

Ganzheitlicher Schutz bietet Sicherheit

Interview mit Kai Wittenburg (Geschäftsführer Neam IT-Services GmbH und lizenziertes ISO 27001-Grundschutz-Auditor) >>> Bei der Datensicherheit im Unternehmen kommt es auf viele Faktoren an. Dabei spielen nicht nur technische, sondern auch infrastrukturelle, organisatorische und vor allem personelle Aspekte eine große Rolle. Im Interview mit Wirtschaft Regional erläutert Neam-Geschäftsführer Kai Wittenburg, selbst vom Bundesamt für Sicherheit in der Informationstechnologie (BSI) lizenziertes ISO 27001-Grundschutz-Auditor, was bezüglich der IT-Sicherheit im Unternehmen zu beachten ist.

Welchen Stellenwert hat ihrer Erfahrung nach die Datensicherheit in kleinen und mittleren Betrieben?

Kleine und mittelständische Unternehmen neigen häufig dazu, die IT-Sicherheit nur aus funktioneller Sicht zu betrachten. Dabei geben sich die Betriebe häufig schon mit Maßnahmen wie Virenschutz, Datensicherung und Firewall zufrieden und wännen sich dadurch in Sicherheit. Diese Punkte bilden jedoch nur die Basis im Hinblick auf die Datensicherheit und reichen allein nicht aus, vor eventuellen Gefährdungen und Zugriffen zu bewahren.

Was gehört zu den Grundvoraussetzungen der IT-Sicherheit?

Zu den Grundvoraussetzungen der IT-Sicherheit gehört ein ganzheitlicher Schutz. Und um diesen zu gewährleisten, müssen die Bereiche Personal, Infrastruktur, Organisation und Technik unter die Lupe genommen und hinsichtlich des Datenschutzes besonders sensibilisiert

werden. Nur wenn auf diesen Gebieten entsprechende Vorkehrungen getroffen sind und die Standards auch eingehalten werden, ist das Unternehmen auf der sicheren Seite.

Welche Gefährdungsquellen sind in den Unternehmen vorrangig vorhanden?

Häufig beobachten wir eine organisatorische Schwäche in den Unternehmen. Die Systeme werden nur unzureichend gepflegt und gewartet. Gefährdungsquellen lauern aber noch an anderen Stellen. Zum Beispiel im personellen Bereich. Bei den Betrieben, die uns als Sicherheitsexperten beauftragen, führen wir gerne so genannte Penetrationstests durch.

Das heißt, wir versuchen, an geheime Informationen wie zum Beispiel Passwörter zu gelangen. Oft genügt dafür bereits ein Anruf in der Firma. Daher ist es nicht nur wichtig, die Systeme regelmäßig zu warten, sondern vor allem

- Storage
- Security
- Systems
- Education
- System Management



Weiß worauf es beim IT-Grundschutz ankommt: Kai Wittenburg.

auch bei den Mitarbeitern den Blick auf die Datensicherheit zu schärfen.

Welche Vorsorgemaßnahmen sind unabdingbar?

Das Grundschutzhandbuch des BSI sieht die Implementierung eines IT-Sicherheitsprozesses vor, der über punktuelle Lösungen wie Datensicherung, Virenschutz und Firewall hinausgeht. Im Mittelpunkt stehen dabei die Informationen, die wegen der Sicherheitsziele Verfügbarkeit, Vertraulichkeit und Integrität geschützt werden müssen. Einzubeziehen in das Gesamtkonzept sind, wie zuvor schon erwähnt, die Bereiche Personal, Infrastruktur, Organisation und Technik. ■