Sicherheitskonzept

Details zu Zutritt, Zugang und Zugriff

November 2024

Inhalt

1	Allgemein	1
2	Prinzipien	1
2.1	Rollenkonzept	1
2.1.1	Verwendung für Mitarbeiterkonten	1
2.1.2	Verwendung für Kundenkonten	1
2.2	Benutzerkonten	1
2.2.1	Prinzipien zu Passwörtern	1
2.2.2	Passwort Rotation	2
2.2.3	Biometrische Erkennung	2
2.2.4	Multi Faktor Authentifizierung	3
2.2.5	User Repository- oder Domänenkopplungen	3
2.2.6	Automatische Kontenlöschung / Deaktivierung von Konten	3
2.3	Administrative/privilegierte Rollen	3
2.3.1	Prinzipien zu Passwörter von privilegierten Konten	3
3	Zutritt im Detail	5
3.1	Öffentlicher Bereich	5
3.2	Privater Bereich	5
3.3	Besonders geschützte Bereiche	6
4	Zugang und Zugriff im Detail	7
4.1	Grundsätzliches	7
4.1.1	Details zum Normalfall „AEB-Netz“	7
4.1.2	Details zum Sonderfall „Remotezugang“ (z.B. HomeOffice)	7
4.1.3	Details zu Anwendungen	7
4.2	Verschlüsselung	8
4.3	Protokollierung	8

5 Anhang - Prozesse 9
5.1 Grundsätzlich 9
5.2 Prozesse 9
5.2.1 Neuer User 9
5.2.2 Neue Rollenzuordnung 9
5.2.3 Rolle abgeben 10
5.2.4 User deaktivieren 10
5.2.5 Regelmäßige Überprüfungen 10

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, Netze und Konten sind, egal wo sie sich befinden, gegen unbefugten Zutritt, Zugang oder Zugriff individuell geschützt.

2.1 Rollenkonzept

AEB gewährt Kunden, Mitarbeitenden und Partnern Zutritt, Zugang und Zugriff mithilfe zentraler User Repositories und einem rollenbasierenden Sicherheitsmodell. Dadurch erhalten Anwender*innen Zugriff nur auf die Anwendungen und Umgebungen, für die sie auch berechtigt sind.

Konten werden in Sicherheitsgruppen zusammengefasst. Es wird nicht das einzelne Konten-Objekt berechtigt, sondern immer die Gruppen-Objekte.

2.1.1 Verwendung für Mitarbeiterkonten

Das Anlegen neuer Konten/Zugängen für Mitarbeitende sowie die Berechtigungsfreigabe und das Zuordnen zu Rollen erfolgen immer nur auf schriftlichen Auftrag und entsprechender Freigabe nach dem „need to know“-Prinzip (siehe Prozesse im Anhang).

2.1.2 Verwendung für Kundenkonten

Für Kunden wird ein erstes Kundenkonto angelegt und in alle kundenindividuellen Administratorgruppen aufgenommen.

Das Anlegen neuer Konten/Zugängen sowie die Zuordnung zu den Sicherheitsgruppen erfolgt danach in Eigenverantwortung des Kunden.

2.2 Benutzerkonten

Alle Mitarbeitende, Kundenkontakte und alle Partner erhelten eine persönliche Zugangskennung und ein Zugangspasswort. Nur dieser Zugang kann und darf genutzt werden.

2.2.1 Prinzipien zu Passwörtern

Für Passwörter sind die Kontoinhaber verantwortlich.

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

Diese Regelungen gelten einheitlich für folgende Konten-Arten: Mitarbeitende, Kunden und Dienste.

Wo immer möglich wird ein zweiter Faktor erzwungen.

Passwörter müssen aus mindestens 11 Zeichen insgesamt bestehen.

Passwörter müssen mindestens drei der vier Punkte enthalten

- Mindestens eine Zahl
- Mindestens ein Sonderzeichen (Nicht alphanumerische Zeichen)
- Mindestens einen Großbuchstaben und
- Mindestens einen Kleinbuchstaben

Das wird automatisch durch eine zentrale Richtlinie erzwungen.

2.2.2 Passwort Rotation

Für Konten der Mitarbeitenden der AEB

AEB folgt für diese Konten den Erkenntnissen und den Empfehlungen von z.B. NIST oder BSI keine Passwortrotation vorzusehen, um die Sicherheit zu erhöhen.

Für Kundenkonten

In der AEB-Plattform (nXt) ist keine Passwortrotation vorgesehen. Dies enspricht den Erkenntnissen und Empfehlungen von z.B. NIST oder BSI .

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

2.2.3 Biometrische Erkennung

Biometrische Erkennung, wenn sie nicht pauschal für einen globalen Account aber für das Login an genau einem Gerät genutzt werden können, sind für AEB Mitarbeitende eine mögliche Alternative. Diese Geräte werden auch entsprechend geschützt. Z.B. durch erzwingbare Regeln für das Login und für remote Wipe (z.B. durch MAM/MDM bei aktuellen Android, iOS oder von AEB bereit gestellten macOS Geräten).

Wir erlauben daher Login per Fingerprint und moderner Gesichtserkennung (mit Tiefenscan) explizit für

- Windows Hello für AEB Notebooks mit mindestens Windows 11
- Aktuelles Mac OS auf AEB Mac Devices
- Apple iOS/iPadOS Devices
- Android Smartphones

Dazu wird erzwungen (zusätzlich zu anderen Regeln):

- Remote Wipe manuell durch einen Administrator auslösbar
- Remote Wipe bei 10 falschen Versuchen
- Für Windows 11 Hello zusätzlich:

- eine 7-stellige Pin

Biometrische Erkennung ist für privilegierte Accounts nicht erlaubt.

2.2.4 Multi Faktor Authentifizierung

Ist für AEB Mitarbeitende und Partner in allen Fällen aktiv.

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

2.2.5 User Repository- oder Domänenkopplungen

Eine Anbindung externer User Repositories, einer Kundendomäne oder die Verwendung von LDAP Verzeichnissen ist in der AEB Private Cloud möglich.

2.2.6 Automatische Kontenlöschung / Deaktivierung von Konten

Ein Account wird nach 180 Tagen Inaktivität deaktiviert/gesperrt

Ein Account wird nach 360 Tagen Inaktivität gelöscht

Ein unbestätigter Account den AEB Mitarbeitenden für jemanden anlegt, wird nach 30 Tagen gelöscht.

Ein unbestätigter Account den man sich selber anlegt, wird nach 7 Tagen gelöscht.

2.3 Administrative/privilegierte Rollen

Auch Anwender*innen mit besonderen administrativen oder privilegierten Rechten sind in geeigneten Sicherheitsgruppen zusammengefasst und unterliegen den entsprechenden Prozessen und Freigaben.

Verantwortliche für dies zugehörigen Rollen sind üblicherweise IT Leitende, der/die IT-Security Manager*in oder die Geschäftsleitung.

Für besonders privilegierte Rechte (z.B. Firewall-Zugriff, Admin Portale, SSH Keys Passphrase, ...) müssen Anwender*innnen ein besonderes personalisiertes Administrations-Konto nutzen, das „normale“ User-Konto bekommt diese Rechte nicht / kann nicht den entsprechenden Rollen zugeordnet werden.

2.3.1 Prinzipien zu Passwörter von privilegierten Konten

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 haben mindestens 14 (vierzehn) Zeichen

Passwörter müssen mindestens drei der folgenden vier Punkte erfüllen:

- Mindestens ein Großbuchstabe
- Mindestens ein Kleinbuchstabe
- Mindestens eine Zahl

- Mindestens ein Sonderzeichen (Nicht alphanumerische Zeichen)

Besonders zu beachten ist, dass die letzten 24 Kennwörter nicht wieder verwendet werden dürfen.

Wo immer möglich wird ein zweiter Faktor erzwungen.

3 Zutritt im Detail

Die AEB Gebäude sind in Sicherheitszonen aufgeteilt. Es gibt

- öffentliche Bereiche
- private Bereiche
- besonders geschützte Bereiche.

Die Detaillierung, die für alle AEB Standorte gilt, finden sich im Folgenden. Für das HQ ist es hier dann nochmal standortspezifisch ausgeprägt. Für alle anderen Standorte findet sich die standortspezifische Ausprägung in der jeweiligen "Sicherheitsmaßnahmen am Standort..." (s.u.). Generell behandeln wir aber Standorte mit Ausnahme des HQ als generell "private Bereiche".

3.1 Öffentlicher Bereich

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

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

Für Mitarbeitende oder für ihre begleiteten Gäste ist der Zutritt in diesen Bereich auch außerhalb der Öffnungszeiten, z.B. mit dem entsprechenden personalisierten Transponder möglich.

Für das HQ:

Die Öffnungszeiten der Haupteingangstüre (manuelle Steuerung) sind Montag bis Freitag zwischen 8:00 und 17:00 Uhr. Die Öffnungszeiten der Tiefgarage weichen ab, Einfahrtseite 7 – 10 Uhr und Ausfahrtseite 15 – 16.50 Uhr. Außerhalb dieser Zeiten sind die Tore geschlossen.

Zutritte außerhalb der Öffnungszeiten sind nur mit autorisierten Transpondern möglich. Zusätzlich wird dieser Bereich durch einen Sicherheitsdienst überwacht.

Teile des Bereichs sind videoüberwacht und entsprechend gekennzeichnet, siehe Videoüberwachung Stuttgart. Der Bereich umfasst die Außenanlagen und die Tiefgarage bis auf die unten genannten "Besonders geschützten Bereiche"

3.2 Privater Bereich

Dieser Bereich ist für Mitarbeitende, begleitete und beaufsichtigte Gäste und wenige Partner zugänglich.

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

Für das HQ

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

Sämtliche Zutrittsberechtigungen werden über die Schließanlage programmiert.

Dieser Bereich umfasst alle Obergeschosse bis auf die unten genannten "besonders geschützten Bereiche"

3.3 Besonders geschützte Bereiche

Als besonders geschützte Bereiche verstehen wir Bereiche, in denen

- Daten mit erhöhtem Schutzbedarf / Schutzbedarfsanalyse gehalten werden
- Tätigkeiten erfolgen, die besondere, besonders geschulte Rollen aus Security erfordern

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.

Dies sind unter anderem:

- die Rechenzentren
- Archiv
- alle Netzwerkverteiler
- Räume mit Personalakten oder Buchhaltungsdaten
- Räume zur technischen Infrastruktur (Energieversorgung und Sicherheitseinrichtungen)

Der Zutritt ist jeweils nur den relevanten Rollen auf ihren personalisierten Transponder kodiert sowie meist mit einem weiteren Secret (z.B. Pin code), so dass z.B. nur IT-Administratoren Zutritt zu den Rechenzentren haben.

Sämtliche Zutrittsberechtigungen werden über die Schließanlage programmiert.

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 Mitarbeitende und Partner immer mit drei Faktoren:

1. Login name
2. Passwort
3. Weiteres Secret (z.B. onetime Password, Transponder, Zertifikat, …)

Der Zugang von AEB-Mitarbeiterende zu Kundenressourcen erfolgt auf Wunsch des Kunden entweder mit zwei Faktoren (Login Name 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“ (z.B. HomeOffice)

Remotezugang auf Kundendaten/-anwendungen kann nicht direkt erfolgen.

Mitarbeitende müssen sich immer erst mit drei Faktoren (Ein Account und zwei Secrets) am AEB-Netz authentifizieren. Und können 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, legen die jeweiligen fachlichen Applikationsmanager zusammen mit den Rollenverantwortlichen, 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.

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 - Prozesse

5.1 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.

5.2 Prozesse

5.2.1 Neuer User

Trigger, die diesen Prozess auslösen

- Antrag durch Personalabteilung im Zuge des Onboardings

Prozess für AEB Mitarbeitende

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

5.2.2 Neue Rollenzuordnung

Trigger, die diesen Prozess auslösen

- Antrag auf Rollenübergabe
- Entstehung einer neuen Rolle
- Antrag auf bestimmte Rechte
- Mitarbeitende füllt eine Rolle bereits aus und bekommt sie daher übertragen

Prozess für AEB Mitarbeitende

- Antrag geht an die Rollenverantwortlichen
- Rollenverantwortliche
  - prüfen ob Mitarbeitende die Rolle bekommen können und ggf. notwendige Voraussetzungen erfüllen
  - klären mit den Mitarbeitenden, ob sie die Rolle und die damit verbundenen Pflichten und Rechte bekommen möchten
- Bei Freigabe: Mitarbeitende werden in die Rolle aufgenommen und bekommt dadurch automatisch die Rechte
- Bei Ablehnung: Mitarbeitende werden über die Ablehnung und die Gründe informiert

5.2.3 Rolle abgeben

Trigger, die diesen Prozess auslösen

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

Prozess für Mitarbeitende

- Antrag geht an die Rollenverantwortlichen
- Die Rollenverantwortlichen
  - klären mit den Antragsteller*innen, warum der User die Rolle/Rechte abgeben soll/will
  - klären mit den Mitarbeitenden, ob sie die Rolle und die damit verbundenen Pflichten und Rechte abgeben möchten oder klären sie darüber auf, dass das nun passiert
- Bei Freigabe: Mitarbeitende werden aus der Rolle genommen und verlieren dadurch automatisch die Rechte
- Bei Ablehnung: Mitarbeitende werden über die Ablehnung und die Gründe informiert

5.2.4 User deaktivieren

Trigger, die diesen Prozess auslösen

- AEB Mitarbeitende verlassen die AEB

Prozess für Mitarbeitende

- Bei „Gefahr in Verzug“ kann das Konto sofort durch den Bearbeiter des Antrags deaktiviert werden. Danach leitet er/sie den Antrag mit einem entsprechenden Hinweis an die Mitarbeiterbetreuung
- Ansonsten wird der Antrag an die Mitarbeiterbetreuung weitergeleitet
- Wenn der/die Mitarbeitende 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

5.2.5 Regelmäßige Überprüfungen

Trigger, die dies auslösen

- Regelmäßige (mindestens jährliche) Routinen der Rollenverantwortlichen und Applikationsmanager
- Jährliche Inventur des Systemmanagements der Rechte in der Domäne
- Regelmäßige Mitarbeitergespräche

Prozess für Mitarbeitende

- Sowohl von Rollenverantwortlichen als auch von Mitarbeiterverantwortlichen werden regelmäßig (mindestens jährlich) die Zuordnungen von Mitarbeitern zu Rollen geprüft und ggf. einer der oben genannten Prozesse (z.B. Mitarbeitende gibt Rolle ab) angestoßen
- Sowohl von Rollenverantwortlichen als auch von den Applikationsmanagern werden regelmäßig (mindestens jährlich) 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 werden alle Konten geprüft:

- Ein Account wird nach 180 Tagen Inaktivität deaktiviert/gesperrt
- Ein Account wird nach 360 Tagen Inaktivität gelöscht
- Ein unbestätigter Account den eine AEB Mitarbeitende für jemanden anlegt wird nach 30 Tagen gelöscht.
- Ein unbestätigter Account den man sich selber anlegt wird nach 7 Tagen gelöscht