Security Concept

Details about access control

April 1, 2021

www.aeb.com

Contents

1 Principles

Applications, data, devices, and setups are protected against unauthorized access wherever they are located.

1.1 Roles concept

AEB grants customers, employees, and partners access using a central user repository and a role-based security model. This way, only authorized users are granted access to the individual applications and landscapes.

User accounts (users) are summarized in role groups. It is not the individual user object which is granted access, but it is always the role objects.

The creation of new accounts is granted only upon written request and upon the respective approval according to the “need-to-know” principle (see processes in the appendix).

The approval of authorizations and the assignment to roles is only granted upon written request and upon the respective approval according to the “need-to-know” principle (see processes in the appendix).

1.2 Administrative/privileged roles

Users with special administrative or privileged rights are summarized in appropriate role groups and are subject to the respective processes and approvals (see processes in the appendix).

The person responsible for these roles is usually the Head of IT, the IT Security Manager, or members of the Executive Board.

For particularly privileged rights (e.g. firewall access, admin portals), the user must use a special, personalized administrator account. The “normal” user account will not be granted these rights / cannot be assigned to the respective roles.

1.3 User accounts

Every employee, customer, and partner is provided with a personalized access code and password. Each employee is responsible for his/her own password. Only this access may be used.

1.3.1 Principles for passwords

The usual principles apply to all passwords. These include “difficult to guess”, “does not contain personal information”, “is not written down” (except in a dedicated password safe).

Passwords must consist of at least 11 characters.

Passwords must contain the following:

- at least one numeral
- at least one special character

- at least one capital letter and
- at least one lower-case letter

A central guideline automatically enforces this.

1.3.2 Password rotation

For employee accounts

For employee accounts, AEB follows the latest findings of global security research and the NIST recommendation not to allow password rotation to increase security.

For customer accounts

The AEB platform (nEXt) does not provide for password rotation. According to the latest findings of security research, this increases security.

In all other applications, the customer decides on the use of password rotation; both variants are possible, but AEB recommends not using password rotation.

1.3.3 Biometric recognition

Currently not planned.

1.3.4 Multi-factor authentication

Active for all AEB employees and partners.

Possible for customers in the AEB Private Cloud or with the help of a user repository coupling (see below).

1.3.5 User repository or domain coupling

A connection to external user repositories, a customer domain, or the use of LDAP directories is possible.

2 Entry in detail

The AEB buildings are divided into security zones. There are

- public areas
- private areas
- specially protected areas

The above and all processes concerning access control are ISO 27001 certified.

This is explained in the following by taking AEB's Stuttgart headquarters as an example.

2.1 Public area

This area is intended for all guests (customers, partners, speakers,...).

During office hours this area is open and accessible without authentication.

At AEB's Stuttgart headquarters, the office hours are between 08:00 a.m. and 06:00 p.m.

The public area includes the complete ground floor, the outdoor facilities, and the underground garage. Parts of this area are video-monitored (marked accordingly).

Outside the office hours, the underground garage and the ground floor are locked automatically. This area is monitored by a security service.

Employees can access this area also outside the regular office hours with the corresponding token (see below). These entries are logged by the locking system.

2.2 Private area

This area is only accessible for employees and a few partners.

Entry is only possible with a special "key" (token).

At the Stuttgart headquarters, this area includes all upper floors.

Access via lifts and stairs is only possible with an electronic token. This token is handed over to employees and selected partners based on their roles. ISO 27001-certified processes ensure that only authorized persons have a corresponding token.

All entries are logged by the locking system.

2.3 Specially protected areas

This includes rooms in which customer applications run, which host network or security facilities, or facilities important for the building technology, or which are particularly required to be protected due to other reasons.

Entry is only possible with a special "key".

These areas are generally video-monitored and secured by an alarm system.

They include, inter alia:

- both data centers
- all network distributors
- Rooms with employee files or accounting data
- Air-conditioning technology

Access is only granted to the relevant roles and therefore coded to their tokens, i.e. only IT administrators have access to the data centers, for example.

All entries are logged by the locking system.

In addition, the data centers are secured 24/7 by an alarm system. Entry is only possible if the alarm system is deactivated in addition.

The data centers are separately video-monitored 24/7.

3 Access in detail

3.1 Basic information

Due to network and application protection mechanisms (e.g. next generation firewall), it is ensured that only permitted relations can be established.

Due to the security concepts in the networks, it is ensured that access is granted only to authorized persons.

There is a password guideline in place, which is enforced upon all accounts (see above).

Three factors are required for the employees' and partners' access:

1. Login name
2. Password
3. Additional secret (e.g. onetime password, token, certificate, etc.)

Access by AEB employees to customer resources is made either by using two factors (login name and password) or three factors (see above) depending on what is requested by the customer.

Access by customers to their resources provided by AEB is normally made by using two factors. If requested by the customer, three factors are also possible (see above).

The above and all processes concerning access control are ISO 27001 certified.

3.1.1 Details about the usual case "AEB network"

Based on a variety of criteria, devices which want to access AEB networks are moved automatically to specific networks.

Special rules apply within the networks.

For the networks, possible relations are documented in the central Rights Management.

3.1.2 Details about the special case "Remote access of AEB employees" (e.g. home office)

Remote access to customer data/applications cannot be made directly.

AEB employees must always first authenticate themselves in the AEB network with three factors (one account and two secrets). From there, the employee can open further access points to the corresponding resources and thus indirectly access them.

All security mechanisms of the AEB networks are therefore also effective in the case of remote access.

3.1.3 Details about applications

The rules who is to get which access to an application is defined by the respective application manager together with the Security Working Group and the Data Protection Officer.

Within the applications, access is also controlled by the role concept. An SSO can be integrated into various applications using the central user repository.

The following is defined and documented for each application:

- Where does it run?
- From which network is access to the application permitted?
- Which network may the application access?

This definition and documentation is part of the application management process.

3.2 Encryption

Access to AEB applications is always encrypted.

3.3 Logging

Each and every access to AEB applications and applications containing customer data is logged.

The above and all processes concerning access control are ISO 27001 certified.

4 Appendix 1 – Security research

4.1 Studies/research about Password Rotation

From the NIST Special Publication 800-63B

(Accessed on July 24, 2018 at https://pages.nist.gov/800-63-3/sp800-63b.html)

"This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal systems…

These guidelines provide technical requirements for federal agencies implementing digital identity services and are not intended to constrain the development or use of standards outside of this purpose. These guidelines focus on the authentication of subjects interacting with government systems over open networks, establishing that a given claimant is a subscriber who has been previously authenticated. The result of the authentication process may be used locally by the system performing the authentication or may be asserted elsewhere in a federated identity system. This document defines technical requirements for each of the three authenticator assurance levels. This publication supersedes corresponding sections of NIST Special Publication (SP) 800-63-2. […]"

5.1.1.2 Memorized Secret Verifiers

Verifiers SHOULD NOT impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorized secrets. Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authenticator."

From the Microsoft Password Guidance:

(Accessed on July 24, 2018 at https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf)

". […]"

Anti-Pater #3: Password expiry for users

Password expiration policies do more harm than good, because these policies drive users to very predictable passwords composed of sequential words and numbers which are closely related to each other (that is, the next password can be predicted based on the previous password). Password change offers no containment benefits cyber criminals almost always use credentials as soon as they compromise them.

Mandated password changes are a long standing security practice, but current research strongly indicates that password expiration has a negative effect. Experiments have shown that users do not choose a new independent password; rather, they choose an update of the old one. There is evidence to suggest that users who are required to change their passwords frequently select weaker passwords to begin with and then change them in predictable ways that attackers can guess easily.

One study at the University of North Carolina found that 17% of new passwords could be guessed given the old one in at most 5 tries, and almost 50% in a few seconds of unthrottled guessing. Furthermore, cyber criminals generally exploit stolen passwords immediately.

Study "The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis"

(Accessed on July 24, 2018 at https://www.cs.unc.edu/~reiter/papers/2010/CCS.pdf)

"6. Abstract

This paper presents the first large-scale study of the success of password expiration in meeting its intended purpose, namely revoking access to an account by an attacker who has captured the account's password. Using a dataset of over 7700 accounts, we assess the extent to which passwords that users choose to replace expired ones pose an obstacle to the attacker's continued access. We develop a framework by which an attacker can search for a user's new password from an old one, and design an efficient algorithm to build an approximately optimal search strategy. We then use this strategy to measure the difficulty of breaking newly chosen passwords from old ones. We believe our study calls into question the merit of continuing the practice of password expiration. [...]"

6. Conclusion

Password expiration is widely practiced, owing to the potential it holds for revoking attackers' access to accounts for which they have learned (or broken) the passwords. In this paper we present the first large-scale measurement (we are aware of) of the extent to which this potential is realized in practice. Our study is grounded in a novel search framework and an algorithm for devising a search strategy that is approximately optimal. Using this framework, we confirm previous conjectures that the effectiveness of expiration in meeting its intended goal is weak. Our study goes beyond this, however, in evaluating susceptibility of accounts to our search techniques even when passwords in those accounts are individually strong, and the extent to which use of particular types of transforms predicts the transforms the same user might employ in the future. We believe our study calls into question the continued use of expiration and, in the longer term, provides one more piece of evidence to facilitate a move away from passwords altogether."

5 Appendix 2 – Processes

5.1 Basics

All processes are subject to an internal audit taking place at a regular basis as well as to the ISO 27001 audit taking place annually.

Customers can request a summary of the audit or can agree for their own audits with AEB.

5.2 Processes

5.2.1 New users

Triggers for this process

- For AEB employees: Request by the HR team as part of the onboarding process
- For customers: Request for a new account

Process for AEB employees

- By entering the data in the HR system, the user account is created automatically and enabled on the date of entry.
- The rights must be applied for separately by the line manager or tutor (see "New role assignment").

Process for customers

- The AEB employee responsible for the request clarifies with the customer's designated contact (e.g. key user) whether the user should receive the account.
- The account is created.
- Depending on the customer's wish, the customer's designated contact (e.g. key user) or the user himself is notified about the initial secret.

5.2.2 New role assignment

Triggers for this process

- Request for role transfer
- Request for certain rights

Process for AEB employees

- Request is sent to the role manager
- The role manager
  - checks whether the employee can be assigned the role and whether the employee meets the necessary requirements;

  - clarifies with the employee whether the employee wants to take over the role together with the associated responsibilities.
- In case of approval: The employee is assigned the role and automatically gets the associated rights
- In case of rejection: The person who initiated the request is informed about the rejection and the reasons for it

Process for customers

- Request is sent to the responsible person
- The responsible person
  - possibly checks whether the user meets the requirements
  - clarifies with the customer's designated contact (e.g. key user) whether the user should receive the rights.
- In case of approval: User is assigned to the group and automatically gets the associated rights.
- In case of rejection: The person who initiated the request is informed about the rejection and the reasons for it

5.2.3 Relinquish a role

Triggers for this process

- Request for relinquishing roles/rights by the user
- Request for relinquishing roles/rights by a third person

Process for employees

- Request is sent to the role manager
- The role manager
  - clarifies with the person who initiated the request as to why the user is to/wants to relinquish the role/rights;
  - clarifies with the employee as to whether the employee wants to relinquish the role and the associated responsibilities and informs the employee that this is going to happen now.
- In case of approval: The employee will be removed from the role and automatically loses the associated rights
- In case of rejection: The person who initiated the request is informed about the rejection and the reasons for it

Process for customers

- Request is sent to the responsible person
- The responsible person clarifies with the customer's designated contact (e.g. key user) whether the rights/role should/can be withdrawn from the user.

- In case of approval: The user will be removed from the group and automatically loses the associated rights
- In case of rejection: The person who initiated the request is informed about the rejection and the reasons for it

5.2.4 Deactivating users

Triggers for this process

- AEB employee leaves AEB
- The customer's employee leaves the company
- Request to deactivate the customer's user

Process for employees

- In case of "imminent danger" the account can be deactivated immediately by the person processing the request. Afterwards, the request is forwarded to the HR team together with a corresponding note.
- Otherwise, the request is forwarded to the HR team.
- If the employee leaves the company, the account is deactivated automatically at the end of the last working day (maintained in the HR system).
- The HR team has the possibility of setting an identifier "Lock network access" in the HR system. As soon as this identifier is set, the user's account is immediately deactivated.

Process for customers

- In case of "imminent danger" the account can be deactivated immediately by the person processing the request. Afterwards or if no immediate action is necessary, the following will take place:
- The AEB employee responsible for the request clarifies with the customer's designated contact (e.g. key user) whether the user should/can lose the account.
- In case of approval: User is deleted
- In case of rejection: The person who initiated the request is informed about the rejection and the reasons for it

5.3 Regular checks

Triggers initiating this for employees

- Regular routines of the role manager and application managers
- Regular employee reviews

Process for employees

- Role managers and line managers check the assignments of employees to roles at a regular basis and, if needed, will initiate one of the above-mentioned processes (e.g. employee relinquishes role).

- Role managers and application managers check the assignment of roles to rights at a regular basis and, if needed, will adjust the assignments of roles and rights.

Triggers initiating this for customers

- Automatic routines taking place at a regular basis

Process for customers

- It is checked every day as to whether an account has not been used for more than 42 days.
- Accounts for which this is true will be deactivated automatically.