Org curity

Last Modified

Intro

In Centero we feel that cyber security is a journey instead of a static state. The landscape of threat is constantly evolving therefore we must do the best can to protect us, our assets and our customers. As a Microsoft Intelligent Security Associate (MISA Partner), Centero relies heavily on Microsoft's security technologies, solutions, policies and best practices.

Our high level approach to Cyber Security consists of Zero Trust model, asset based security prioritization and governance and our secure software development instructions. We have not reinvented a bicycle but we have learnt and taken advantage of existing and well recognized cyber security frameworks:

- ISO27001. Guidelines for IT asset management. No certification.
- NIST. Guidelines for IT asset management and security policies. No certification.
- NIST. Secure Software Development Framework.
- Microsoft. Zero Trust Implementation Guides.

Security Culture

We all are responsible for improving organizational cyber security. Security policies and security controls can be a big help but a security aware employee is the most valuable asset for us. At Centero we want to have a constant dialog about different threats and cyber security overall. Therefore an employee has a low threshold to ask, talk and report anything cyber security related to security team.

As our overall cyber security readiness is a journey so it is for an individual employee. The security team trains and challenges all the employees. Cyber Security trainings for personnel are held semi-annually. Centero wants to ensure that personnel have suitable understanding to modern threat landscape and especially how to act when cyber security incidents occur.

Physical Security

For our products and services, we rely on Microsoft Azure. Therefore all the security on physical level is Microsoft's responsibility. In addition we have purchased some IaaS from Finnish hosting-vendor. But this is only for our internal services such as Active Directory and other on-premises utility services.

We have 2 office locations in Finland and both of them are secured with access control.

Security Controls

Centero takes an advantage of numerous security controls by different security solutions. As stated earlier we heavily rely on Microsoft's cloud based security technologies.This section reviews different parts of our cyber security approach.

Identity and access management

Zero Trust culture is very strict on identity and access management. We want to meet the demand in both, authent [illegible] stems, devices and solutions we develop and verify authentications explicitl [illegible] ssible a strong multi-factor authentication is required. We also monitor and log [illegible] authentications. To ensure that this is the case we use following technologies:

- [illegible]
- Conditional Access
- Defender for Cloud Apps
- Microsoft Defender for Identity
- And other controls

As important Zero Trust principle for us is using the least privilege access. This principle comes true in our assets. Following technologies are used to enforce the policy:

- Azure Privileged Identity Management for Microsoft Azure
- Centero Carillon for Windows endpoints

The privileged roles and groups periodically reviewed and audited.

Endpoints

Centero allows only managed devices to be used. In addition to explicitly verifying identity, our conditional access also makes sure that only managed devices can access our services.

We have enforced a set of specific security hardening policies to all of our endpoints. Just to mention couple of requirements:

- Storage encryption is required.
- Device access control is required: PIN Code, Windows Hello for Business and Strong Biometric.
- Defender for Endpoint is required.

In addition all the endpoints are continuously monitored by Defender for Endpoint. This means that we are on top of vulnerabilities and other security recommendations that are related to our machines.

Endpoint lifecycle is also important matter for us. All the devices are enrolled with same kind of process and device end of life is always a managed action.

Monitoring, alerting and logging

The criticality of different IT-assets define how they are monitored and logged. Variety of assets are constantly monitored and logged. Centero mostly uses Microsoft's technologies in this.

1. Log Analytics in Azure Monitor
2. Microsoft Sentinel
3. Various Microsoft Defender family solutions

All the security alerts are then forwarded to internal ticketing system. Then security personnel will asses the alert and decide how to continue. If specific requirements are met then the security event is escalated to an security incident [illegible]

Vulnerability management

Servers [illegible] devices are continuously monitored for vulnerabilities. This includes monitoring for the operating systems, third-party applications and other components.

When it comes to operating systems, applications and application versions we try to be as standardized as possible. The devices have a required set of components and applications which are then managed and patched by automatic systems. End users are allowed to install other applications for their own devices but this is also monitored on multiple levels. For installing applications the device admin privileges are only temporal with justification reason required. In addition employee installed applications are still included in the vulnerability monitoring.

Dealing vulnerabilities in our environment is mostly automatic. This includes the operating systems, components and standardized applications. Non-standardized applications are dealt with individually in co-operation with employees and cyber security personnel. Patching operating systems and application is done with minimal delay.

Cyber Security team have also conducted a vulnerability monitoring for network devices.

Although automatic vulnerability monitoring is a great asset security team also conducts monthly Security Update Monitoring Service (SUMS). This means that all the Microsoft patch Tuesday vulnerabilities and updates are reviewed and prioritized.

Malware prevention

All the endpoints and servers are protected with Microsoft Defender for Endpoint. This means that no devices are left out from malware prevention. All the devices must comply with enabled Defender components. Exceptions are monitored.

Secure Software Development

Our secure development framework consists of different main categories.

- Security Requirements for Software Development
- Roles and Responsibilities
- Supported Toolchain
- Toolchain and 3rd Party Library Vulnerability Monitoring
- Security Status Checks
- Incident Escalation
- Protecting Software
- Guidelines for producing well-secured Software
    - OWASP'S Top 10 & CWE Top 25
- Responding to Vulnerabilities

For more detailed information please contact our sales.