

Security Policy

Intrusion Detection & Prevention

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Intrusion Detection and Prevention | |  |
| Number | [Number] | |
| Issued on | 04.07.2022 | |
| Through | Chief Information Security Officer | |
| Entry into force | 04.07.2022 | |
| Scope of application | SÜDVERS Holding GmbH & Co. KG and its majority-owned subsidiaries, as well as SÜDVERS International GmbH | |
| Topic | Compliance | |
| Responsible function | Information security | |
| Responsible person | Dirk Franken | |
| Overriding regulation | Information security policy | |
| Replaces | n/a | |
| Applicable documents |  | |
| Validity | Until further notice | |
| Last | 14.07.2025 | |
| Next review | 14.07.2025 | |
| Publication | SÜDVERS Intranet | |
| Classification | Internal | |
| Archive | Document management system | |
| Organizational system | [Organizational system] | |
| Languages |  | |
| Formats |  | |
| Remarks |  | |

Table of contents

[1 Principle 4](#_Toc107911880)

[2 Objective 4](#_Toc107911881)

[3 Controls 4](#_Toc107911882)

# Principle

Mechanisms for detecting and preventing intrusions (IDS and IPS) must be installed on critical systems, in critical networks and between network segments that have a high trustworthiness gradient in relation to the source and destination addresses of the systems involved in the communication.

# Objective

Identify suspicious or actual malicious attacks and enable SÜDVERS to respond before serious damage can be done.

# Controls

Mechanisms (IDS and IPS) for detecting and preventing intrusions must be used on business-critical applications, systems and network gateways in order to recognize predetermined and new types of attack. Different IDS and IPS must be used by the server systems on network gateways.

Intrusion detection and prevention methods must be supported by IT documented standards/procedures that include the following

* Methods for detecting unauthorized activities
* Analysis of suspected intruders
* Reactions to different types of attacks
* Cooperation with IT and specialist departments

IT must establish a baseline of normal, acceptable and expected system and network activity to detect potential and actual intrusions by

* Communication paths in connected systems and networks are identified and documented
* the type, volume and timing of network traffic are monitored
* Analyze patterns of system and network user activity
* Determines where and how remote maintenance connections are established
* Event logs are analyzed

Intrusion detection and prevention mechanisms must recognize the following

* the unplanned termination of processes or applications
* Activities typically associated with malware or traffic originating from known malicious IP addresses or network domains (e.g. those associated with botnet command and control servers)
* Known attack characteristics (such as denial of service and buffer overflows)
* unusual or abnormal system behavior (e.g. recording of keystrokes, process injection and deviations in the use of standard protocols)
* unauthorized (actual or attempted) access to systems or information

The mechanisms for detecting and preventing intrusions must be configured in such a way that:

* new or updated attack characteristics are taken into account in good time
* Suspicious activity alerts, supported by documented procedures for responding to suspected intruders
* the intrusion detection and prevention systems are protected from attack (e.g. by hiding the presence of intrusion detection and prevention software)

Intrusion detection and prevention methods must be supported by specialized software, such as host-based intrusion detection and prevention systems (HIPS) and network-based intrusion detection and prevention systems (NIPS).

Network intrusion detection and prevention systems (e.g. special hardware to detect unauthorized or abnormal activity in network traffic) must be protected against attacks (e.g. by preventing the transmission of outbound network traffic or by eavesdropping on the network to hide the presence of the sensor).

The intrusion detection and prevention software must:

* be tested before use
* updated automatically and within specified deadlines
* be configured in such a way that
  + a warning is issued in the event of suspicious activity (e.g. via an administration console, e-mail messages or SMS messages to cell phones)
  + the communication connections are interrupted during predefined activities

Regular checks must be carried out to confirm that:

* the configuration of the intrusion detection and prevention software meets the requirements
* the intrusion detection and prevention software has not been deactivated or manipulated
* updates were carried out within the specified time frame.

Suspected attacks must be analyzed and the potential impact on the business assessed, which includes

* Confirmation of whether an attack is actually taking place (e.g. by eliminating false positives)
* Determination of the type of attack (e.g. worms, buffer overflows or denial of service)
* the identification of the original point of attack
* Quantification of the potential impact of the attack

There must be a documented process for reporting serious attacks as part of security incident handling.