

Spis treści

15	Wstęp
A	
17	Abandonware
18	Account harvesting
19	Account hijacking
20	Adaptive Authentication
21	Ad blocker
23	Address bar
23	Address bar spoofing
24	Address Resolution Protocol (ARP)
25	Ad fraud
26	Ad rotator
27	Ad-supported software lub Adware
28	Advanced Encryption Standard AES
29	Advanced Persistent Threats, APT
30	Advanced Research Projects Agency Network, ARPANET
31	Advertising-Supported Software
33	Air-Gapped
34	Always-On
35	American Standard Code for Information Interchange ASCII
35	Analog
36	Android
36	Android app
37	Annoybot
37	Annoyware
38	Anomaly Detection
39	Anonymization
40	Anonymizer
40	Anti-ransomware
40	Anonymous
41	Anti-virus (AV) killer
41	Antivirus Software
42	Anything-as-a-Service XaaS
43	Applet
44	Application programming interface API
45	Application Security
46	Approved Scanning Vendor ASV
47	Artificial intelligence AI
48	Artificial intelligence data protection
48	Artificial Intelligence Liability Directive AILD
50	Artificial intelligence risk management)
51	Artificial intelligence Privacy
52	Astroturfing
52	Asymmetric cryptography
53	Atak 51%
54	Augmented reality (AR)
56	Authentication
57	Authentication 2 FA
58	Authentication factor
58	Autonomous system

B

60	Backdoor
60	Bad sector
61	Bait advertising
62	Baiting
63	Banking Trojan
64	Beacon
64	Behavior
67	Big Data BD
68	Big-game hunting BGH
68	Binary
69	Biohacking
69	Biometrics
70	BIOS
71	Bitcoin
72	BitTorrent
73	Black Friday
73	Black Hat
74	Blacklist
74	Blended threat
75	Bloatware
76	Blockchain
77	Block cipher
78	Bluejacking
79	Blue Screen of Death (BSoD)
79	Bluesnarfing
80	Bluetooth
80	Boot sector
81	Boot sector virus
82	Bot
82	Bot herder
83	Botnet
84	Breach and Attack Simulation BAS
86	Bricking
87	Bring your own device (BYOD)
88	Browlock
88	Browser helper object (BHO)
89	Browser isolation
90	Brute Force Attack
92	Buffer
93	Bug bounty
94	Buffer overflow
95	Bundler
96	Bundleware
96	Burn
97	Business continuity management (BCM)
98	Business Email Compromise (BEC)
99	Business process compromise (BPC)

C

101	Cache
101	Children's Online Privacy Protection Act (COPPA)
102	Cipher

102	Ciphertext
103	Clickbait
104	Click fraud
104	Clickjacking
105	Client/Server Network
106	Cloud
107	Cloud Access Security Broker (CASB)
108	Cloud computing
109	Cloud phishing
110	Cloud Security
111	Cobalt Strike
112	Cold boot
112	Cold boot attack
113	Command & control (C&C, C2)
114	Common Vulnerabilities and Exposures – CVE
115	Companion virus
116	Compromised sites or servers
118	Computer-Aided Design CAD
119	Computer ethics
120	Computer Network Exploitation (CNE)
121	Configuration Management Database (CMDB)
122	Consumer fraud protection
123	Continuous Adaptive Risk and Trust Assessment (CARTA)
124	Control Objectives for Information and Related Technologies (CoBIT)
126	Cookie
127	Crack
128	Cracking
129	Credential stuffing
130	Crimeware
132	Cross-site scripting (XSS)
133	Crypter
134	Cryptocurrency
135	Cryptocurrency mining
136	Cryptography
137	Cryptojacking
138	Customer Relationship Management (CRM)
139	Cyberbullying
140	Cybercrime
141	Cyber espionage
142	Cyber liability insurance
142	Cyber Monday
143	Cyber Threat Intelligence (CTI)

D

145	Dark Web
145	Data breach
146	Data editing
147	Data loss prevention (DLP)
148	Data Masking
149	Data mining
150	Data Privacy Day (DPD)
150	Data Protection
151	Data swapping
153	Decryption

154	Decryptor
155	Deepfake
155	Deep Web
156	Definition
156	Defragmentation
157	Denial of Service (DoS)
158	Destruction of service (DeOS)
159	Device control
160	Dialer
161	Dictionary attack
162	Digital footprint
163	Digital forensics and incident response (DFIR)
164	Digital Rights Management (DRM)
165	Directory
166	Distributed Denial of Service (DDoS)
167	DNS Hijacking
168	DNS filtering
169	DNS over HTTPS (DoH)
170	DNS over TLS (DoT)
171	Domain administrator privileges
172	Domain Name
173	Domain Name System (DNS)
174	Domain Name System Security Extensions (DNSSEC)
175	Downloader
175	Dox
176	Drive-by download
177	Drive-by mining
177	Dropper
178	Dwell Time

E

179	Echelon
179	Electronic sports eSports
181	Encryption
182	Endpoint Detection and Response (EDR)
183	Endpoint Security
184	End-user
185	Enterprise Resource Planning (ERP)
186	EternalBlue
187	Eternal Champion
188	Eternal Romance
188	Ethernet
189	Executable and Link format (ELF)
191	Exploit
192	Exploit kit

F

196	Fear, uncertainty, and doubt (FUD)
197	File-based attack
198	Fileless Attacks
199	File type
200	Fingerprinting
202	Firewall
202	Firewall as-a-Service (FWaaS)

203	Firmware
205	Foothold expansion
206	Forensic Data Analysis (FDA)
206	Fraud
207	Freeware
208	Frequently asked questions (FAQ)

G

209	Generalization
210	Generation of synthetic data
211	Globally unique identifier (GUID)
213	Graphical user interface GUI
214	Graymail
215	Greyware
216	Griefing

H

217	Hacker
218	Hardware authentication
219	Hash value
220	Heap spraying
220	Heartbleed
221	Heuristic analysis
222	Hibernation
223	Hijacker
224	Homograph
225	Homograph attacks
226	Homomorphinc encryption
226	Honeypot
228	Host
229	Host-based solution
230	Host Intrusion Prevention System HIPS
232	Hyper-Text Transfer Protocol http

I

233	Identity and access management (IAM)
234	Identity theft
235	Impersonation
236	Incident Response IR
237	Incident scope
238	Indicator of Attack IOA
239	Indicator of Compromise IOC
240	Infection Vector
241	Information System
243	Information Technology (IT)
244	Initial access brokers (IABs)
245	Injection attacks
247	Injection SQLi
248	Input/Output (I/O)
249	Insider
249	Intellectual Property (IP)
251	Internal risk
252	Internationalized domain names (IDN)
253	Internet Of Things (IoT)

254	Internet Service Provider (ISP)
254	Intrusion
255	Intrusion Detection Systems (IDS) and Intrusion Prevention Systems
(IPS)	
257	Intrusion Prevention System (IPS)
258	IP address

J

260	Jailbreak
261	Joke programs
262	Juice jacking
263	Junk mail
264	Key generator
265	Keylogger
266	Keystream
267	Keystroke
268	Kryptojacking
269	Kryptomining
270	Latency
271	Lateral movement
272	Layered Service Provider (LSP)
272	Linux
274	Local Area Network (LAN)
275	Localhost

M

277	Machine code
278	Machine learning ML
279	Machine-to-machine M2M
280	Macro virus
282	Madware
283	Magecart
284	Mail bomb
285	Malicious/Destructive payload
286	Malspam
287	Malvertising
288	Malware
289	Managed Detection and Response MDR
289	Managed service provider (MSP)
290	Management of artificial intelligence
291	Man-in-the-Browser (MitB)
292	Master Boot Record (MBR)
293	Mean time to detect (MTTD)
294	Media Access Control (MAC)
295	Memory dump
297	Memory resident
297	Micro-Segmentation
299	Miner
300	Mitigation
301	MITRE ATT&CK Framework
302	Mixed reality
303	Mobile security
304	Multi-factor authentication (MFA)
305	Multimedia Messaging Service (MMS)

306	Multiplatform
306	Multi-tenancy
308	Mumblehard malware

N

310	National Cyber Security Centre NCSC
311	National Institute of Standards and Technology (NIST)
313	National Security Agency (NSA)
313	Near-field communication (NFC)
314	Net neutrality
315	Network
318	Network Intrusion
319	Network perimeter
320	Network Segmentation
322	NewTab
323	Next Generation Antivirus (NGAV)
323	Norma ISO/IEC 20000
324	Norma ISO/IEC 27001

O

326	Obfuscation
327	OpenSSL
328	Open Systems Interconnection OSI
330	Operating system (OS)
331	Opportunistic attack

P

333	Packer
334	Packet Sniffers
335	Packet
336	Packet Sniffers
337	Passphrase
338	Password
339	Password cracking application
339	Password guessing
340	Password manager
341	Patch management software
342	Payload
343	Payment Card Industry Data Security Standard (PCI DSS)
344	Peer-to-peer (P2P)
345	Penetration testing
346	People ware
347	Personal identification number (PIN)
348	Personally Identifiable Information (PII)
349	Perturbation
350	Pharma
351	Phishing
353	Phishing kit
355	Phishing attack
356	Phishing whale
357	Phreaking
359	Plaintext
360	Platform
361	Point-of-sale (PoS) malware

362	Polymorphism
362	Portable device
364	Portable Executable PE file header
365	Potentially Unwanted Programs (PUP)
366	PowerShell
367	Power User
368	Preinstalled software
369	Privileged Access Management (PAM)
370	Privilege escalation
372	Professional Service Automation (PSA)
374	Proof of concept (PoC)
375	Protector
375	Pseudocode
376	Pseudonymization
377	Punycode

Q

379	Quick Response Code (QR Code)
380	Quarantine

R

381	RAM scraping
382	Random access memory RAM
383	Randomizacja
384	Ransomware
385	Ransomware-as-a-service (RaaS)
387	RAR
387	Recon
388	Red Team
389	Remote access
390	Remote administration tool (RAT)
392	Remote code execution (RCE) attack
393	Remote desktop protocol (RDP)
394	Remote monitoring and management (RMM)
395	Remote access
397	Report on Compliance for PCI (ROC)
398	Responsible artificial intelligence
398	Retrovirus
399	Riskware
400	Robocall
401	Rootkit
402	RunPE Technique

S

404	Safe Mode
404	Sandbox solution
405	Scam
406	Screen lock
407	Script
408	Script kiddie
410	Script Kiddie
410	Search Engine Optimization (SEO)
411	Search neutrality
412	Secure artificial intelligence

413	Secure multiparty computation SMPC
413	Security Awareness Training
414	Security Information and Event Management (SIEM)
415	Security Orchestration, Automation and Response (SOAR)
417	Seed
418	Server
418	Service-level agreement (SLA)
419	Serverless
420	Server Message Block (SMB)
421	Service-level agreement (SLA)
422	Server proxy
423	Sextortion
424	Shadow IT
425	Shareware
427	Shimming
428	Shoulder Surfing
429	Signature
430	SIMjacking
432	Skimming
433	Smart home
433	Smishing
435	Social Engineering
436	Software
437	Software add-on
438	Software Composition Analysis (SCA)
439	Software-Defined Networking (SDN)
441	Software-Defined WAN (SD-WAN)
442	Software Delivery Layer
443	Software licenses
444	Software vulnerability
445	Spambot
446	Spear phishing
448	Spoofing
449	Spyware
451	SSL certificate
452	Stalkerware
454	Stands for potentially unwanted modification (PUM)
455	Static Application Security Testing (SAST)
457	Steganography
458	Stream
460	Stream cipher
461	Structured Query Language (SQL) Injection
462	Stuxnet
464	Supply-chain attack
465	Surface Web
466	Suspicious activity
467	Symbian malware
468	Synthetic data
469	System on a Chip (SoC)
470	System optimizer
T	
472	Targeted attack
473	The Health Insurance Portability and Accountability Act (HIPAA)

474	The United States Computer Emergency Readiness Team (US-CERT)
475	Third party
476	Third party patch management
477	Third-party risk management TPRM
478	Threat actor
478	Threat Detection and Response
480	Threat hunting
480	Threat intelligence
482	Threat modeling
483	Token
483	Tokenizacja
484	Token MFA Multi-Factor Authentication (MFA)
484	Top Level Domain TLD
486	Tor
487	Trackware
488	Transport Layer Security (TLS)
489	Triada CIA
490	Trojan
490	Trolling
491	Troubleshooting
492	Trusted execution environment (TEE)
492	Typosquatting

U

494	Ubiquitous computing
495	Ubuntu
496	Unauthorized Access
497	Unicode Transformation Format (UTF)
498	Uniform Resource Locator
499	Universal authentication
500	Universal serial bus USB
501	UNIX
502	Urban legend
503	USB attack
505	USB boot
505	USENET
506	User Interface UI

V

508	Vaporware
509	Variant
510	Virtual Local Area Network (VLAN)
511	Virtual machine
513	Virtual memory
514	Virtual private network (VPN)
515	Virtual reality VR
516	Virus
518	Virus hoax
518	Vishing
520	Voice authentication
521	Voice over Internet Protocol (VoIP)
522	Vulnerabilities
522	Vulnerability Management

W

524	Walled garden
525	WAP Stands for Wireless Application Protocol
526	Warez
527	Warm boot
528	Warm standby
529	Watering hole attack
530	Wayback Machine
531	Wearable computer
532	Web application security
532	Web Browser
533	Web Crawler
534	Web-enabled
534	Web inject
535	Web of Things (WoT)
536	Web scraping
537	Website defacement
538	Website spoofing
539	Web skimmer
541	Wetware
541	Whack-a-mole
542	Wide Area Network (WAN)
544	Whaling
544	What You See Is What You Get WYSIWYG
545	White hat hacker
546	Whitelist
547	White Screen of Death (WSOD)
547	White space padding
548	WHOIS
549	Wide Area Network (WAN)
550	Wi-Fi
551	Wi-Fi Protected Access II (WPA2)
552	Wi-Fi Protected Access Pre-Shared Key (WPA)
553	Windows Sockets API (Winsock)
553	Wireless
554	Wireless Application Service Provider (WASP)
555	Wireless Hotspot
556	Wireless Local Area Network (WLAN)
557	Wireless Personal Area Network (WPAN)
558	Wiretap Trojan
559	Worm
560	Write protection
561	WWW

Y

563	Y2K
-----	-----

Z

564	Zbot
565	Zero Administration for Windows (ZAW)
566	Zero-day
566	Zero-trust
567	Zombie proces
568	Zoombombing

Bibliografia

570	www.inforafinacja.pl/literatura
-----	--