A1 Information Security Standard für den sicheren Servicebetrieb

Standard für das
A1 Informationssicherheitsmanagement

Versionshistorie

Version 2.2		
betrifft:	**Erstellung**	**Freigabe**
Änderungen: - Dokumenthistorie eingefügt - Hinweise bzgl. Schutzbedarfserhöhung eingefügt - Telefon-Nummer des SOC korrigiert - eMail-Adressen korrigiert - Kapitel 2 gestrichen - Kapitel 2.1.6 eingefügt - Kapitel 2.2.10 eingefügt - Kapitel 2.3.8 eingefügt - Inhaltsverzeichnis aktualisiert	Friedrich HEIGL Information Security 25.01.2022	Alexandra FEHRINGER Leitung Information Security 25.01.2022
Anmerkung: Zu früheren Versionen dieses Dokumentes liegt keine Versionshistorie vor.		

Feststellung Schutzbedarf

Für A1 Mitarbeiter:

Der Schutzbedarf bestimmt die notwendigen Sicherheitsmaßnahmen und ist am Ende dieser Seite durch einen, für das betroffene Service verantwortlichen, A1 Mitarbeiter zu dokumentieren. Informationen zur Bestimmung des **Schutzbedarfs** („Standard", „Erweitert" oder „Hoch") sind in den A1 Information Security Guidelines (Kap. 3 – Schutzbedarfsklassifizierung, Zugriff nur für A1 Mitarbeiter) zu finden, Security@A1.at unterstützt gerne.

Der Schutzbedarf wird automatisch auf mindestens **Erweitert** erhöht, sobald die Verarbeitung **personenbezogener Daten** auf Systemen außerhalb des Geltungsbereichs der EU-Verordnung 2016/679 (DSGVO / GDPR) erfolgt. Das gilt **nicht** für die Verarbeitung von Anmeldedaten.

Als Anmeldedaten gelten folgende Informationen, jeweils auch einzeln:

- eMail-Adresse
- Vorname und/oder Nachname
- IP-Adresse

Für A1 Lieferanten:

Der Lieferant erklärt sich bereit, dass er alle 3 Jahre für ein Sicherheits-Review-Gespräch mit einem A1 Mitarbeiter zur Verfügung steht.

Die geltenden Sicherheitsanforderungen für den definierten Schutzbedarf sehen Sie anhand der folgenden Tabelle:

Schutzbedarfs-Anforderung	Kapitel 3.1	Kapitel 3.2	Kapitel 3.3
Standard	x	-	-
Erweitert	x	x	-
Hoch	x	x	x

Festgelegter Schutzbedarf: ☐ **Standard** ☐ **Erweitert** ☐ **Hoch**

Inhaltsverzeichnis

Gender-Klausel

Aus Gründen der besseren Lesbarkeit wird in diesem Dokument darauf verzichtet, geschlechtsspezifische Formulierungen zu verwenden. Soweit personenbezogene Bezeichnungen nur in männlicher Form angeführt sind, beziehen sie sich auf Männer und Frauen in gleicher Weise.

1 Geltungsbereich & generelle Zielsetzung

Das Vertrauen unserer Kunden und der Schutz der Unternehmenswerte sind unverzichtbare Voraussetzungen für den wirtschaftlichen Erfolg. Deswegen hat sich A1 zum Ziel gesetzt, Informationssicherheit entsprechend dem Stand der Technik zu gewährleisten, neue Entwicklungen und Tendenzen zu identifizieren, auf ihre Anwendbarkeit zu evaluieren sowie das Sicherheitsniveau der A1 unter dem Aspekt der Wirtschaftlichkeit und Praktikabilität zu halten und kontinuierlich zu verbessern.

Neben der A1 Information Security Policy[1] als übergeordnetes Leitdokument und den A1 Information Security Guidelines[1], die das Rahmen- und Regelwerk für die Informationssicherheit der A1 darstellen, dient der vorliegende Standard dem Betrieb von A1 Services und Servicekomponenten. Während die Policy und Guideline nur Mitarbeitern der A1 zugänglich sind, richtet sich dieses Dokument explizit an externe Lieferanten und Partner.

Der vorliegende Standard für den Betrieb von Services und Servicekomponenten richtet sich an Lieferanten und Partner von A1 (nachstehend auch: Auftragnehmer, Supplier, Provider, Dienstleister, Auftragsverarbeiter) sowie alle A1 Mitarbeiter, die mit der Planung, Entwicklung, Einrichtung, Konfiguration, Betrieb, Wartung und Außerbetriebnahme von IT-Services betraut sind. Enthaltene Vorgaben sind insbesondere im Zuge von Projekten, innerhalb des A1 Change-Managements und des A1 Beschaffungs- bzw. Einkaufsprozesses zu berücksichtigen.
Sie gelten sowohl für innerhalb der A1 IT-Infrastruktur (On-Premises) betriebene Services und Anwendungen, wie auch für außerhalb der A1 IT-Infrastruktur betriebene Dienste, Services und (Cloud-) Anwendungen.

Die vorliegende Version dieses Standards ersetzt alle vorangegangen Versionen.
Die jeweils aktuelle Version kann hier[1] heruntergeladen werden.

Für Fragen und Beratung steht Security@A1.at zur Verfügung.

[1] http://www.a1team.at/sicherheitsrichtlinien (Zugriff nur für A1 Mitarbeiter)

2 Sicherheitsanforderungen

In den nachfolgenden Kapiteln sind die Anforderungen gemäß den Schutzbedarfsklassen an Anwendungen und Services, welche A1 Informationen / Daten verarbeiten, beschrieben.

Es gelten jeweils die Anforderungen auf den folgenden Seiten gemäß des auf Seite 3 festgestellten und dokumentierten Schutzbedarfs.

2.1 Sicherheitsanforderungen an die Schutzbedarfsklasse „Standard"

Alle durch oder im Auftrag von A1 betriebenen Services müssen die Anforderungen an diese Schutzbedarfsklasse „**Standard**" erfüllen. Services mit dem Schutzbedarf „**Erweitert**" und „**Hoch**" unterliegen zusätzlichen Bestimmungen (siehe Kap. Sicherheitsanforderungen an die Schutzbedarfsklasse „Erweitert" 2.2 ab Seite 9 und für „Hoch" 2.3 ab Seite 15.).

2.1.1 Vulnerability & Incident Management

- Die eingesetzte Software muss unter Support stehen und darf keine bekannten Sicherheitsschwachstellen (Vulnerabilities) enthalten. Updates und Security-Patches werden zeitnah eingespielt. Für die Behebung von Sicherheitsschwachstellen dürfen keine Kosten verrechnet werden.
- Es werden Sicherheitsmaßnahmen gegen Malware (Viren-, Spam-, Trojaner) eingesetzt.
- Incidents und Data Breaches sind unverzüglich an das A1 Service Operations Center (SOC) zu melden:

A1 Service Operation Center
T 0800 501 511
@ Attacke@A1.at

2.1.2 Netzwerksicherheit

- **Network Devices:**
  Endgeräte dürfen sich erst nach erfolgreicher Authentifizierung mit dem A1 Netzwerk („Client Zone") verbinden. Maßgebend für die Authentifizierung der Geräte ist der aktuelle Stand der Technik für den LAN-Zugang. Neue Geräte im internen A1 Netz müssen jedoch IEEE 802.1X unterstützen. Jedes Gerät in den Netzen von A1 muss einzeln identifizierbar sein.
- IoT-Devices dürfen nicht direkt aus dem Internet erreichbar sein. Security-Updates müssen über den ganzen Lebenszyklus automatisiert und ohne manuellen Eingriff eingespielt werden. Es dürfen keine Passwörter in den Devices fest (hardcoded) hinterlegt sein, default Passwörter müssen bei Erst-Inbetriebnahme geändert werden.

2.1.3 Software-Architektur

- Sind mehrere Mandanten auf demselben Service eingerichtet, ist eine saubere Mandantentrennung zu anderen Kundendaten zu gewährleisten.

2.1.4 Verschlüsselung

- Die Daten-Kommunikation zwischen einem Lieferanten (und dessen IT-Services) und A1 erfolgt verschlüsselt über sichere Kommunikationskanäle (SSH, VPN, TLS, https, ...) auf dem aktuellen Stand der Technik. SSL darf nicht mehr eingesetzt werden.

2.1.5 Authentifizierungsmethoden

- Benutzer (A1 Mitarbeiter) müssen sich mittels SSO (Single Sign-On) gegenüber einem IT-Service authentifizieren (AD / Kerberos). Für den Fall, dass weniger als 50 Benutzer das Service nutzen oder falls SSO nicht möglich ist, liegt die Benutzerverwaltung in der Verantwortung des A1 Applikationsdatenschutzverantwortlichen. Jedenfalls muss die Benutzerverwaltung durch A1 (anlegen, löschen, sperren, ändern) möglich sein. Jeder angelegte Benutzer muss auch im A1 Corporate Directory (CD) geführt werden und der gewählte Ablauf der Authentifizierung muss in der A1 Konfigurationsdatenbank (CMDB) durch den A1 Verantwortlichen dokumentiert sein.
- **Passwortschutz:**
  Wenig komplexe und kurze Passwörter dürfen technisch nicht zugelassen sein. Regelmäßige Passwortwechsel werden technisch unterstützt. Eine Passwortspeicherung und -übertragung im Klartext ist nicht zulässig.
- **Biometrische Authentifizierung:**
  - Bei biometrischer Authentifizierung dürfen die Authentifizierungsdaten ausschließlich lokal und sicher am jeweiligen Gerät gespeichert werden und sind nicht mit Standard-Rechten (beispielsweise von der Festplatte) auslesbar.
  - Bei Verfahren zur Gesichtserkennung werden Kriterien wie Dreidimensionalität oder Temperatur mitgeprüft.
  - Bei Verfahren zum Fingerabdruck-Scanning werden Kriterien wie Fingerpuls oder Temperatur mitgeprüft.
  - Die Falschakzeptanzrate der biometrischen Authentifizierungsverfahren (unberechtigte User werden autorisiert) liegt bei maximal bei 1 zu 50.000.
  - Die Falschrückweisungsrate (berechtigter User wird nicht autorisiert) liegt in einem akzeptablen Rahmen.
  - Um sich bei einer Falschrückweisung (berechtigter User wird nicht autorisiert) trotzdem authentifizieren zu können, muss alternativ ein Passwortschutz gemäß den oberen Angaben möglich sein.
- **Alternative Authentifizierungsmethoden:**
  Alternative Authentifizierungsmethoden sind zulässig, sofern sie ein gleich- oder höherwertiges Schutzniveau als die oben angegebenen Verfahren aufweisen.

2.1.6 Checkliste für Schutzbedarf „Standard"

Anhand der folgenden Liste können die relevanten Kriterien für 4 Service-Kategorien bei Schutzbedarf „**Standard**" überprüft werden.

Question		SW-Supplier	HW-Supplier	Cloud-Service	Human-Supplier
1	Do you use a cloud service/storage?			X	
2	Is there a process for alerting if a data breach happens?	X	X	X	X
3	Do you know where the data reside?			X	
4	Do you have a NDA and DPA signed with 3rd party?			X	X
5	The software is supported by the vendor?	X		X	
6	Security-Updates and -Patches are installed or made available in a speedy manner?	X	X	X	
7	Security measures are in place against malware (anti-virus, spam- and trojans protection)?	X	X	X	X
8	Is there awareness of handling incidents and data breaches?	X	X	X	X
9	Is there a guaranteed service time?	X	X	X	X
10	Ist es möglich, jedes einzelne Gerät / jeden einzelnen Benutzer zu identifizieren, das / der über das A1-Netzwerk zugreift?			X	X
11	Is there a clean seperation of client data.			X	X
12	Are secure (encrypted) protocols used for communication (eg. Https, ftps, ssl)?	X	X	X	X
13	Are you using (A1) AD authentication			X	
14	Is Single-Sign On supported?	X		X	
15	Multi-Factor Authentication is supported and can be enforced?	X		X	
16	Do password rules reflect the current the A1 Security Guide Lines?	X	X	X	
17	Are passwords stored hashed?	X	X	X	
8	Does a documentation covering the security concepts and measures exist?		X	X	X

2.2 Sicherheitsanforderungen an die Schutzbedarfsklasse „Erweitert“

Zusätzlich gelten für die Schutzbedarfsklasse „**Erweitert**“ neben den Anforderungen an die Schutzbedarfsklasse „**Standard**“ (Siehe Kap. 2.1 Seite 6), auch die nachfolgenden Bestimmungen in diesem Kapitel.

IT-Dienstleister in dieser Schutzbedarfsklasse *sollten* ein starkes Sicherheitsbewusstsein demonstrieren können und *sollten* auch über eine aufrechte **Security-Zertifizierung** (Bsp. ISO 27001) für ihre angebotenen Leistungen verfügen. Die A1 Security Überprüfung kann in diesem Fall reduziert durchgeführt und damit beschleunigt werden. Die langfristige Strategie der A1 ist eine Zusammenarbeit mit derart zertifizierten IT-Dienstleistern zu vertiefen und intensivieren.

IT-Dienstleister, welche über einen längeren Zeitraum hinweg vertrauliche A1 Daten (Schutzbedarf ab „Erweitert“) auf eigener Infrastruktur außerhalb des A1 Netzes speichern (Cloud-Anbieter, externes Hosting, XaaS), **müssen** eine derartige Zertifizierung vorweisen können und für den gesamten Zeitraum der Zusammenarbeit für die angebotenen Leistungen aufrechterhalten.
Halten derartige Anbieter personenbezogene Kundendaten in größerem Umfang vor, ist außerdem eine Datenschutz-Zertifizierung (z.B. ISO 27018) erwünscht. Auch genutzte Rechenzentren **müssen** jedenfalls über eine entsprechende Security-Zertifizierung verfügen.

2.2.1 Formale Kriterien

- Die Rechnerstandorte, an denen Daten gespeichert und verarbeitet werden, müssen gegenüber A1 offengelegt werden.
- Die Daten dürfen nur dann externen A1 Partnern (Auftragsverarbeitern) zugängig gemacht werden, wenn eine Vertraulichkeitsvereinbarung (NDA) und eine Datenschutzvereinbarung (DPA, sofern personenbezogene Daten verarbeitet werden) mit A1 vereinbart und unterzeichnet wurden. Auch für Prototyping, Laboraufbauten und POCs (Proof of Concept) sind derartige Vereinbarungen zu unterzeichnen, wenn der Zugriff oder Zugang zu/auf A1 Echtdaten erfolgt.
- Alle Änderungen und Implementierungen von A1-Assets oder an von A1 genutzten Applikationen müssen gemäß einem dokumentierten Change-Prozess durchgeführt werden. Vor Inbetriebnahmen erfolgen mehrere Prüfungen, die im Zuge des A1 Change-Management Prozesses durchgeführt werden. Unter anderem muss eine umfassende Security Prüfung durchgeführt werden. (Diese ist unter A1 Greenlight[3] durchzuführen)
- **Auditrecht**:
  Der A1 Lieferant lässt sich im Bedarfsfall nach entsprechender Vorankündigungszeit von A1 auditieren.

[3] https://greenlight.a1.inside (Zugriff nur für A1 Mitarbeiter)

2.2.2 Vulnerability & Incident Management

- Die eingesetzten Komponenten haben eine sichere Grundkonfiguration (z.B. Härtung).
- Vulnerability Scans müssen in regelmäßigen Abständen auf die durch das A1 Service genutzte Infrastruktur durchgeführt werden.
- Relevante Logdateien für forensische Analysen müssen in geeigneter Form verfügbar sein und bereitgestellt werden.
- Alle A1 On-Premises Services sowie durch A1 betriebene PaaS & IaaS Cloud-Services müssen an das A1 On-Premises SIEM System (Splunk) angebunden werden[4]
- Administratoren- und Benutzerverhalten (Log-on, Log-off, Passwortwechsel, relevante Kopiervorgänge, etc.) sind zu protokollieren. Die Logdateien müssen auf Bedarf für forensische Analysen zur Verfügung gestellt werden.
- Regelmäßige Datensicherungen sind durchzuführen, zudem müssen die Anforderungen an die Verfügbarkeit in einem Service Level Agreement (SLA) mit A1 vereinbart und eingehalten werden.

2.2.3 Netzwerksicherheit

- Es müssen Sicherheitsmaßnahmen gegen netzbasierte Angriffe (IPS, Firewall) im Einsatz sein.
- Es existiert eine Netzsegmentierung (vor allem die Trennung von Management-Netz / User-Daten). Eine Unterteilung in definierte Netzwerk-Schutzzonen, ausgerichtet am Schutzbedarf der darin enthaltenen Assets, ist eingerichtet.

2.2.4 Secure Coding & Software-Architektur

- Im Entwicklungsprozess folgt die Softwareentwicklung sicheren Entwicklungsmethoden, indem z.B. die OWASP Top10[5] (bzw. API Security Top 10[6]) Risiken berücksichtigt werden.
- Applikationen sind in mehreren Tiers (Ebenen) aufzubauen, die sicher voneinander zu trennen sind. Beim Zugriff darf kein Tier übersprungen werden. Der Zugriff von einem Tier zum Nächsten, darf nur über definierte Protokolle (Ports) erfolgen. Es muss eine Trennung in Test-, Integrations- und Produktivsysteme erfolgen.
- Entwicklungs- oder Test-Umgebungen dürfen keine personenbezogenen Echtdaten enthalten.
- Zugriffe auf Produktivsysteme die Echtdaten enthalten sind auf einen reduzierten Personenkreis mit dokumentierten Businessneed einzuschränken, das Need-to-know Prinzip sowie Seperation-of-Duties für kritische Aktionen ist zu gewährleisten.

[4] Siehe: https://getsplunk.at.inside (Zugriff nur für A1 Mitarbeiter) Kontakt: .GRP.A1-TA.splunk.operation
[5] https://www.owasp.org/index.php/Top_10-2017_Top_10
[6] https://owasp.org/www-project-api-security/

2.2.5 Verschlüsselung

- Daten mit erweitertem Schutzbedarf (z.B. vertrauliche Daten) dürfen nur verschlüsselt übertragen werden.
- Wenn die zugrundeliegende IT-Infrastruktur nicht durch A1 verwaltet wird (Bsp. externes Hosting, Cloud) müssen Daten mit erweitertem Schutzbedarf (vertrauliche A1 Daten, z.B. A1 Kundendaten) verschlüsselt gespeichert werden. Hierzu kann Verschlüsselung auf Dateisystem-, Betriebssystem-, Datenbank- oder Applikationsebene eingesetzt werden.
- Kryptographische Schlüssel müssen in sicherer Umgebung erzeugt, aufbewahrt und archiviert werden.
- State-of-the-Art Verschlüsselung wird eingesetzt: AES (Schlüssellänge 128-256 Bit), Camellia (128-256 Bit), ECIES (>250 Bit), DLIES (>3000 Bit), RSA (>3000 Bit)
- Veraltete Verfahren werden nicht eingesetzt: Triple-DES, Serpent, Twofish, DES, RC4, Blowfish
- Die Netzwerkkommunikation zu Subdienstleistern und zwischen den Rechnerstandorten erfolgt verschlüsselt.

2.2.6 Authentifizierungsmethoden

- Der Zugriff auf vertrauliche A1 Daten über ungeschützte Netze (Bsp. Internet, Cloud-Services) oder ausgehend von IT-Infrastruktur von Dritten, welche nicht in der Verwaltung von A1 steht (BYOD, IT-Ausrüstung des Partners), muss geschützt per verpflichtender 2-Faktor Authentifizierung erfolgen.
- **Passwortschutz:**
  Initialpasswörter müssen zufallsbedingt erzeugt werden, verschlüsselt übertragen werden, dürfen nur ein einziges Mal eingesetzt werden und dürfen nur maximal 2 Wochen gültig sein.
  Nach dem Ersteinstieg mittels Initialpassword wird sofort ein Passwortwechsel erzwungen. Im Bedarfsfall, beispielsweise nach einem Angriff, ist es möglich, die Anmeldeinformation zu ändern.
- Nach 15 fehlgeschlagenen Anmeldeversuchen muss der Zugriff für min. 15 Minuten gesperrt werden, oder gleichwertige Methoden zur Verhinderung unberechtigter Zugriffe auslösen.
- Passwörter müssen mindestens 14 Zeichen umfassen und Buchstaben (Groß- und Kleinbuchstaben), min. 1 Ziffer und min. 1 Sonderzeichen enthalten.
- Die Bezeichnung oder der Name des Benutzers sollen als Passwort nicht möglich sein, Wörter aus Wörterbüchern oder simple Zahlenfolgen (z.B.: 1, 2, 3, ...), sowie Geburtsdaten oder häufig verwendete Passwörter (z.B.: „passwort") sind nicht zulässig.

2.2.7 Physische Sicherheit

- Der physische Zutritt zu Büros und Rechnerräumen muss überwacht werden.
- Der Betrieb eingesetzter datenverarbeitender Komponenten erfolgt in zutrittsgeschützten Räumen.

2.2.8 Berechtigungsmanagement

- Die regelmäßige Überprüfung von Rollen und Rechten durch den A1 Applikations-datenschutzverantwortlichen muss möglich sein.
- Für die Autorisierung ist der Standard-Genehmigungsprozess der A1 Benutzerverwaltung anzuwenden. Der Dienstleister muss es A1 ermöglichen, Berechtigungen nach A1 internen Anforderungen flexibel vergeben bzw. entziehen zu können. Eine zentrale Auflistung bzw. die Einsicht und eine automatische Auswertung aller Berechtigungen müssen ermöglicht werden.

2.2.9 Deprovisionierung & Datenlöschung

- Sicheres Löschen/Deprovisionieren muss möglich sein: Dies kann durch mehrmaliges Überschreiben der Daten, durch die Vernichtung kryptographischen Schlüssel oder zertifizierte Zerstörung der Datenträger erreicht werden. Zu Vertragsende muss die Möglichkeit geboten werden, dass A1 sämtliche bestehenden Daten übergeben werden. Jeder Lieferant hat die Daten sicher zu löschen, wenn sie nicht mehr zur Erfüllung der vertraglichen Pflichten benötigt werden.

2.2.10 Checkliste für Schutzbedarf „Erweitert“

Zusätzlich zu den unter 2.1ff angeführten Anforderungen für Schutzbedarf „**Standard**“ gelten für den Schutzbedarf „**Erweitert**“ folgende, weitere Kriterien:

	Question	SW-Supplier	HW-Supplier	Cloud-Service	Human-Supplier
19	Is the documented change process for software development, testing, staging, deployments and maintenance implemented?	X		X	
20	Are there security checks in place before releasing a mayor software release?	X		X	
21	Are we (A1) allowed to test the used environment at the vendor?	X		X	
22	Are regular 3rd party security tests scheduled?	X		X	
23	Does the vendor hold a relevant security certification?	X		X	
24	Are the used datacenter(s) holding a relevant security certification?	X		X	
25	Have the used components been hardened?		X	X	
26	Are there vulnerability scans scheduled on a regular base?	X	X	X	
27	Do we have access to the log files on request?			X	
28	Is the access to the log files available at least for 18 months?			X	
29	Are there regular backup and restore tests scheduled			X	
30	Are there recovery tests scheduled?			X	
31	Is it possible to split between data- and management network?			X	
32	Is there a segmentation between management and data network?			X	
33	Are there security measurements in place to protect the software/the environment? (please specify in the comments field)	X	X	X	
34	Is there a process implemented for software releases?	X		X	
35	Are there secure coding methods in place?	X		X	
36	Are the applications structured in independent tiers?	X		X	

Sicherheitsanforderungen

	Question	SW-Supplier	HW-Supplier	Cloud-Service	Human-Supplier
37	Are there separated environments for development/quality&integration/production?	X		X	
38	Is software configured on a safe base?	X		X	
39	Are confidential data (e.g. personally identifiable information, passwords) transferred and stored encrypted by default?			X	X
40	Are the used certificates/cryptographic key stored secure?	X	X	X	
41	Is A1 holding the encryption keys?	X	X	X	
42	Is State-of-the-Art encryption used?	X	X	X	
43	Is it possible to enforce regular password change?	X	X	X	
44	Are passwords stored in plain text?	X	X	X	
45	Is a first-time access password change enforced?	X	X	X	
46	Is there an access control for offices and server rooms?			X	
47	Are the used component in an access restricted room?			X	
48	Is there a process scheduled for review user/admin roles and rights?			X	
49	Is an automatic report about user/admin roles & rights available?			X	
50	Is a secure data erasure process in place?	X		X	
51	Is there an agreement how A1 data will be archived at A1 at the end of service consumption?	X		X	
52	Are there retention policies in place?			X	

2.3 Sicherheitsanforderungen an die Schutzbedarfsklasse „Hoch"

Zusätzlich zu den Anforderungen aus den Schutzbedarfsklassen „**Standard**" (Seite 6) und „**Erweitert**" (Seite 9) gelten für Services mit dem Schutzbedarf „Hoch" die nachfolgenden Bestimmungen in diesem Kapitel.

2.3.1 Externes Hosting

- Als geheim klassifizierte Daten/Informationen dürfen nur mit einer expliziten Ausnahmegenehmigung durch den A1 CISO (Security@A1.at) außerhalb der A1 On-Premise IT-Infrastruktur (Cloud, externes Hosting etc.) gespeichert werden.

2.3.2 Formale Kriterien

- Ein definiertes Vorgehensmodell für das Service Management muss eingehalten werden (beispielsweise COBIT, ITIL, ISO 20.000)
- Es gibt einen definierten Ansprechpartner für Sicherheit und Kryptographie.
- Ein monatliches Reporting (Verfügbarkeit) ist aufgesetzt.
- Backgroundchecks beim eingesetzten Personal (beispielsweise Strafregisterbescheinigung) werden durchgeführt

2.3.3 Vulnerability & Incident Management

- Alle Services und Dienste müssen an das A1 On-Premise SIEM System (Splunk) angebunden werden[4].
- Das Notfallmanagement ist geplant, dokumentiert und aufgesetzt.
- Recovery-Tests der Datenbackups werden regelmäßig durchgeführt.
- Manuelle Sicherheitsüberprüfungen („Penetration Tests") auf die durch das Service genutzte Applikationen, Datenbanken und Infrastruktur werden regelmäßig durchgeführt.

2.3.4 Authentifizierung

- Technische Maßnahmen unterbinden die folgenden Passwortvarianten: Wörter aus Wörterbüchern, gängigen Passwörter (z.B. admin/admin, admin/1234, root/root, passwort ...), Bezeichnung oder der Name des Benutzers, allgemeines Wort mit unmittelbarem Rückschluss auf den Anwender (z.B. Vorname, Nachname, Geburtsdatum), wiederholenden oder aufeinanderfolgende Zeichen (z.B. Aaaaaaa1!, bBbbbbbb2, 3Cccccccc), simple Zahlenfolgen (z.B.: 1, 2, 3, ...), Passwörter aus früheren Leaks oder Veröffentlichungen (z.B. Have I Been Pwned oder Darkweb)

2.3.5 Netzwerksicherheit

- Ein Tool zur automatisierten Denial-of-Service (DoS) Mitigation wird eingesetzt.
- Alle wichtigen Versorgungskomponenten sind redundant ausgelegt.
- Eine Standortredundanz über mindestens 2 Rechnerstandorte ist gegeben.
- Alle Komponenten sind in ein zentrales Management eingebunden.

2.3.6 Secure Coding & Software-Architektur

- Sicherheit ist Teil des Softwareentwicklungsprozesses (Changes, Tests, Scans, Freigaben).
- Es werden statische Sourcecode-Analysen zur Vermeidung von Sicherheitsschwachstellen durchgeführt.

2.3.7 Verschlüsselung

- Die verwendeten kryptographischen Schlüssel für die Verschlüsselung von gespeicherten Daten („Data-at-rest") sind unter A1 Kontrolle.
- Regelmäßige Schlüsselwechsel können technisch unterstützt durchgeführt werden. Prozesse zum Schlüsselwechsel liegen vor. Schlüsselwechsel können beauftragt werden.
  ODER: Der Schlüssel ist in A1 Hoheit und wird bei A1 generiert.

2.3.8 Checkliste für Schutzbedarf „Hoch“

Zusätzlich zu den unter 2.1ff angeführten Anforderungen für Schutzbedarf „**Standard**“ und den unter 2.2ff angeführten Anforderungen für den Schutzbedarf „**Erweitert**“ gelten folgende weitere Kriterien für den Schutzbedarf „**Hoch**“.

	Question	SW-Supplier	HW-Supplier	Cloud-Service	Human-Supplier
53	Do you follow the standard service management process?	X	X	X	X
54	Is there a named contact for cryptography and security?	X		X	
55	Do you have a monthly reporting?	X	X	X	X
56	Are people working/administrating this environment been screened?	X		X	X
57	Is there a performance monitoring in place?			X	
58	Have you connected the service with A1 SIEM?			X	
59	Do you have an emergency management established?			X	
60	Is the used environment geo-redundant?			X	
61	Is there a tool for automatic mitigate DDOS attacks?	X	X	X	
62	Is the service included in a central management.			X	
63	Will the encryption key be changed regular?	X	X	X	

3 Publikation & inhaltliche Verantwortung

Der Inhalt wurde erstellt von:
A1 Information Security
Security@A1.at