MEDIALINE

IT Security

Security Workshop in a Box

Do the security check: modular - goal-oriented - budget-friendly

Safe is not safe enough

»Security Workshop in a Box« is a service product offered by Medialine AG. The aim of the workshop is to show you areas in which there is still a need for action in your IT security. „Security Workshop in a Box" contains various conversation guidelines and templates, with which our technical staff, together with you, will examine your IT security and determine the need for action. We will show you precisely what IT security risks exist in your company and offer solutions that will make your IT more secure.
The workshop is modular in design. This means that you decide which aspects of your IT security should be considered. In this way, you have direct influence on how much you want to invest in the IT security of your company. Each module has a time key. The total effort per module is calculated by adding the times. Each module includes the following content: tasks, questions for the customer, times, and results.

Objective

The questions are intended to assess to what extent you have already thought about IT security and whether certain requirements have already been fulfilled. For questions that require documentation, it may be useful to review some of these documents together. This can serve two purposes: firstly, to verify whether the documentation is up-to-date or whether there is a need for redesign, and secondly, to create such documentation early on if it does not yet exist (after consulting with you).

Outcome

As a result of the Security Workshop, a recommendation for action to improve your IT security will be created. These recommendations can include both organizational and technical measures. If the investigation reveals an unacceptable residual risk, it may be necessary to refrain from connecting the network in question to the internet or other insecure networks.

We will always inform you about any residual risks even after the protective measures you requested have been implemented. This will allow you to continue to react and gradually improve your IT security in the future if necessary.

The workshop modules at a glance

We advise - you decide: Where do you see a need for action, which area is critical to your business, and what is the available budget?

Choose from the following five modules to create a Security Workshop in a Box tailored to the needs of your company.

Modul Network Security

Content excerpt:

- Inventory of all systems
  (Firewall, modem, server, bridge, router, switches) network topology, documentation of firewall software, check maintenance contracts, documentation, reaction scenarios & network integration, firewall as gateway
- Firewall & Router
  Current patch status, software version, hardware maintenance, access via personal admin access, logging of configuration changes
- Switche
  Current firmware, hardware maintenance, spanning tree configuration, access possibilities

Modul Email Security

Content excerpt:

- Inventory of all systems
  (Server, Mail, Gateway, Antispam, Antivirus) Documentation of Email server configuration, permissions, authentication, checking maintenance contracts, documentation of reaction scenarios & network integration Mail Relay, Gateway, Fax / Modem / Mailserver
- Email Server
  Current patch status, supported software & OS, hardware maintenance, configuration of receiving connectors, encryption used & set up, hardware monitoring
- Mail Gateway
  Current patch status & firmware, hardware maintenance, hardware monitoring
- Antispam & Antivirus
  Current patch status Gateway, software version, hardware maintenance, email checking, exclusion of harmful emails on receipt, hardware monitoring
- Active Directory
  Personalization of Email administrators

Modul Backup/Data Loss Prevention

Content excerpt:

- Inventory of all systems
  (Server, Backup, Proxy, Backup-Target, tape drive) Documentation of backup systems settings, restoration processes, authentication, check maintenance contracts, documentation of reaction scenarios & backup targets
- Backup server & optionally proxy
  Current patch status, supported software & OS, hardware maintenance, backup job errors, integration of backup target, encryption set up, hardware monitoring
- Backup target
  Current patch & firmware status, software version, hardware maintenance, hardware monitoring
- Tape drives
  Current patch status of drive, software version, hardware maintenance, hardware

Modul Data Protection

Content excerpt:

- Inventory of all systems
  (Antivirus server), documentation of antivirus systems, functional settings, control processes, authentication, check maintenance contracts, documentation of response scenarios
- Antivirus server
  Current patch level, supported software & OS, system security through firewall, current client policies, all clients monitored, updating & updating virus signatures, notification in case of virus detection

Module Archiving

Content excerpt:

- Inventory of all systems
  (archiving system) Documentation of archiving processes, control processes, authentication, maintenance contract checks, documentation of response scenarios
- Archiving system
  Current patch level, archiving system configuration, updating and updating virus signatures, notification of virus detection

as of: 03/2021