

Inhaltsverzeichnis

Kurzfassung..... I

Abstract..... II

1 Einleitung 1

2 Hintergrundinformationen 5

3 IT-Bedrohungslage 9

3.1 Ransomware 10

3.2 Supply-Chain-Angriffe..... 15

3.3 Datentechnische Kommunikation..... 20

3.4 ICS-spezifische Werkzeuge, Schwachstellen und Angriffe 24

3.5 IT-Angriffe mit physischen Schäden..... 28

3.6 IT-Angriffe auf den Energiesektor 29

3.7 IT-Angriffe auf kerntechnische Anlagen und Anlagen mit radioaktiven
Stoffen sowie auf Systemen zur Strahlungsüberwachung..... 32

3.8 Auswirkungen der COVID-19-Pandemie auf die Informationssicherheit... 35

3.9 IT-Angriffe in Zusammenhang mit dem Krieg in der Ukraine..... 37

3.10 Kollateralschäden 40

3.11 APT for hire 42

3.12 APT-Gruppierungen..... 43

3.12.1 APT28/Fancy Bear 43

3.12.2 APT29/Cozy Bear/Nobelium 46

3.12.3 APT 38/ Lazarus Group 47

3.12.4 Chernovite 50

3.12.5 Dragonfly/Energetic Bear..... 52

3.12.6 Electrum 53

3.12.7 Erythrite/SolarMarker 54

3.12.8 Kimsuky (teilweise beinhaltet in Hidden Cobra) 55

3.12.9 Kostovite..... 58

3.12.10	REvil	59
3.12.11	Sandworm	61
3.12.12	Tonto Team	64
3.12.13	Turla	66
3.12.14	Xenotime	68
4	Zusammenfassung und Fazit.....	71
	Quellen	81
	Relevante Fachbegriffe	111
	Abbildungsverzeichnis.....	125
	Abkürzungsverzeichnis.....	127
	Anhang	129
A	Schwachstellen und IT-Angriffswerkzeuge	129
A.1	2017	129
A.1.1	Brutal Kangaroo – IT-Angriffswerkzeug der CIA	129
A.2	2018	132
A.2.1	Meltdown – Schwachstellen in CPUs.....	132
A.2.2	Spectre – Schwachstellen in CPUs.....	135
A.3	2019	136
A.3.1	SPPA-T3000 – Schwachstellen in ICS.....	136
A.3.2	S7 und PCS7 – Schwachstellen in ICS.....	138
A.4	2020	139
A.4.1	Profinet – Schwachstellen in einem Kommunikationsstandard.....	139
A.4.2	ABB 800xA – Schwachstellen in ICS	141
A.4.3	ZeroLogon – Schwachstelle im Windows Netlogon Remote Protocol.....	142
A.4.4	Amnesia:33 – Schwachstellen in Netzwerkstacks.....	144
A.4.5	Ramsay – IT-Angriffswerkzeug für Cyberspionage	146
A.4.6	Schwachstelle in Hirschmann Switchen.....	147

A.5	2021	149
A.5.1	Microsoft Exchange – Schwachstelle des Microsoft Exchange Servers ..	149
A.5.2	NAME:WRECK – Schwachstellen in Netzwerkstacks	151
A.5.3	Schwachstellen in Bachmann Controllern	152
A.5.4	INFRA:HALT – Schwachstellen in Netzwerkstacks	154
A.5.5	Nucleus:13 – Schwachstellen in Netzwerkstacks	155
A.5.6	Schwachstellen im DDS Protocol	156
A.5.7	BadAlloc – Schwachstellen in echtzeitfähigen OT- und IoT-Geräten	157
A.5.8	Siemens SIPROTEC 4	159
A.5.9	Kameras Geutebrück	161
A.5.10	DIAEnergie	162
A.5.11	Schwachstelle in Johnson Controls Videoüberwachungs- und Zugangskontrollsystem	164
A.5.12	Log4Shell: Kritische Zero-Day Schwachstelle in der Java Bibliothek log4j	166
A.6	2022	169
A.6.1	Incontroller/Pipedream – Set aus ICS-spezifischen IT-Angriffswerkzeugen	169
A.6.2	ICEFALL	172
A.6.3	Retbleed – Schwachstellen in CPUs	174
A.6.4	SpringShell – Schwachstelle in der Java Bibliothek Spring	175
A.6.5	Schwachstelle in Schneider Electric Easergy P3 und P5	177
A.6.6	TL Storm 2.0, Schwachstelle in Aruba und Avaya Switches	179
A.6.7	SATAn	181
A.6.8	Schwachstellen in GPS-Trackern	182
A.6.9	Schwachstellen in Videoüberwachungssystemen und Network Attached Storage von QNAP	185
B	IT-Sicherheitsvorfälle und IT-Angriffe	189
B.1	2007	190
B.1.1	Stuxnet 0.5	190
B.2	2008	191

B.2.1	BlackEnergy 1 – IT-Angriffe auf georgische Einrichtungen	191
B.3	2010	194
B.3.1	Stuxnet – IT-Angriff auf Natanz.....	194
B.4	2011	195
B.4.1	Chinese Gas Pipeline Intrusion Campaign.....	195
B.5	2012	197
B.5.1	Shamoon – IT-Angriff auf Saudi Aramco.....	197
B.5.2	BlackEnergy 2 – Globaler IT-Angriff.....	198
B.5.3	Spear-Phishing-Angriff durch ehemaligen U.S. NRC Mitarbeiter.....	201
B.6	2014	202
B.6.1	IT-Angriff auf südkoreanisches Kernkraftwerk.....	202
B.6.2	IT-Angriff auf ein deutsches Stahlwerk.....	203
B.6.3	Havex und Karagany – Erste IT-Angriffswelle durch APT Dragonfly	204
B.6.4	Epic Turla – Globaler IT-Angriff.....	205
B.7	2015	207
B.7.1	BlackEnergy 3 – IT-Angriff auf das ukrainische Stromnetz.....	207
B.7.2	GreyEnergy – IT-Angriff auf Stromnetze in Osteuropa	209
B.8	2016	211
B.8.1	Crashoverride/Industroyer – IT-Angriff auf die Stromversorgung in Kiew.....	211
B.8.2	Mirai – IT-Angriff auf IoT-Systeme	212
B.9	2017	215
B.9.1	Ccleaner Hack – IT-Angriff über schadsoftwarebehaftete Ccleaner Version	215
B.9.2	Triton/TriSIS – IT-Angriff auf Petro Rabigh.....	217
B.9.3	Karagany.B und Heriplot – Zweite IT-Angriffswelle durch APT Dragonfly	219
B.9.4	WannaCry – Globaler IT-Angriff.....	221
B.9.5	Bad Rabbit – Globaler IT-Angriff	223
B.9.6	NotPetya – IT-Angriffe auf ukrainische Behörden, Infrastruktur und weltweite Unternehmen	225
B.10	2018	226

B.10.1	Shadowhammer – IT-Angriff über schadsoftwarebehaftete ASUS Steuerungssoftware.....	226
B.10.2	IT-Angriff auf den französischen Baukonzern Ingérop	227
B.10.3	Emotet – Globale IT-Angriffe auf Behörden und Infrastruktur.....	228
B.10.4	Operation Sharpshooter – Globale IT-Angriffe auf Behörden und Infrastruktur	230
B.10.5	Shamoon v3 – IT-Angriff auf Saipem	231
B.11	2019	231
B.11.1	IT-Sicherheitsvorfall durch Cryptomining in KKW Südukraine	231
B.11.2	IT-Angriff auf KKW Kudankulam	232
B.11.3	Weiterer IT-Sicherheitsvorfall in Zusammenhang mit Triton/Trisis	234
B.11.4	ZeroCleare – IT-Angriffe auf den Energiesektor im mittleren Osten	235
B.11.5	IT-Angriff mit LockerGoga auf Norsk Hydro	237
B.11.6	IT-Angriffe über VPN-Schwachstellen.....	239
B.11.7	IT-Angriff auf Windkraftanlage in den USA.....	240
B.12	2020	241
B.12.1	IT-Angriff auf US-amerikanischen Pipeline Betreiber	241
B.12.2	SNAKE/EKANS – IT-Angriffe auf weltweite Unternehmen	242
B.12.3	IT-Angriff auf die Stromversorgung von Mumbai.....	244
B.12.4	SolarWinds – IT-Angriffe über schadsoftwarebehaftete SolarWinds Produkte	245
B.13	2021	247
B.13.1	Oldsmar Attack – IT-Angriff auf Wasserwiederaufbereitungsanlage in Tampa, Florida	247
B.13.2	DarkSide – IT-Angriff auf brasilianischen Energiesektor	248
B.13.3	Codecov – IT-Angriff über Bash Uploader Dev Tool	249
B.13.4	Kaseya – Globaler IT-Angriff.....	249
B.13.5	DarkSide – IT-Angriff auf Colonial Pipeline	251
B.13.6	IT-Angriff auf Kisters AG	254
B.13.7	Black Matter – IT-Angriffe auf kritische Infrastrukturen.....	256
B.13.8	APT28 – IT-Angriff auf Google.....	258
B.13.9	APT28 – IT-Angriffe im Rahmen einer Brute Force Kampagne.....	259

B.13.10	REvil – IT-Angriff auf US-Fleischkonzern JBS	260
B.13.11	Conti - IT-Angriff auf den irischen Gesundheitsdienst	262
B.13.12	IT-Angriffe mit SparrowDoor	263
B.13.13	IT-Angriff auf WestRock.....	265
B.13.14	Cuba – IT- Angriffe auf kritische Infrastruktur	266
B.13.15	Conti – IT-Angriff auf ONTEC	267
B.13.16	Tiny Turla- Globale IT-Angriffe.....	268
B.13.17	IT-Angriff auf Vestas	269
B.13.18	IT-Angriffe auf die Vereinten Nationen	271
B.13.19	Ransomware – IT-Angriff auf Sogin	272
B.13.20	SquirrelWaffle-Loader	273
B.14	2022	275
B.14.1	WhisperGate – IT-Angriffe auf ukrainische Einrichtungen	275
B.14.2	AcidRain – IT-Angriff auf die Satellitenkommunikation via KA-Sat	277
B.14.3	Killnet – IT-Angriffe auf Webseiten von Regierungseinrichtungen.....	283
B.14.4	IT-Angriff auf Rosneft.....	283
B.14.5	Industroyer-2 – IT-Angriff auf die ukrainische Energieversorgung	285
B.14.6	Khouzestan Steel Co. – IT-Angriff auf iranisches Stahlwerk	286
B.14.7	LockBit – IT-Angriff auf Top Aces	288
B.14.8	Conti – IT-Angriff auf Regierungsstellen Costa Ricas	290
B.14.9	IT-Angriff auf israelische Regierungsw Webseiten	292
B.14.10	IT-Angriffe mit Bumblebee	292
B.14.11	IT-Angriff auf Dienstleister von Okta	294
B.14.12	IT-Angriffe im Jahr 2021/2022 auf den VPN Client Pulse Connect Secure	296
B.14.13	IT-Angriff auf T-Mobile US und folgende SIM-Swaps.....	298
B.14.14	IT-Angriffe mit DeadBolt.....	300
B.14.15	IT-Angriff über USB-Sticks.....	302
B.14.16	IT-Angriff auf Oiltanking	304
B.14.17	IT-Angriff auf Nordex	305
B.14.18	IT-Angriff mit Black Basta Ransomware.....	306
B.14.19	IT-Angriff mit BlackCat Ransomware	309

B.14.20	IT-Angriffe mit Quietexit	311
B.14.21	IT-Angriffe mit Hyperbro.....	314
B.14.22	IT-Angriff auf WatchGuard Firewalls	315
B.14.23	Physischer Angriff auf IT-Infrastruktur in Frankreich	317
B.14.24	IT-Angriff auf ein Unterseekabel	318
B.14.25	Strahlenschutz Spanien	319
B.14.26	ZuoRAT	321