Sec ape
Last Modified

software manager

Organization Security

Introduction

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

securit

Identi nent

Zero entity and access management. We want to meet the demands in both, authentication and authorization. The systems, devices and solutions we develop and verify authentications explicitly. This means that whenever possible a strong multi-factor authentication is required. We also monitor and log anomalies in sign-ins and authentications. To ensure that this is the case we use following technologies:

- Multifactor authentication
- 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. M
3. V y solutions

All the arded to int ticketing system. The security personnel will sses the alert and c fic requirements are met then the security event is escalated to an security incident.

Vulnerability and Patch Management

Servers, Workstations and Mobile 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

- R) 25

For mo se contact ur sales

Centero Customer Portal Security Controls

Network connections

Network connections to Customer Portal is protected by Azure Front Door service. All connections to Customer Portal use HTTPS (minimum of TLS 1.2).

Authentication

Access to Customer Portal is restricted by Azure Active Directory authentication and authorization is based on roles. Customer Portal is Microsoft Azure Active Directory application so Customer can define additional authentication requirements for the application (like conditional access and MFA). Roles each user has in Customer Portal can be managed by Customer admin users in Customer Portal.

Logging

Audit logging for actions performed in Customer Portal are available for customers only trough separate service requests.

Platform

Customer Portal is running on Microsoft Azure platform. Location of the services in Microsoft Azure is in Europe either North Europe or West Europe datacenters.

Physical Security

As Customer Portal is running on Microsoft Azure platform the description how physical security is handled can be found from Microsoft documentation: Physical security of Azure datacenters - Microsoft Azure | Microsoft Docs

Compute Security

Access to Customer Portal service related Azure resources is restricted for specific Centero personnel using Azure Security Control and limited only to persons responsible for maintaining the Customer Portal. Microsoft Defender for Cloud is used to protect Azure resources. Access from Internet is restricted only to HTTPS based Centero Portal. Access to databases is restricted only to selected Centero public IP addresses.

Data security (Data-at-rest)

Data stored in Azure for Centero Portal is encrypted at rest. This includes Azure storage and databases. Encryption keys are managed by Azure platform.

Netw it)

All data Azure and going out from Azure is always SSL (minimum TLS 1.2) encryp

Availability and monitoring

Customer Portal platform availability is based on Microsoft Azure service availability. Recovery from technical platform errors is handled by Microsoft. Backups for Centero Portal content is taken by Azure Recovery Services with short term and long term backup strategy. Customer Portal is monitored internally on Azure using Azure Monitor service and externally from Internet. Azure Alerts service is used to open internal service tickets for issues and Azure Sentinel service is used for monitoring overall security of the Customer Portal.

Centero Software Manager Product Security Controls

Network connections

Network connections to CSM backend (excluding Azure Function App backends) are protected by Azure Front Door service.

Clients

CSM Integration Client and CSM Cloud Client open SSL protected outbound connections to CSM backend services. Detailed connection addresses and ports can be found from system requirements page under each CSM product. Inbound connections to clients are not used.

Management

Local CSM component management is always done locally at the device where component is installed on Customer environment.

Authentication

Clients

Each client will authenticate to backend services using customer identifier and authentication key that are available for each customer in Centero Portal. Customer identifier and authentication key are specified by customer during the client installation or in client UI when first time connecting to backend services. Authentication identifier can be reset by the customer on Centero Portal if existing authentication key is compromised.

Management

Local components are not using any authentication or authorization on product level but are using Operating System security to require either local administrative privileges or delegated access. Detailed information about privileges required by the CSM client can be found from each CSM product requirements page.

Logging

Client

Chang processes are logged to local log files or Operating System event log.

Ma

Local components does not have audit logging available.

Platform

Background services for CSM product are running on Microsoft Azure platform. Location of the services in Microsoft Azure is in Europe either North Europe or West Europe datacenters. This platform security chapter is only for platform hosted by Centero. Each Customer is responsible for platform security on Customers own environment.

Physical Security

As CSM platform is running on Microsoft Azure platform the description how physical security is handled can be found from Microsoft documentation: Physical security of Azure datacenters - Microsoft Azure | Microsoft Docs

Compute Security

Access to CSM service-related Azure resources is restricted for specific Centero personnel using Azure Security Control and limited only to persons responsible for maintaining the CSM platform. Microsoft Defender for Cloud and Microsoft Defender ATP are used to protect Azure resources. Access from Internet is restricted only to HTTPS based backend APIs. Access to virtual machines or databases is restricted only to selected Centero public IP addresses.

Data security (Data-at-rest)

Data stored in Azure for CSM services is encrypted at rest. This includes Azure storage, virtual machine disks and databases. Encryption keys are managed by Azure platform.

Network security (Data-at-transit)

All data for CSM services coming in to Azure and going out from Azure is always SSL (minimum TLS 1.2) encrypted. All CSM Installation Packages that are downloaded from Azure to Customer environment are verified by calculating hash value and compared to hash value received from CSM backend before download has been started.

Availability and monitoring

CSM services platform availability is based on Microsoft Azure service availability. Recovery from technical platform errors is handled by Microsoft. Backups for service content is taken by Azure Recovery Services with short term and long term backup strategy. CSM services are monitored internally on Azure using Azure Monitor service and externally from Internet for publicly available backend API's. Azure Alerts service is used to open internal service tickets for issues and Azure Sentinel service is used for monitoring overall security of the CSM platform.

Centero Software Manager Supported Application

Pro[illegible] Centero Software Manager supported application process

This is a description of process for new Supported Application versions released by software vendors. This process is used with all the Supported Applications in CSM Services. In addition the same process is used for Application Packaging as a Service Apps (APaaS).

Monitoring for the new application versions and vulnerabilities

This part of the process consists of two simultaneous tasks.

- Centero's specialist goes through all the Supported Applications and APaaS applications daily. This means reviewing the sources of software vendors for any new versions available. The reviewing process includes all the different type of updates: security, quality, feature, bug fixes etc.
- In addition we have a background automation going through new software vulnerabilities every few hours. This is done with assist of Microsoft Defender for Endpoint, Advanced Hunt Queries and Microsoft Logic Apps.

New software version is detected

Whenever a new software version is detected Centero's specialist enters a record in our systems. At the same time the media of the new software version is introduced to our systems. This also means saving a SHA1 hash of the downloaded media to our systems. On top of that the specialist selects which kind of update is in question. This helps us to prioritize security updates over others for an example.

The SHA1 hash can be used at any later point of the process. It can be used for verifying that the media has not been altered by anything malicious.

When the specialist downloads the installation media of the new version for the first time, Defender for Endpoint also keeps track of the SHA1 hash and any possible changes to the hash.

Packaging specialist downloads the media

According to our packaging process a packaging specialist will start the work on the new version. This means downloading the media to an endpoint. Once again, Defender for Endpoint will scan and monitor the media. Microsoft Defender for Endpoint also uses Virus Total for signature based monitoring.

The packacing process starts

Centero Kapellimestarin Apulainen copies packaging project files to the endpoint of the specialist. These files also includes the media of the previous version. All the files are automatically scanned by Defender for Endpoint.

Different methods for creating the new installation media

The me s then either packaged or modified. The part of the process requires differe method: AdminStudio Repackager, Adminstudio InstallShield, InstEd anD Po lkit.

The di g specialist uses:

1. **Repackacing an EXE (.exe) executable file.** The specialist uses a fresh packaging virtual machine with Administudio Repackager to find out all the changes the executable does. All the necessary changes, files etc are then build into a new MSI-package. The finished installation media (.msi) is then tested on a fresh testing virtual machine.
2. **MSI package built by software vendor.** Whenever a software vendor already has a MSI-package available, then all the necessary changes are built into a MST-package. The MST package includes all the necessary configuration for the MSI-package. The finished installation media (.msi + .mst) is then tested on a fresh testing virtual machine.
3. **EXE files including a MSI or multiple MSI files.** The EXE file in extracted and then built into a single MSI package. All the necessary changes are built into a MST-package. The MST package includes all the necessary configuration for the MSI-package. The finished installation media (.msi + .mst) is then tested on a fresh testing virtual machine.
4. **EXE package released by software vendor.** On rare occasions an existing EXE-file is used. It is then tested on a fresh testing virtual machine.
5. **Using Powershell App Deployment Toolkit (PSADT).** PSADT is used to install either MSI or EXE package. Powershell script includes all the necessary configuration for EXE- or MSI-package.The finished installation media (script with .EXE or .MSI) is then tested on a fresh testing virtual machine.

Technical testing of the media for new software version

No matter what packaging method is used or what the type of the finished media is, the testing is always done on a fresh testing virtual machine. The tests include:

- Installation
- Removal
- Update

Publishing the new version for internal testing

The new version will be published by using our own utility tool Centero Kapellimestarin Apulainen. It means publishing the finished packages in format of .INTUNEWIN and .ZIP. The files are then scanned with Microsoft Defender. After that, all the necessary files are copied to Microsft Azure Storage.

Executing the internal tests

All the software versions are then tested by us. It includes the technical testing in earlier phase but also acceptance testing in the following management systems:

- M
- M
- M

We make sure that the new version is successfully imported to the management system and then delivered to testing endpoints.

Malware scanning

Before the final step of releasing the new media for customers we do extensive malware scans for the media. This is done with assistance of MetaDefender. MetaDefender includes multiple different anti malware engines.

If the scan is successful and no abnormalities are reported we proceed with the publishing process. If there is anything anomalous it is reported to the security team which will determine the what happens next.

Publishing to customers

This is the final part of the process. We used our our own utility tool Centero Kapellimestarin Apulainen to make the final publish for all our customers.

Assets used in the process

- Centero Kapellimestarin Apulainen utility tool
- AdminStudio Repackager
- AdminStudio InstallShield
- InstEd
- PowerShell App Deployment Toolkit
- Host machine
- Fresh Virtual Machine for Packaging
- Fresh Virtual Machine for Testing