Sicherheitskonzept

Details zu Zutritt, Zugang und Zugriff

01.04.2021

www.aeb.com

Inhalt

1 Allgemein

Dieses Dokument fasst zum Thema passende Informationen aus dem „Sicherheitskonzept“ der AEB zusammen und vertieft diese. Sie finden das Sicherheitskonzept in dem AEB TrustCenter (https://www.aeb.com/TrustCenter)

2 Prinzipien

Applikationen, Daten, Geräte und Einrichtungen sind, egal wo sie sich befinden, gegen unbefugten Zutritt, Zugang oder Zugriff geschützt.

2.1 Rollenkonzept

AEB gewährt Kunden, Mitarbeitern und Partnern Zutritt, Zugang und Zugriff mithilfe eines zentralen User Repositories und einem rollenbasierenden Sicherheitsmodell. Dadurch erhält jeder nur auf die Anwendungen und Umgebungen Zugriff, für die er auch berechtigt ist.

Benutzer Konten (User) werden in Rollengruppen zusammengefasst. Es wird nicht das einzelne User-Objekt berechtigt, sondern immer die Rollen-Objekte.

Das Anlegen neuer Konten/Zugängen erfolgt immer nur auf schriftlichen Auftrag und entsprechender Freigabe nach dem „need to know“-Prinzip (siehe Prozesse im Anhang).

Die Berechtigungsfreigabe und das Zuordnen zu Rollen erfolgt immer nur auf schriftlichen Auftrag und entsprechender Freigabe nach dem „need to know“-Prinzip (siehe Prozesse im Anhang).

2.2 Administrative/privilegierte Rollen

Auch Anwender mit besonderen administrativen oder privilegierten Rechten sind in geeigneten Rollengruppen zusammengefasst und unterliegen den entsprechenden Prozessen und Freigaben (siehe Prozesse im Anhang).

Der Verantwortliche für diese Rollen ist üblicherweise der Leiter IT, der IT-Security Manager oder die Geschäftsleitung.

Für besonders privilegierte Rechte (z.B. Firewall-Zugriff, Admin Portale,..) muss der Anwender ein besonderes personalisiertes Administrator-Konto nutzen, sein „normales“ User-Konto bekommt diese Rechte nicht / kann nicht den entsprechenden Rollen zugeordnet werden.

2.3 Benutzerkonten

Jeder Mitarbeiter, jeder Kunde und jeder Partner erhält eine persönliche Zugangskennung und ein Zugangspasswort. Für dieses Passwort ist jeder selbst verantwortlich. Nur dieser Zugang kann und darf genutzt werden.

2.3.1 Prinzipien zu Passwörtern

Für alle Passwörter gelten die üblichen Prinzipien wie „schwer zu erraten“, „enthält keine persönlichen Informationen“, „wird nicht notiert“ (außer in einem speziellen Passwort Tresor).

Passwörter müssen aus mindestens 11 Zeichen insgesamt bestehen.

Passwörter müssen enthalten

- Mindestens eine Zahl
- Mindestens ein Sonderzeichen
- Mindestens einen Großbuchstaben und
- Mindestens einen Kleinbuchstaben

Das wird automatisch durch eine zentrale Richtlinie erzwungen.

2.3.2 Passwort Rotation

Für Mitarbeiterkonten

AEB folgt für die Mitarbeiterkonten den Erkenntnissen aktueller Sicherheitsforschung und der NIST-Empfehlung keine Passwortrotation vor zu sehen, um die Sicherheit zu erhöhen.

Für Kundenkonten

In der AEB Plattform (nEXt) ist keine Passwortrotation vorgesehen. Dies erhöht nach Erkenntnissen der aktuellen Sicherheitsforschung die Sicherheit.

In allen anderen Anwendungen entscheidet den Einsatz von Passwort Rotation der Kunde selber; beide Varianten sind möglich, aber AEB empfiehlt auf eine Passwortrotation zu verzichten.

2.3.3 Biometrische Erkennung

Ist im Moment nicht vorgesehen.

2.3.4 Multi Faktor Autentifizierung

Ist für AEB Mitarbeiter und Partner in allen Fällen aktiv.

Ist für Kunden möglich in der AEB Private Cloud oder mit Hilfe einer User Repository Kopplung (s.u.)

2.3.5 User Repository- oder Domänenkopplungen

Eine Anbindung externer User Repositories, einer Kundendomäne oder die Verwendung von LDAP Verzeichnissen ist möglich.

3 Zutritt im Detail

Die AEB Gebäude sind in Sicherheitszonen aufgeteilt. Es gibt

- öffentliche Bereiche
- private Bereiche
- besonders geschützte Bereiche.

Das und alle Prozesse rund um den Zutritt sind durch die ISO 27001 zertifiziert.

Im Folgenden wird dies am Beispiel HQ exemplarisch erklärt.

3.1 Öffentlicher Bereich

Dieser Bereich ist für alle Gäste (Kunden, Partner, Vortragende, ...)

Während der Öffnungszeiten ist dieser Bereich offen und ohne Authentifizierung betretbar.

Im HQ in Stuttgart sind die Öffnungszeiten zwischen 8:00 und 18:00 Uhr.

Der Bereich ist das gesamte EG, die Außenanlagen und die Tiefgarage. Teile des Bereichs sind Videoüberwacht (entsprechend gekennzeichnet)

Außerhalb der Öffnungszeiten sind die Tiefgarage und das EG automatisch verriegelt. Und dieser Bereich wird durch einen Sicherheitsdienst überwacht.

Für Mitarbeiter ist der Zutritt in diesen Bereich auch außerhalb der Öffnungszeiten mit dem entsprechenden Token (s.u.) möglich. Diese Zutritte werden über die Schließanlage protokolliert.

3.2 Privater Bereich

Dieser Bereich ist für Mitarbeiter und wenige Partner zugänglich.

Ein Zutritt ist nur mit einem besonderen „Schlüssel“ (Token) möglich.

Im HQ in Stuttgart umfasst dieser Bereich alle Obergeschosse.

Der Zutritt ist über Aufzüge und Treppen nur mit einem elektronischen Token möglich. Dieser Token wird Mitarbeitern und den entsprechenden Partnern anhand ihrer Rolle übergeben. ISO 27001 zertifizierte Prozesse stellen sicher, dass nur Berechtigte einen entsprechenden Token haben.

Sämtliche Zutritte werden über die Schließanlage protokolliert.

3.3 Besonders geschützte Bereiche

Dies umfasst die Räume in denen Kundenapplikationen laufen, die sensible Netzwerk oder Sicherheitseinrichtungen beherbergen, für die Gebäudesteuerung relevante Einrichtungen beherbergen oder aus anderen Gründen besonders schützenswert sind.

Ein Zutritt ist nur mit einem entsprechenden „Schlüssel“ möglich.

Diese Bereiche sind in aller Regel zusätzlich videoüberwacht und separat alarmgesichert.

Dies sind unter anderem:

- die beiden Rechenzentren
- alle Netzwerkverteiler
- Räume mit Personalakten oder Buchhaltungsdaten
- Klimatechnik

Der Zutritt ist jeweils nur den relevanten Rollen auf ihren Transponder kodiert, so dass z.B. nur IT-Administratoren Zutritt zu den Rechenzentren haben.

Sämtliche Zutritte werden über die Schließanlage protokolliert.

Die Rechenzentren sind zusätzlich 24/7 alarmgesichert. Ein Zutritt ist nur möglich, wenn zusätzlich die Alarmanlage entschärft wird.

Die Rechenzentren sind 24/7 separat videoüberwacht.

4 Zugang und Zugriff im Detail

4.1 Grundsätzliches

Durch Netz- und Applikationsschutzmechanismen (z.B. Next-Generation Firewall) ist sichergestellt, dass nur die erlaubten Beziehungen eingegangen werden können.

Durch Sicherheitskonzepte in den Netzen ist sichergestellt, dass Zugang nur für die entsprechend Berechtigten erfolgen kann.

Es existiert eine Passwortrichtlinie, die zentral für alle Konten erzwungen wird (s.o.)

Der Zugang erfolgt für Mitarbeiter und Partner immer mit drei Faktoren:

1. Loginname
2. Passwort
3. Weiteres Secret (z.B. onetime Password, Token, Zertifikat, ...)

Der Zugang von AEB-Mitarbeitern zu Kundenressourcen erfolgt auf Wunsch des Kunden entweder mit zwei Faktoren (Loginname und Passwort) oder drei Faktoren (s.o.).

Der Zugang von Kunden auf ihre, von AEB bereit gestellten, Ressourcen erfolgt normalerweise mit zwei Faktoren, auf Wunsch des Kunden sind auch drei Faktoren möglich (s.o.).

Das und alle Prozesse rund um den Zugang sind durch die ISO 27001 zertifiziert.

4.1.1 Details zum Normalfall „AEB-Netz“

Anhand verschiedener Kriterien werden Geräte, die auf AEB-Netze zugreifen wollen, automatisch in bestimmte Netze verschoben.

Innerhalb der Netze gelten besondere Regeln.

Für Netze sind die möglichen Beziehungen in dem zentralen Rights Management dokumentiert.

4.1.2 Details zum Sonderfall „Remotezugang der AEB-Mitarbeiter“ (z.B. HomeOffice)

Remotezugang auf Kundendaten/-anwendungen kann nicht direkt erfolgen.

Ein AEB-Mitarbeiter muss sich immer erst mit drei Faktoren (Ein Account und zwei Secrets) am AEB-Netz authentifizieren. Und kann von dort weitere Zugänge zu den entsprechenden Ressourcen öffnen und somit indirekt zugreifen.

Alle Sicherheitsmechanismen der AEB Netze wirken daher auch für den Remotezugang.

4.1.3 Details zu Anwendungen

Die Regeln, wer wie auf eine Applikation Zugriff bekommt, legt der jeweilige fachliche Applikationsmanager zusammen mit dem AK Security und ggf. dem Datenschutzbeauftragten fest.

In den Anwendungen wird der Zugriff auch durch das Rollenkonzept gesteuert. Über das zentrale User Repository ist ein SSO in verschiedene Anwendungen möglich.

Pro Applikation ist Folgendes festgelegt und dokumentiert:

- Wo läuft sie?
- Aus welchem Netz darf auf die Applikation zugegriffen werden?
- Auf welches Netz darf die Applikation zugreifen

Diese Festlegung und Dokumentation ist Teil des Application-Management-Prozesses.

4.2 Verschlüsselung

Zugang zu und Zugriffe auf AEB Anwendungen erfolgen stets verschlüsselt.

4.3 Protokollierung

Alle Zugänge und Zugriffe auf AEB Anwendungen und auf Anwendungen die Kundendaten beinhalten werden stets protokolliert

Das und alle Prozesse rund um den Zugang sind durch die ISO 27001 zertifiziert.

5 Anhang 1 – Security Forschung

5.1 Studien / Forschungen zum Thema Password Rotations

Aus der NIST Special Publication 800-63B

(Gefunden am 24.07. 2018 unter 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.”

Aus der Microsoft Password Guidance:

(Gefunden am 24.07.2018 unter 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.

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

(Gefunden am 24.07-2018 unter 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."

6 Anhang 2 - Prozesse

6.1 Grundsätzlich

Alle Prozesse unterliegen einem regelmäßig stattfindenden internen Audit ebenso wie dem jährlich stattfindenden ISO 27001 Audit.

Kunden können auf Wunsch eine Zusammenfassung der Audits bekommen oder auch eigene Audits mit der AEB vereinbaren.

6.2 Prozesse

6.2.1 Neuer User

Trigger, die diesen Prozess auslösen

- Bei AEB Mitarbeiter: Antrag durch Personalabteilung im Zuge des Onboardings
- Bei Kunden: Antrag auf neuen Account

Prozess für AEB Mitarbeiter

- Durch die Pflege der Daten im Personalsystem wird der User Account automatisch angelegt und zum Eintrittsdatum aktiviert.
- Die Rechte müssen vom Mitarbeiterverantwortlichen oder Fachbetreuer separat für den MA beantragt werden (siehe „Neue Rollenzuordnung“).

Prozess für Kunden

- Der für den Request verantwortliche Mitarbeiter der AEB klärt mit dem vom Kunden benannten Ansprechpartner (z.B. Key user), ob der User den Account bekommen soll/kann.
- Der Account wird angelegt.
- Das initiale Secret wird je nach Wunsch des Kunden dem vom Kunden benannten Ansprechpartner (z.B. Key user) oder dem User selber mitgeteilt.

6.2.2 Neue Rollenzuordnung

Trigger, die diesen Prozess auslösen

- Antrag auf Rollenübergabe
- Antrag auf bestimmte Rechte

Prozess für AEB Mitarbeiter

- Antrag geht an den Rollenverantwortlichen
- Der Rollenverantwortliche

  - prüft, ob der Mitarbeiter die Rolle bekommen kann und ggf. notwendige Voraussetzungen erfüllt
  - klärt mit dem Mitarbeiter, ob er die Rolle und die damit verbundenen Pflichten und Rechte bekommen möchte
- Bei Freigabe: Mitarbeiter wird in die Rolle aufgenommen und bekommt dadurch automatisch die Rechte
- Bei Ablehnung: Antragsteller wird über die Ablehnung und die Gründe informiert

Prozess für Kunden

- Antrag geht an den Verantwortlichen
- Der Verantwortliche
  - prüft ggf., ob der User die notwendigen Voraussetzungen erfüllt
  - klärt mit dem vom Kunden benannten Ansprechpartner (z.B. Key user), ob der User die Rechte bekommen soll/kann
- Bei Freigabe: User wird in die Gruppe aufgenommen und bekommt dadurch automatisch die Rechte
- Bei Ablehnung: Antragsteller wird über die Ablehnung und die Gründe informiert

6.2.3 Rolle abgeben

Trigger, die diesen Prozess auslösen

- Antrag auf Rollen/Rechte abgeben durch den User
- Antrag auf Rollen/Rechte abgeben durch Dritten

Prozess für Mitarbeiter

- Antrag geht an den Rollenverantwortlichen
- Der Rollenverantwortliche
  - klärt mit dem Antragsteller, warum der User die Rolle/Rechte abgeben soll/will
  - klärt mit dem Mitarbeiter, ob er die Rolle und die damit verbundenen Pflichten und Rechte abgeben möchte oder klärt ihn darüber auf, dass das nun passiert
- Bei Freigabe: Mitarbeiter wird aus der Rolle genommen und verliert dadurch automatisch die Rechte
- Bei Ablehnung: Antragsteller wird über die Ablehnung und die Gründe informiert

Prozess für Kunden

- Antrag geht an den Verantwortlichen
- Der Verantwortliche klärt mit dem vom Kunden benannten Ansprechpartner (z.B. Key user), ob der User die Rechte/Rolle entzogen bekommen soll/kann
- Bei Freigabe: User wird aus der Gruppe genommen und verliert dadurch automatisch die Rechte
- Bei Ablehnung: Antragsteller wird über die Ablehnung und die Gründe informiert

6.2.4 User deaktivieren

Trigger, die diesen Prozess auslösen

- AEB Mitarbeiter verlässt die AEB
- Mitarbeiter des Kunden verlässt das Unternehmen
- Antrag den User des Kunden zu deaktivieren

Prozess für Mitarbeiter

- Bei „Gefahr in Verzug“ kann das Konto sofort durch den Bearbeiter des Antrags deaktiviert werden. Danach leitet er den Antrag mit einem entsprechenden Hinweis an die Mitarbeiterbetreuung
- Ansonsten wird der Antrag an die Mitarbeiterbetreuung weitergeleitet
- Wenn der Mitarbeiter das Unternehmen verlässt, wird mit Ende des letzten Arbeitstags (gepflegt im Personalsystem) automatisch das User-Konto deaktiviert
- Die Mitarbeiterbetreuung hat die Möglichkeit im Personalsystem eine Kennung zu setzen „Netzzugang sperren“. Sobald das gesetzt ist, wird das User Konto automatisch sofort deaktiviert

Prozess für Kunden

- Bei „Gefahr in Verzug“ kann das Konto sofort durch den Bearbeiter des Antrags deaktiviert werden. Danach oder wenn keine unmittelbare Handlung notwendig ist, findet das Folgende statt:
- Der für den Request verantwortliche Mitarbeiter der AEB klärt mit dem vom Kunden benannten Ansprechpartner (z.B. Key user), ob der User den Account verlieren soll/kann.
- Bei Freigabe: User wird gelöscht
- Bei Ablehnung: Antragsteller wird über die Ablehnung und die Gründe informiert

6.3 Regelmäßige Überprüfungen

Trigger, die dies für Mitarbeiter auslösen

- Regelmäßige Routinen der Rollenverantwortlichen und Applikationsmanager
- Regelmäßige Mitarbeitergespräche

Prozess für Mitarbeiter

- Sowohl von Rollenverantwortlichen als auch von Mitarbeiterverantwortlichen werden regelmäßig die Zuordnungen von Mitarbeitern zu Rollen geprüft und ggf. einer der oben genannten Prozesse (z.B. MA gibt Rolle ab) angestoßen
- Sowohl von Rollenverantwortlichen als auch von den Applikationsmanagern werden regelmäßig die Zuordnungen von Rollen zu Rechten geprüft und ggf. entsprechend Rechte und Rollen Zuordnungen korrigiert.

Trigger, die dies für Kunden auslösen

- Regelmäßig automatisch anlaufende Routinen

Prozess für Kunden

- Jeden Tag wird geprüft, ob ein Konto länger als 42 Tage nicht mehr benutzt worden ist.
- Konten, die dem entsprechen, werden automatisch deaktiviert