



Cyber-Sicherheit im 21. Jahrhundert

Sicherheitskonzepte und praktische Umsetzung für KMU

Andreas Wisler





Andreas Wisler

Cyber-Sicherheit im 21. Jahrhundert

**Sicherheitskonzepte und
praktische Umsetzung für KMU**

BPX-Edition
Rheinfelden/Schweiz



BPX Best Practice Xperts
E-Mail edition@bpx.ch
Internet www.bpx.ch

Andreas Wisler

**Cyber-Security im 21. Jahrhundert
Sicherheitskonzepte und praktische
Umsetzung für KMU**

Rheinfelden/Schweiz
BPX-Edition 2018
ISBN 978-3-905413-58-8

© 2018 BPX-Edition Rheinfelden

Hinweis: In diesem Booklet wird bei Bezeichnungen die männliche Form verwendet. Dies dient lediglich der Lesefreundlichkeit und schliesst die weibliche Form mit ein.

Alle Rechte, insbesondere die Übersetzung in fremde Sprachen, sind dem BPX-Verlag vorbehalten. Kein Teil des Buches darf ohne schriftliche Genehmigung des Verlages fotokopiert oder in irgendeiner anderen Form reproduziert oder in eine von Maschinen verwendbare Form übertragen oder übersetzt werden.

Herstellung: BPX-Edition, Rheinfelden/Schweiz

Druck und Verarbeitung: Galledia AG, Flawil

Inhalt

1	Management Summary	4
2	Managementverantwortung	6
2.1	Managed Security Services	7
2.2	Begrifflichkeiten	8
2.3	Rechtliche Aspekte	9
2.4	Organisatorische IS-Massnahmen	11
3	Grundschutz für KMU	12
3.1	Grundschutz nach BSI	13
3.2	ISO 27000	14
4	Praxis der Informationssicherheit	15
4.1	Bedrohungsszenarien	15
4.2	Risk Assessment / Risk Management	18
4.3	Risiko-Minimierung	21
4.4	Business Continuity Management	22
4.5	Die Bedeutung der Mitarbeiterschulung	23
5	Gefahren	25
5.1	Spam	25
5.2	Malware	27
5.3	Botnetze	28
5.4	Mobiler Zugriff	28
5.5	Phishing	29
5.6	Social Media	29
5.7	Social Engineering	29
5.8	Spuren im Netz	29
6	Sicherheitsmassnahmen	31
6.1	E-Mail	31
6.2	Verschlüsselung	32
6.3	Netzwerksicherheit	36
6.4	Firewall	37
6.5	Personal Firewall	39
6.6	Patchen	41
6.7	Back-up/Restore	41
6.8	Cloud	43
6.9	Intrusion Detection	39
6.10	Biometrie	44
7	goSecurity GmbH	46
8	Autor & BPX	48

1 Management Summary

Praktisch jeden Tag kann von Cyber-Angriffen gelesen werden: «Tausende Zugangsdaten gestohlen und im Internet verfügbar.» Auch die gefundenen Schwachstellen in diversen Programmen haben einen neuen Höchstwert erreicht.

Der Hauptzweck für ein Unternehmen ist, dass die Informationen zur richtigen Zeit, in der richtigen Qualität, am richtigen Ort und der richtigen Person zur Verfügung stehen.

Daher ist es wichtig, dass die Informationssicherheit heute zuoberst auf der Prioritätenliste weitsichtiger KMU-Führungskräfte steht. In allen Betrieben spielt Information eine entscheidende Rolle, und diese gilt es zu schützen.

Die Angriffsszenarien auf der anderen Seite werden immer ausgefeilter. Viele davon zielen auf den Faktor Mensch ab. Nur gut ausgebildetes und sensibilisiertes Personal kann die wichtigen Informationen sicher handhaben. Von nicht ausgebildetem Personal richtige Entscheidungen zu erwarten, ist sinnlos. Vier wichtige Punkte sollen besonders hervorgehoben werden:

- Informationssicherheit (IS) ist eine Managementaufgabe.
- Ein Vorsorgeplan (BCM) hilft im Worst Case zu überleben.
- Für IS und deren Unterhalt muss Budget bereitgestellt werden.
- Zuverlässiges Personal gibt es nur mit Ausbildung.

Kleinere KMU haben meist die personellen Ressourcen nicht, um einen eigenen Chief Information Security Officer (CISO) einzustellen. In diesen Fällen ist es sinnvoll, die Aufgaben an ein spezialisiertes Unternehmen auszulagern. Doch auch beim Outsourcing von IS bleibt die Verantwortung bei der Unternehmensführung.

Gelebte IS bringt auch eine Reihe von Vorteilen, z.B.: