esri Deutschland
THE SCIENCE OF WHERE

Benutzerdefiniert

APP: Business-Anwendungen

APP.bd.1: ArcGIS Enterprise

1 Beschreibung

1.1 Einleitung

ArcGIS Enterprise ist eine IT-Standardplattform zur Verarbeitung von Daten mit Orts- und Zeitbezug. Die zugrundeliegenden Daten beschreiben die Geometrie, Topologie, Thematik und Dynamik von Orten in lokaler Individualität oder globaler Dimension. Man spricht von georeferenzierten Daten oder kürzer „Geodaten“. Für 90% aller Daten trifft es zu, dass ein solcher Orts- und Zeitbezug vorliegt oder mittelbar abgeleitet werden kann. Diese Daten werden oftmals grafisch-visuell (z. B. auf einer Karte oder einem Globus) dargestellt, um die Anschaulichkeit und Aussagekraft für den Nutzer zu erhöhen. Orts- und zeitabhängige Zusammenhänge werden durch Analysen der Daten aufgedeckt. Planungen werden durch diese Ergebnisse optimiert. Orts- und Zeitbezug sind wesentliche Merkmale heute verfügbarer Daten, die durch Sensoren aller Art erfasst werden. Neben Auswertungen für Lagebilder (z. B. für den Status oder die Logistik) lassen sich verschiedenartigste Datenströme, wie Sensor-Daten oder GPS-Daten, für eine Beurteilung durch Verknüpfung mit Geoinformationen aufbereiten. ArcGIS Enterprise dient der Integration dieser Geodaten in die digitalen Prozesse der Institution. ArcGIS Enterprise stellt dazu die notwendigen Daten, Funktionen, Schnittstellen, definierte APIs und Anwendungen bereit. ArcGIS Enterprise wird auf der von der Institution verwalteten IT-Infrastruktur betrieben.

1.2 Zielsetzung

Das Ziel dieses Bausteins besteht darin, geeignete Anforderungen von ArcGIS Enterprise zu formulieren, die beim Aufbau eines Managementsystems für Informationssicherheit (ISMS) zu erfüllen sind.

Der Begriff ArcGIS Enterprise umfasst im Sinne dieses Bausteins die Deployment-Varianten Kubernetes, Linux sowie Windows. Bei den beiden letztgenannten Varianten umfasst der Baustein die Komponenten Portal for ArcGIS, ArcGIS Server, ArcGIS Data Store und ArcGIS Web Adaptor als so genannte ArcGIS Enterprise-Basisbereitstellung. Bei der Variante auf Kubernetes umfasst der Baustein die funktionsgebenden Microservices der ArcGIS Enterprise-Basisbereitstellung auf Kubernetes.

1.3 Abgrenzung

Der Baustein APP.bd.1 *ArcGIS Enterprise* ist auf jedes ArcGIS Enterprise System anzuwenden.

Dieser Baustein weist dazu spezifische Gefährdungen und Anforderungen für die Nutzung aus. Sicherheitsaspekte des IT-Systems der Institution, auf dem ArcGIS Enterprise aufsetzt, werden in den entsprechenden Bausteinen der Schicht IT-Systeme behandelt: SYS.1.1 *Allgemeiner Server*, SYS.1.2 *Allgemeiner Client*, betriebssystemspezifische Bausteine und gegebenenfalls SYS.1.5 *Virtualisierung*. Bei der Deployment-Variante ArcGIS Enterprise on Kubernetes sind außerdem die Bausteine SYS.1.6 *Containerisierung*, sowie APP.4.4 *Kubernetes* zu berücksichtigen.

ArcGIS Enterprise stellt Webanwendungen sowie Webservices bereit. Daraus ergibt sich, dass diese Bausteine gleichfalls zu berücksichtigen sind: APP.3.1 *Webanwendungen und Webservices* und APP.3.2 *Webserver*.

Werden die Anwendungen des ArcGIS Enterprise für mobile Endgeräte eingesetzt, so ist ferner dieser Baustein zu berücksichtigen: SYS.3.2.2 *Mobile Device Management*.

ArcGIS Enterprise ist eine marktverfügbare IT-Standardplattform, entsprechend finden die Bausteine CON.8 *Software-Entwicklung* sowie CON.10 *Entwicklung von Webanwendungen* keine Anwendung. Dafür sind die Bausteine APP.6 *Allgemeine Software* sowie OPS.1.1.3 *Patch- und Änderungsmanagement* zu berücksichtigen.

2 Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den benutzerdefinierten Baustein APP.bd.1 *ArcGIS Enterprise* von besonderer Bedeutung.

2.1 Offenlegung von schützenswerten Geodaten

Auch wenn Geodaten teilweise öffentlich einsehbare Landschaften abbilden, sind nicht alle diese Daten öffentlich. Es gibt Geodaten, z. B. Standorte von kritischen Infrastrukturen oder von für die Institution wichtigen Assets, die nicht veröffentlicht werden sollen. Ein Beispiel ist der exakte Verlauf von institutionseigenen Versorgungsleitungen. Die Offenlegung dieser Informationen bietet einem potenziellen Angreifer einen Angriffsvektor zur Störung oder Manipulation.

2.2 Geodaten aus unzuverlässiger Quelle

Geodaten werden oftmals von externen Stellen außerhalb der Institution erfasst. Die Bandbreite reicht dabei von professionellen Anbietern, behördlichen Stellen (z. B. Copernicus) bis hin zu öffentlich zugänglichen Verfahren (z. B. freiwillige Helfer). Zudem sind viele Geodaten und dazugehörige Metadaten über einen „Open Data“ Ansatz für die Institution verfügbar. Werden diese Geodaten und Metadaten in der Institution ohne weitere Prüfung verwendet, so besteht die Gefahr das veraltete, inhaltlich falsche oder sogar bewusst manipulierte Daten verwendet werden. Darauf aufbauende Prozesse und Entscheidungen würden verfälscht und gestört.

2.3 Manipulation von Geodaten

Geodaten beeinflussen Investitionen. Der Verkehrswert von Grundstücken ist abhängig von den umliegenden Geofaktoren (Geodaten). Die richtige Standortwahl wird auf Basis von Geofaktoren getroffen. Geodaten wirken sich unter Umständen auf Leib und Leben aus. Es hat schwere Folgen, wenn die Durchfahrtshöhe und Tragfähigkeit einer Brücke verfälscht wird und ein Gefahrguttransporter in der Folge einen Verkehrsunfall erleidet. Jede Person trifft Entscheidungen auch aufgrund der Geofaktoren, die Sie örtlich umgeben (z. B. Entfernungen, nächste Bahnstation). Im Umkehrschluss besteht die Gefahr, dass Geodaten manipuliert werden, um Abläufe zu stören, Schaden zu verursachen, Personen zu manipulieren oder einen wirtschaftlichen Vorteil zu erlangen.

2.4 Kapazitätsmangel des IT-Systems

Das IT-System der Institution muss den Anforderungen genügen. Bei nicht ausreichend dimensionierten Ressourcen besteht die Gefahr, dass die Nutzung der Geodaten nicht wie gefordert gelingt. Ein einschlägiges Beispiel ist der fehlende Speicherplatz, um Geodaten zu speichern und zu sichern. Luftbilder und Satellitenbilder, die Deutschland im hohen Detail abbilden, benötigen redundanzfrei ca. 10 Terrabyte Speicherplatz. Sehr häufig wird die Ressourcen-Planung durch Personal durchgeführt, dem Geodaten nicht hinreichend bekannt sind. Die mitunter besonderen Kapazitätsanforderungen würden in diesem Falle bereits in der Planungsphase unzureichend berücksichtigt.

2.5 Verhinderung oder Störungen der Funktionen des ArcGIS Enterprise

Werden Funktionen gezielt verhindert oder gestört, so kann dies weitreichende Folgen haben. In einsatzkritischen Systemen (z. B. in einem Einsatzleitsystem) stehen wichtige Funktionen nicht mehr zur Verfügung: die Disposition und Verortung der Einsatzkräfte oder Logistikflotte auf der Karte fällt im Extremfall aus.

2.6 Verlust von Geodaten aufgrund deren besonderer Eigenschaften

Der Einkauf und die Erhebung von Geodaten bedeuten für die Institution eine erhebliche Investition. Der anteilige oder vollständige Verlust gefährdet die Investitionssicherheit. Hinzu kommt, dass oftmals zusätzlich erhebliche Ressourcen eingesetzt werden müssen, um Geodaten qualitativ zu verbessern: Prüfen, Strukturieren, Ergänzen, Erfassen von Metadaten, Korrigieren, Anreichern. Dadurch steigt die Bedeutung dieser Geodaten für die Institution und auch Ihr Verkehrswert. Hierzu werden spezifische Workflows eingesetzt um z. B. Plausibilitätsprüfungen (eine Straße darf nicht unmittelbar an eine Hausmauer angrenzen) durchzuführen. Die zu Grunde liegenden Datenmodelle und Prüfungsroutinen sind für Geodaten spezifisch ausgeprägt (Beispiel: Geodaten zur automatischen Navigation eines Containerschiffes in Binnengewässern). Werden diese besonderen Eigenschaften missachtet z. B. bei der Sicherung der Daten, dann droht die Gefahr des Beschädigens oder Verlustes der Daten.

2.7 Fehlendes oder nicht zeitnahes Einspielen von Patches und Sicherheitshinweisen für ArcGIS Enterprise

Es werden regelmäßig Sicherheitsempfehlungen für ArcGIS Enterprise durch den Hersteller veröffentlicht. Bekannt gewordene Schwachstellen werden geschlossen („Patches“). Wenn die Sicherheitsempfehlungen und Patches ignoriert oder erst sehr spät umgesetzt werden, besteht die Gefahr, dass Angreifer Sicherheitslücken ausnutzen. Es besteht gegebenenfalls die Gefahr des Datenabflusses, Ausfalles von Funktionen und schließlich der Störung von wichtigen Prozessen.

2.8 Mängel am Berechtigungskonzept für ArcGIS Enterprise

Fehlt ein Berechtigungskonzept, so besteht z. B. die Gefahr, dass Benutzer mehr Berechtigungen haben als notwendig. Diese Nutzer könnten die Konfiguration des ArcGIS Enterprise versehentlich beschädigen oder vorsätzlich Störungen herbeiführen. Es könnten zudem Schäden an den verarbeiteten Geodaten verursacht werden. Fehlt es an der hinreichenden Dokumentation des Berechtigungskonzeptes oder an stetiger Aktualisierung, dann können unter Umständen Berechtigungen oder Veränderungen des Systems, bzw. der Geodaten nicht mehr nachvollzogen werden.

2.9 Fehlende Dokumentation und unzureichende Notfallkonzepte für ArcGIS Enterprise

Die Dokumentation des Herstellers ist im Mindesten so zu ergänzen, dass die spezifischen Einstellungen der Institution nachvollzogen werden können. Fehlt diese Dokumentation, so kann dies im Falle einer Störung oder eines Ausfalles dazu führen, dass die Funktion nur sehr verzögert oder gar nicht wiederhergestellt werden kann. Analog führen unzureichende oder fehlende Notfallkonzepte für ArcGIS Enterprise dazu, dass lange Ausfallzeiten großen Schaden verursachen können.

2.10 Ausfall von an ArcGIS Enterprise ausgebildetem Personal

Der Ausfall von an ArcGIS Enterprise ausgebildetem Personal kann Störungen der Funktion zur Folge haben. Wird z. B. bei der Wiederherstellung eines Systems mit ArcGIS Enterprise lediglich geprüft, ob die Softwaredienste des Betriebssystems wieder gestartet wurden, wie es in der IT-Administration üblich ist, so ist nicht gewährleistet, dass auch die Dienste für die Bereitstellung von Geodaten bereits wieder lauffähig sind.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des benutzerdefinierten Bausteins APP.bd.1 *ArcGIS Enterprise* aufgeführt. Der ISB ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachabteilung, Benutzer, Notfallbeauftragter

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt.

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig umgesetzt werden.

APP.bd.1.A1 Planung und Dokumentation des Einsatzes von ArcGIS Enterprise [Fachabteilung, Benutzer]

Bevor ArcGIS Enterprise eingesetzt wird, MUSS die Institution den Einsatz sorgfältig planen. Dabei MUSS sie mindestens folgende Punkte beachten:

- Systemvoraussetzungen der Komponenten,
- zu nutzende Funktionen,
- anzubindende Clients beziehungsweise Server,
- Speicherbedarf und erwartetes Netzwerkaufkommen für die Geodaten sowie
- Redundanz und Hochverfügbarkeit der Komponenten.

Die Dokumentation MUSS die vom Hersteller bereitgestellte Dokumentation entsprechend den individuellen Anforderungen der Institution ergänzen, so dass die Planungen von Dritten nachvollzogen werden können. Die Dokumentation MUSS im späteren Betrieb entsprechend vorgenommener Änderungen aktualisiert werden.

APP.bd.1.A2 Spezifische Datensicherung der Geodaten [Fachabteilung]

Es MUSS zwischen Fachverantwortlichen und IT-Betrieb abgestimmt werden, in welcher Weise die Datensicherung durchgeführt wird, so dass spezifische Aspekte der Geodaten berücksichtigt werden. Im Besonderen MÜSSEN diese spezifischen Merkmale beachtet werden: Indizierung in objektrelationalen Datenbanken, Zusatzdateien im Filesystem wie z.B. Pyramiden oder „Caches“ und Vollständigkeit der Daten (Geodaten bestehen oftmals aus mehreren Files, die logisch zu einem Datensatz in dem verwendeten Format zusammengehören).

APP.bd.1.A3 ENTFALLEN

Diese Anforderung ist entfallen.

APP.bd.1.A4 ENTFALLEN

Diese Anforderung ist entfallen.

APP.bd.1.A5 Erstellung eines Rollenkonzeptes [Fachabteilung]

Zusätzlich zum allgemeinen Berechtigungskonzept MUSS die Institution ein Berechtigungskonzept für die Zugriffssteuerung des ArcGIS Enterprise erstellen, geeignet dokumentieren und anwenden.

Es MUSS insbesondere der Zugriff auf die Funktionen des ArcGIS Enterprise sowie die dort hinterlegten Geodaten berücksichtigt werden. Dabei MÜSSEN die Berechtigungen so zugewiesen werden, dass diese nur zur Ausführung der erforderlichen Funktion genutzt werden können (Least-Privilege-Model).

APP.bd.1.A6 Schulung und Einweisung in die Funktion des ArcGIS Enterprise [Fachabteilung]

Zusätzlich zum allgemeinen Schulungsprogramm MUSS die Institution ein Schulungskonzept erarbeiten, das sowohl die IT-technischen Besonderheiten als auch die Funktionsbeschreibungen aus dem Rollenkonzept abdeckt. Die Institution MUSS die Benutzer und Betreiber von ArcGIS Enterprise regelmäßig entsprechend dem Konzept schulen.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.bd.1.A7 Authentifizierung der Nutzer des ArcGIS Enterprise

Es SOLLTE ein zentraler Identitätsspeicher (z.B. Active Directory) angebunden werden. Die Entscheidung SOLLTE dokumentiert werden. Bei der Anbindung SOLLTEN die Vorgaben des Herstellers für eine sichere Konfiguration der Authentifizierung mittels des gewählten Identitätsspeichers befolgt werden. Außerdem SOLLTE die Authentifizierung über einen zentralen Identitätsanbieter stattfinden oder in ArcGIS Enterprise so eingestellt werden, dass eine Authentifizierung auf Webebene stattfindet.

APP.bd.1.A8 Verschlüsselung der Kommunikationswege von ArcGIS Enterprise

Die ausschließliche Nutzung von HTTPS in ArcGIS Enterprise SOLLTE aktiviert bleiben. Dabei SOLLTE eine vorhandene Zertifikatinfrastruktur verwendet werden, bei der die eingesetzten Zertifikate von einer für die Institution vertrauenswürdigen Zertifizierungsstelle signiert wurden.

APP.bd.1.A9 Sicherheitseinstellungen für Komponenten, integrierte Anwendungen und Schnittstellen des ArcGIS Enterprise

Es SOLLTEN die empfohlenen Sicherheitseinstellungen des Herstellers umgesetzt werden:

- Zugänge Ports/Protokolle SOLLTEN so konfiguriert werden, dass nur die notwendigen Ports/Protokolle für ArcGIS Enterprise geöffnet und alle weiteren geschlossen werden.
- Zugriffe auf die Installationsverzeichnisse, den „Configuration Store“ sowie die Arbeitsverzeichnisse z.B. zum Fileaustausch, SOLLTEN nur für den Zugriff durch einen gezielt dafür vorgesehenen Account zugelassen werden.
- Anwendungen zum Management des ArcGIS Enterprise SOLLTEN nicht offen innerhalb der Institution oder von außerhalb der Institution zugänglich sein.
- Das zentrale Service-Register SOLLTE deaktiviert werden.
- Das Konto des Haupt-Administrators des ArcGIS Enterprise SOLLTE nach der Installation deaktiviert werden.
- Die Sicherheitsoption “standardisierte SQL-Abfragen" in „ArcGIS Server“ SOLLTE aktiviert bleiben.
- Die Proxy-Funktion des Portals SOLLTE beschränkt werden, damit das Portal nicht missbraucht werden kann, um Denial-of-Service- (DoS-) oder serverseitige Anfragenfälschungs-Angriffe (SSRF) gegen andere Computer zu starten.

APP.bd.1.A10 Protokollierung und Überwachung des ArcGIS Enterprise

Neben den üblichen Überwachungsparametern, wie den Systemauslastungskennzahlen, dem Zustand von Systemdiensten und der Verfügbarkeit von REST-Endpunkten, SOLLTEN auch ArcGIS Enterprise spezifische Kennzahlen überwacht und nach Möglichkeit in ein SIEM (Security Information and Event Manager) integriert werden. Dabei SOLLTE die Verfügbarkeit von bereitgestellten Geoinformationsdiensten (Karten-, Geokodierungs-

, Geoanalysediensten, etc.) überwacht werden. Um eine revisionssichere Protokollierung von relevanten Ereignissen wie das Veröffentlichen bzw. Löschen von Geoinformationsdiensten zu gewährleisten, SOLLTEN die Protokolldateien der einzelnen ArcGIS Enterprise Komponenten in eine zentrale Log-Serverinstanz integriert werden. Es SOLLTE das Log-Level entsprechend angepasst werden, um alle sicherheitsrelevanten Ereignisse zu protokollieren.

APP.bd.1.A11 Überprüfung der Quellen der Geodaten auf Zuverlässigkeit [Fachabteilung]

Die verwendeten Quellen, von denen die Institution Geodaten bezieht, SOLLTEN auf Ihre Vertrauenswürdigkeit hin überprüft werden. Es SOLLTE regelmäßig überprüft werden, ob die Qualität und Aktualität sowie Vollständigkeit der bezogenen Geodaten den Anforderungen der Institution bzw. der zu Grunde liegenden Geschäftsprozesse/ Aufträge entsprechen.

APP.bd.1.A12 Einbindung in die Notfallplanung [Notfallbeauftragter]

ArcGIS Enterprise SOLLTE im Notfallmanagementprozess berücksichtigt werden. Es SOLLTEN die geschäftsrelevanten Funktionen des ArcGIS Enterprise dokumentiert und in Wiederanlaufpläne integriert werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

APP.bd.1.A13 Explizite Einschränkung des Aufrufs von vertrauenswürdigen Servern (CIA)

Es SOLLTE eine Liste mit Servern konfiguriert werden, für die Inhalte von ArcGIS Enterprise freigegeben werden sollen (z.B. https://otherportal.domain.com/arcgis).

Es SOLLTE eine Liste mit vertrauenswürdigen Servern konfiguriert werden, an die Clients Ihre Anmeldeinformationen senden, wenn CORS (Cross-Origin-Resource-Sharing) Anforderungen für den Zugriff auf Services getätigt werden, die mit Authentifizierung auf Webebene gesichert sind.

Es SOLLTEN domänenübergreifende Anforderungen beschränkt werden. Die Verwendung der Funktionen des ArcGIS Enterprise durch Dritt-Anwendungen SOLLTE auf Anwendungen beschränkt werden, die in einer “WHITELIST” vertrauenswürdiger Domänen erfasst werden.

APP.bd.1.A14 Sichere Konfiguration der Token-Verwendung (CI)

Die Ablaufzeit der Token SOLLTE auf ein vertretbares Minimum (i.d.R. 1 Tag) verkürzt werden, um den Angriffsvektor eines kompromittierten Tokens zeitlich weiter einzuschränken.

Der gemeinsam verwendete Schlüssel, der zum Generieren der ArcGIS-Token verwendet wird, SOLLTE als komplexe und zufällige Zeichenfolge definiert werden. Der gemeinsam verwendete Schlüssel SOLLTE regelmäßig geändert werden.

APP.bd.1.A15 Sichere Konfiguration von TLS-Protokollen und Standard-Verschlüsselungsalgorithmen (CI)

Es SOLLTE festgelegt werden, welche SSL-Protokolle und Verschlüsselungsalgorithmen für die sichere Kommunikation der ArcGIS Enterprise Komponenten untereinander und mit den Clients verwendet werden. Es SOLLTEN die Empfehlungen aus der Technischen Richtlinie [TR-02102-2] zur Verwendung von TLS des BSI umgesetzt werden. Es SOLLTE die strikte Verwendung von HTTPS (HSTS) erzwungen werden.

APP.bd.1.A16 Kennzeichnung der Geodaten während der Bearbeitung [Fachabteilung] (IA)

Geodaten SOLLTEN bezüglich Ihres Ursprungs und durchgeführter Modifikation gekennzeichnet werden. Es SOLLTEN mindestens der Zeitpunkt der Bearbeitung sowie der bearbeitende Nutzer innerhalb der Institution erfasst werden. Zudem SOLLTEN Geodaten mit einem Mindestsatz an Metadaten gekennzeichnet werden. Der Mindestsatz SOLLTE die Quelle, das Format, das Datum und den räumlichen Bezug („Footprint“) umfassen. In weiteren Verarbeitungsschritten (z.B. Qualitätsüberprüfung, strukturierte Ablage in das Stammdatenmodell der Institution) SOLLTEN die Metadaten angereichert werden. Die inhaltliche Anreicherung der Metadaten SOLLTE wesentliche Inhalte für die Institution ausweisen (z.B. Qualitätsmerkmale). Es SOLLTE die Historie bzw. der Verlauf der Bearbeitung der Geodaten gespeichert werden.

APP.bd.1.A17 Verschlüsselung der Datenspeicherung von Geodaten (CI)

Es SOLLTE eine transparente Datenverschlüsselung (TDE) für Datenbanken nach Stand der Technik des eingesetzten Datenbankmanagementsystems verwendet werden, in dem ArcGIS Enterprise Geodaten verwaltet.

Es SOLLTE eine vollständige Datenträgerverschlüsselung für „Datei-Repositories“ verwendet werden.

APP.bd.1.A18 Multifaktor-Authentifizierung für ArcGIS Enterprise (CI)

Es SOLLTE eine Multifaktor-Authentifizierung bspw. über PKI- „SmartCards“ verwendet werden.

APP.bd.1.A19 Verstärkte Absicherung des Informationsaustausches [Fachabteilung] (CI)

Der anonyme Zugriff auf institutionsweit freigegebene Inhalte („Portal for ArcGIS“) SOLLTE deaktiviert werden.

Es SOLLTEN folgende Einstellungen bei der Bereitstellung von Diensten (Web-Services) vorgenommen werden:

- Für Karten-Dienste SOLLTEN die Funktionen „Feature Access“, „Mobile Data Access“, „WFS“ und „Query“ deaktiviert werden. Außerdem SOLLTEN Daten als „File Geodatabase“ veröffentlicht werden.
- Für „Feature“-Dienste SOLLTEN die Funktionen „Sync“, „Insert“, „Update“ und „Delete“ deaktiviert werden. Außerdem SOLLTEN die Funktionen „Always Secure“ und „Use Versioned Data“ aktiviert werden.
- Für Geodaten-Dienste SOLLTEN die Funktionen „Always Secure“, „Use Versioned Data“ und „Grant ArcGIS Account Read-Only (RDBMS)“ aktiviert werden.

APP.bd.1.A20 Ausschließen von MIME-Typen in Anforderungen

Im Webserver SOLLTEN alle nicht von ArcGIS Enterprise genutzten MIME-Typen ausgeschlossen werden.

APP.bd.1.A21 Scannen nach Cross-Site-Scripting Angriffen

Das Scannen nach Cross-Site-Scripting Angriffen für Feature-Services SOLLTE vollständig für Eingaben und Ausgaben aktiviert werden.

APP.bd.1.A22 Verwenden eines gruppenverwalteten Service-Kontos

Bei der Deployment-Variante Windows SOLLTE als Konto für die Ausführung der ArcGIS Enterprise-Services ein gruppenverwaltetes Service-Konto (gMSA; Group Managed Service Account) verwendet werden.

4 Weiterführende Informationen

Weiterführende Informationen zu Gefährdungen und Sicherheitsmaßnahmen für den benutzerdefinierten Baustein APP.bd.1 *ArcGIS Enterprise* finden sich in der Dokumentation zu ArcGIS Enterprise von Esri unter https://enterprise.arcgis.com/de sowie im Trustcenter von Esri unter https://trust.arcgis.com/de.

Empfehlungen für den Einsatz des kryptographischen Protokolls Transport Layer Security (TLS) für die sichere Übertragung von Informationen in Datennetzwerken finden sich in der technischen Richtinline “TR-02102-2 "Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)” des BSI.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Aus jeder Anforderung (A) in diesem Baustein können Sicherheitsmaßnahmen abgeleitet werden. Die Umsetzung dieser Maßnahmen wirkt denjenigen elementaren Gefährdungen (G0) entgegen, die für das Thema bzw. Zielobjekt relevant sind. In der Kreuzreferenztabelle (KRT) zu diesem Baustein sind jeder Anforderung die entsprechenden elementaren Gefährdungen zugeordnet.

Anhand der KRT lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Die Buchstaben in der zweiten Spalte zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Diese Grundwerte sind Confidentiality (C) für Vertraulichkeit, Integrity (I) für Integrität sowie Availability (A) für Verfügbarkeit.

Die folgenden elementaren Gefährdungen sind für den benutzerdefinierten Baustein APP.bd.1 *ArcGIS Enterprise* von Bedeutung:

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.25 Ausfall von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.33 Personalausfall

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen

Elementare Gefährdungen Anforderungen	G 0.19	G 0.20	G 0.21	G 0.22	G 0.25	G 0.27	G 0.28	G 0.30	G 0.31	G 0.32	G 0.33	G 0.40	G 0.45	G 0.46
A1					X	X			X		X			
A2					X				X			X	X	X
A5	X			X		X		X	X	X	X	X		X
A6						X			X		X		X	

A7	X			X				X	X	X	X	X		X
A8	X			X				X		X				X
A9	X		X					X	X	X		X		
A10		X	X		X			X	X	X				X
A11		X		X									X	X
A12					X	X					X		X	
A13	X							X				X		
A14	X			X					X			X		X
A15	X							X		X				X
A16		X		X				X	X	X			X	X
A17	X			X										X
A18	X			X						X				X
A19	X		X					X	X	X		X		X
A20			X		X		X	X	X			X		
A21	X	X	X	X										X
A22								X	X	X				