Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Exposure Management

Visible but not vulnerable

Introduction

If you want to protect your organisation against digital threats, you need to know the extent to which your networks and systems are exposed to external threats. Exposure management lets you map the visibility of your digital assets and lift their resilience to the required level. This publication gets you started with practical tips to organise exposure management.

Constituents

This publication is intended for IT and security professionals (administrators, ISOs and CISOs) who are aware that they need to get a better grip on the exposure of their organisation's network and information systems so they can improve their resilience.

This publication was created with contributions from

Digital Trust Centre (DTC)

Definition: Exposure management

Exposure management means the process through which you gain insight into, and get a grip on, your organisation's system exposure. Exposure management allows you to lift your organisation's digital resilience to a suitable level.

Reading guide

This publication helps you with your first steps in setting up exposure management on outward-facing systems in your internal network. We start by discussing exposure and exposure management, after which we present a roadmap to set up exposure management within your organisation.

Table of Contents

Background

Exposure and exposure management are interrelated. Exposure involves the extent to which your organisation's network and information systems are visible and accessible to threats. A threat can only manifest if a network or information system is exposed to that threat. If you want to get a grip on your digital risks, you must be aware of your systems' exposure level.

Exposure management is highly relevant in the context of the NIS2 Directive. Article 21 specifies that organisations must conduct a risk assessment and implement suitable security measures. Exposure management provides focus for organisations to comply with this requirement. This article focuses on systems with a direct internet connection since these are most easily accessible to malicious parties. Be aware of what is visible and gain insight into what you don't see – because you can't protect what you don't see.

Exposure and exposure management: what are they?

Exposure

Exposure of network and information systems is necessary for your organisation to function property. Employees can consult a database, exchange e-mails, and sometimes change a configuration as part of your regular operations, in the office, in the production space, or on the road. The network and information systems your employees use for these purposes must be visible and accessible to them, but this also exposes them to malicious parties.

In addition to the network and information systems your IT organisation manages, employees sometimes use other digital systems for their work as well, for instance personal devices such as their own mobile phones or online file transfer services. Such 'shadow IT' is not managed by the IT management department, yet also represents exposure of your organisation. The NCSC and DTC websites provide more information and tips on how to handle shadow IT.

As shown in Table 1, network and information systems can be exposed to the outside world in various ways. Physical interaction may be necessary to operate a system, or an employee needs to log on to a local network to be able to do their work, for instance, which would limit exposure since a malicious party must also be physically present to perpetrate an attack. However, network and information systems are increasingly accessible via the internet, which increases exposure. This is the most relevant and urgent category for most organisations, which is why we focus on it most closely in this publication.

Category	How is the system accessed?	Where can the attacker be located?	Examples of assets that can be attacked
External network-facing	Open to the internet	Anywhere in the world	Websites, cloud servers, online APIs
Adjacent network-facing	Access to specific network	Within the same network	(Company) WiFi, internal systems
Local	Local access to the system	Within the same system	Local databases (in-house management)
Live in-person	Physical interaction required	Must be present at the device's location	Server rooms (in-house management)

Table 1: Exposure categories and threat types. The scope of this publication is external network-facing.

Exposure Management

Exposure management is a process that aims to gain insight into, and get a grip on, the exposure of your organisation's network and information systems, and to ensure that it is controlled before malicious parties can gain unauthorised access.

Exposure management has three key characteristics:

1. It is an ongoing process. Your organisation and its network and information systems are in continuous development, requiring continuous adaptation and improvement.
2. It is a combination of processes and analyses executed by people on the one hand, and automatic tooling on the other. Tooling can be used to detect, assess, prioritise and limit the exposure of digital assets with minimum effort. However, its results must be analysed and understood by actual people.
3. It must be embedded within your organisation's risk management process. Exposure management helps to analyse, prioritise and control digital risks.

It is not an independent process but is closely intertwined with other cybersecurity processes. Key aspects in this context are *asset management*, *vulnerability management, and risk management*.

- ***Asset management*** is the process that provides ongoing insight into all of the information and network systems in your organisation. Some form of asset management is always required when setting up exposure management.
- **Vulnerability management**[1] is the process that allows you to stay on top of the vulnerabilities in your information and network systems. To determine the extent to which a vulnerability represents a risk to your organisation, you must know the associated system's exposure level. In other words, exposure management is a precondition for vulnerability management. At the same time, you are giving the information and network systems that are exposed additional attention from the vulnerability management perspective, so there is a strong interrelationship between vulnerability and exposure management.

[1] https://www.ncsc.nl/documenten/publicaties/2025/januari/28/verbeter-je-kwetsbaarhedenbeheer

- **Risk management** is the overarching process that enables you to minimise the uncertainties that may disrupt your organisation's objectives. You should use exposure management as a key part of your risk management process to map, prioritise and handle risks.

Course of action: How do I set up exposure management?

Use the roadmap below to configure exposure management in your organisation. Thinking big is absolutely fine but *starting small* is the main thing here. Don't aim for an all-encompassing roll-out that is bound to run aground, but rather limit your scope and go through all of the individual steps of the exposure management process. You can expand, refine or improve the process in a general sense in the next round. The roadmap below helps you conduct a first complete 'round' in the process of exposure management so you can start working with tangible results.

The roadmap consists of four steps, each of which refers to the steps as presented in the NCSC's Risk Management Roadmap, i.e. Governance and Preconditions, Risk Assessment, Risk Treatment, and Continuous Monitoring.[2] We have also included a few questions in each step that will help you get started, as well as specifying the link to other relevant cybersecurity processes.

Step 1: Define your goal and preconditions (Governance and Preconditions)

Describe the why, what and how of exposure management within your organisation and what you need to realise it. Be complete and concrete and keep it small.

1. What concrete results should setting up exposure management yield (output) and what higher purposes (outcome) will I achieve with this?
2. Who and what do I need to set up exposure management? Who needs to be collaborate and who can issue the 'go ahead' for this plan? What are this person's direct interests in the process? Am I able to argue, justify and communicate all of this in an adequate manner?
3. How are our current asset, vulnerability and risk management processes configured and how do I align with exposure management?

When you complete this step, you will have written down what you will do, why it is important, how you plan to do it, how it fits into the bigger picture. You will also have secured the required support, collaboration and capacity in your organisation.

An example: An organisation wants to set up exposure management and defines its output as an up-to-date and complete overview of all systems that can be accessed via the internet. The higher purpose is being able to monitor the attack surface in a structural manner and thereby improve cybersecurity processes that are related to exposure management, such as vulnerability and risk management.

[2] https://www.ncsc.nl/wat-kun-je-zelf-doen/routekaart-risicomanagement

Step 2: Map and asses exposure levels (Risk Assessment)

List existing information and network systems in your organisation, determine their exposure, and assess the extent to which that exposure level represents risks to your organisation.

1. Map all of your organisation's information and network systems.
    a. Can I use what is already there? Have we already mapped our information and network systems (in part), for instance in the context of asset management or an earlier risk analysis? Can I trust that the list is complete and up-to-date?
    b. Edge devices require extra attention in the context of exposure management. These are devices that exist at the edge of your network and therefore have a direct external connection. Do I know which devices these are and where they are located? Please refer to our website for tips and background information on edge devices.[3]
    c. Do I have a good overview of the shadow IT within my organisation? Talk to colleagues to get an idea whether shadow IT is used and to what extent.
2. Use the mapped information and network systems to determine whether and how they are visible and/or accessible from the internet.
    a. Work with the IT department to determine for each information and network system whether it is visible and/or accessible via the internet.
    b. If you work with an external IT supplier, ask for their input.
3. (Automated) tools can help you supplement the resulting overview.
    a. What tools are available and which tool is most suitable for my situation?
    b. What do the outcomes that a tool generates mean? Am I able to interpret them correctly?
    c. Do we have the in-house knowledge to execute the steps above? If not, do I want to rely on an external party to do this?
4. Link to your vulnerability management here. Prioritise assessing the exposure of systems that contain vulnerabilities.
5. For each system, assess whether the detected exposure is necessary. You want to limit unnecessary exposure.
    a. Who can see/access the system? Why is it necessary?
    b. How well do I understand my organisation's needs? For instance, is a port being open 'highly critical' but does it serve an important process in your organisation?

[3] https://www.digitaltrustcenter.nl/edge-devices, https://www.digitaltrustcenter.nl/veilig-omgaan-met-edge-devices

When you complete this step, you will have insight into your organisation's information and network systems, know which ones are visible and accessible via the internet, and have started considering to what extent this level of exposure is acceptable within your organisation.

An example: After an inventory, a personal laptop is found to have access to the organisation's stock management system (via the properly secured intranet). However, the employee also uses that same laptop at home so the organisation cannot monitor for any potentially dangerous connections with the open internet.

Step 3: Managing exposure (Risk treatment)

Manage your organisation's exposure after having gained insight into it.

1. Align the exposure with the wider risk management situation within your organisation.
    a. What forms of exposure represent the highest risk to the organisation?
    b. How do I communicate these findings to the management in an effective manner?
2. Implement measures to prevent undesirable exposure.
    a. What existing security measures must be improved first to limit undesirable exposure? This might involve adapting specific configurations.
    b. What new security measures must be implemented first to limit undesirable exposure?

When you complete this step, you will have aligned exposure management with the broader risk management process in your organisation and taken measures to prevent undesirable exposure.

An example: The fact that the laptop cannot be managed adequately does not align with the policies concerning the organisation's general cyber risk management. As a result, the organisation decides that BYOD devices are no longer allowed to conduct work processes. At the same time, the organisation decides to facilitate personal laptops to respond to this clearly existing wish for its employees.

Step 4: Assessment and monitoring (Continuous monitoring)

Measure progress and document all findings.

1. Monitor the exposure of your network and information systems continuously and determine whether any changes have occurred.
    a. Do I have real-time insight in continuously changing threats and vulnerabilities?
    b. Use an automated tool for this purpose if necessary. Do we have the in-house knowledge to execute this? If not, do I want to rely on an external party to do this?
    c. Do I prioritise vulnerabilities on the basis of the likelihood that they will be exploited?

2. Integrate exposure management in your organisation's business processes
    a. How do I ensure that my management board understands our exposure-related risks?

b. Am I consistently working to incorporate the findings of my exposure management into my organisation's security policies?
c. Have I documented and saved the findings from all of the foregoing steps?

When you complete this step, you will have set up your exposure management in such a way that you can monitor exposure-related changes on a continuous basis and keep on top of the way your exposure management progresses.

An example: Continuous monitoring shows that the new policy measure has ensured that external devices can no longer connect to the organisation's intranet, thus remedying the undesirable exposure via the personal laptop that was detected. The findings are presented to the board and all documentation is stored on the security management platform for future policy-making purposes.

In conclusion

Exposure management is part of the wider risk management process within your organisation. Just like asset and vulnerability management, among other things, exposure management helps the organisation make the right decisions with regard to digital risks.

The roadmap presented in this article will help you take the first steps in setting up exposure management in your organisation. It is important to realise that the exposure management process is an ongoing process that requires continuous improvement and modification. Exposure management is never 'done'.

Be aware of what is visible and gain insight into what you don't see – because you can't protect what you don't see. Exposure management is not a luxury but rather a necessity to improve your organisation's protection against digital threats.

Related publications

Would you like to know more, for instance about topics related to exposure management?
Explore our other publications:

Publication	URL
Vulnerability Management (NL)	https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/detecteren/kwetsbaarhedenbeheer
Risk Management Roadmap (NL)	https://www.ncsc.nl/wat-kun-je-zelf-doen/routekaart-risicomanagement
Edge devices (NL)	https://www.digitaltrustcenter.nl/edge-devices
Managing edge devices. (NL)	https://www.digitaltrustcenter.nl/veilig-omgaan-met-edge-devices

Publication
National Cyber Security Centre (NCSC)
PO Box 117, 2501 CC The Hague
Turfmarkt 147, 2511 DP The Hague
+31 (0)70 751 5555

More information
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

June 2025