

Inhalt

Vorwort: Safety first!	9
Einleitung	13
Digitalisierungsgrad im deutschen Mittelstand	17
Digitalisierungsstufe 1: digitale Basisinfrastruktur	18
Digitalisierungsstufe 2: vernetzte Information und Kommunikation	19
Digitalisierungsstufe 3: vernetzte Produkte und Dienstleistungen	20
Geringe Investition in Digitalisierungsprojekte	21
IT-Sicherheit als größte Digitalisierungshürde	22
Zwischenfazit: Mittelstand liegt digital hinter Konzernen	23
IT-Sicherheitsgrad im deutschen Mittelstand	25
Große Unsicherheit in Sachen IT-Sicherheit	26
Keine durchgängige Sicherheitsarchitektur	27
Ungeschützter E-Mail-Verkehr als Hauptsicherheitsrisiko	28
Drei Viertel der Mitarbeiter haben kein IT- Sicherheitsbewusstsein	28
Nur jedes vierte Unternehmen hat einen Notfallplan ..	29
Zwischenfazit: Ganzheitlicher Ansatz erforderlich	30
Datenverluste und Datenvorfälle als Bedrohung für den Mittelstand	31
Kosten von Datenpannen	32
Dauer zur Erkennung und Beseitigung	33

Zukunftsprognose für Datenvorfälle.	34
Zwischenfazit: Steigerung der IT-Sicherheit erforderlich	34
Leichtes Spiel für Hacker.	35
Gründe für Datenverluste und Sicherheitsprobleme ..	36
Verschiedene Formen der Attacken	39
Drei exemplarische Beispiele	41
Experteninterview mit Prof. Dr. Martin Uzik	47
Mitarbeiter als IT-Sicherheitsrisiko	51
Social Hacking/Social Attacks	52
Passwort-Diebstahl	55
Gefahr durch unsichere E-Mails	56
Spam-Mails	57
Virenschutz ist essentiell	58
Verschlüsselung von Nachrichten.	59
Risiken mobiler Geräte und Datenträger	60
Bedienfehler	61
Schreibtischtäter.	63
Zwischenfazit: Mitarbeiter sensibilisieren	65
Die unterschätzten Gefahren	67
Drucker und Kopierer	67
Die neuen Gefahren	71
Big Data braucht neue Schutzmechanismen	71
Cloud-Server als Hacker-Eldorado.	72
Blockchain mit ungeklärtem Datenschutz	74
Künstliche Intelligenz birgt Chancen und Risiken	75
Quantencomputer als Sicherheitsrisiko	76

Rechtliche Anforderungen	79
DSGVO als Treiber der IT-Sicherheit	79
Informationssicherheit und Zertifizierung nach ISO 27001	84
Experteninterview mit Ulrich Seibold	87
IT-Sicherheitsarchitektur für den Mittelstand	95
Organisatorische Maßnahmen	96
Soll-Ist-Vergleich.	96
Sicherheitskonzept	97
Benutzerkonzept.	98
Notfallkonzept.	99
Mitarbeiter-Schulungen	100
Technische Maßnahmen	101
Netzwerksicherheit.	102
Datensicherung.	103
Verschlüsselung	105
Virenschutz	106
Updates	108
Experteninterview mit Hans-Wilhelm Dünn	111
Der Bindig IT-Security Score: eine maßgeschneiderte IT-Sicherheitsarchitektur aufbauen	115
Ergebnisse und Auswertung des Bindig IT-Security Scores	119
Zwischenfazit: Just do it!	121
Professionelle Datenwiederherstellung	123
Was sollte man tun, wenn der Ernstfall eingetreten ist? ..	123

Wie funktioniert die Datenrettung am Beispiel von Festplatten?	124
Wie werden Daten wiederhergestellt?	125
Geht es bei der Datenrettung nur um Festplatten oder auch um andere Speicherarten?	126
Wie erfolgt die Wiederherstellung von Daten bei Serverdaten, die über mehrere Datenträger verteilt sind?	127
Anforderungen bei der Datenlöschung	129
Löschen durch Überschreiben.	130
Entmagnetisieren	131
Starkes Erhitzen	131
Das Schreddern von Datenträgern	132
Zwischenfazit: Angst vor Datenverlust sollte kein Hemmnis sein	132
Experteninterview mit Arnold Krille	135
Neue Ideen für mehr IT-Sicherheit in KMUs	141
IT-Lotse navigiert KMUs auf Sicherheitskurs	141
Sicherheits-Know-how von der Berufsschule in die Betriebe tragen	142
Hacken für mehr IT-Sicherheit	143
Fazit: IT strategisch managen – Datensicherheit ist Chefsache	145
Glossar	155
Anmerkungen	159