Whitepaper

Common NIS2 Use Cases for IAM v1.0

BOOLEANS

Honesty meets Excellence

Introduction

Currently, local governments are working to implement the Network and Information Security 2 guideline (NIS2) into local legislation. For the Netherlands, this means that by October 2024, the local legislation needs to be adapted to accommodate for the NIS2 guideline. In the meantime, the Dutch government is advising organizations to already focus on the baseline information security (BIS) guideline, in order to get prepared.

In essence, both sets of legislation mean that organizations within certain sectors (see appendix A) are considered essential entities and therefore need to take additional steps in order to become more resilient to cyber attacks and more prepared in case there is a cyber attack. In a nutshell, the steps that these organizations need to take are:

- Perform a risk assessment to see what cyber risks the organization is facing in relation to the systems and processes the organization operates. Risks should be identified with regards to:
  - Continuity of the service when under attack.
  - Safety of the service when under attack.
  - Impact the above on national security.
  - Ability to recover after an attack.
- Implement control procedures to monitor and mitigate the above mentioned risks
- Implement an incident response procedure that also loops in the local authorities.

Booleans understands that the above is very high level and might have you wondering how to drill this down to your organization's specifics, especially when it comes down to Identity and Acces Management (IAM).

IAM is the gatekeeper to your digital organization

The risk assessment that needs to be performed in the light of the NIS2 guideline not only focuses on digital risks, but also on physical risks. Eventually, these physical risks can lead to a compromised digital system, hence they need to be assessed. In a simplified world, three types of risks can be categorized:

1. Risk of compromising a system due to failing physical security. This could range from infrastructure components not being protected, critical connections to infrastructure components not being protected or compromised digital security due to failing physical access control.

2. Risk of compromising a system due to failing digital security. This could range from digital systems being compromised due to an attack, a vulnerability exploit or incorrect configuration.

3. Risk of compromising a system due to external risks. This could range from (dependencies on) third party contractors, (dependencies on) third party systems or simply common infrastructure failing.

In all three categories, risks can be identified that relate to the operation, configuration and functioning of an IAM system. An IAM system serves as a central point within your digital infrastructure where the identity is mapped against its privileges and a starting point of decision making within access control. Because of this it is good to consider:

- How is your digital access control currently linked to your HR procedures?
- How do you handle third party contractors within your digital environment?
- How is your IAM stack currently managed? How quickly do you process updates and patches?
- How is redundancy engineered into your IT infrastructure, does this also apply to your IAM stack?
- How fine-grained is your access control?
- Have you linked your incident response procedure to your digital access control?
- How resilient have you designed your digital access controls in relation to common attack vectors such as brute force attacks, denial of service attacks, detecting compromised credentials, multi-factor authentication requirements?

IAM use cases within NIS2

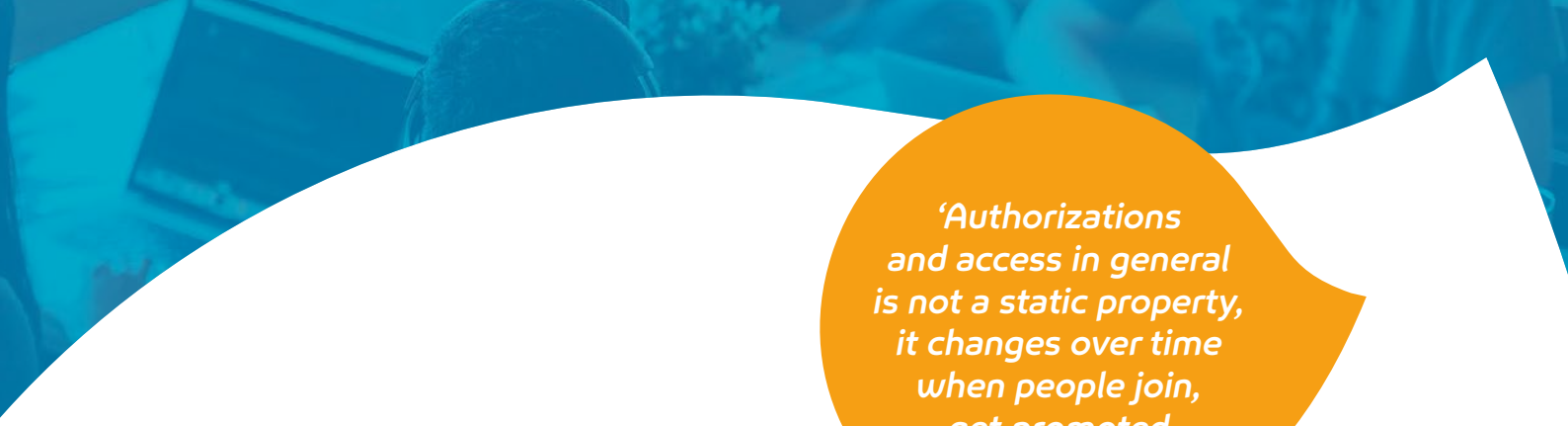
Depending on the outcomes of the risk assessment, you might see different levels of maturity regarding the use and configuration of your IAM stack. Booleans can assist with several common use cases to help increase the level of maturity.

Implementation of multi-factor authentication

Increasing the security of your authentication procedures by adding an additional factor can be a crucial step towards becoming more resilient to attacks. Most common factors are OTPs, push notifications, TOTPs or Passkeys. Each of these factors has its own pros and cons and it might make sense to understand the context you are going to use it in prior to implementing it. Besides adding a second factor to all authentication flows, it might also make sense to look at the concept of level-of-assurance as this allows you to ask for a higher level of security only when the process demands for it.

Implementation of detection- and response technologies

In most modern systems, traditional static security policies aren't sufficient to counteract attacks and serve your user at the same time. Modern remote working policies, working with contractors and third parties and bring-your-own-device policies demand a more flexible mechanism of detecting what's right or wrong. It is often recommended to adopt a zero-trust or CARTA approach, but what does that really mean? And what capabilities does your IAM stack need to have in order to facilitate for this? Selecting technology that helps you become future-proof and best practices to configure these technologies are aspects that are often overlooked when selecting an IAM stack.



'Authorizations and access in general is not a static property, it changes over time when people join, get promoted or leave.'

Implementation of authorization and just-in-time-access

The most basic way of configuring an authentication flow is in a boolean fashion: you either get access or you don't. Fortunately a lot of modern access control systems allow for much more detailed control of access, typically referred to as authorization. To what extent these capabilities are leveraged within your IAM stack and how well they are automatically linked to a changing environment, is an area that is often overlooked. Authorizations are frequently considered as complex as it requires alignment between various business units to understand what an authorization entails and how it should be enforced. Having someone that can talk cross-domain to model authorizations in the right way and in the capabilities of the IAM stack is very important. Especially if you want to take authorizations to the next level by granting them only when they are needed for the user to perform its job at that point in time.

Connect IAM systems to identity lifecycle management

Authorizations and access in general is not a static property, it changes over time when people join, get promoted or leave. Especially organizations working with third parties and contractors have increasing challenges in managing the lifecycle of access and authorizations. Implementing an identity lifecycle management process and automating it is typically one of the first steps that can greatly reduce the security risks introduced by an ever changing environment. Selecting a system for lifecycle management and setting up proper lifecycle processes is something that organizations typically can use some help with.

Design for failover and resiliency

When IAM is a crucial component in your business continuity planning, resilience and failover design becomes a crucial factor. Besides the architecture design, the decision between on-premise, cloud or hybrid also play a role in terms of management and total cost of ownership. Especially with the increase of ransomware attacks, it becomes more interesting to start to look at cloud offerings for access control as opposed to self-managed and deployed infrastructure, as the upgrading and maintenance process is outsourced with modern cloud offerings.

Conclusion

As the NIS2 guidelines demand organizations to perform risk assessments and build risk mitigation strategies, an increasing emphasis will be placed on the design, maintenance and monitoring of the IAM stack. Even though IAM is much more of a commodity product today, proper configuration and management still requires dedicated skills not widely available on the IT market today. Many organizations already have acquired capable IAM products, but aren't necessarily using them in the optimal way to ensure maximum resilience. Furthermore, a lot of organizations are still choosing for on-premise deployments as they feel this level of control provides them with maximum security, but are overlooking the fact that they need skilled staff to configure these deployments in the right way. Finally, organizational processes are changing at an increasing pace and require lifecycle management to evolve with it. Having the tools and controls in place to do so as an organization requires expertise. Booleans is specialized in assisting with all the common steps in implementing an IAM stack: from vendor selection, deployment, architecture, configuration all the way up to maintenance and support.

Appendix A

The following sectors are considered to be essential to national security and therefore are subject to the NIS2 guidelines:

- Energy
- Transportation
- Banking
- Financial infrastructure
- Healthcare
- Drinking water infrastructure
- Digital infrastructure
- ICT administration
- Wastewater infrastructure
- Government services
- Space exploration
- Digital service providers
- Postal- and courier services
- Waste management
- Food supply
- Chemical industry
- Research industry
- Manufacturing industry

Additional criteria apply to determine whether an organization qualifies as essential towards NIS2. More information can be found here.

Booleans

De Corridor 5
3621 ZA Breukelen (NL)

+31 (0)88 001 0400

info@booleans.com
www.booleans.com

BOOLEANS
Honesty meets Excellence