server or direct malware *command and control* sessions.
- **IP connections between zones in OT (Operational Technology) networks.** As a minimum, capturing 5-tuple metadata from critical OT zone boundaries such as the IT/OT interface is important. This IP traffic is likely to contain evidence of an attacker's actions against cyber-physical systems and so detection strategies should be in place to identify the indicators of a compromise of OT systems.
- **Host-based activity**. A host-based monitoring system can detect unauthorised activity on computer systems themselves (e.g. unusual or unauthorised activity by software systems), which might evade detection systems focused on network interfaces."

Your log collection should capture staff use of corporate systems, both regular users and system administrators, at the application and operating system layers. This helps to identify suspicious user behaviour for either an attacker or insider.

Duration and level of logging is a corporate choice, balancing storage cost with ability to retrospectively query data during (and after) an incident. Consider any legal data protection laws you may need to adhere to on the collected information, for example if collecting personal data in logs.

The audit and log information should be held in a database with access controls that limit access to monitoring analysts, and is isolated from other corporate trust domains. This is important as it will prevent an attacker from deleting or modifying logs.
Your organisation's asset management processes should ensure knowledge of network assets is sufficiently detailed and accurate to quickly and efficiently trace observed events to their sources.

Monitoring and analysis tools

The collected logs should be compared against Indicators of Compromise (from threat intelligence sources) to detect known threats.

You should choose appropriate tools to help analyse and correlate differently structured and normalised network datasets, to identify and investigate events of interest. These tools should be chosen to optimally scale to and use the types of network and logging data you expect to analyse and the workflows you have designed to analyse, triage and investigate security events. Your staff should receive the appropriate training to use these tools.

Consider the flexibility of the tools used, as you do not want to preclude your analysts from proactively finding unknown threats (as described in C2). Avoid purchasing black box tools that do not allow flexible querying, or provide results without showing the corresponding rationale.

Threat intelligence

This is a key requirement for any security monitoring capability and can come in many formats, volumes and quality. Threat intelligence can be collected from open discussion forums, trusted relationships, paid-for contracts with threat intelligence companies or even generated internally.

Threat intelligence can be either automated feeds that describe Indicators of Compromise (e.g. hashes of known nefarious files or lists of IP addresses) or more descriptive human readable reports documenting indicators of attacks or reporting on a type of malware. You should consume both types of threat intelligence appropriately.

We would recommended that when choosing automated threat intelligence feeds, favour quality over quantity (false positives can be costly for analyst time) and ensure the feeds can be automatically ingested by your chosen analysis platform.

Governance, roles and workflows

Your operational monitoring teams should comprise roles and responsibilities that cover both security and performance related monitoring. Combining these functions can help bring greater business benefit and multi-purpose use of the same datasets.

The size and structure of these teams will vary between organisations, but should usually include people who know the network, its hardware and software and the types of data that they process and produce. The team should also include investigators, who can work with threat intelligence to identify, investigate and triage security events and managers who understand the organisation's business and are able to assess the significance of security events in terms of their potential to cause harm, such as disrupting operations or leaking sensitive corporate or personal data.

Your monitoring capability should work seamlessly with Incident Management (see Objective D), knowing when and how to alert on or escalate events and how to share the right sort of information with incident managers. Monitoring and Incident Management may even comprise some of the same staff, working as part of a Security Operations Centre (see NCSC guidance - SOC Buyer's Guide).

Regular review and update

Your monitoring strategy and capability should evolve with your business requirements, networks and systems. That is, as the system develops (e.g. new systems, networks or software versions), the monitoring capability is updated in order to ensure that all essential services and related assets are covered. Your capabilities should also evolve to keep up with changes in the threats you need to mitigate.

Your tools should be configurable and adjustable to handle new datasets and your monitoring staff should be able to work with these changes. New IT systems should be designed to produce logging data that allows the appropriate level of monitoring, before they are made operational.

References

10 Steps: Monitoring
NCSC - SOC Buyer's Guide
CREST - Protective Monitoring Guidance
NIST - Continuous Security Monitoring
NIST Guide to Intrusion Detection and Intrusion Prevention Systems
ISO 27002 / 27019
IEC 62443

C2. Proactive security event discovery

Principle

The organisation detects, within networks and information systems, malicious activity affecting, or with the potential to affect, the delivery of essential services even when the activity evades standard signature based security prevent/detect solutions (or when standard solutions are not deployable).

Description

Some cyber attackers will go to great lengths to avoid detection via standard security monitoring tools such as anti-virus software, or signature-based intrusion detection systems, which give a direct indication of compromise.

Other, less direct, security event indicators may provide additional opportunities for detecting attacks that could result in disruption to essential services.
Examples of less direct indicators could include the following:

- Deviations from normal interaction with systems (e.g. user activity outside normal working hours).

- Unusual patterns of network traffic (e.g. unexpectedly high traffic volumes, or traffic of an unexpected type etc).
- 'Tell-tale' signs of attack, such as attempts to laterally move across networks, or running privilege escalation software.
- The retrieval of large numbers of essential service design documents

It is not possible to give a generic list of suitable indicators since their usefulness in detecting malicious activity will vary considerably, depending on how a typical attacker's actions might reveal themselves in relation to the normal operation of an organisation's networks and information systems.

Opportunities for exploiting these less direct security event indicators to improve network and information system security should be proactively investigated, assessed and implemented when feasible e.g. technically possible, cost effective etc.

Successful attack detection by means of less direct security event indicators may depend on identifying combinations of network events that match likely attacker behaviour, and will therefore require an analysis and assessment capability to determine the security significance of detected events.

Wherever possible, network and information systems supporting the delivery of essential services should be designed with proactive security event discovery in mind.

Guidance

Proactive security event discovery is more difficult than standard security monitoring because it looks beyond the known or prescriptive threat signatures and indicators described in C1. Security Monitoring.

The aim is to build on what is known of past attacks to hypothesise what new or previously unseen intrusions might look like in essential services environments. As such, this heuristic sort of monitoring should not be prioritised unless standard monitoring (see Principle C1) is already effective, or is not possible or practicable for some reason.

It requires more experienced knowledge of network and system behaviour and of the general characteristics that a malicious intrusion might exhibit. This sort of proactive monitoring or threat discovery would normally involve:

1. Designing your own alerts or trip-wires, using experience or reasoning of what an intrusion might do, rather than specifically around what past attacks have done
2. A good understanding of normal system behaviour (e.g. what software is authorised and how it would normally behave, how user accounts normally access network resources or how network components connect to each other and transfer data)
3. A good understanding of the ways that different types of anomaly might signify a malicious intrusion, based on a comprehensive and advanced understanding of threat intelligence

The science of anomaly detection, which goes beyond using pre-defined or prescriptive pattern matching, is a challenging but growing area. Capabilities like machine learning are increasingly demonstrated as having applicability and potential in the field of intrusion detection, but are often expensive, difficult to implement and can produce high false-alarm rates.

Objective D: Minimising the impact of cyber security incidents

Capabilities to minimise the impact of a cyber security incident on the delivery of essential services including the restoration of those services where necessary.

Principles under this Objective

D1. Response and recovery planning
Putting suitable incident management and mitigation processes in place.

D2. Lessons learned
Learning from incidents and implementing these lessons to make a more resilient service.

D1. Response and recovery planning

Principle

There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential services in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.

Description

Incidents will invariably happen. When they do organisations should be prepared to deal with them, and as far as possible, have mechanisms in place that minimise the impact on the essential service.

The particular mechanisms required should be determined as part of the organisation's overall risk management approach. Examples might include things such as DDoS protection, protected power supply, critical system redundancy, rate-limiting access to data or service commands, critical data backup or manual fail-over processes.

The NIS Directive has mandatory reporting requirements around cyber security incidents that have the potential to affect essential services. As well as NIS, organisations will typically have many other internal and external reporting obligations.

Guidance

NCSC's 10 Steps: Incident Management is the most concise guidance here, but organisations should use other more detailed guidance as and when appropriate. Other authoritative guidance pieces are referenced below.

Preparation - An Incident Response Plan

In addition to meeting the expectations of 10 Steps: Incident Management, you should ensure that your organisation's incident response plans are grounded in thorough and comprehensive risk assessments. Response plans should prioritise essential services along with the assets and

systems that are required to ensure their delivery, such as operational technologies, or key datasets.

The business continuity implications of any compromise should also be taken into account and your cyber incident response plans should link to other business response functions. You should form a cyber response team that is capable of implementing the plan, with the appropriate skills, tools and reach into other parts of your organisation, such as security monitoring and business continuity.

In practice, the Incident Response function should interoperate with the security monitoring function. The Incident Response Function needn't be a dedicated team and some members may have non-response related roles. Collectively, the team should have knowledge of IT security, IT infrastructure and Business Management, any specialist technologies (e.g. Operational Technologies or datacentres), incident reporting requirements, and Communications plans.

Your plan should cover all relevant potential incidents. It should be auditable and testable (via exercises) across a range of incident scenarios and should encompass all realistic descriptions of what might constitute an incident and its severity. Your test scenarios should draw on threat intelligence, past incidents, exercises and the ways in which security capabilities (e.g. security monitoring and alerting) would feature in your response options. Your scenarios should also consider incidents that involve suppliers and your wider supply chain (e.g. incidents arising through supplier relations, or relying on suppliers as part of your response).

These scenarios could include, but is not limited to:

- malware infection
- denial of service
- hacker infiltration
- an Insider Incident
- an inability to view status of the network or operational system
- emergency patching or antivirus signature roll-out
- system backup and restore
- confirmation of normal operations

Your plan should work seamlessly with other system management and security functions, such as security monitoring. Changes and improvements to response plans should reflect changes to these functions and vice versa, where appropriate.
Plans should articulate clear governance frameworks and roles with procedures for reporting to relevant internal or external stakeholders, such as regulators and competent authorities.

Your plan should also set out a comprehensive range of containment, eradication and recovery strategies, specifying how and when they should be used.
Your organisation should be able to describe its own state of readiness, using any criteria or expected standards from regulators or competent authorities, or from your internal governance arrangements, where appropriate.
You should run exercises to test your ability to respond to incidents that could affect the delivery of essential services. These exercises should reflect past experience, red-teaming/scenario

planning, or threat intelligence and should draw heavily on your risk assessment, considering all relevant assets and vulnerabilities, especially where they relate to essential services.

Exercises should record lessons learned, covering governance, roles and internal communication, quality of network and security monitoring data, containment and recovery strategies, or any other factors relevant to their effectiveness. This should integrate with lessons learned activities (see D2 Lessons Learned).

In order to report coherently on incidents when required, your plan should set out reporting thresholds (i.e. what does and does not need to be reported) and standards (i.e. the level of detail that should be reported) and which authorities to report to.

More detailed guidance on developing an incident response plan, and the underlying capability to implement it, can be found in Section 2 of the NIST Computer Security Incident Handling Guide, Part 4 of CREST Cyber Security Incident Response Guide or the Prepare section of ISO 27035.

Response and Containment

Your organisation's security monitoring function should be capable of alerting with enough detail for a response team to triage and determine the most appropriate response, which might be to investigate further, to take predetermined action, or to take no action. Eventualities not covered in the plan should be dealt with by risk-based decisions, taking account of factors like potential disruption, cost-effectiveness of response and the need for evidence preservation.

The resilience measures your organisation has in place should support incident response (see B5 Resilient Networks and Systems).

Incidents should be reported to the appropriate internal and external authorities, in line with the relevant reporting thresholds and standards. The response team should be capable of prioritising incidents, according to the potential consequences and disruption to essential services, using risk-based methods. These events should be documented, including alerts provided, information passed and decisions taken.

In addition to adhering to mandatory reporting requirements, organisations should seriously consider voluntarily reporting cyber security incidents to the NCSC, who may be able to provide situational awareness, drawing on incident reporting from other victims, as well as response and protective security advice. Assistance may also be sought from Cyber Incident Response (CIR) companies - see CIR scheme.

Further guidance is found in Section 3 of NIST Computer Security Incident Handling Guide, Part 5 of CREST Computer Security Incident Response Guide or Part 4 of ISO 27035.

References

10 Steps: Incident Management
NIST Computer Security Incident Handling Guide
CREST Cyber Security Incident Response Guide
Prepare section of ISO 27035
CIR scheme
ENISA Good practice guide for incident management

D2. Lessons learned

Principle

When an incident occurs, steps must be taken to understand its root causes and ensure appropriate remediating action is taken.

Description

If an incident does occur, it is important your organisation learns lessons as to why it happened and, where appropriate, takes steps to prevent the issue from reoccurring. The aim should be to address the root cause or to identify systemic problems, rather than to fix a very narrow issue. For example, to address the organisation's overall patch management process, rather than to just apply a single missing patch.

Guidance

You should use all of the guidance points below to learn lessons and address shortfalls in:

- your overall protective security (see Objectives A - C) and
- your incident response plan (see D1. Response and Recovery Planning).

Root Causes and Shortfall

Each incident or exercise should include assessment of root causes and any other factors that obstructed the required standard of recovery. You should consider what measures would need to be in place to prevent similar incidents in the future or to improve your response capabilities.

This might mean improving the quality or timeliness of detection, or designing the system so that simpler or more effective actions can be taken more quickly, or introducing mitigations to reduce the likelihood of such incidents occurring.

Your organisation should produce good quality reporting during incident response and exercising. Factors that affect the quality of reporting include information sharing, governance or processes, or clearly defined roles, responsibilities and training.

You should keep sufficiently detailed records to show how information was used to make decisions, so that the root causes of an incident can be identified and any shortfalls in response and preventive strategies can be assessed. These might include gaps in security monitoring, poor understanding of networks, insufficient business continuity planning, or inadequate internal communication.

These lessons should be clearly and comprehensively documented and fed into your protective security as well as your response plans. Further details can be found in Sections 3.1-2 of NIST Computer Security Incident Handling Guide, Part 5 of CREST Computer Security Incident Response Guide and parts 2-3 of ISO 27035.

Reduced Risk

You should use post-incident and post-exercise reviews to actively reduce the risks associated with the same, or similar, incidents happening in future.

Lessons learned can inform any aspect of your cyber security, including:

- System configuration
- Security monitoring and reporting
- Investigation procedures
- Containment/recovery strategies
- Governance and communication around incident management

Reporting
Lessons drawn from incidents or exercising should be shared with all relevant internal and external stakeholders e.g. regulators and competent authorities, as and when required, but also to internal governance, who can approve new preventive/responsive measures, or to organisations such as NCSC, who can provide insight around incident trends.

Data Retention
Many incidents go undetected for long periods. You should consider your organisation's data retention policies, especially the retention period and quality of historical data (e.g. any data aggregation performed after a time may restrict investigation), in order to ensure that incidents detected several months after they occurred can still be analysed adequately.

In determining adequate retention periods, you should consider how effective your monitoring capability is (i.e. how long might an incident go undetected), experience of past incidents and any examples available in threat intelligence.

Ensure that, if an incident occurs, your organisation would have sufficient data to perform the required level of post-incident analysis, learn lessons from the analysis, and report the right details to the right people (e.g. internal decision-makers or external regulators or competent authorities).

References

NCSC 10 Steps: Incident Management
Chapter 8 of ENISA Good Practice Incident Management Guide
ISO 27035:2016 - Principles of Incident Management
Section 3 NIST Computer Security Incident Handling Guide
Part 6 CREST Cyber Security Incident Response Guide

Table view of principles and related guidance

A tabular breakdown of the Objectives, principles and underlying guidance.

This page is intended as a handy summary of the 14 NIS principles and their related external guidance. Each individual principle page contains detailed introductory material which you should review before consulting the guidance referenced here.

Objective A. Managing Security Risk

Principle	Guidance and references
A1. Governance	NCSC Introduction to Security Governance ISO/IEC 27001:2013 IEC 62443-2-1:2010
A2. Risk Management	NCSC Risk Management Guidance NCSC assurance blog NCSC Penetration Testing Guidance NCSC Cloud Security Collection: Having confidence in cyber security NCSC Risk frameworks and methods
A3. Asset management	ISO/IEC 27001:2013 ISO 55001:2014 - Asset Management ITIL
A4. Supply chain	NCSC Supply Chain Security NCSC cloud security principle 8: supply chain Cloud Security Alliance (CSA) Security, Trust & Assurance Registry (STAR)

Objective B. Defending systems against cyber attack

ple	nce and references
B1. Service protection policies and processes	CPNI's Personnel and People Securinty ISO/IEC 27002:2013 section 5 & 7 IEC 62443-2-1:2010 section 5.8 & IEC 62443-2-1:2010 section 4.3.2.6 SANS blog post SANS security policy templates HP & University College London whitepaper *The Compliance Budget*
B2. Identity and access control	CPNI physical security guidance NCSC Security Design Principles for Digital Services NCSC Introduction to identity and access management ISO/IEC 27002:2013 section 9 IEC 62443-2-1:2010 NIST Identity and Access Management publications
B3. Data Security	NCSC 10 Steps Mobile devices and removable media NCSC End user device management guidance ISO/IEC 27002:2013 section 8 IEC 62443-2-1:2010 section 4.3.4.4 ENISA Big Data Security (2016)
B4. System security	NCSC Reducing the impact of common cyber attacks IEC 62443-2-1:2010 ISO/IEC 27002:2013 NCSC 10 Steps malware prevention NCSC penetration testing guidance NCSC obsolete platform guidance NCSC Secure by default platforms
B5. Resilient Networks & Systems	ISO/IEC 27002:2013 section 17 PD ISO 27019:2013 section 14 IEC 62443-2-1:2010 IEC 62443-2-1:2010 section 4.3.2 HMG Emergency preparedness HMG Emergency Response and Recovery BCI introductory business continuity guidance
B6. Staff Awareness & Training	CPNI's guidance on developing a security culture GCHQ certified training scheme NCSC 10 Steps: User Education and Awareness

Objective C. Detecting cyber security events

Principle	Guidance
C1. Security Monitoring	NCSC 10 Steps: Monitoring NCSC - SOC Buyer's Guide CREST - Protective Monitoring Guidance NIST - Continuous Security Monitoring NIST Guide to Intrusion Detection and Intrusion Prevention Systems ISO/IEC 27002:2013 / 27019 IEC 62443-2-1:2010
C2. Proactive Security Event Discovery	All in-page

Objective D. Minimising the impact of cyber security incidents

Principle	Guidance
D1. Response and Recovery Planning	**NCSC 10 Steps: Incident Management** **NIST Computer Security Incident Handling Guide** **Part 4 of CREST Cyber Security Incident Response Guide** **Part 4 ISO 27035** **CIR scheme**
D2. Improvements	NCSC 10 Steps: Incident Management Chapter 8 of ENISA Good Practice Incident Management Guide Parts 2-3 of ISO 27035. Section 3 of NIST Computer Security Incident Handling Guide Part 6 of CREST Cyber Security Incident Response Guide