Datenschutz PRAXIS

DSGVO: So setzen Sie die erweiterte Zugangskontrolle um

9. Juni 2017

Im neuen Datenschutzrecht – Datenschutz-Grundverordnung und BDSG-neu – bekommt die Zugangskontrolle eine erweiterte Bedeutung. Passen Sie daher die Überprüfungen im Unternehmen an.

Es war ein Klassiker, wenn es um Datenschutzkontrollen und technisch-organisatorische Maßnahmen [1] (TOM) im Datenschutz ging: Zugangskontrolle und Zutrittskontrolle wurden gern vermischt.

Das war einerseits nachvollziehbar. Denn man kann in ein Gebäude auch Zugang und nicht nur Zutritt erhalten. Andererseits konnte es ein Problem sein, wenn man sich über Mängel in der Zugangskontrolle unterhielt und einer der Gesprächspartner eigentlich an die Zutrittskontrolle dachte.

Zugangskontrolle umfasst nun Zutrittskontrolle

Mit dem Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU [2]) und damit mit dem neuen Bundesdatenschutzgesetz (BDSG-neu [3]) gehört das der Vergangenheit an.

Nicht nur die Datenschutz-Grundverordnung (DSGVO) nennt die Zutrittskontrolle nicht. Auch das neue Bundesdatenschutzgesetz kennt keine Zutrittskontrolle mehr, zumindest als Begriff. Aber sie findet sich in § 64 BDSG-neu, der Unternehmen wichtige Orientierung bietet.

Die Zugangskontrolle umfasst dort die Kontrolle der Zutritte, passend zur Definition „Verwehrung des Zugangs zu Verarbeitungs-Anlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte". Im Zuge der Vorbereitung auf die DSGVO ist es daher sinnvoll, die internen Prüfkataloge zur Zugangskontrolle zu erweitern.

Maßnahmen der Zutrittskontrolle aufnehmen

Damit die Maßnahmen der Zutrittskontrolle nicht in Vergessenheit geraten, führen Sie die bisher getrennten Prüf- und Maßnahmen-Kataloge in eine Liste für die erweiterte Zugangskontrolle zusammen.

Beispiele für Maßnahmen

Zu der erweiterten Kontrolle gehören somit Maßnahmen wie

Absicherung der Gebäude, Fenster und Türen,
Sicherheitsglas,
Bruch- und Öffnungsmelder,
Videoüberwachungs-Anlagen,
Alarmanlagen,
Zutrittskontroll-Systeme mit Chipkarten-Leser und

Besucher-Dokumentation [4].
Aber auch Vorkehrungen wie

Passwortrichtlinien,
Zwei-Faktor-Benutzeranmeldung,
Firewalls,
digitale Zertifikate,
Verschlüsselung [5],
Schutz vor Schadsoftware,
Bildschirmsperre und
aktuelle Nutzerverwaltung.

Ziel: Unbefugten Zugang zur IT verhindern

Bei der Suche nach geeigneten Maßnahmen muss immer die Sicherheit des Zugangs zur IT und zu den Daten im Fokus stehen. Dazu überlegen Sie sich am besten, welchen Weg ein externer Angreifer geht, um bis an die IT und bis an die Daten zu gelangen.

Ist der Angreifer bereits im Gebäude und steht vor dem IT-System oder erfolgt der Angriff über das Internet, greifen die bisherigen Maßnahmen der Zugangskontrolle. Befindet sich der Angreifer vor Ort, aber noch vor dem Firmengelände oder Gebäude, kommen die bisherigen Maßnahmen der Zutrittskontrolle hinzu.

Oliver Schonschek

Oliver Schonschek ist Diplom-Physiker, Analyst und IT-Fachjournalist im Bereich IT-Sicherheit und Datenschutz.
