

Mehrstufiges Sicherheitskonzept Hardware-, software- und mitarbeiterseitig

Die Ausgangssituation:

Das Unternehmen, möchte in Vorbereitung auf die ISO 27001-Zertifizierung seine Bemühungen zum IT-Grundschutz verstärken.



Die Lösung:

- Die COWIC implementiert ein mehrstufiges Sicherheitskonzept.

Die Vorteile:

- Softwareseitiger Schutz.
- Hardwareseitiger Schutz.
- Mitarbeiterseitiger Schutz.
- Sicherheit durch Dokumentation.
- Sicherheit durch klare Verantwortlichkeiten.

Die Umsetzung:

Die Sicherheitskonzepte der COWIC zielen auf die Abdeckung dreier kritischer Bereiche ab: Software, Hardware und Personal.

So wurde im Rahmen dieses Konzeptes beispielsweise eine leistungsfähige Firewall installiert. Leistungsfähig im Hinblick auf die Datenanbindung bei gleichzeitiger Flexibilität der Filterung. Zudem wurde nicht nur auf der Firewall ein Virenschanner installiert sondern auch auf den Clients. Logischerweise von zwei verschiedenen Herstellern - zwei Augenpaare sehen mehr als nur eines - im Verbund mit intelligenten Spamfiltern.

Parallel erhielten Mitarbeiter Schulungen zum Thema Sicherheit. Wie erkenne ich eine gute/schlechte Mail? Welche Gefahr droht von DVD-Brennern? Welche von USB-Ports? Wie organisiere ich mich (Stichwort: keine gelben Post-it mit Passwörtern auf den Rechner kleben)?

Auch eine Vereinheitlichung der Hardware hilft seitdem dem Unternehmen mögliche Sicherheitslücken überschaubar zu halten.

Und zuletzt sorgen festgelegte Prozesse und Verantwortlichkeiten klare Verhältnisse. Von der Schlüsselregelung über Beschaffungsprozesse bis hin zu Notfallplänen - jeder weiß, wer für was verantwortlich ist.

*Stichworte:
Sicherheit,
Software,
Hardware,
Mitarbeiter,
Dokumentation*