Adware

ENISA

Aktivní kybernetická obrana

Aktivum

Analýza hrozeb

Analýza počítačového viru

Antispamový filtr

Antivirový program

Asymetrická kryptografie

Autenticita

Autentizace (dat, identity, klíče, zprávy)

Autorizace

Bezpečnost

Bezpečnost informací

Bezpečnost informací/informačních systémů

Bezpečnostní audit

Bezpečnostní hrozba

Bezpečnostní incident

Bezpečnostní politika

Bezpečnostní požadavky

Bezpečnostní zranitelnost

Bot

Bot herder

Botnet

BYOD

Captcha

Certifikace

Certifikační autorita

Cloud computing

Cookie

Crack

Cracker

Cross-site scripting (XSS)

Červ

Člověk uprostřed (Man in the Middle - MitM)

Databáze

Datové centrum

Dialer

Digitální podpis

Distribuované odmítnutí služby (DDoS – Distributed Denial of Service)

DNS server

Doména nejvyšší úrovně

Doménové jméno

Doménové pirátství (cybersquatting)

Dost dobré soukromí (Pretty good privacy – PGP)

Důvěrnost

Dostupnost

Integrita

Elektronický boj

Firewall

Firmware

Forensní analýza

Freeware

Fyzické řízení přístupu

Generátor náhodných čísel

GNU/GPL

Grey hat

Hack / Hacking

Hacker

Hackers for Hire (H4H)

Hacktivism

Heslo

Hodnocení rizik

Hodnocení zranitelností

Hodnota aktiv

Honeypot

Hromadné rozesílání nevyžádané pošty (spamming)

HTTP a HTTPS

Charakteristika viru

ICMP záplava

Identifikace

Incident

Informační (kybernetická) společnost

Informační a komunikační technologie

Informační kriminalita

Informační operace

Information assurance

Infoware

Infrastruktura jako služba

Infrastruktura veřejných klíčů

Inicializační vektor

Insider

Integrita dat

Integrita sítě

Integrita systému

Internet control message protocol (ICMP)

Internet Protocol (IP)

Internet

Interoperabilita

Intranet

IP adresa

Internet Relay Chat (IRC)

IT síť

Keylogger

Klepání na porty

Kompromitace

Kriminalita, související s pokročilými technologiemi

Kritická informační infrastruktura

Kritická infrastruktura

Krizová situace

Krizové plánování

Krizové řízení

Krizový plán

Krizový stav

Kryptografický klíč

Kryptografický prostředek

Kryptografie

Kybernetická bezpečnost

Kybernetická kriminalita

Kybernetická obrana

Kybernetická strategie

Kybernetická špionáž

Kybernetická válka

Kybernetický prostor

Kybernetický protiútok

Kybernetický útok

Kyberterorismus

Logická bomba

Lokální síť (LAN)

MAC adresa

Management bezpečnostních informací a událostí

Modrá obrazovka smrti

Monitorovací prostředky

Monitoring

Národní autorita

NATO CCD COE

Nevyžádaná pošta

Obecné zahlcení

Obnova dat

Obranná infrastruktura

Odmítnutí služby

Odolnost

Odposlech

Odposlech / Nežádoucí odposlech

Ochrana dat

Ochrana kritické infrastruktury

Operační systém

Paket

Pár klíčů

Páteřní síť

Penetrační testování

Pharming

Phishing

Phreaker

Phreaking

Ping

Ping of death

Počítačová bezpečnost

Počítačová kriminalita

Počítačová síť

Počítačový virus

Podrobná inspekce paketů (DPI)

Podvržení IP adresy

Pokročilá a trvalá hrozba

Politika řízení přístupu

Poplašná zpráva

Port

Port scanner

Portál

Poskytovatel služby

Povolení přístupu

Privátní IP adresa

Proces

Program

Prolamovač hesel

Prolomení

Prostředky Informační války

Protokol

Proxy trojan

Průmyslový řídící systém

Prvek kritické infrastruktury

Přesměrovávače

Příklad dobré praxe, osvědčený způsob

Přístupové právo

Ransomware

Redukce rizik

Redundance

Registr doménových jmen

Riziko

Rootkit

Rovný s rovným (Peer to peer – P2P)

Řízení přístupu

Řízení zranitelností

Sandbox

Secure shell (SSH)

Secure socket layer (SSL)

Serverová farma

Service set identifier (SSID)

Seznam pro řízení přístupu

Shareware

Schopnost pro reakci na počítačové hrozby (CIRC)

Simple mail transfer protocol (SMTP)

Simulace

Síť

Skript

Skupina pro reakce na počítačové bezpečnostní incidenty

Skupina pro reakci na počítačové hrozby

Slovníkový útok

Sniffer

Sociální inženýrství

Sociální síť

Software (programové vybavení)

Software jako služba

Soubor

Soubor logů

Souborový systém

Spear phishing (rybaření oštěpem)

Spolehlivost

Správa bezpečnosti operací

Správce systému

Spyware

SQL

SQL injection

Stav kybernetického nebezpečí

Subjekt kritické infrastruktury

Symetrický algoritmus

Symetrická kryptografie

SYN-flood

Systém detekce průniku

Systém doménových jmen

Systém prevence průniku

Systém řízení identit

Šifrování

Tajná vrátka / Přístup ke službám

Technické prostředky (vybavení)

Telefonní phishing

TOR (anonymní síť)

Transmission control protocol (TCP)

Transport layer security (TLS)

Trojský kůň

Úmyslné oklamání, podvržení

Uniform resource locator (URL)

Útok na počítačovou síť

Útok s použitím hrubé síly

Uzavřené bezpečnostní prostředí

Validace dat

Validace identity

Veřejná IP adresa

Virtuální lokální síť

Virtuální privátní síť

Virus

Vstup přes autorizovaného uživatele

Vycpávka (Padding)

Vytěžování počítačové sítě

Využití návnady

Významná síť

Významný informační systém

Webový vandalizmus

White hat

Whois

WiFi

Wireshark

World wide web (WWW)

Zadní vrátka

Zahlcení pingy

Zahlcení TCP SYN

Zahlcení UDP

Záložní soubor

Záplata

Zaplavení, zahlcení

Zkreslení webových stránek

Zlovolná logika

Známá chyba

Zneužití

Zombie

Zranitelnost

Životní cyklus