UDV Technologies

Company: Large Enterprise Telecom Holding
Project: Granular Control and Access Management Automation

OVERVIEW

The goal: automation of the access control process in a dynamic business environment.
The Process: Design and implement access management process by developing the algorithms and a role-model based on the labor functions defined by the Customer. Launch a Self-Service Portal for end users.

The Result: The implemented solution based on One Identity Manager (IDM) allows the Customer to automate access management for IT systems. Additional benefits include a deep process control and informational log generation for analysis and review.

The Plans: Further solution development focuses on update and maintenance of labor functions lifecycle, integration with new IT systems and SIEM

CUSTOMER PROFILE

The Customer is a telecommunication holding that provides services associated with broadband access to Internet, telephony, digital TV, access to Wi-Fi networks, VPN, LoRaWAN, video surveillance and comprehensive solutions based on the internet of things (IoT) technology stack.

Customer facts:

- Owns one of the largest managed optical networks in Europe that covers 80% of Russian Federation
- Provides telecommunication services in 567 cities in the Russian Federation.
- 20 000 employees (full-time and non-staff)
- Over 5000 workstations running *nix-based operating systems

info@udvtech.com udvtech.com

CURRENT PROCESSES

The Customer has implemented centralized HR processes. New user accounts are created based on the record management system events. The access to Company information resources is based on requests. The request processing may take up to 3 days based on the number of information resources and users.

The distinctive company factor is a large number of information systems that can be accessed by company employees and external contractors who service and maintain information systems data. Request-based access control management requires significant efforts to process and approve such requests. Another reason for increased timeframe for granting access to end users is the need to establish communication channels between the user and the approver on a case-by-case basis.

There's no unified method to grant access to internal employees and to 5 specific categories of external employees and there's no centralized permission provisioning control.

MANAGEMENT CONCERNS

The company actively participates in reshaping telecommunication market. It unites new providers under the single brand that leads to Company restructuring and increase in information systems and staff.

Rapidly changing infrastructure requires access provisioning process to be fast, transparent and providing privileges in real-time.

SECURITY ADMINISTRATOR FEEDBACK

Efficient and mature tools are needed for providing granular access for various users to Company information resources.

IMPLEMENTATION

Along with IDM implementation the Customer decided to formalize employee duties into the Labor Functions description based on a set of basic operations associated with business process execution.

Role-based access model is being developed for granting, changing and revoking access based on employee labor functions.

IDM enriches labor functions taken from the HR record management system with access privileges and rights according to the role-based model and automatically grants/revokes access to the target information resources.

One Identity Manager can be integrated with the existing IT systems and can connect to SAP-based HR systems (SAP BPC, SAP S4/HANA, SAP BObj), access management systems (MS AD) and target IT systems (MS SQL, Oracle DB, MS Skype for Business, MS Exchange).
The message broker Apache Kafka deployed on the Customer system is used for integration with the HR and workflow systems.

Often enough, employee work includes not only the basic operation execution, but also requires generating a unique list of available information resources. User “access request” function is developed to customize access. End users can go to the self-service portal for a structured catalog comprising systems, resources and roles that allow users to request access and where IT system owners can promptly approve such requests.

RESULTS

One Identity Manager is the access control and management tool for the Customer.
Access to the resources is granted automatically in about 3 minutes, based on the role model and labor functions.

Any HR event leads to employee labor functions change and therefore employee privileges and rights also change. One Identity Manager allows to promptly block access to information resources in case of employee dismissal or reassignment to another position.

IDM-based access management allows to control privileges of every user and every information resource.

One Identity Manager allows to generate various analytical information that can later be used for IT and security incident investigation.

Apart from the access that was granted automatically, any user can request access to required information resources via the unified self-service portal. The self-service portal allows to approve and provide access to the Company and contractor employees on-the-fly and eliminates the need for any additional workflow management.

FUTURE PLANS

Further development of IDM-based access management processes includes labor functions lifecycle support and role-model improvement.

One Identity Manager supports implementing new business processes essential for Company development using built-in graphical editor.

IDM can be integrated with new target systems such as general or specialized IT resources. Integration with security incident management systems is also available in order to increase the company's IT security posture.