Privileged Identity Management (PIM) in on-prem Microsoft Active Directory environments

We make it possible to perform Privileged Identity Management in on-prem Microsoft Active Directories.

PRIVILEGED IDENTIY MANAGEMENT

With our Privileged Identity Management-as-a-Service we offer a service based on a Microsoft PowerApp in which user can request access to the on-premise Microsoft Active Directory environments. this allows you to get control of the number of administrators and prove who asked for which rights at what time or date. The rights are divided divided into different types and are administered according to the security model.

WHAT DOES THIS SOLVE?

- Gain control of the number of (domain) administrator accounts
- Traceability of who requested which rights at what time (and who approved)
- Accounts will created but also deleted so no more pollution of the system
- Service can be cancelled per month
- Connecting this service to a SOC or SIEM service is possible (optional)

ADVANTAGES OF USING PIM

- Control and audit on administrator accounts
- Minimize surface attacks on administrator accounts
- Service can be cancelled per month so no long term commitment necessary

COMPANIES WHO BENEFIT

- Are still using an on-premises Microsoft Active Directory environment
- Without an Identity and Access Management tool in place for administrator accounts
- Without the ability to audit administrator accounts

HOW WE DELIVER THIS

PIM-as-a-service can be delivered in two ways:

- As-a-Service (RawWorks hosted environment).
- As a project embedded into your environment (at additional costs for license, remote patching and decentralized maintenance)

CONTENT OF THE SERVICE

For Privileged Identity Management we create a layer for the different forms of administrator accounts. Employees who need administrator rights for their on-premises environment can request these rights via a Microsoft PowerApp. By design roles are implemented within the security model. Securing these process will be implemented within our tool.

There is then clarity on who can request which role(s) and who will be the approver of these assignments and roles.

As mentioned the request will be done by a Microsoft PowerApp. In the design we create the roles based on the Security model and these will be handled by a pipeline and the necessary scripts. Within Microsoft Active Directory a new administrator account will be created by a template account. Login details will be shared by mail and passwords for example by SMS. If necessary current administrator accounts can be disabled or enabled.

We advise to have a “break the glass” account in your safe in case of a disturbance to the Microsoft Azure infrastructure.

ADDITIONAL SERVICES FROM RAWWORKS:

- An Infrastructure-as-Code Landing Zone in Microsoft Azure
- OneSecure
- Competence-as-a-service
- An IaC Workspace (DevOps Workspace)
- Datalake-as-a-Service (OneData and OnePlatform)