

# Cybergefahr

Wie wir uns gegen Cyber-Crime und Online-Terror wehren können

Bearbeitet von  
Eddy Willems

1. Auflage 2015. Buch. XVIII, 188 S. Softcover

ISBN 978 3 658 04760 3

Format (B x L): 16,8 x 24 cm

[Weitere Fachgebiete > EDV, Informatik > Hardwaretechnische Grundlagen > Computerkriminalität, Schadsoftware](#)

Zu [Leseprobe](#)

schnell und portofrei erhältlich bei



Die Online-Fachbuchhandlung beck-shop.de ist spezialisiert auf Fachbücher, insbesondere Recht, Steuern und Wirtschaft. Im Sortiment finden Sie alle Medien (Bücher, Zeitschriften, CDs, eBooks, etc.) aller Verlage. Ergänzt wird das Programm durch Services wie Neuerscheinungsdienst oder Zusammenstellungen von Büchern zu Sonderpreisen. Der Shop führt mehr als 8 Millionen Produkte.

---

# Inhaltsverzeichnis

<b>1</b>	<b>Dreißig Jahre Malware – ein kurzer Abriss</b>	1
1.1	Was ist Malware?	1
1.2	Was ist ein Virus?	1
1.3	Die erste Generation	3
1.4	Generation Internet	5
1.5	Die mobile Generation	9
1.6	Zum Schluss	11
<b>2</b>	<b>Profile der Malware-Verfasser</b>	15
2.1	Die Graffiti-Sprayer und Script-Kids	15
2.2	Die Cyberkriminellen	15
2.3	Die unwissend Böswilligen	16
2.4	Die Behörden und Ministerien	16
2.5	Und was ist mit den Hacktivisten?	16
2.6	Gigabyte: Made in Belgium	17
2.7	Virenschreiber und Virenjäger	18
<b>3</b>	<b>Digitale Untergrundwirtschaft</b>	23
3.1	Wie ist die digitale Untergrundwirtschaft organisiert?	25
3.2	Was können wir alles kaufen?	31
3.3	Wie ein Massenangriff funktioniert: Botnets und ihr Aufbau	42
3.4	Und was ist mit der Beute?	42
3.5	Schlussfolgerung: E-Crime ist auf dem Vormarsch	44
<b>4</b>	<b>Von Cyberkrieg bis Hacktivismus</b>	47
4.1	Cyberkrieg	47
4.2	Cyberterrorismus	51
4.3	Hacktivismus	52
4.4	Cyberespionage	55
4.5	Überlegungen zu guter Letzt	59

<b>5 Die Antiviren-Unternehmen</b> . . . . .	65
5.1 Die Hersteller . . . . .	65
5.2 Non-Profit-Organisationen im Kampf gegen Cyberkriminalität . . . . .	68
5.2.1 CARO . . . . .	68
5.2.2 EICAR . . . . .	69
5.2.3 AMTSO . . . . .	72
5.2.4 The Wild List . . . . .	75
5.2.5 Andere Organisationen . . . . .	75
<b>6 Die Bedrohungen von heute</b> . . . . .	79
6.1 Botnets . . . . .	79
6.2 Ransomware . . . . .	83
6.3 Soziale Netzwerke . . . . .	85
6.4 Tragbare Medien . . . . .	86
6.5 Attacke... und diesmal auf die Unternehmen! . . . . .	87
6.6 Mobile Ziele . . . . .	89
6.7 Onlinebanking: Vorsicht vor dem Mann im Browser . . . . .	93
<b>7 Mythen über Malware</b> . . . . .	101
7.1 Mythos 1: Wenn ich nichts Verdächtiges am Computer bemerke, ist er auch nicht infiziert . . . . .	101
7.2 Mythos 2: Teurer Virenschutz muss gar nicht sein, auch kostenlose Programme bieten optimalen Schutz! . . . . .	102
7.3 Mythos 3: Die meiste Schadsoftware wird per E-Mail verschickt . . . . .	103
7.4 Mythos 4: Mein PC oder Netzwerk kann durch den Besuch einer Webseite nicht infiziert werden, wenn ich nichts herunterlade . . . . .	103
7.5 Mythos 5: Am häufigsten wird Malware über Downloads von Peer-to-Peer und Torrent-Sites verbreitet . . . . .	105
7.6 Mythos 6: Die Gefahr, sich mit Malware zu infizieren, ist beim Besuch einer Pornoseite größer als bei einer Seite über Pferdesport . . . . .	105
7.7 Mythos 7: Wenn ich eine infizierte Datei nicht öffne, passiert auch nichts . . . . .	106
7.8 Mythos 8: Die meiste Schadsoftware wird über USB-Sticks verbreitet . . . . .	106
7.9 Mythos 9: Sicherheitssoftware oder -hardware kann ich mir sparen, weil ich mich auskenne und nur auf sicheren Seiten unterwegs bin . . . . .	106
7.10 Mythos 10: In meinem PC gibt es keine wertvollen Daten – warum sollte ich also angegriffen werden? . . . . .	107
7.11 Mythos 11: Ich besitze kein Windows, also ist mein PC sicher . . . . .	108
7.12 Mythos 12: Schadsoftware wird von Antiviren-Herstellern geschrieben . . . . .	108

<b>8 Tipps für Verbraucher – nur so können auch Sie sicher im Netz unterwegs sein .....</b>	111
8.1 Legen Sie sich eine Antivirensoftware zu und aktualisieren Sie sie regelmäßig .....	111
8.2 Aktualisieren Sie auch Ihr Betriebssystem und andere Programme regelmäßig .....	112
8.3 Fahren Sie Ihren Computer grundsätzlich herunter! .....	112
8.4 Verwenden Sie schwierige Passwörter .....	113
8.5 Führen Sie regelmäßig Backups durch .....	114
8.6 Achten Sie darauf, wo und wie oft Sie Ihren persönlichen Fingerabdruck im Netz hinterlassen .....	115
8.7 Reagieren Sie grundsätzlich nicht auf Spam .....	115
8.8 Gesunder Menschenverstand ist gefragt .....	116
8.9 Sicher in den Urlaub .....	116
8.10 Nicht alles, was installiert werden kann, sollte auch installiert werden .....	118
8.11 Machen Sie sich über Antivirensoftware kundig .....	118
8.12 Überprüfen einer verdächtigen Datei .....	119
8.13 Her mit dem Medientraining für alle! .....	120
8.14 Ihre Privatsphäre muss Ihnen am Herzen liegen .....	120
8.15 Deinstallieren Sie ungenutzte Software .....	121
8.16 Achten Sie auf Hoaxes .....	122
8.17 Kleben Sie Ihre Webcam ab .....	122
8.18 Erstellen Sie auch von Ihrem Smartphone regelmäßige Backups .....	122
8.19 Für Fortgeschrittene und (mutige) Anfänger: Verschlüsseln Sie Ihre Festplatte .....	123
8.20 Tipp für Fortgeschrittene: Verwenden Sie ein VPN .....	123
8.21 Tipp für Fortgeschrittene: Setzen Sie auf Microsoft EMET .....	124
8.22 Tipp für Fortgeschrittene: Deaktivieren Sie Java .....	124
8.23 Aktivieren Sie die Sperrfunktionen Ihres Handys .....	125
<b>9 Tipps, wie Unternehmen im Netz (über-)leben können .....</b>	127
9.1 Das A und O ist eine solide Sicherheitspolitik im Unternehmen .....	127
9.2 BYOD oder nicht, Schutz muss allgegenwärtig und ausreichend sein .....	132
9.3 Vorsicht in der Cloud .....	133
9.4 Seien Sie auf der Hut vor Social Engineering .....	137
9.5 Patch Management: Kleben Sie ein Pflaster auf Ihre Wunden! .....	138
9.6 Die größte Gefahr lauert oftmals innerhalb der eigenen Wände .....	140
9.7 Besuchen Sie Sicherheitskonferenzen .....	141
<b>10 Und was ist mit Väterchen Staat? .....</b>	143
10.1 Spionage .....	143
10.2 Spionage mittels Malware .....	145

10.3 Wider besseres Wissen . . . . .	147
10.4 Gesetzgebung und mögliche Strafen . . . . .	148
10.5 CERTs und CCUs . . . . .	153
<b>11 Die Medien . . . . .</b>	<b>155</b>
11.1 Medien als Verbündeter . . . . .	155
11.2 Medien und ihr Einfluss . . . . .	156
11.3 Medien als Opfer . . . . .	158
11.4 Nachrichtenseiten und Malware . . . . .	159
<b>12 Die digitale Zukunft . . . . .</b>	<b>161</b>
<b>13 Beängstigend – Eine Kurzgeschichte . . . . .</b>	<b>171</b>



<http://www.springer.com/978-3-658-04760-3>

Cybergefahr

Wie wir uns gegen Cyber-Crime und Online-Terror wehren  
können

Willems, E.

2015, XVIII, 188 S. 61 Abb., Softcover

ISBN: 978-3-658-04760-3