Du kannst vertrauen.

Informationssicherheit von A1

Ihre Sicherheit - ist unser Auftrag

Grundsätze der Informationssicherheit.

Die Digitalisierung birgt neben ihrem enormen Potential vor allem auch besondere Risiken mit denen entsprechend umgegangen werden muss.

Aus diesem Grund haben wir bei A1 die Organisation so aufgestellt, dass die drei Säulen

- Strategie
- Prävention
- Reaktion

optimal wahrgenommen werden können und wir somit vor den aktuellen und zukünftigen Risiken gewappnet sind.

Unsere Maßnahmen dienen dabei dem Schutz von Daten und Informationen, um

- die Vertraulichkeit (Confidentiality)
- die Integrität (Integrity)
- und die Verfügbarkeit (Availability)

aller bei A1 verwalteten, verarbeiteten und bearbeiteten Daten und Informationen zu gewährleisten, unabhängig von der Daten- und Informationsart, um die es sich handelt, und der Form (Papier oder elektronisch) in der jene Daten und Informationen vorliegen.

Unsere Verteidigungslinien.

Grundsätze der Informationssicherheit

Verteidigungslinien

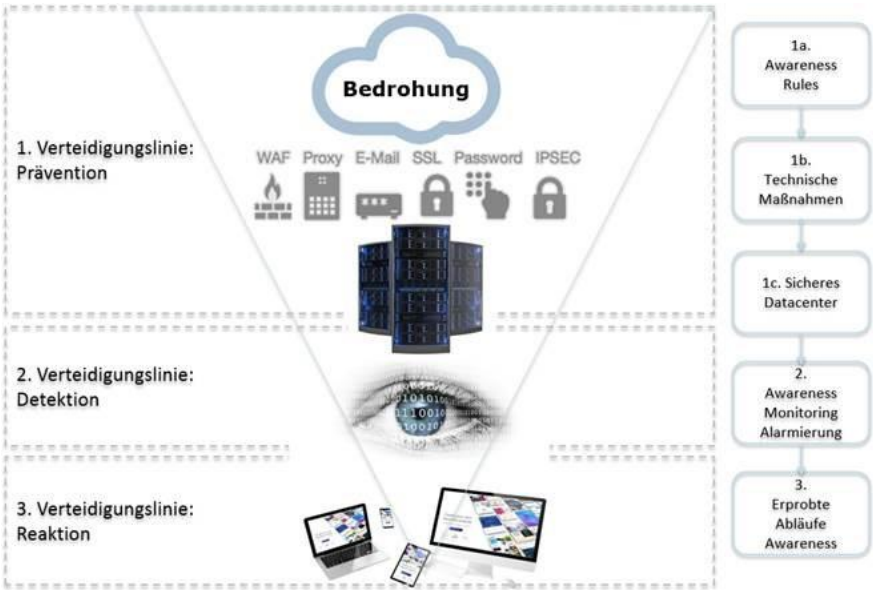
Strategische Security

Präventive Security

Reaktive Security

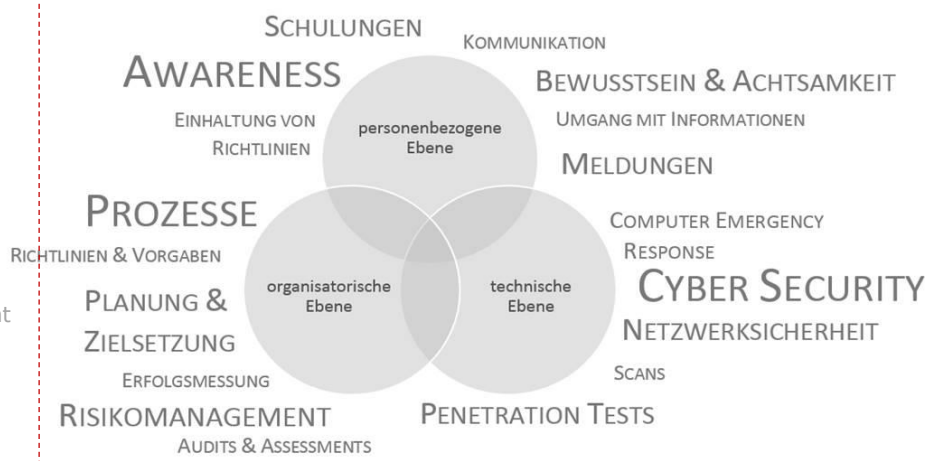
Sicherheitsmanagement

- Sicherheitspolicies
- Sicherheitsschulungen
- Verschlüsselung
- Verantwortlichkeiten
- Rollen in der Informationssicherheit
  - CERT
  - Threat Intelligence
  - SIEM
  - Security Service Desk
  - SOC
- Prozesse der präventiven Sicherheit
  - Risikomanagement
  - Auditmanagement
  - Sublieferantenmanagement
  - Personalprozess
  - User Management
  - Logging & Monitoring
  - Vulnerability Management Prozess
  - Patch Management Prozess
  - Business Continuity
- Prozesse der reaktiven Sicherheit
  - Security Incident
  - Management von großen Sicherheitsvorfällen
  - Eventmanagement
- Umsetzung
  - Physische Sicherheit
  - Systemsicherheit



Strategische Security.

Die strategische Security beschäftigt sich mit der mittel- und langfristigen Ausrichtung der Security im Unternehmen, mit dem Alignment (Ausrichtung) der Security Strategie an die Unternehmensstrategie unter Berücksichtigung aktueller Trends des Marktes und der aktuellen und künftigen Bedrohungslage. Die strategische Security formuliert Leitsätze und Ziele für das präventive und reaktive Security Management.



Die Information Security ist ein integrierter Bestandteil der Aufbau- und Ablauforganisation und wird in allen Systemebenen wahrgenommen. Wir unterscheiden präventive und reaktive Schutzmaßnahmen, die auf technischen, organisatorischen und personenbezogenen Handlungsfeldern angewendet werden, um Informationssicherheit normativ, strategisch und operativ in der A1 zu verankern.

Präventive Security.

Grundsätze der Informationssicherheit
Verteidigungslinien
Strategische Security
Präventive Security
Reaktive Security
Sicherheitsmanagement

- Sicherheitspolicies
- Sicherheitsschulungen
- Verschlüsselung
- Verantwortlichkeiten
- Rollen in der Informationssicherheit
  - CERT
  - Threat Intelligence
  - SIEM
  - Security Service Desk
  - SOC
- Prozesse der präventiven Sicherheit
  - Risikomanagement
  - Auditmanagement
  - Sublieferantenmanagement
  - Personalprozess
  - User Management
  - Logging & Monitoring
  - Vulnerability Management Prozess
  - Patch Management Prozess
  - Business Continuity
- Prozesse der reaktiven Sicherheit
  - Security Incident
  - Management von großen Sicherheitsvorfällen
  - Eventmanagement
- Umsetzung
  - Physische Sicherheit
  - Systemsicherheit

Die präventive Security definiert die aktuelle Bedrohungslage, umfasst das Risk und Chancen Management, das Configuration und Security-Asset Management, das Ausarbeiten von Prozessen und die Einführung neuer Tools.

Im Transition Prozess wird besonderes Augenmerk auf die sichere Inbetriebnahme neuer Lösungen und Komponenten gelegt. Die Wirksamkeit wird im Rahmen von Audits laufend überprüft und liefert Input für das kontinuierliche Verbesserungsmanagement.

Risikomanagement

Auditmanagement

Sublieferanten-management

Personalprozess

User Management

Logging & Monitoring

Vulnerability Management Prozess

Patch-Prozess

Business Continuity

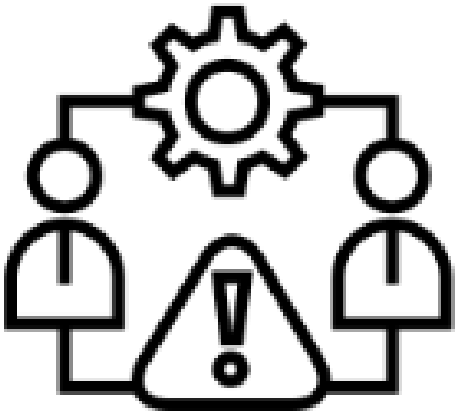
Reaktive Security.

Die reaktiven Security Teams verwalten Security Events, Incidents, Major Incidents und Problems. Sie überwachen Security Schwellwerte und konfigurieren Security Tools. Störungen, Vorfälle und Attacken werden erfasst, diagnostiziert und möglichst automatisiert mitigiert.

Zu diesen gehören unter anderem:

- das Computer Emergency Response Team (CERT)
- das Security Information and Event Management (SIEM)
- der Security Service Desk
- das Security Operation Center (SOC)
- und das Abuse Team

Diese werden näher unter „Rollen der Informationssicherheit“ beschrieben.



Sicherheitsmanagement.

Die Sicherheit der Infrastruktur und der Daten hat für uns oberste Priorität. Wir unternehmen umfangreiche und vielfältige Anstrengungen, um die Sicherheit der Daten unserer Kunden und von A1 zu gewährleisten. Aus diesem Grund berücksichtigt das Sicherheitsmanagement alle in der Norm ISO 27001 geforderten Sicherheitsprozesse und Kontrollen. Seit dem Jahr 2005 ist dieses Sicherheitsmanagement nach der Norm ISO 27001 zertifiziert. Zudem nutzen wir für die Gestaltung der Sicherheitsmaßnahmen und Kontrollen auch andere Standards und Frameworks wie beispielsweise CobIT 5.0, ISAE3402 oder SANS Top 20. Für die Integrität der Finanzprozesse hat A1 ein internes Kontrollsystem aufgebaut, welches den strengen amerikanischen Börsengesetzen (bekannt als Sarbanes & Oxley Act - SOX) entspricht.

Das Sicherheitsmanagement bei A1 besteht aus folgenden Komponenten:

1. Sicherheitspolicies / Sicherheitsschulungen / Verschlüsselung
2. Rollen und Verantwortlichkeiten
3. Sicherheitsprozesse
4. Umsetzung

Sicherheitsmanagement.

Sicherheitspolicies.

Wir haben ein Gesamtkonzept an Sicherheitsrichtlinien im Unternehmen etabliert, das unterschiedliche Themen der Informationssicherheit adressiert. Kerndokument ist die A1 Information Security Policy sowie weitere Richtlinien, die grundlegende Themen der technischen und organisatorischen Informationssicherheit wie zum Beispiel Clientsicherheit, Incidentmanagement, Netzwerksicherheit und vieles mehr ansprechen. Neben internen Sicherheitsrichtlinien, regeln wir über Vorgaben auch die Sicherheitsanforderungen an unsere Lieferanten und Subauftragnehmer.

Sicherheitsschulungen.

Uns ist das Sicherheitsbewusstsein des A1 Teams ein wesentliches Anliegen. Aus diesem Grund ist ein breites Angebot an Informationssicherheits- und Datenschutzschulungen etabliert. Angeboten und durchgeführt werden fachspezifische Klassenraumtrainings, spezielle Sicherheitsschulungen für das Management und auch unternehmensweite E-Learning Programme. Ergänzend wird in Intranet Artikeln oder E-Mail Aussendungen auf aktuelle Sicherheitsthemen Bezug genommen.

Die gemeinsame Zusammenarbeit aller Prozesse über die Normen hinweg (ISO 20000, 9000, 14000, 50000) bietet dem A1 Team ein Big Picture und fördert das Verständnis für qualitatives Arbeiten nach Compliance-Vorgaben und Gesetzen.

Sicherheitsmanagement.

Verschlüsselung.

Um die Vertraulichkeit & Integrität der Daten sicherstellen zu können, werden Kryptographische, „State of the Art", Verfahren eingesetzt.
Dies trifft sowohl bei der Übertragung, zum Beispiel von Mails, als auch bei der Speicherung von Daten zu. So sind beispielsweise alle Mitarbeiter dazu verpflichtet vertrauliche Informationen auf Dienstgeräten und externen Datenträger verschlüsselt zu speichern.

Verantwortlichkeiten.

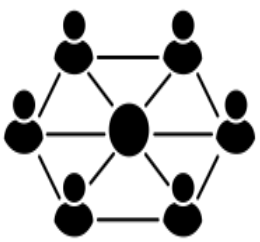
Die Verantwortlichkeiten der Informationssicherheit sind klar ausformuliert und in den Jobprofilen der Mitarbeiterinnen und Mitarbeiter hinterlegt.
Um die bereichsübergreifende Koordination der Sicherheitsaufgaben sicherzustellen sind bei A1 mehrere Gremien eingerichtet, u.a. zum Beispiel das Security Steering Board mit Vertretern aus allen wertschöpfenden Prozessen, für gemeinsame Entscheidungen, welche die Informationssicherheit betreffen.

Rollen in der Informationssicherheit.

CERT (Computer Emergency Response Team).
Die Hauptaufgaben des A1 CERT sind schnelle Angriffserkennung und koordinierte Angriffsabwehr. Die Aufgaben umfassen folgende Aktivitäten:

1. Bedrohungen analysieren und angemessen darauf reagieren
2. Angriffe erkennen und abwehren
3. Sicherheitsvorfälle bearbeiten und nachvollziehbar dokumentieren
4. Kommunikation mit externen Stellen (z.B.: Kunden, Cert.at, Behörden, ISPs)
5. Incident Management und Problem Management

Das A1-CERT besteht aus einem Team von technischen Spezialisten, die sich sowohl proaktiv, als auch reaktiv um Sicherheitsvorfälle kümmern und aus einem Dispatcher, mehreren Analysten und Security Architekten besteht.

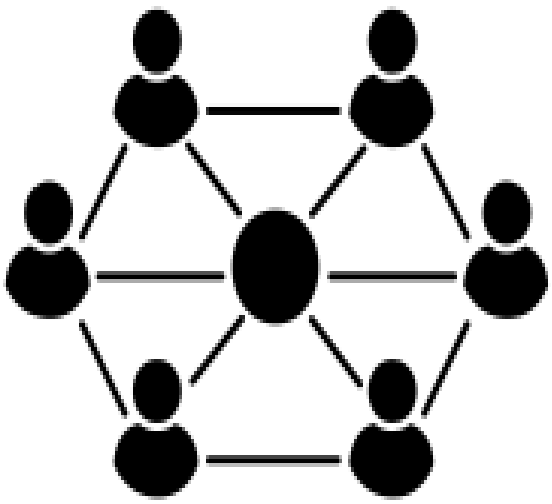


Rollen in der Informationssicherheit.

Threat Intelligence.

Eine wichtige Voraussetzung für ein gut funktionierendes CERT ist das umfangreiche Wissen über die aktuelle Bedrohungslage. Dieses erreicht man durch ständiges Studium einschlägiger Informationskanäle und Vernetzung mit anderen CERTs. Das A1-CERT tauscht Informationen sowohl mit nationalen als auch mit internationalen CERT Organisationen aus und ist Mitglied bei folgenden CERT Organisationen:

1. CERT Verbund Österreich
2. CERT Austrian Trust Circle
3. ETIS CERT-SOC Telco Network
4. KSÖ Forum



Rollen in der Informationssicherheit.

Security Information and Event Management (SIEM).

Der Security Analyst beschäftigt sich mit dem SIEM Tool zur Korrelation von Ereignissen um Angriffe möglichst frühzeitig zu erkennen, aus vergangenen Vorfällen zu lernen, das System weiter zu entwickeln und auf aktuelle und künftige Bedrohungen anzupassen.

Security Service Desk.

Der Security Service Desk ist Teil des Service Operation Centers und rund um die Uhr für das A1 Team erreichbar.
Es ist die erste Anlaufstelle für die Entgegennahme von Sicherheitsvorfällen in der A1. Hier erfolgt die Erstdiagnose, Klassifizierung, Priorisierung, Ticketanlage und Zuweisung an die 2nd Level Support Teams in der Data Privacy Unit, den Technikteams oder dem CERT. Major Incidents werden sofort an geeignete Management Kanäle weitergegeben und mit hoher Priorität behandelt. Im Fall des Falles wird auch das Krisenteam informiert.

Rollen in der Informationssicherheit.

Security Operation Center (SOC).

Wir betreiben ein Security Operation Center, eine Kombination aus Experten, Werkzeugen und Prozessen mit dem Ziel, IT Sicherheits-Risiken

- zu verhindern
- zu entdecken
- zu analysieren,
- zu bewerten

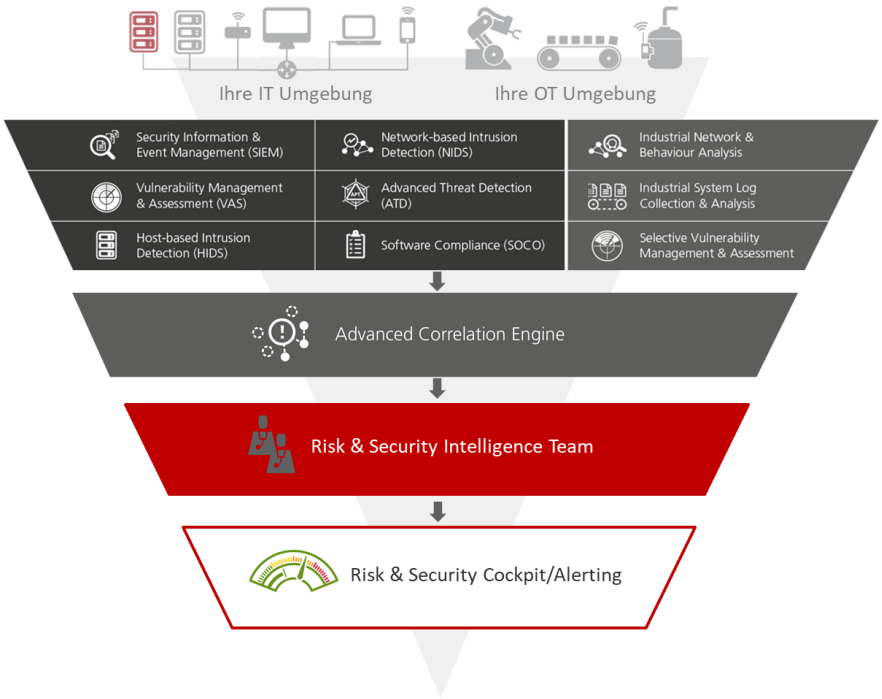
deren Behebung zu beschreiben und zu kontrollieren, sowie im Bedarfsfall die Beweissicherung einzuleiten.

In der Betriebsstelle Wien werden die Information Security Alerts, Ergebnisse von Vulnerability Scans, Daten zu Netzwerkanomalien und mehr gesammelt, bewertet, priorisiert, korreliert, gefiltert und der Kunde über mögliche Schwachstellen und erkannte Angriffe informiert.

Der Kunde hat über ein Security Cockpit jederzeit einen Überblick über seine Sicherheitslage und kann aufgrund der Priorisierung sofort erkennen, wo am dringendsten Handlungsbedarf betsteht.

Rollen in der Informationssicherheit.

Security Operation Center (SOC).



Prozesse der präventiven Sicherheit I.

Für die Abläufe in der Information Security wie Risiko- und Auditmanagement, User Management, Vulnerability Management und vieles mehr haben wir Prozesse definiert und auch operativ umgesetzt. Sie werden im Rahmen unseres kontinuierlichen Verbesserungsprozesses (KVP) laufend überprüft und bei Bedarf optimiert.

Risikomanagement.
Bei der Speicherung, Übermittlung und Verarbeitung von Daten und Informationen können Risiken entstehen die systematisch erkannt, analysiert und bewertet werden müssen. Auf dieser Basis wird dann eine Entscheidung über die wirtschaftlich sinnvollen Maßnahmen zur Eliminierung oder Reduzierung dieser Risiken getroffen. Diese systematische Bearbeitung der Risiken wird bei uns im Rahmen eines festgelegten Risikomanagementprozesses regelmäßig durchgeführt.

Auditmanagement.
Die Einhaltung der Daten- und Informationssicherheitsvorgaben wird regelmäßig überprüft. Diese Überprüfung geschieht in der Form technischer und organisatorischer Audits. Diese Audits werden sowohl von internen als auch von externen Experten durchgeführt. Im Vorfeld wird ein jährlicher Auditplan mit den zu überprüfenden Themengebieten festgelegt.

Prozesse der präventiven Sicherheit II.

Sublieferantenmanagement.
Für die Gewährleistung eines konsistenten Sicherheitsniveaus ist es wichtig, dass auch alle Sublieferanten den von uns festgelegten Schutzbedarf berücksichtigen. Dazu haben wir eine eigene Richtlinie verfasst, die Bestandteil der Verträge mit unseren Sublieferanten ist.

Personalprozess.
New Manager Trainings, Welcome Veranstaltungen und zielgerichtete Informationen per Mail sowie im Self Service Portal helfen dabei, Newcomers abzuholen und kontrolliert in die Prozesslandschaft einzuführen. Verpflichtende eLearnings zu Compliance, GDPR und Informationssicherheit helfen dabei, das Ausbildungsniveau auf einem Minimum Standard zu halten und immer wieder aufzufrischen. Zusätzlich muss jeder Mitarbeiter ein „Non Disclosure Agreement" und eine „Company Compliance" Erklärung abgeben.

Prozesse der präventiven Sicherheit III.

User Management.

Für uns sind die Begriffe „Least Privilege" und „Need to Know" oberstes Gebot in der Rechtevergabe. Erweiterte Sicherheits- und Kontrollmaßnahmen sind für privilegierte / Administrationsuser etabliert. Auch SOX hat zur Steigerung der Qualität dieses Prozesses viel beigetragen – zahlreiche Kontrolldurchführungen, Stichproben und Management Reviews schützen unsere Systeme vor nicht befugten Zugriffen.

Logging & Monitoring.

Logging, also das Aufzeichnen von Aktivitäten und Ereignissen, helfen uns bei der Angriffserkennungen und ermöglichen forensische Analysen um den Hergang von Sicherheitsvorfällen aufklären zu können.
Log-Dateien werden vor Verlust, Löschung, Modifizierung und unberechtigtem Zugriff geschützt und entsprechend der Unternehmensrichtlinien über einen bestimmten Zeitraum aufbewahrt.

Prozesse der präventiven Sicherheit IV.

Vulnerability Management Prozess.

Schwachstellen sind Verwundbarkeiten von Systemen, die von Angreifern ausgenutzt werden können. Wir prüfen neu kommende Hardware und Software im Zuge des Transition Prozesses als auch laufende Services monatlich auf Schwachstellen. Dazu verwenden wir marktführende Softwarelösungen und führen (selbst oder extern) Penetration Tests durch.
Über qualitative und sichere Kanäle treten wir gerne mit Sicherheitsforschern in die Diskussion und gehen den Hinweisen von Herstellern und dem A1 Team nach.
Alle erkannten Schwachstellen werden dabei im Zuge des Vulnerability Management Prozesses bewertet und einer geeigneten Behebung unterzogen beziehungsweise im bewährten Patch Management Prozess behoben.
In unserem Reporting sind das Vulnerability Age und die Scan Rate mitunter die wichtigsten und am häufigsten kontrollierten Kennzahlen.

Patch Management Prozess.

Ein kurzes Schwachstellen Alter – also die Zeit vom Erkennen einer Vulnerability bis zur Behebung – wird durch unseren Patch Management Prozess optimal unterstützt.
Die Überprüfung des aktuellen Patchingstands ist eine wichtige qualitative Maßnahme um unabhängig von Systemadministratoren zu prüfen, ob alle erforderlichen Sicherheitspatches rechtzeitig eingespielt werden. Vier Changeprozesse (Standard, Nonstandard, Minor und Emergency) helfen dabei, die Systeme zeitnah zu patchen und gegen Angriffe auf bekannte, identifizierte Sicherheitsschwachstellen abzusichern.

Prozesse der präventiven Sicherheit V.

Business Continuity.

Ein Bedrohungsszenario kann durch Menschen, aus technischen Gründen, oder auch durch Naturkatastrophen (höhere Gewalt) verursacht werden. Dabei ist die Datensicherung essentiell für die Verfügbarkeit und notfalls auch für die Wiederherstellbarkeit verloren gegangener Daten.

Egal welches Bedrohungsszenario eintreten sollte, die Verfügbarkeit der Daten und Systeme sind durch eine Reihe von Maßnahmen z.B. durch eine georedundante Aufstellung der Systeme sichergestellt.

Um eine Auslastung der Server zu verhindern, welche die Verfügbarkeit gefährden könnte, werden Load Balancer eingesetzt und die Performance kritischer Services überwacht und bei Überlast alarmiert.

In Bezug auf Disaster Recovery werden je nach Anwendungsfall unter anderem Systemsicherungen, Komplett- oder Vollsicherungen und differenzielle/inkrementelle Sicherungen durchgeführt damit diese im Falle einer notwendigen Wiederherstellung zur Verfügung stehen. Die Datensicherungsintervalle sowie die Wiederherstellbarkeit der Daten sind in unseren Security Guidelines definiert und werden in regelmäßigen Abständen überprüft.

Wir sind in Kontakt mit allen anderen kritischen Infrastrukturbetreibern und Behörden, um im Krisenfall rasch für die Wiederherstellung der erforderlichen Dienste sorgen zu können.

Prozesse der reaktiven Sicherheit.

Information Security Incident.

Bei A1 gilt jeder Vorfall oder jede angenommene Handlung, die in ungesetzlicher, nicht autorisierter oder unannehmbarer Art die Vertraulichkeit, Integrität oder Verfügbarkeit der Systeme, Applikationen oder Informationen bei A1 bedroht, stört und gegen die Informationssicherheitsvorgaben in der TAG (Telekom Austria Group) und bei A1 verstößt, als Informationssicherheitsvorfall („Incident"). Werden die Zuordenbarkeit und Nichtabstreitbarkeit von Aktionen oder Handlungen in Systemen bewusst verhindert, wird ein solcher Vorfall ebenfalls als Incident bewertet. Die Incidents können über die Kanäle Security Service Desk, A1 CERT und Security Management gemeldet werden. Die Nachvollziehbarkeit und Statusüberprüfung eines Incidents ist anhand eines Ticketsystems jeder Zeit möglich.

Management von großen Sicherheitsvorfällen.

Ist ein vitales Service, Teile der kritischen Infrastruktur oder Kundendaten von einem Sicherheitsvorfall betroffen oder handelt es sich um Ereignisse mit hohem medialem Impact dann sprechen wir von einem großen Sicherheitsvorfall. Das Managen von diesen unterliegt zusätzlichen Anforderungen um diese schnellstmöglich beheben und den Schaden eingrenzen zu können.

Eventmanagement.

Security Events sind sicherheitsrelevante Ereignisse, die mit Hilfe von Tools festgestellt werden und meistens mithilfe einfacher Automatismen bereinigt werden können (Automitigierung). Kann ein Event nicht automatisiert behoben werden oder reicht es nicht aus, dieses in ein Logfile wegzuschreiben, wird es im Incident Management weiter behandelt.

Umsetzung.

Physische Sicherheit.

Der berechtigte Zugang in A1 Objekte wird sowohl für interne, als auch für externe Personen durch festgelegte Prozesse geregelt. Des weiteren wird das Verhalten im Umgang mit Gebäudesicherheit sensibilisiert. Videosysteme, Zutrittssysteme und Alarmsysteme bilden die Säulen der physischen Sicherheit, die durch den Einsatz von Sicherheitspersonal ergänzt werden. Besonders schutzbedürfte Bereiche wie zum Beispiel Data centers (Rechenzentren) werden häufig auditiert und Stichproben unterzogen.

Systemsicherheit.

Um zu verhindern, dass Schadsoftware auf den Systemen unserer Kunden und der A1 gelangen und die Sicherheit der Netze und Computersysteme bedrohen, haben wir zahlreiche Schutzmaßnahmen an der IT Infrastruktur umgesetzt:

- verpflichtende Installation eines Virenschutzprogrammes,
- eines Data Loss Prevention (DLP) Programmes
- Unterteilung des Data Centers in Zonen, die das Ausbreiten von Störungen verhindern
- Firewalls
- Proxys
- Intrusion Prevention Systeme
- Sicherheitsvorkehrungen gegen DDOS Attacken
- SIEM
- Multitier Architektur
- Trennung von Entwicklung und Produktion
- Erfassung aller sicherheitsrelevanten Assets in einem Inventory (CMDB)

Weitere Informationen unter:
https://cdn11.a1.net/m/resources/media/pdf/LB-A1-IT-Security.pdf

Wir setzen eine Reihe von Maßnahmen um, damit unsere IT-Infrastruktur nicht nur vor den aktuellen sondern auch vor den zukünftigen Bedrohungen geschützt ist und wir unseren eigenen strengen Anforderungen gerecht werden.

Informationen zum Thema Datenschutz finden Sie unter: https://www.a1.net/datenschutz

A1 Telekom Austria AG
Lassallestraße 9
1020 Wien
A1.net