Security Whitepaper

MABEX-CyberCore

1. Einführung

Die Sicherheit und der Schutz der Daten unserer Kunden steht bei MABEX-CyberCore im Mittelpunkt. Unser System ist darauf ausgelegt, moderne Sicherheitsstandards zu erfüllen, zuverlässigen Betrieb zu ermöglichen und die gesetzlichen Datenschutzvorgaben wirksam umzusetzen. Transparenz, Zuverlässigkeit und Vertrauenswürdigkeit sind dabei die Leitprinzipien unserer Arbeit.

MABEX-CyberCore setzt auf ein umfangreiches Sicherheitskonzept, bei dem sämtliche Kommunikationswege und Systembereiche voneinander getrennt und überwacht sind. Angriffsversuche werden durch verschiedene Kontroll- und Schutzmechanismen auf mehreren Ebenen erkannt und abgewehrt. Sämtliche Daten werden zudem regelmäßig verschlüsselt gesichert.

2. Infrastruktur und Schutzmaßnahmen

2.1 MEHRSCHICHTIGE SICHERHEITSARCHITEKTUR

- Segmentierung und Zugriffskontrolle

  Die Infrastruktur ist logisch in getrennte Bereiche gegliedert. Öffentlich erreichbare Dienste, administrative Zugänge und Backup-Prozesse werden voneinander getrennt und durch technische Zugriffsbeschränkungen geschützt. Administrative Zugriffe erfolgen ausschließlich über abgesicherte Wege.

- Firewall- und Angriffserkennung

  Der gesamte Netzwerkverkehr wird durch Schutzsysteme überwacht und analysiert, um unberechtigte Zugriffe und Angriffsversuche frühzeitig zu erkennen und automatisch zu blockieren.

- Verschlüsselung

  Alle externen und internen Verbindungen sind durch starke Verschlüsselung abgesichert, um die Vertraulichkeit und Integrität der Daten zu gewährleisten.

- Schutz vor Überlastungsangriffen (DDoS)

  Um die Erreichbarkeit der Dienste auch bei Überlastungsangriffen (DDoS) bestmöglich sicherzustellen, sind externe Schutzmechanismen vorgeschaltet. Angriffe werden automatisch erkannt und es werden geeignete Gegenmaßnahmen eingeleitet. Ein vollständiger Schutz vor DDoS-Angriffen kann jedoch (wie branchenweit üblich) nicht garantiert werden.

2.2 SYSTEMHÄRTUNG UND WARTUNG

- Regelmäßige Sicherheitsupdates

  Betriebssysteme, Anwendungen und sämtliche Systemkomponenten werden laufend überwacht (Monitoring) und bei Bedarf unverzüglich aktualisiert.

- Zugangsmanagement

  Verwaltungsschnittstellen und sensible Bereiche sind durch starke Passwörter, Zwei-Faktor-Authentifizierung und zusätzliche Schutzmaßnahmen gesichert. Zugangsdaten werden verschlüsselt aufbewahrt und regelmäßig überprüft.

2.3 DATENSICHERUNG UND NOTFALLMANAGEMENT

- Backups

  Alle betriebskritischen Daten werden täglich gesichert. Die Backups werden gemäß der 3-2-1-Backup-Strategie (drei Kopien, zwei Medientypen, eine Kopie extern) erstellt und verschlüsselt sowohl lokal als auch an externen, geografisch getrennten Standorten innerhalb Deutschlands gespeichert.

- Erprobte Wiederherstellungsmaßnahmen

  Die Wiederherstellung der Systeme und Daten ist erprobt, um eine schnelle und zeitnahe Wiederinbetriebnahme im Notfall sicherzustellen.

2.4 KOMMUNIKATIONSSICHERHEIT

- E-Mail-Provider

  Für die sichere und zuverlässige Abwicklung des E-Mail-Verkehrs und anderer Kommunikationsdienste werden ausschließlich bewährte und DSGVO-konforme externe Anbieter genutzt.

- Kommunikationssicherheit

  Der gesamte E-Mail-Verkehr ist durch moderne Authentifizierungs- und Überprüfungsverfahren wie DMARC, DKIM und SPF abgesichert. So wird verhindert, dass E-Mails im Namen von MABEX-CyberCore (sowie die von uns betriebenen Projekte) gefälscht oder missbraucht werden können. Gleichzeitig sorgt diese Konfiguration für eine hohe Zustellbarkeit und einen zuverlässigen Schutz vor Phishing.

3. Anwendungssicherheit

- Strikte Transportverschlüsselung

  Der gesamte Datenverkehr zwischen Nutzer und System wird ausschließlich über verschlüsselte Verbindungen abgewickelt. Zusätzlich ist die Infrastruktur so konfiguriert, dass ausschließlich sichere HTTPS-Verbindungen erlaubt sind. Durch den Einsatz von HTTP Strict Transport Security (HSTS) wird sichergestellt, dass Browser ausschließlich verschlüsselte Verbindungen aufbauen können. Ein Zugriff über unverschlüsselte Kanäle ist technisch ausgeschlossen.

- Strenge Eingabevalidierung

  Alle Benutzer- und Systemeingaben werden umfassend geprüft (client- und serverseitig), um Manipulation und Missbrauch zu verhindern.

- Geschütztes Sitzungsmanagement

  Sitzungen werden automatisch überwacht und nach Inaktivität oder bei Unregelmäßigkeiten beendet.

- Datenverschlüsselung

  Sämtliche sensiblen Eingaben, die Dritte betreffen oder besonders schützenswert sind, werden ausschließlich verschlüsselt in der Datenbank gespeichert (AES-256-Verschlüsselung) und sind für MABEX-CyberCore nicht im Klartext einsehbar.

- Kennwortsicherheit

  Kennwörter und API-Schlüssel werden ausschließlich als unlesbare Hashwerte (inkl. individueller Salt) unter Anwendung aktueller kryptografischer Verfahren gespeichert. Ein Auslesen der Klartext-Passwörter ist technisch ausgeschlossen.

- Mehrfaktor-Authentifizierung

  Der Zugriff auf sensible Systembereiche ist durch Mehrfaktor-Authentifizierung (sofern möglich) abgesichert.

4. Datenschutz und Compliance

- Datenverarbeitung

  Die Produktiv- und Backupebene von MABEX-CyberCore ist redundant und räumlich getrennt aufgebaut. Die produktiven Systeme werden in einem professionellen deutschen Rechenzentrum betrieben. Für Sicherungs- und Wiederherstellungsprozesse kommen zusätzlich eigene Server- und Speichersysteme zum Einsatz. Betriebskritische Daten werden täglich gesichert, verschlüsselt übertragen und getrennt von der Produktivumgebung gespeichert. Zusätzlich werden die Sicherungen an einen weiteren, geografisch getrennten Rechenzentrumsstandort in Deutschland übertragen. Produktivsystem, lokale Sicherungsebene und externe Offsite-Sicherung sind dadurch technisch und räumlich voneinander getrennt. Vor jeder erstmaligen Datenübertragung wird mit jedem eingesetzten Dienstleister ein entsprechender Auftragsverarbeitungsvertrag (AVV) abgeschlossen. Eine Übermittlung in Drittländer findet nicht statt.

- DSGVO-Konformität

  Sämtliche Prozesse und Systeme entsprechen den Vorgaben der DSGVO und den einschlägigen nationalen Datenschutzgesetzen.

- Datensparsamkeit und Transparenz

  Es werden nur solche Daten verarbeitet, die zur Leistungserbringung erforderlich sind. Alle Verarbeitungen sind dokumentiert und nachvollziehbar.

5. Überwachung und Angriffserkennung

- Echtzeit-Überwachung

  Die gesamte Infrastruktur wird rund um die Uhr automatisiert überwacht. Auffälligkeiten und potenzielle Angriffe werden sofort erkannt und umgehend behandelt.

- Automatische Schutzmechanismen

  Wiederholte unberechtigte Zugriffsversuche werden automatisch erkannt und blockiert.

6. Physische Sicherheit und Ausfallschutz

- Die physische Sicherheit der produktiven Serverinfrastruktur wird durch den eingesetzten Rechenzentrumsdienstleister sichergestellt. Die produktiven Systeme befinden sich in einer professionellen Rechenzentrumsumgebung mit kontrolliertem Zutritt, stabiler Stromversorgung, Klimatisierung, Brandfrüherkennung, Überwachung und abgesicherter Netzwerkanbindung.

- MABEX-CyberCore ergänzt diese Rechenzentrumsmaßnahmen durch eigene Schutzmaßnahmen auf Server-, Netzwerk- und Anwendungsebene. Dazu gehören insbesondere restriktive Zugriffskontrollen, gehärtete Serverkonfigurationen, Firewall-Regeln, Web Application Firewall, Protokollauswertung, System- und Verfügbarkeitsmonitoring sowie regelmäßige Datensicherungen.

- Ergänzend wird eine eigene Backup-Infrastruktur betrieben, die getrennt von der Produktivumgebung arbeitet. Dadurch werden Produktivbetrieb, lokale Sicherungsebene und externe Offsite-Sicherung klar voneinander getrennt.

7. Fortlaufende Optimierung

- Regelmäßige Prüfungen

  Die eingesetzten Schutzmaßnahmen werden fortlaufend durch Überprüfungen auf Wirksamkeit und Aktualität kontrolliert.

- Prozesse zur Verbesserung

  Sicherheitsprozesse werden regelmäßig überprüft und an neue Anforderungen und Bedrohungslagen angepasst.

8. Ihr Mehrwert mit MABEX-CyberCore

Mit MABEX-CyberCore erhalten Sie Lösungen, die auf modernste Sicherheitsstandards und höchste Datenschutzanforderungen setzen, ohne Kompromisse bei Zuverlässigkeit, Transparenz und Nutzerfreundlichkeit.

9. Kontakt bei offenen Fragen

Kontaktieren Sie uns bei offenen Fragen zum Whitepaper gerne per E-Mail unter: whitepaper@mabex-cybercore.de