Bundesamt
für Sicherheit in der
Informationstechnik

ANALYSEN

Durch IS-Revisionen häufig festgestellte Sicherheitsmängel

Im Rahmen der Durchführung von IS-Revisionen hat das BSI eine Reihe von Sicherheitsmängeln identifiziert, die gleichermaßen bei vielen geprüften Institutionen festgestellt wurden. Die Reihenfolge stellt keine Priorisierung dar:

- Die Verantwortungsübernahme für das Thema „Informationssicherheit“ durch die Leitung der Institution ist oftmals nicht ausreichend erkennbar bzw. dokumentiert.
- Sicherheitskonzepte sind unvollständig, inkonsistent und nicht an der Vorgehensweise des BSI Standards 100-2 orientiert.
- Die Dokumentationslage weicht oft erheblich von den tatsächlich umgesetzten Maßnahmen ab.
- IT-Sicherheitsbeauftragte werden nicht rechtzeitig in Beschaffungen und Projekte eingebunden.
- Schulungen und Sensibilisierungsmaßnahmen zu Fragen der Informationssicherheit finden insbesondere für die Zielgruppe der „normalen“ Mitarbeiter nicht oder nur in geringfügigem Umfang statt.
- Der physische Zutritt zu Gebäuden – insbesondere über Anlieferungsbereiche, Tiefgaragen und Nebeneingänge (Raucherecken etc.) – wird lückenhaft überwacht und Besucher sowie Reinigungskräfte werden unzureichend kontrolliert.
- Die Release-Stände von Betriebssystemen und Applikationen sind veraltet und verfügbare Sicherheitsmechanismen werden nicht umfassend genutzt.
- Eine Netzwerkzugangskontrolle (auch für Wartungszugänge und -verbindungen), die ausschließlich autorisierten Endgeräten den Zugang zum Hausnetz ermöglicht, ist nicht implementiert.
- Maßnahmen zu Netzwerkmanagement und -überwachung sind nicht oder lediglich als Insellösungen existent. Logdaten werden lediglich lokal auf den Komponenten selbst vorgehalten und nur anlassbezogen manuell ausgewertet.
- Mobile Datenträger und mobile Endgeräte werden nicht kontrolliert (Schnittstellenkontrolle) und kryptiert.
- Änderungen an Anwendungen und Betriebssystemen werden ohne angemessenes Änderungs- und Versionsmanagement in den Produktivbetrieb eingestellt und großteils nicht dokumentiert.

Nähere Informationen zum Thema „IS-Revision“ finden Sie auf der Webseite des BSI im Informationsbereich der Sicherheitsberatung unter „IS-Revision“:

Link: https://www.bsi.bund.de/ContentBSI/Themen/IS-Revision/isrevision.html
Kontakt: isrevision@bsi.bund.de