

# Inhaltsverzeichnis

*Matthias H. Hartmann (HTW Berlin)*

Vorwort des Herausgebers ..... V

*Henrik Klohs (Handwerkskammer Frankfurt (Oder) – Region Ostbrandenburg)*

Grußwort ..... VII

Ansprechpartner IT-Sicherheit für die Region Berlin/Brandenburg ..... IX

## Teil 1: IT-Sicherheitstage in Brandenburg und Berlin

*Henrik Klohs (Handwerkskammer Frankfurt (Oder) – Region Ostbrandenburg)*

1. Rückblick IT-Sicherheitstage ..... 1

1.1 Zunehmende Nachfrage nach IT-Sicherheit ..... 1

1.2 Inhalte der bisher fünf durchgeführten IT-Sicherheitstage ..... 2

1.3 Hohe Bedeutung von IT-Sicherheit ..... 6

*Matthias H. Hartmann, Madlen Böer, Ralf Waubke, Leonhard Gebhardt  
(HTW Berlin)*

2. Der 6. IT-Sicherheitstag Mittelstand 2017 an der HTW Berlin ..... 7

2.1 Gestaltung der Konferenz ..... 7

2.2 Impressionen und Eindrücke ..... 10

2.3 Meinungsbild zur IT-Sicherheit ..... 12

2.3.1 Methodischer Ansatz ..... 12

2.3.2 Zahlen und Fakten zu den Teilnehmern des IT-Sicherheitstages ..... 12

2.3.3 Ergebnisse zur IT-Sicherheit ..... 16

## Teil 2: Gefährdungspotentiale und Hinweise

*Olaf Borries*

*(ZAC des LKA Berlin mit Unterstützung der ZAC Brandenburg und ZAC Sachsen)*

3. Aktuelle Cybercrime-Phänomene aus polizeilicher Sicht ..... 21

3.1 Einleitung ..... 21

3.2 Ransomware ..... 22

3.3 Backup-Strategien und Notfall-Management ..... 25

3.3.1 Backup-Strategien ..... 25

3.3.2 Notfall-Management.....	26
3.4 CEO-Fraud.....	27
3.5 Das Bundesamt für Sicherheit in der Informationstechnik – BSI.....	28
3.6 Fazit.....	29
<i>Knuth Thiel, Jens Jankowsky (IHK Ostbrandenburg)</i>	
4. Die Digitalisierung des Verbrechens.....	31
4.1 Einleitung – Cyberkriminalität im Blick.....	31
4.2 Belastung der Unternehmen mit Kriminalität.....	32
4.3 Anzeigeverhalten der Unternehmer.....	33
4.4 Schäden durch Kriminalität.....	34
4.5 Fazit.....	35
<i>Michael Hendrix (TH Wildau)</i>	
5. Sicherheitsrisiken von Internetanwendungen.....	37
5.1 Motivation.....	37
5.2 Überblick.....	37
5.3 Schutz einer Webanwendung vor geläufigen Angriffen.....	38
5.3.1 Authentifizierung.....	39
5.3.2 Session-Hijacking.....	40
5.3.3 Cross-Site-Request-Forgery (CSRF).....	41
5.3.4 Cross-Site-Scripting (XSS).....	42
5.3.5 SQL-Injection.....	43
5.3.6 Rainbow-Table-Angriff.....	44
5.3.7 Pufferüberlauf.....	45
5.3.8 Brute-Force-Angriff.....	46
5.3.9 Man-in-the-Middle-Attacke.....	46
<i>Heiko Behrendt (ISO 27001 Auditor)</i>	
6. Datenlecks in Handwerksbetrieben.....	49
6.1 Einleitung.....	49
6.2 Datenschutz.....	52
6.3 Hinweise zur neuen EU-Datenschutz-Grundverordnung (EU-DSGVO).....	53
6.4 Informationssicherheit.....	53
6.5 Was ist zu tun?.....	55
6.6 Fazit.....	56

*Manuela Püschel (Die Netz-Werker AG)*

7. Viren und Trojaner: Übersicht und Abwehr .....	58
7.1 IT-Sicherheit bei der Netz-Werker AG.....	58
7.2 Die Begrifflichkeit Virus.....	59
7.3 Malwareinfektion und -Impfung .....	60
7.4 Fazit.....	64

### Teil 3: Regelungen, Checklisten und Empfehlungen

*Matthias Hartmann, Ralf Waubke (HTW Berlin)*

8. Pragmatische IT-Sicherheit für Kleine und Mittlere Unternehmen (KMU) .....	66
8.1 Besonderheiten Kleiner und Mittlerer Unternehmen (KMU) .....	66
8.2 Vorgaben für die IT-Sicherheit.....	67
8.2.1 Normenreihe ISO 27000ff. ....	67
8.2.2 BSI-Grundschatz .....	67
8.2.3 VdS Quick-Check .....	68
8.2.4 NIST Rahmenkonzept für Cyber Security .....	69
8.2.5 Prüfkriterien nach SANS .....	69
8.3 Sicherheitsbedarf im Internet der Dinge .....	71
8.3.1 Angriffe auf die büronahe IT.....	72
8.3.2 Angriffe auf die produktionsnahe IT .....	73
8.3.3 Angriffe auf unser tägliches Leben .....	74
8.4 Pragmatische IT-Sicherheit für KMU und Handwerksbetriebe .....	74

*Gerd M. Fuchs (Rechtsanwaltskanzlei FOXLAW)*

9. Sichere Verwaltung digitaler Daten .....	78
9.1 Einleitung .....	78
9.2 Die rechtskonforme Erhebung und Verarbeitung von personenbezogenen Daten ...	78
9.2.1 Gesetzliche Ermächtigungsgrundlagen.....	79
9.2.2 Einwilligung des Betroffenen .....	79
9.3 Sichere Verarbeitung personenbezogener Daten .....	81
9.3.1 Technische und organisatorische Maßnahmen.....	81
9.3.2 Einzelne Maßnahmen.....	82
9.3.3 Bestellung eines Datenschutzbeauftragten .....	83
9.3.4 Sanktionen .....	83
9.4 Fazit.....	84

*Sascha Wilms (Deutschland sicher im Netz e.V.)*

10. IT-Sicherheit durch Mitarbeiterschulung .....	86
10.1 Der Faktor Mensch und IT-Sicherheit .....	86
10.2 Passgenaue Schulungsangebote für den Mittelstand .....	87
10.3 Hoher Bedarf in Betrieben für IT-Sicherheitswissen .....	87
10.4 Auszubildende bewähren sich als Multiplikatoren .....	88
10.5 IT-Sicherheit im Mittelstand verankern .....	88
10.6 Verstärkte Aufklärung gegen Social Engineering und Phishing .....	89
10.7 Fazit: Chancen für Ausbildungsbetriebe .....	89

*Vanessa Grühser (IHK Berlin), Carsten Vossel (CCVOSSEL GmbH)*

11. Digitalisierung und Sicherheit müssen Hand in Hand gehen .....	92
11.1 Einleitung .....	92
11.2 Digitalisierung der Wirtschaft und Kriminalität .....	93
11.3 Investition in IT-Sicherheit für Wettbewerbsfähigkeit .....	94
11.4 Sensibilisierung und Weiterbildung von Mitarbeitern .....	95
11.5 Horrorszenario „Angriff auf die Unternehmens-IT“ .....	96
11.5.1 Schulungen zur IT-Sicherheit und die interne Akzeptanz .....	98
11.5.2 Möglichkeiten der Mitarbeiter-Schulung .....	98
11.6 Fazit .....	99

*Hartmut Schmitt (HK Business Solutions GmbH), Luigi Lo Iacono (TH Köln)*

12. Usable Security – Mit Benutzerfreundlichkeit zu mehr IT-Sicherheit .....	101
12.1 Digitale Transformation erfordert adäquaten Schutz .....	101
12.2 Nutzerzentriertes Security Engineering .....	102
12.3 Lösungen für mittelständische Unternehmen .....	104

*Michael Holzhüter*

*(HTW Berlin / Fraunhofer-Institut für Offene Kommunikationssysteme)*

13. Bedrohungen und Maßnahmen zur IT Sicherheit für Kleine und Mittlere Unternehmen: Eine Checkliste .....	109
13.1 Einleitung .....	109
13.2 Unternehmensgröße .....	109
13.3 Bedrohungen und Maßnahmen .....	110
13.4 Wahl eines IT-Dienstleisters .....	115
13.5 Fazit .....	115

*Matthias Hartmann, Leonhard Gebhardt (HTW Berlin)*

14. Schutzbedarfsanalyse für nachhaltiges Unternehmertum .....	117
14.1 Nachhaltigkeit bedarf der IT-Sicherheit .....	117
14.2 Verfügbarkeit, Integrität und Vertraulichkeit .....	118
14.3 Schutzbedarfsanalyse .....	118
14.4 (Sofort-)Maßnahmen und Reaktionsleitfäden .....	120

#### Teil 4: Unterstützungsangebote für KMU und Handwerksbetriebe

*Matthias Hartmann, Stefan Wittenberg, Jan Wirsam, Madlen Böer  
(HTW Berlin)*

15. EFRE Projekt „Digital Value“ für Berliner Unternehmen .....	122
15.1 Die Hochschule für Technik und Wirtschaft Berlin (HTW Berlin) .....	122
15.1.1 Top Rankings für die Lehre .....	122
15.1.2 Hohe Forschungsintensität .....	123
15.2 Kooperationsforschungsprojekt „Digital Value“ .....	123
15.2.1 Digital Business Lab .....	124
15.2.2 Lean Factory Lab .....	124
15.2.3 Mobile Business Lab .....	125
15.3 Vorgehensweise im Digital Business Lab .....	126
15.4 Zwischenergebnisse des Projektes bis September 2017 .....	127
15.4.1 Business Model Canvas für 50 Unternehmen .....	127
15.4.2 Feststellung des digitalen Reifegrades für 50 Unternehmen .....	128
15.4.3 Identifikation digitaler Ansatzpunkte in den Unternehmen .....	131
15.5 Perspektive des Projektes „Digital Value“ .....	132

*Henrik Klohs (HWK Frankfurt (Oder) – Region Ostbrandenburg)*

16. Digitales Handwerk in Ostbrandenburg .....	134
16.1 Einleitung .....	134
16.2 Dienstleistungsangebot der Handwerkskammer .....	134
16.3 IT-Sicherheit im Handwerk .....	135
16.4 Digitalisierung im Handwerk .....	135

*Kerstin Wiktor (HWK Berlin)*

17. Beratung zu Innovation und Digitalisierung im Berliner Handwerk.....	137
17.1 Einleitung.....	137
17.2 Struktur des Berliner Handwerks.....	137
17.3 Beratungsleistungen der Handwerkskammer.....	138
17.3.1 Dienstleistungen und neutrale Beratung.....	138
17.3.2 Kooperationen und Netzwerke .....	139
17.4 Innovationen im Handwerk.....	140
17.4.1 Innovationen prägen das Handwerk .....	140
17.4.2 Strukturiertes Erfinden ist im Handwerk selten .....	141
17.5 Digitalisierung im Berliner Handwerk .....	142
17.6 Fazit.....	143

*Joern Kinzel (Technologiezentrum Teltow)*

18. Sicherung Kritischer Infrastrukturen .....	145
18.1 Kritische Infrastrukturen: Eine Definition.....	145
18.2 Darstellung Kritischer Infrastrukturen nach Branchen .....	145
18.3 Die Kritischen Infrastrukturen nach dem IT-Sicherheitsgesetz .....	146
18.4 Kritikalität von Infrastrukturen.....	147
18.5 Im IT-Sicherheitsgesetz berücksichtigte Organisationen.....	148
18.6 Die Arbeit des Kooperationsnetzwerkes DiSiNet .....	149
18.7 Beispiel der Entwicklungsarbeit.....	152
18.8 Nano-Firewall .....	152
18.9 ScanBox .....	152
18.10 Alarmierungspriorisierung .....	153
Autorenverzeichnis .....	155