Digital Trust.

A1 Information Security

Your security is our mission

Principles of information security.

In addition to its enormous potential, digitisation also entails special risks that must be dealt with accordingly.

That is why A1 has set up the organisation in such a way that the three pillars

- Strategy
- Prevention
- Response

can be optimally perceived and are as such prepared for current and future risks.

Our measures are designed to protect data and information in order to ensure

- the confidentiality
- the integrity
- and the availability

of all data and information that is managed, processed and handled at A1, regardless of the type of data and information involved and the form (paper or electronic, etc.) in which the data and information is available.

Our defences.

Principles of information security

Our defences

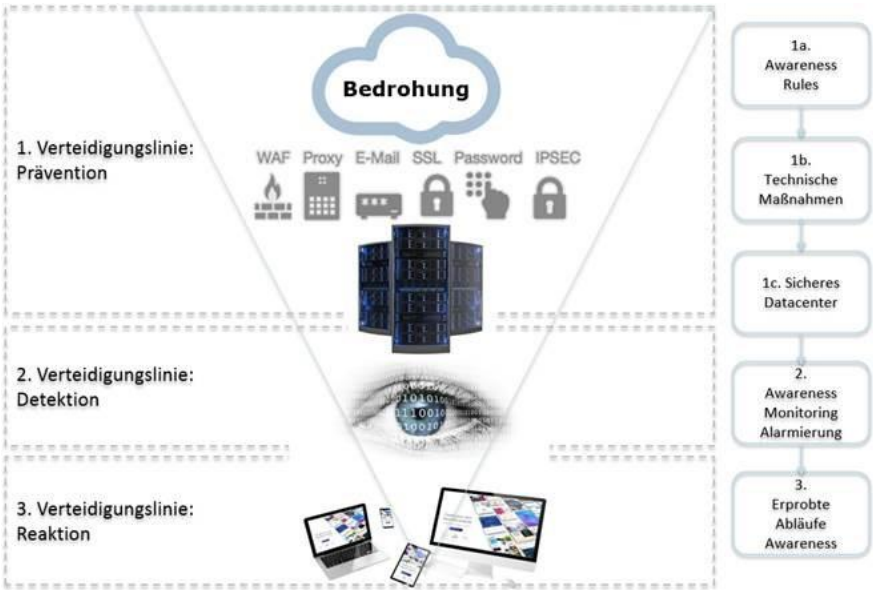
Strategic Security

Präventive Security

Reaktive Security

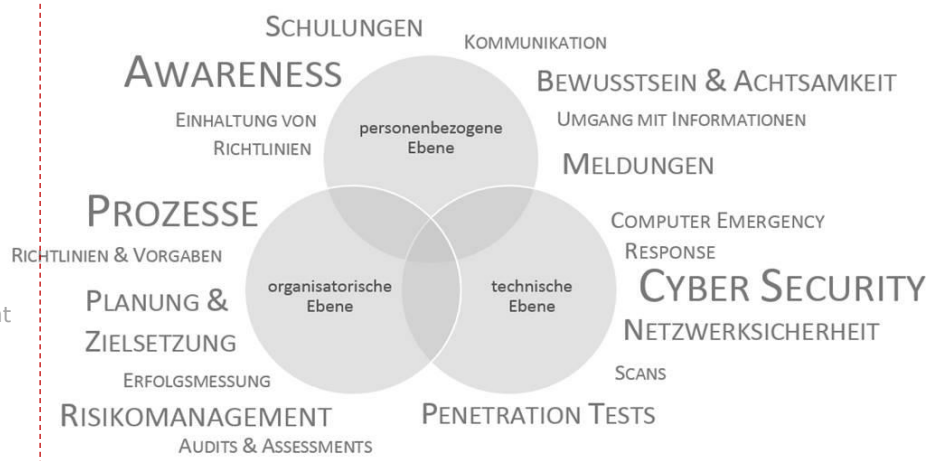
Security Management

- Security Policies
- Security Training
- Encryption
- Responsibilities
- Roles in Information Security
  - CERT
  - Threat Intelligence
  - SIEM
  - Security Service Desk
  - SOC
- Preventive Security Processes
  - Risk Management
  - Audit Management
  - Subcontractor Management
  - Personnel Process
  - User Management
  - Logging & Monitoring
  - Vulnerability Management Prozess
  - Patch Management Prozess
  - Business Continuity
- Reactive Security Processes
  - Security Incident
  - Managing Big Security Incidents
  - Event Management
- Implementation
  - Physical Security
  - System Security



Strategic Security.

Strategic security concerns itself with the medium-term and long-term orientation of security within the company, with the alignment of the security strategy with the company strategy, taking into account current market trends, and with the current and future threat situation. Strategic security formulates guidelines and objectives for preventive and reactive security management.



Information security is an integrated part of the structural and process organisation and is performed on all system levels. We distinguish between preventive and reactive protective measures, which are applied to technical, organisational and personal fields of action in order to anchor information security normatively, strategically and operationally within A1.

Preventive Security.

Principles of information security
Our defences
Strategic Security
Präventive Security
Reaktive Security
Security Management

- Security Policies
- Security Training
- Encryption
- Responsibilities
- Roles in Information Security
  - CERT
  - Threat Intelligence
  - SIEM
  - Security Service Desk
  - SOC
- Preventive Security Processes
  - Risk Management
  - Audit Management
  - Subcontractor Management
  - Personnel Process
  - User Management
  - Logging & Monitoring
  - Vulnerability Management Prozess
  - Patch Management Prozess
  - Business Continuity
- Reactive Security Processes
  - Security Incident
  - Managing Big Security Incidents
  - Event Management
- Implementation
  - Physical Security
  - System Security

Preventive security defines the current threat situation, includes risk and opportunity management, configuration and security asset management, process development, and the introduction of new tools.

In the transition process, special attention is paid to safely starting up new solutions and components. Its effectiveness is continuously checked during audits and provides input for continuous improvement management.

Risikomanagement

Auditmanagement

Sublieferanten-management

Personalprozess

User Management

Logging & Monitoring

Vulnerability Management Prozess

Patch-Prozess

Business Continuity

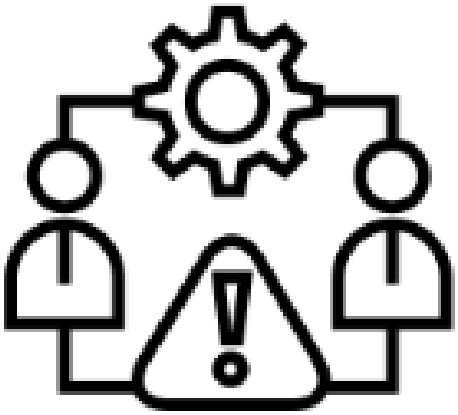
Reactive Security.

The reactive security teams manage security events, incidents, major incidents and problems. They monitor security thresholds and configure security tools. Malfunctions, incidents and attacks are recorded, diagnosed and mitigated—automatically where possible.

It includes, but is not limited to:

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

More information:
"Roles in Information Security".



Security Management.

The security of the infrastructure and the data is a top priority for us. We go to great lengths to ensure the security of our customers' and A1's data. For this reason, security management considers all security processes and controls required by the ISO 27001 standard. Since 2005, this security management has been ISO 27001-certified. We also use other standards and frameworks such as CobIT 5.0, ISAE3402 or SANS Top 20 to design security measures and controls. A1 has established an internal control system for the integrity of financial processes, which complies with the stringent U.S. stock exchange laws (known as the Sarbanes & Oxley Act, or SOX).

A1’s security management consists of the following components:

1. Security Policies/Security Training/Encryption
2. Roles and Responsibilities
3. Security Processes
4. Implementation

Security Management.

Security Policies.

We have established a security master guideline within the company that addresses various information security issues. The A1 Information Security Policy is the core document as are other guidelines, which address fundamental issues of technical and organisational information security such as client security, incident management, network security, and much more. In addition to internal security guidelines, we also regulate the safety requirements for our suppliers and subcontractors via specifications.

Security Training.

The A1 team's security awareness is very important to us. For this reason, we set up a wide range of information security and data protection training courses. We offer and conduct specialised classroom training, special security courses for management, and company-wide eLearning programmes. Moreover, current security topics are addressed in articles on the intranet or in email newsletters.

The joint cooperation of all processes across the standards (ISO 20000, 9000, 14000, 50000) helps the A1 team see the big picture and promotes the team's appreciation for high-quality work in accordance with compliance requirements and laws.

Security Management.

Encryption.

In order to ensure the confidentiality & integrity of data, we use cryptographic, state of the art procedures.
This applies to both the transmission (such as of emails) and the storage of data. For example, all employees are required to encrypt confidential information when storing it on service devices and external storage media.

Responsibilities.

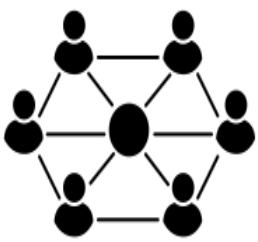
The responsibilities for information security have been clearly developed and are stored in the employee's job profiles.
So as to ensure cross-departmental coordination of security tasks, A1 has set up several committees, including the Security Steering Board with representatives from all value-adding processes, to make joint decisions concerning information security.

Roles in Information Security.

CERT (Computer Emergency Response Team).
The main tasks of A1's CERT is to quickly detect attacks and to coordinate their defence. The tasks include the following activities:

1. Analysing threats and responding to them in an appropriate manner
2. Recognising and fending off attacks
3. Responding to security incidents and documenting them in a traceable and comprehensible manner
4. Communicating with external bodies (e.g. customers, Cert.at, authorities, ISPs)
5. Incident management and problem management

The A1 CERT consists of a team of technical specialists, who proactively and reactively deal with security incidents, and of a dispatcher, several analysts, and security architects.

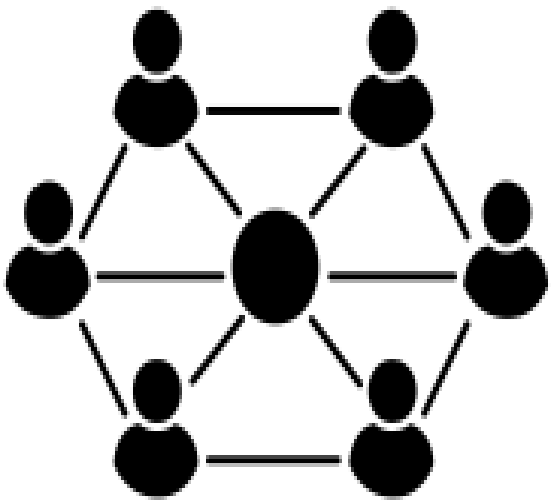


Roles in Information Security.

Threat Intelligence.

An important prerequisite for a well-functioning CERT is having extensive knowledge of the current threat situation. That is achieved through continuously studying relevant information channels and networks with other CERTs. The A1 CERT exchanges information with both national and international CERT organisations and is a member of the following CERT organisations:

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



Roles in Information Security.

Security Information and Event Management (SIEM).
The security analyst deals with the SIEM tool for correlating events so as to detect attacks as early as possible, to learn from past incidents, to further develop the system, and to adapt to current and future threats.

Security Service Desk.
The Security Service Desk is part of the Service Operation Center and is available to the A1 team around the clock.
It is the first point of contact at A1 for receiving security incidents. Here, the initial diagnosis, classification, prioritisation, ticket creation, and assignment to the 2nd level support teams in the Data Privacy Unit, the technical teams, or the CERT takes place. Major incidents are immediately forwarded to appropriate management channels and given high priority. In the event of a crisis, the crisis team is also informed.

Roles in Information Security.

Security Operation Center (SOC).

We operate a Security Operation Center, which is a combination of experts, tools, and processes with the goal of

- preventing
- discovering
- analysing
- evaluating

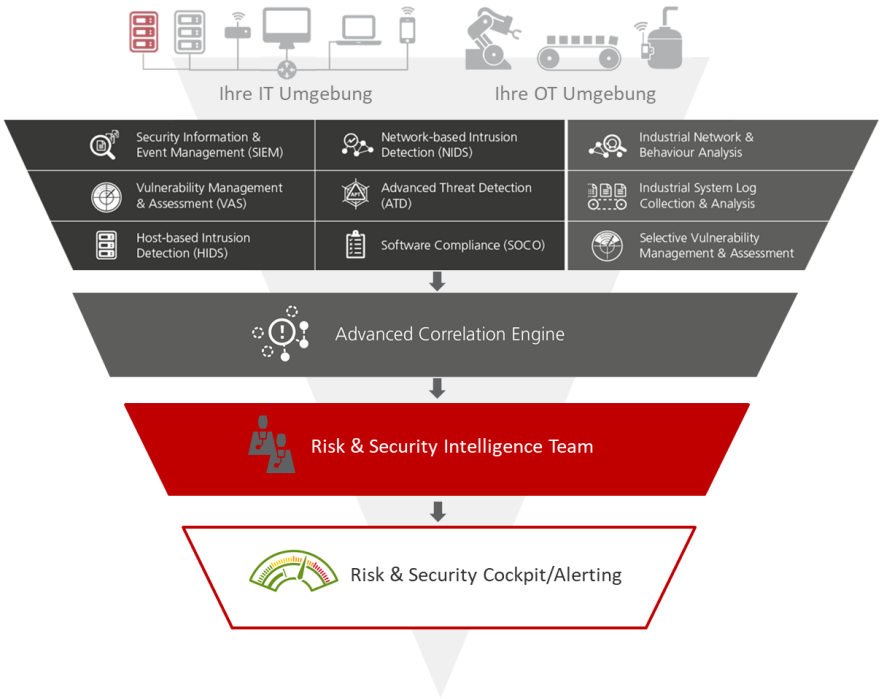
IT security risks, to describe and control their remedy and, if necessary, to initiate the preservation of evidence.

The Vienna office collects, evaluates, prioritises, correlates, and filters information security alerts, results of vulnerability scans, data on network anomalies, etc. and informs the customer about possible weak points and detected attacks.

A security cockpit provides the customer with an overview of its security situation at all times and can immediately identify where the most urgent need for action has arisen due to prioritisation.

Roles in Information Security.

Security Operation Center (SOC).



Preventive Security Processes I.

We have defined processes for information security procedures such as risk and audit management, user management, vulnerability management, etc. and have also implemented them operationally. As part of our continuous improvement process (CIP), they are reviewed on an ongoing basis and optimised where required.

Risk Management

The storage, transmission, and processing of data and information can bring about risks that must systematically be identified, analysed, and evaluated. On this basis, a decision is then made on the economically viable measures to eliminate or reduce these risks. We regularly carry out the systematic processing of risks as part of a defined risk management process.

Audit Management

Compliance with data and information security requirements is checked on a regular basis. This review takes place in the form of technical and organisational audits. These audits are carried out by both internal and external experts. An annual audit plan is defined in advance for the issues that are to be reviewed.

Preventive Security Processes II.

Subcontractor Management

In order to ensure a consistent level of security, it is important that all subcontractors take into account the protection needs that we define. For this purpose, we have drawn up our own guidelines, which form part of the contracts we conclude with our subcontractors.

Personnel Process.

New manager training, welcome events, targeted information via email and self-service portals are helpful ways of easing newcomers into the process landscape in a controlled manner. Compulsory eLearning courses on compliance, GDPR, and information security help to maintain a minimum standard for the level of training and to continuously refresh the know-how. In addition, each employee must sign a non-disclosure agreement and a company compliance declaration.

Preventive Security Processes III.

User Management.

For us, the terms "least privilege" and "need to know" have top priority when assigning rights. Advanced security and control measures are established for privileged/administrative users. SOX has also made a major contribution to improving the quality of this process: numerous controls, random checks, and management reviews protect our systems from unauthorised access.

Logging & Monitoring.

Logging, i.e. recording activities and events, helps us detect attacks and enables forensic analyses to reconstruct the security incident.
Log files are protected against loss, deletion, modification, and unauthorised access and stored for a specified period of time in accordance with corporate policy.

Preventive Security Processes IV.

Vulnerability Management Process.

Vulnerabilities are system weaknesses that can be exploited by attackers. We check new hardware and software in the course of the transition process and current services for weak points on a monthly basis. We use market-leading software solutions and carry out penetration tests (ourselves or externally).
We are willing to enter into discussions with security researchers via qualitative and secure channels and follow the manufacturer's and the A1 team's advice.
All identified vulnerabilities are evaluated in the course of the vulnerability management process and subjected to a suitable remedy or remedied in the tried and tested patch management process.
In our reporting, the vulnerability age and the scan rate are among the most important and most frequently controlled indicators.

Patch Management Prozess.

A short vulnerability age, i.e. the time from when the vulnerability is detected to when it was remedied, is optimally supported by our patch management process.
Checking the current patch status is an important qualitative measure to see independently from system administrators whether all required security patches are applied on time. Four change processes (standard, nonstandard, minor, and emergency) help patch the systems promptly and secure them against attacks on known, identified security vulnerabilities.

Preventive Security Processes V.

Business Continuity.

A threat scenario can be caused by humans or natural disasters (force majeure) or happen for technical reasons. Backing up data is essential for the availability and, if necessary, the recoverability of lost data.

No matter which threat scenario should occur, the availability of the data and systems is ensured by a series of measures such as through a geo-redundant installation of the systems.

Load balancers are used to prevent a server from reaching full capacity, which could jeopardise availability; further, the performance of critical services is monitored and an alert sent out in the event of an overload.

With regard to disaster recovery, system backups, complete or full backups, and differential/incremental backups are performed depending on the application so that they are available in the event a recovery becomes necessary. The data backup intervals and the recoverability of the data are defined in our security guidelines and are checked at regular intervals.

We keep in contact with all other critical infrastructure operators and authorities to be able to quickly restore the necessary services in the event of a crisis.

Reactive Security Processes.

Information Security Incident.

At A1, any incident or assumed action that, in an unlawful, unauthorised or unacceptable manner, is a threat or a disruption to the confidentiality, integrity or availability of the systems, applications or information at A1 and is in breach of the information security requirements at TAG (Telekom Austria Group) and A1, is considered to be an information security incident. If the assignability and non-repudiation of actions or procedures in systems are deliberately prevented, such an incident is also considered to be an incident. Incidents can be reported through the Security Service Desk, A1 CERT, and Security management channels. The traceability and status check of an incident can be done with a ticket system at any time.

Managing Big Security Incidents.

If a vital service, parts of the critical infrastructure, or customer data is affected by a security incident, or if it is an event with a high media impact then we speak of a big security incident. Managing them is subject to additional requirements in order to remedy them as quickly as possible and to limit the damage.

Event Management.

Security events are security-relevant events that are detected with the help of tools and can usually be cleaned using simple automatisms (auto-mitigation). If an event cannot be remedied automatically or if it is not enough to write it to a log file, incident management will further handle it.

Implementation.

Physical Security.

Authorised access to A1 properties is regulated by defined processes for both internal and external persons. Furthermore, awareness of the importance of building security is increased. Video systems, access systems, and alarm systems form the pillars of physical security, which are supplemented by the deployment of security personnel. Places that are in particular need of protection, such as data centres, are frequently audited and subjected to random checks.

System Security.

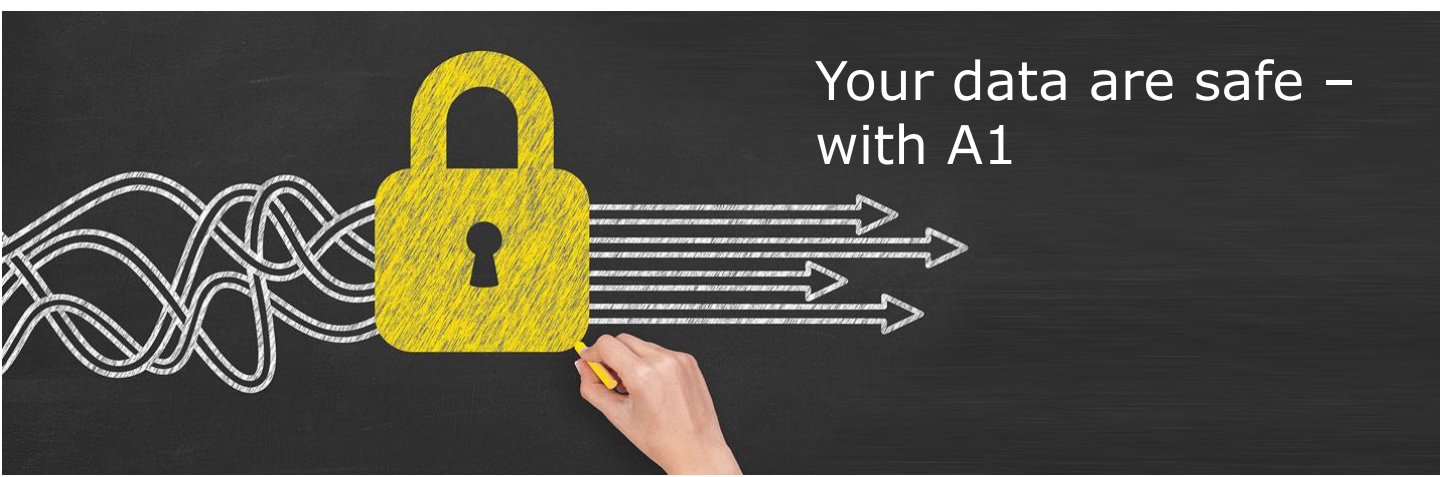
To prevent malware from reaching our customers' and A1's systems and threatening the security of networks and computer systems, we have implemented numerous protective measures on our IT infrastructure:

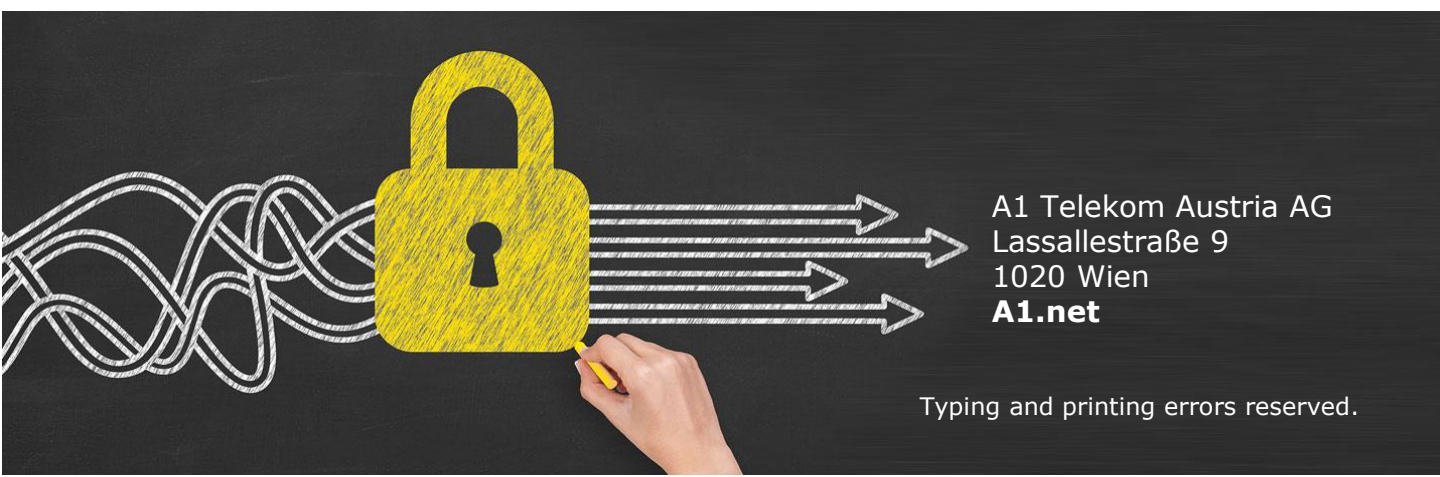
- Mandatory installation of an antivirus software
- Data loss prevention (DLP) programmes
- Subdividing the data centre into zones that prevent disruptions from spreading
- Firewalls
- Proxies
- Intrusion prevention system
- Security precautions against DDoS attacks
- SIEM
- Multitier architecture
- Separating development and production
- Recording all security-relevant assets in an inventory (CMDB)

More information :
https://cdn11.a1.net/m/resources/media/pdf/LB-A1-IT-Security.pdf

We implement a number of measures to ensure that our IT infrastructure is protected not only against current but also future threats and that we can meet our own strict demands.

Information on data protection can be found at: https://www.a1.net/datenschutz





A1 Telekom Austria AG
Lassallestraße 9
1020 Wien
A1.net