MEDIALINE

IT Security

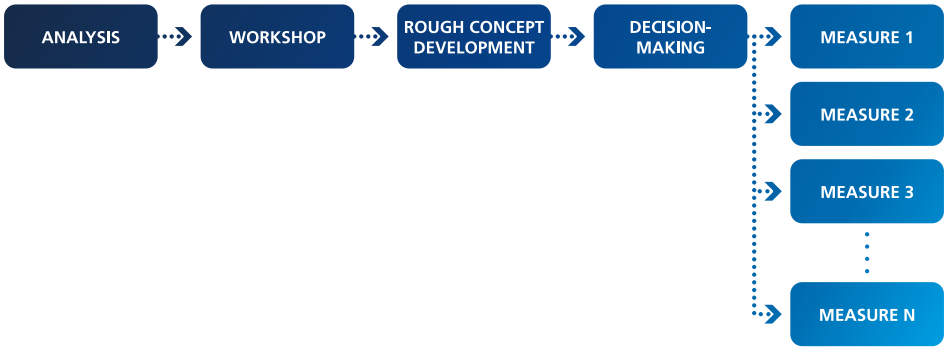
Security Awareness Process

Cyber attacks have existential consequences for companies

Employees are considered to be the weakest link in a company's IT security concept. That is why they are the first victims of attacks and thus the door openers into corporate IT.

The Medialine Cyber Security Awareness Process was designed and developed to address this challenge. It serves as an effective method to increase employees' security awareness. It also helps to implement a sustainable security awareness strategy in companies and internalize and increase awareness of various security risks among all those involved As security awareness of employees is heightened so too is the extent of their own security responsibility. Through the Cyber Security Awareness Process, employees are no longer a risk, but become a critical part of the IT security concept.

Cyber Security Awareness Process Flow



Analysis

The Medialine Cyber Security Awareness Process was designed and developed to address this challenge. It serves as an effective method to increase employees' security awareness. It also helps to implement a sustainable security awareness strategy in companies and internalize and increase awareness of various security risks among all stakeholders. As security awareness of employees is heightened so too is the extent of their own security responsibility. Through the Cyber Security Awareness Process, employees are no longer a risk, but become a critical part of the IT security concept.

Workshops

The workshops aim to create initial awareness among the participants. Different departments in all areas of the business and at all levels are informed about current cyber risks, the costs and consequences of incidents are presented as examples, and various IT security topics are discussed.

Rough concept creation

Based on the findings from the analysis phase and the workshops, our Awareness Officers develop a security awareness concept tailored to the individual circumstances and needs. Different approaches, campaigns, and measures are presented to significantly increase security awareness in the company and effectively minimize security risks.

Decision

After the presentation by our Security Awareness Officer, a joint vote is taken as to which measures should be implemented. For this purpose, a schedule is drawn up in which the implementation of the selected campaigns and measures is coordinated.

Measures

The agreed measures are prepared, implemented and evaluated together with our security experts. The measures can be, for example, sporadic phishing email campaigns or recurring e-learning courses.

Monthly recurring services

Managed Hornetsecurity SAT-Portal

With the Security Awareness Suite, customers receive a comprehensive security awareness training. Various automation techniques, such as the Awareness Engine and the Spear Phishing Engine, are used for training control In this way, employees are trained according to their needs in order to reliably recognize and effectively ward off cyber attacks - without administrators or CISOs having to familiarize themselves with the underlying psychology and didactics. The foundation of the awareness training is a patented procedure for measuring the security behavior of all groups and users participating in the security awareness training. The scientific indicator Employee Security Index (ESI®) and the training KPI are calculated based on the measured security behavior. Spear phishing emails are sent at different levels of difficulty. The managed SAT portal requires the use of the Hornetsecurity mail security service.

Network Box One-Time Managed Phishing Campaign Levels 1+2

In this program, phishing attacks are simulated within a previously defined framework. The details of user behavior are used exclusively for the evaluation of the campaign.

Network Box Awareness eLearning Module

In this module, your employees are trained in the basics of IT security. Topics include: Clear Desk, password management, secure browsing, phishing, and two-factor authentication.

Network Box Managed Phishing Campaign Levels 1+2+eLearning

This module combines the two monthly services offered by Network Box. Customers receive 2 phishing campaigns and the respective reports. Additionally, participants are trained through eLearning, must take exams, and receive certificates of completion. Customers can also access the „NB Detector" browser plug-in for free, which warns against fake websites.

One-time services

Management Impulse Keynote

This event is focused on educating attendees about risks, incidents, and consequences, and also teaches classic security techniques, sets challenges and to-dos for management. In addition to a vulnerability scan, there are action recommendations for customers.

Workshop Situations Analysis

This module can be tailored to different company departments. Based on a checklist, the company's information security awareness is determined. This is just an inventory. Based on the results, the customer receives a rough concept as a recommendation for action.

Workshop Outline and Recommendations

This workshop presents the results of the situational analysis. Participating departments also receive recommended measures. We teach communication options within the company and launch the first campaign with a set goal.

Employee Awareness Workshop

This workshop is based on interactive knowledge transfer. Employees are informed about security risks when using end devices. We convey forms, types and possibilities of social engineering and go into the motives of the hackers. At the same time, employees are given tips on how to defend themselves and how to avoid attacks or IT failures. With the feedback round and a collection and summary of what has been learned, the participants receive an overview so that the security awareness does not get lost after the workshop. The workshop can be held both in person and online.

Consulting Hornetsecurity SAT

This one-time service follows a „workshop rough concept and recommended course of action". With the Hornetsecurity SAT, a campaign is set up by a Medialine awareness expert. This Cyber Security Awareness Training tests the risk awareness of employees. You will then be presented with a complete report of the campaign and can select suitable measures.

Cyber Security Awareness Officers

Cyber security and cyber security awareness are in-depth topics. We provide cyber security officers to ensure that customers do not have to deal with the current challenges alone.

Scope of services

- Anchor IT security in the corporate culture
- Plan and organize campaigns
- Make IT security the topic of internal communication
- Train conscious handling of digital communication and internet use
- Plan and organize trainings, courses, and workshops
- IT security consultation for management and leadership
- Establish a fear-free culture when reporting cyberattacks
- Participation and documentation in the analysis of security incidents

as of: 01/2023