EXTRA Group | TRUST CENTER

Security Whitepaper

Technische Sicherheitsarchitektur, Verschlüsselungs- und Zugriffsmodelle, Backup- & Recovery-Konzepte

EXTRA Group GmbH – Digital Innovation Studio

Version: 1.0
Stand: 19.02.2024

1. Management Summary

Die EXTRA Group GmbH („EXTRA Group“) entwickelt und betreibt Enterprise-fähige digitale Plattformen, Community-Layer-Lösungen, AI-Automation und Digital Commerce Systeme für Kunden aus Medien, Handel, Hospitality und weiteren Branchen. Sicherheit, Verfügbarkeit und Compliance sind grundlegende Designprinzipien und kein nachgelagerter Zusatz.

Dieses Whitepaper gibt einen kompakten, aber technisch fundierten Überblick über die Sicherheitsarchitektur, das Verschlüsselungs- und Zugriffsmodell sowie die Backup-, Recovery- und Business-Continuity-Konzepte der EXTRA Group.

- Zielgruppe des Dokuments sind insbesondere:
- CISOs und IT-Sicherheitsverantwortliche
- IT-Architekt:innen und technische Entscheider
- Compliance-, Datenschutz- und Procurement-Teams

2. Sicherheitsgrundsätze & Governance

Unsere Sicherheitsarchitektur folgt klaren Leitprinzipien:

- Security by Design & by Default – Sicherheitsanforderungen werden bereits in der Architekturphase definiert und in allen Projektphasen berücksichtigt.
- Least Privilege & Need to Know – Jede Person und jeder Service erhält nur die Berechtigungen, die zur Aufgabenerfüllung unbedingt erforderlich sind.
- Defense in Depth – Mehrschichtige Schutzmechanismen auf Infrastruktur-, Netzwerk-, Applikations- und Datenebene minimieren das Risiko einzelner Komponentenausfälle oder Kompromittierungen.
- Data Residency & Data Ownership – Kunden behalten die volle Datenhoheit; produktive Daten werden in Rechenzentren in Deutschland/EU verarbeitet.
- Transparente Governance – Richtlinien zu Informationssicherheit, Zugriff, Entwicklung und Incident Response sind dokumentiert, werden regelmäßig überprüft und Mitarbeitenden vermittelt.

3. Architekturüberblick

Die Sicherheitsarchitektur der EXTRA Group lässt sich auf drei Ebenen zusammenfassen:

- Infrastruktur- & Netzwerkebene – Rechenzentren, Netzsegmentierung, Firewalls, Security Groups.
- Applikations- & Serviceebene – modularisierte Architektur, abgesicherte Schnittstellen, zentrales Monitoring.
- Daten- & Identitätsebene – Trennung von Datenarten, zentrales Identity & Access Management, Verschlüsselung.

4. Infrastruktur- & Netzwerksicherheit

4.1 Rechenzentren & Hosting

- Nutzung von Rechenzentren mit ISO-27001-Zertifizierung und hoher physischer Sicherheit:
- Zutrittskontrollen (Zugangskarten, Videoüberwachung, Logging).
- Redundante Strom- und Klimaversorgung sowie Brandfrüherkennung.
- Geo-redundante Auslegung kritischer Systeme, wo erforderlich.

4.2 Netzwerksegmentierung & Perimeterschutz

- Trennung der Umgebungen in Development, Staging und Production.
- Segmentierung der Produktivumgebungen in Sicherheitszonen (DMZ, Application Zone, Data Zone).
- Einsatz von Firewalls und Security Groups zur Beschränkung der Kommunikation auf notwendige Ports und Protokolle.

4.3 Schutz vor Angriffen

- Einsatz von Web Application Firewalls (WAF) für öffentlich erreichbare Services.
- Rate Limiting, IP-Blocking und Bot-Erkennung für kritische Endpunkte.
- Regelmäßige Schwachstellenscans auf Infrastruktur- und Betriebssystemebene.

5. Identity & Access Management (IAM) – Zugriffsmodell

5.1 Benutzeridentitäten & Authentifizierung

- Individuelle Benutzerkonten – keine geteilten Accounts.
- Multi-Faktor-Authentifizierung (MFA) für Administratorzugriffe und besonders schützenswerte Bereiche.
- Optionale Anbindung an Kunden-Identitätslösungen (z. B. SAML / OpenID Connect für Single Sign-on).

5.2 Rollen- & Rechtekonzept (RBAC)

- Zugriffsmodell auf Basis von Role Based Access Control (RBAC):
- Definition von Rollen (z. B. Viewer, Editor, Admin, Security Officer, Customer Project Admin).
- Zuweisung von Rechten zu Rollen, Zuweisung von Rollen zu Benutzern nach Funktion.
- Minimierung individueller Einzelrechte, klare Zuordnung von Verantwortlichkeiten.
- Regelmäßige Rezertifizierung von Berechtigungen (z. B. halbjährlich oder projektabhängig).

5.3 Service-to-Service-Authentifizierung

- Authentifizierung zwischen Microservices und Backend-Komponenten über kurzlebige Tokens (z. B. JWT) oder mTLS.
- Verwaltung von Secrets (API-Keys, Tokens, Zertifikate) in dedizierten Secret-Stores, nicht im Code oder in Repositories.

6. Daten- & Verschlüsselungsmodell

6.1 Datenklassifizierung

- Daten werden pragmatisch klassifiziert, um passende Schutzmaßnahmen anzuwenden:
- Öffentlich – frei zugängliche Informationen.
- Intern – interne Informationen ohne besondere Schutzbedürftigkeit.
- Vertraulich – Kunden- und Betriebsdaten.
- Hochvertraulich – personenbezogene Daten mit erhöhtem Schutzbedarf, Zugangsdaten, kryptographisches Material.

6.2 Verschlüsselung im Transit

- Grundsatz: TLS everywhere für alle relevanten Kommunikationskanäle.
- Öffentliche Services sind mindestens mit TLS 1.2/1.3 abgesichert.
- Zertifikatsmanagement mit automatisierter Erneuerung und Härtung der Cipher Suites.

6.3 Verschlüsselung at Rest

- Datenbanken und Speicher werden, wo technisch möglich, mit Encryption at Rest betrieben (z. B. AES-256).
- Backups und Snapshots werden standardmäßig verschlüsselt.
- Schlüsselverwaltung über dedizierte Key-Management-Systeme bzw. KMS/HSM-Lösungen der Infrastrukturprovider.

6.4 Pseudonymisierung & Minimierung

- Einsatz von Pseudonymisierung, wo fachlich möglich (z. B. interne User-IDs in Logs).
- Keine produktiven personenbezogenen Daten in Entwicklungs- oder Testumgebungen; Einsatz anonymisierter oder synthetischer Daten.
- Erhebung nur der Daten, die für den jeweiligen Zweck erforderlich sind (Privacy by Design & Default).

7. Application Security & Secure Development Lifecycle (SDLC)

7.1 Entwicklungsprozesse

- Etablierter Secure Software Development Lifecycle (SSDLC):
- Security-Anforderungen bereits in der Architekturphase.
- Bedrohungsmodellierung für kritische Komponenten.
- Security-Checklisten bei Code-Reviews.
- Versionskontrolle über Git mit Branching-Strategien und Pull Requests.
- Vier-Augen-Prinzip für kritische Änderungen.

7.2 Statische & dynamische Prüfungen

- Statische Codeanalyse (SAST) für relevante Sprachen und Frameworks.
- Dependency-Scanning für Bibliotheken und Frameworks (Überwachung bekannter Schwachstellen).
- Dynamische Tests (DAST) auf Staging-Umgebungen für kritische Anwendungen (z. B. OWASP Top 10).

7.3 Härtung & Konfiguration

- Standardisierte Härtung von Betriebssystemen, Containern und Images (Secure Baselines).
- Deaktivierung unnötiger Dienste und Ports.
- Konfigurationsmanagement mit deklarativen Templates (Infrastructure as Code) und Versionierung.

8. Logging, Monitoring & Incident Response

8.1 Logging & Audit Trails

- Zentrale Protokollierung von sicherheitsrelevanten Ereignissen (Authentifizierungen, Berechtigungsänderungen, Konfigurationsänderungen, kritische Fehler).
- Manipulationssichere Speicherung von Logs mit definierten Aufbewahrungsfristen.

8.2 Monitoring & Alerting

- Zentrales Monitoring von Verfügbarkeit, Antwortzeiten, Ressourcenauslastung und definierten Security-Events.
- 24/7-Alerting mit abgestuften Eskalationsplänen und On-Call-Rotation.

8.3 Incident Response

- Dokumentierte Incident-Response-Prozesse (Erkennung, Bewertung, Eindämmung, Behebung, Post-Mortem).
- Forensische Sicherung relevanter Daten bei sicherheitsrelevanten Vorfällen.
- Abgestimmte Kommunikation mit Kunden und ggf. Aufsichtsbehörden durch den Verantwortlichen.
- Regelmäßige Übungen und Simulationen zur Überprüfung der Abläufe.

9. Backup, Recovery & Business Continuity

9.1 Backup-Strategie

- Regelmäßige Backups von Datenbanken, Datei- und Objekt-Speichern sowie Konfigurations- und Infrastrukturdefinitionen.
- Verschlüsselte Speicherung der Backups an geo-redundanten Standorten innerhalb Deutschlands/EU.
- Klare Aufbewahrungsfristen (z. B. tägliche Backups, Rolling Retention).

9.2 Recovery-Konzepte

- Definierte Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) je Systemklasse.
- Dokumentierte Wiederherstellungsprozesse für komplette Plattformen, einzelne Datenbanken und Services.
- Regelmäßige Test-Restores zur Validierung von Datenintegrität und Anwendungsfunktionalität.

9.3 Business Continuity

- Analyse kritischer Geschäftsprozesse und Abhängigkeiten.
- Notfallpläne bei Ausfall einzelner Rechenzentren/Regionen oder kritischer Lieferanten.
- Abstimmung von Business-Continuity-Maßnahmen mit Kunden für geschäftskritische Plattformen.

10. Lieferanten- & Subprozessor-Management

- Auswahl von Infrastruktur- und Softwarepartnern nach klaren Kriterien:
- Technische Leistungsfähigkeit und Skalierbarkeit.
- Sicherheitszertifizierungen (z. B. ISO 27001, SOC 2) und Auditberichte.
- Transparente Vertrags- und AV-Regelungen inkl. Datenschutz.
- Abschluss von Auftragsverarbeitungsverträgen mit allen Subprozessoren.
- Regelmäßige Review-Zyklen für Zertifikate, Sicherheitsnachweise und Vertragsupdates.

11. Zusammenfassung & Kontakt

Die Sicherheitsarchitektur der EXTRA Group ist darauf ausgelegt, Enterprise-Anforderungen großer Unternehmen zu erfüllen. Hosting in zertifizierten Rechenzentren in Deutschland/EU, mehrschichtige Sicherheitsmechanismen, ein klares Zugriffs- und Berechtigungsmodell, durchgängige Verschlüsselung sowie etablierte Prozesse für Secure Development, Monitoring, Incident Response und Backup/Recovery bilden die Grundlage.

Auf Anfrage stellen wir projektspezifische Unterlagen (z. B. Netzwerkdiagramme, Detail-TOMs, Penetrationstest-Berichte oder ausgefüllte Sicherheitsfragebögen) zur Verfügung.

Kontakt Security & Compliance:

EXTRA Group GmbH – Security & Compliance Team
Mathes-Deutsch-Weg 24B
84036 Landshut, Deutschland
E-Mail: service@extra-group.com (Betreff: „Security Whitepaper / Anfrage“)