KNOWIT DATAUNIT

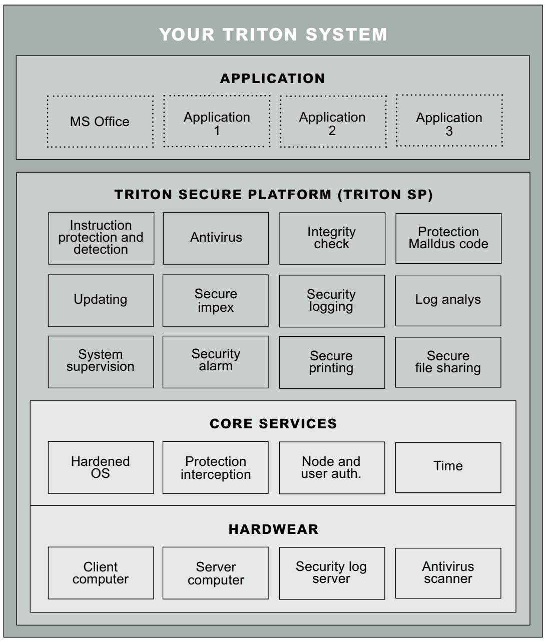
Triton Secure Platform

Triton Secure Platform provides a high level of security combined with a modular concept, allowing for a security solution tailored to the security needs of different systems.

TRITON SECURE PLATFORM (Triton SP) is a modular security solution aimed for use in IT-systems intended to handle classified information up to the level of HEMLIG/SECRET (comparable with NATO SECRET).

On Triton SP, different applications can easily be integrated to ensure a system with high level of security.

The Platform is module based to ensure a high grade of flexibility and the possibility to meet the diverse needs that occurs in such a complex environment as that of the Swedish Armed Forces or your own organization.



YOUR TRITON SYSTEM

APPLICATION

MS Office | Application 1 | Application 2 | Application 3

TRITON SECURE PLATFORM (TRITON SP)

Instruction protection and detection | Antivirus | Integrity check | Protection Malldus code

Updating | Secure impex | Security logging | Log analys

System supervision | Security alarm | Secure printing | Secure file sharing

CORE SERVICES

Hardened OS | Protection interception | Node and user auth. | Time

HARDWEAR

Client computer | Server computer | Security log server | Antivirus scanner

The Triton SP consists of Hardware, Core Services and separate service modules and together they form the base of a flexible secure system.

On the top of Triton SP your applications are integrated in a controlled manner and the user will go almost unnoticed about the high level of security.

Hardware

A set of prepared hardware including tempest certified computers and devices with a limited transmission of signals makes it easy to build a system based on the secure platform.

If specific customers' requirements exist additional hardware can also be integrated to the system.

Core services

HARDENED OS

The installation of Triton SP hardens the operating system (Windows 10/Server 2016) with the use of CIS (Center for Internet Security) guidelines. The hardening can be modified to conform to certain hardening requirements.

PROTECTION AGAINST INTERCEPTION OF COMMUNICATION

The combination of tempest certified hardware and the use of IP-sec communication internally protects the system from interception of communication.

AUTHENTICATION OF NODE/USER

Triton SP support authentication both at a user level (using smartcard or password) and at a node level. This means that apart from authenticating the user there is also authentication between clients and the server. This is done in order to achieve a security domain that spans the entire IT-system.

TIME

The system also includes a common time to ensure traceability regarding events.

Service modules

INTRUSION PROTECTION AND DETECTION

Host-based software firewall and network-based hardware firewall protects the system. The intrusion detection is done by a log analysis tool and integrity check of file contents.

ANTIVIRUS

Traditional antivirus software is included in the system and beside this system a separate stand-alone system is used when importing or exporting data

INTEGRITY CHECK

Triton SP checks file integrity on the client/server on start-up to detect conscious/unconscious changes in the file system that might affect the security in the system

PROTECTION AGAINST MALICIOUS CODE

Application whitelisting combined with the separate import/export component (antivirus scanner) and hardening of the system gives a robust protection against malicious code.

UPDATING

The system is designed for easy and centralized updates of both security patches and applications feature updates.

SECURE IMPEX

A separate offline antivirus scanner for detecting malicious code in files that are imported to the system. The USB flash drive is scanned for traces of insecurity using several antivirus scanners, and only files that pass the scan is transferred to a destination USB flash drive. The solution also includes a mechanism to ensure only USB flash drive that passed the malicious code check is possible to import to the system.

SECURITY LOGGING

Triton SP includes a physical separated computer that collects all logs from the system. The log server is managed by a separate operator to ensure that the logs is not tampered with after it has reached the log server.

LOG ANALYSIS

The log server contains an ELK (ElasticSearch, LogStash, Kibana) stack for further real time log analysis and intrusion detecting. For further assurance, it is possible to send logs in a one way fashion using a data diode.

PROTECTION AGAINST MALICIOUS CODE

Application whitelisting combined with the separate import/export component (antivirus scanner) and hardening of the system gives a robust protection against malicious code.

SYSTEM SUPERVISION WITH SECURITY ALARMS

Triton SP continuously supervise the system for erroneous behavior, e.g. connection loss, antivirus out of order, disk space shortage and informs the user of current state by issuing security alarms.

SECURE PRINTING

Triton SP contains a solution for printing to a shared printer with personal access to the personal printer queue.

SECURE FILE SHARING

Triton SP contains an integrated solution for file sharing between clients. The files are stored on the server. Traceability to which user that accesses or changes a file is supported.

References

Triton Secure Platform is the base of the security solution in Triton MMHS 2.0 in the Swedish Armed Forces. ■