Information security and cybersecurity – vocabulary

Dawid Mrowiec, B-secure

Kraków 2023r.

W „Information security and cybersecurity – vocabulary” znajdziesz zestaw ponad 500 słówek i zwrotów związanych z bezpieczeństwem informacji (w tym bezpieczeństwem IT).

Niniejsza publikacja jest pierwszym „obszarowym” rozszerzeniem „Risk management – vocabulary”, poświęconego szeroko rozumianemu zarządzaniu ryzykiem i ciągłości działania. Wspomnianą publikację bazową jak i kolejne zestawy słówek z zakresu innych specjalistycznych obszarów zarządzania bezpieczeństwem organizacji znajdziesz na blogu: https://bezpieczenstwobiznesu.com.pl

Słówka przedstawione są w formie angielsko-polskiej, niemniej jeśli chcesz w prosty sposób sprawdzić odwrotne tłumaczenie, wystarczy, że zastosujesz skrót CTRL + F i skorzystasz z opcji wyszukiwania – wpisując interesujące cię hasło po polsku.

A

abnormal behavior signature – sygnatura nienormalnego zachowania
abnormal condition – warunek nienormalny
absence of confirmation – brak potwierdzenia
acceptable use policy – zasada dopuszczalnego wykorzystania
access address – adres dostępu
access by key – dostęp według klucza
access control – kontrola dostępu
Access Control List (ACL) – lista uprawnień powiązanych z konkretnym zasobem w komputerze lub sieci
Access Control Service (ACS) – usługa kontroli dostępu
access key – klucz dostępu
access management – zarządzanie dostępem
Access Point (AP) – punkt dostępowy
Access Point Name (APN) – nazwa bądź adres bramy pomiędzy siecią komórkową operatora a zewnętrzną siecią komputerową
access privileges – przywileje dostępu
Account Information Services (AIS) – usługa dostępu do informacji o rachunku
account management – zarządzanie kontami
account servicing payment services provider (ASPSP) – podmiot prowadzący rachunek płatniczy
active content – aktywna zawartość
adaptive defense – obrona adaptacyjna (model)
adaptive testing – (komputerowe) testy adaptacyjne
administrative account – konto administracyjne
administrative controls – administracyjne środki bezpieczeństwa
Advanced Encryption Standard (AES) – symetryczny szyfr blokowy
Advanced Persistent Threats (APT) – zaawansowane trwałe zagrożenia
advance-fee schemes – zaawansowane oszustwa z opłatami
adversary – przeciwnik, oponent
adware – oprogramowanie z reklamami
aggregation (of data) – gromadzenie (danych)
air gap – szczelina powietrzna (środek bezpieczeństwa polegający na oddzieleniu komputera lub sieci od Internetu)
all source intelligence – pozyskiwanie informacji z wielu źródeł (potencjalnie wszystkich dostępnych)
alternate processing site – zapasowy ośrodek dla prowadzenia biznesowych działań operacyjnych
alternate storage site – ośrodek dla danych odtworzeniowych
analyzing – analizowanie
anti-spyware – oprogramowanie przeciwdziałające szpiegowaniu
antivirus – antywirus
antivirus software – oprogramowanie antywirusowe
application security – bezpieczeństwo aplikacji

application security testing (AST) – testowanie bezpieczeństwa aplikacji
archival – archiwalny
archive (also records room) – archiwum (jako miejsce przechowywania dokumentów/ folder komputerowy do przechowywania danych/ skompresowany plik na komputerze)
assembly metadata – metadane zestawu
asset – zasób (który wymaga ochrony), atut, zaleta
asset management – zarządzanie aktywami
assets – aktywa, majątek
asymmetric warfare – konflikt asymetryczny
attachment – załącznik
attack map – mapa ataków
attack method – metoda ataku
attack pattern – wzorzec ataku
attack surface – powierzchnia ataku (całkowita liczba podatności i punktów dostępu, którą może wykorzystać atakujący)
attack tree – drzewo ataków (wizualizacja pomocna przy ocenie podatności i scenariuszy ataku)
attack vector – wektor ataku
attacker – napastnik, atakujący
Attribute-Based Access Control (ABAC) – kontrola dostępu oparta na atrybutach/zasobach
audit log – dziennik kontroli
audit trail – dziennik kontroli (w komputerze), dane do audytu, ścieżka audytu
auditing – audytowanie
authentication – potwierdzenie autentyczności, poświadczenie oryginalności, uwierzytelnienie
authenticity – autentyczność
authorization – autoryzacja
availability – dostępność, osiągalność, dyspozycyjność

B

back issue (also back copy, back number) – numer archiwalny, oznaczenie archiwalne
backdoor – potocznie tylne drzwi lub furtka (umyślnie pozostawiona luka w zabezpieczeniach)
backing up – tworzenie kopii zapasowych
backup – kopia zapasowa
Backup and Recovery Plan – plan tworzenia kopii zapasowej i odtwarzania
baiting – przynęta na haczyk (element mający sprowokować i ujawnić napastnika)
banner grabbing – przechwytywanie banerów (technika służąca do zbierania informacji przydatnych w trakcie ataku)
baseline controls – podstawowa ochrona
baselining – metoda analizy wydajności sieci komputerowej
behavior monitoring – monitorowanie zachowań (np. użytkowników systemu)
behavioral analytics – analiza (wzorców) zachowań
behavioral biometrics – biometryka behawioralna
behavioral detection – detekcja behawioralna

big data analytics – analityka dużych zbiorów danych
binary tree – drzewo binarne
biometric – biometryczny
biometric authentication – uwierzytelnianie biometryczne
black box testing – testy funkcjonalne
black hat (hacker) – haker kierujący się złymi intencjami (wrogo nastawiony), haker łamiący przepisy prawa
blacklist – czarna lista
blind spot – martwe pole, martwy punkt (niezabezpieczony fragment systemu)
Blue Team – zespół niebieski (grupa osób, które przeprowadzają analizę systemów informatycznych w celu zapewnienia ich bezpieczeństwa)
bluejacking – wysyłanie niepodpisanych wiadomości przez Bluetooth
botnet – grupa komputerów-zombie zainfekowanych szkodliwym oprogramowaniem
boundary defense – ochrona brzegowa
Bring Your Own Device (BYOD) – przynieś swoje urządzenie (model pracy zdalnej, w ramach którego pracownicy korzystają z prywatnego sprzętu)
broadband – szerokopasmowy
browser – przeglądarka
browser security extension – rozszerzenia bezpieczeństwa do przeglądarki
browser hijacker – porywcza przeglądarek (rodzaj złośliwego oprogramowania)
brute force attack – atak siłowy (sposób łamania haseł dostępowych)
buffer overflow – przepełnienie bufora
Business Email Compromise (BEC) – oszustwo „na dyrektora”

C

certification – certyfikacja
certification body – jednostka certyfikująca
chain of custody – kontrola pochodzenia produktu, łańcuch dostaw
chain of evidence – łańcuch dowodowy (kontrola pochodzenia dowodu)
change management – zarządzanie zmianami
chargeback – zwrot obciążenia
check character system – system znaków kontrolnych
Chief Information Officer (CIO) – osoba odpowiedzialna w organizacji za stan, rozwój i wdrożenia technologii informacyjnych
Chief Information Security Officer (CISO) – osoba odpowiedzialna w organizacji za bezpieczeństwo informacji
Chief Technology Officer (CTO) – dyrektor ds. technologii (osoba odpowiedzialna za strategię technologiczną firmy)
child grooming – uwodzenie dziecka w Internecie
Chinese Wall model – model Muru Chińskiego (koncepcja polegająca na separacji podmiotów w celu zapobieżenia wypływowi poufnych informacji)
cipher – szyfr
cipher text – tekst zaszyfrowany, szyfrogram
classified information – informacje niejawne

clientless – bez klientów, w odniesieniu do oprogramowania - nie wymagający instalacji na urządzeniu
cloud computing – chmura obliczeniowa, przetwarzanie danych w chmurze
cloud security – bezpieczeństwo chmury (obliczeniowej)
code – kod
code injection – wstrzyknięcie kodu
collision – kolizja, zderzenie
co-location – kolokacja
Common Criteria – wspólne kryteria
Common Vulnerability Scoring System (CVSS) – powszechny system oceny podatności
communication pair – para komunikujących się stron
communication party – strona komunikująca się
communication technology – technologia komunikacyjna
communications security – bezpieczeństwo komunikacji
Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) – rodzaj techniki stosowanej jako zabezpieczenie na stronach www, celem której jest dopuszczenie do przesłania danych tylko wypełnionych przez człowieka
compliance issues – kwestie związane ze zgodnością
compromise – naruszenie tajności/ zabezpieczeń
Computer Emergency Response Team (CERT) – Zespół Reagowania na Zagrożenia Komputerowe
computer forensics – informatyka śledcza
Computer Incident Response Team (CIRT) – zespół reagowania na incydenty komputerowe
Computer Network Defense (CND) – ochrona sieci komputerowej (ogół środków bezpieczeństwa wprowadzonych w celu ochrony)
computer network defense analysis – analiza bezpieczeństwa sieci komputerowej
Computer Security Incident Response Team (CSIRT) – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego
conduct crisis exercises – przeprowadzać ćwiczenia reakcji na kryzys
confidentiality – poufność
Confidentiality, Integrity and Availability (CIA) – poufność, integralność, dostępność (triada CIA)
configuration management – zarządzanie konfiguracjami
consequence – konsekwencja, następstwo, efekt wydarzenia bądź incydentu
content filtering – filtrowanie treści
Control Objectives for Information and related Technology (COBIT) – Cele Kontrolne dla Technologii Informacyjnych i Powiązanych (zbiór dobrych praktyk i wskazówek z zakresu zarządzania procesami IT)
cookies – ciasteczka (fragmenty kodu pozwalające na identyfikację i monitorowanie aktywności użytkownika w sieci)
Co-ordinated Universal Time (also UTC) – skoordynowany czas uniwersalny
cost benefit analysis – analiza kosztów i korzyści
counter – licznik
countermeasure – środek zaradczy, przeciwśrodek

cracker – włamywacz komputerowy
credentials – referencje
Critical National Infrastructure (CNI) – państwa infrastruktura krytyczna
critical update – krytyczna aktualizacja
cryptographic key – klucz kryptograficzny
customer data – dane dotyczące klientów/ konsumentów
cyber attack – cyberatak
cyber deception – cyber-oszustwo, cyber-decepcja
cyber espionage (also cyber spying) – cyberszpiegostwo
cyber exercise – ćwiczenia w zakresie cyberbezpieczeństwa
cyber hygiene – cyberhigiena
cyber insurance – ubezpieczenie od ryzyk cybernetycznych
cyber kill chain – potocznie łańcuch cyberzabójstwa, określenie struktury ataku
cyber security – cyberbezpieczeństwo
cyber security profession – specjaliści ds. (cyber)bezpieczeństwa (jako grupa zawodowa)
Cyber Security Qualifications Framework (CSQF) – ramy kompetencyjne specjalistów ds. cyberbezpieczeństwa
Cyber Threat Intelligence (CTI) – analiza/rozpoznawanie cyberzagrożeń
cyber warfare – walka w sieci, cyber-konflikt
cybersecurity analytics – analityka cyberbezpieczeństwa
cybersecurity automation – automatyzacja cyberbezpieczeństwa
cybersecurity awareness training – szkolenie mające na celu budowanie świadomości w obszarze cyberbezpieczeństwa
cybersecurity culture – kultura cyberbezpieczeństwa
cybersecurity framework – struktura ramowa cyberbezpieczeństwa
cybersecurity governance – zarządzanie cyberbezpieczeństwem/ ład organizacyjny odnoszący się do cyberbezpieczeństwa
Cybersecurity Incident Response Plan (CIRP) – plan reagowania na incydenty cyberbezpieczeństwa
Cybersecurity Information Technology (IT) Audit – audyt cyberbezpieczeństwa w obszarze IT
cybersecurity operations – operacje cyberbezpieczeństwa
cybersecurity risk assessment – ocena ryzyka w obszarze cyberbezpieczeństwa
cybersecurity risk management (CSRM) – zarządzanie ryzykiem w cyberbezpieczeństwie
cybersecurity risk register (CSRR) – rejestr ryzyk z obszaru cyberbezpieczeństwa
cyberspace – cyberprzestrzeń
cybersurfer (also cybertraveler) – szperacz internetowy (osoba, której zabiera to mnóstwo czasu)
cyberterrorism – cyberterroryzm
Cyclic Redundancy Check (CRC) – cykliczna kontrola środków nadmiarowych (zapasowych)

D

Dark Web – ukryta sieć (ukryta część Internetu niedostępna dla klasycznych wyszukiwarek)
data at rest – dane w spoczynku

data breach – naruszenie ochrony danych (przez ujawnienie informacji poufnych)
data classification – klasyfikacja danych
data decryption – odszyfrowywanie danych
data in transit – dane w ruchu
Data Leakage Prevention (DLP) – ochrona przed wyciekiem danych, zapobieganie utracie danych
data loss – utrata danych
data masking – maskowanie danych
data mining – pozyskiwanie danych, eksploracja danych, głęboka analiza danych
data origin authentication – uwierzytelnienie pochodzenia danych
data server – serwer z danymi
data storage – nośnik danych
data warehousing – magazynowanie danych (w dużych bazach danych w jednej lokalizacji)
database – baza danych
database security – bezpieczeństwo baz danych
decipherment – deszyfrowanie
declaration of conformity – deklaracja zgodności
declassification – odtajnienie
decrypt – deszyfrować, rozszyfrować
Deep Packet Inspection (DPI) – głęboka inspekcja pakietów
deepfake – fotomontaż wideo wygenerowany dzięki sieciom neuronowym
defamation – zniesławienie (kogoś), oszczerstwo
Defense in Depth – dogłębna obrona (koncepcja)
degausser – urządzenie służące do rozmagnesowania
deleted file – usunięty plik
delivery authority – organ dostarczający
Denial of Service (DoS) – odmowa usługi (rodzaj ataku)
DevSecOps – rozwój, utrzymanie i bezpieczeństwo (zwykle oprogramowania)
dictionary attack – atak słownikowy
digital certificate – certyfikat cyfrowy
digital forensics – cyfrowe techniki śledcze
digital native – osoba, która urodziła się i wychowała w epoce cyfrowej/Internetu
digital store – magazyn cyfrowy (danych)
digital preservation – ochrona zasobów cyfrowych
Digital Rights Management (DRM) – zarządzanie prawami cyfrowymi
digital signature – podpis cyfrowy, podpis elektroniczny
digital watermarking – cyfrowy znak wodny
digitisation – cyfryzacja
Disaster Recovery (DR) – odtwarzanie po katastrofie
disk imaging – obraz dysku
disruption – zakłócenie, przerwanie, wstrząs
Distributed Denial of Service (DDoS) – rozproszona odmowa usługi (rodzaj ataku)
Domain Name Server (DNS) – system nazw domen
doomsurfing – nawyk ciągłego przeglądania katastroficznych wiadomości w Internecie

doxing – publiczne udostępnianie informacji umożliwiających identyfikację osoby lub organizacji, zwykle za pośrednictwem Internetu
Dual Factor Authentication (2FA) – uwierzytelnianie dwuskładnikowe
duplexing – dyski zdublowane

E
eavesdropping – podsłuchiwanie, wścibski
e-crime – e-przestępczość (przestępczość bazująca na wykorzystaniu środków elektronicznych, głównie komputera i Internetu)
effectiveness – skuteczność
efficiency – wydajność
electronic crime – przestępczość elektroniczna
electronic funds transfer crime – przestępstwa związane z elektronicznym transferem środków
encryption (also encipherment) – szyfrowanie
Endpoint Detection and Response (EDR) – wykrywanie i reagowanie w punkcie końcowym
end-to-end – od końca do końca
enterprise architecture – architektura korporacyjna
entity authentication – uwierzytelnienie podmiotu
Ethernet – Ethernet (standard sieci lokalnej)
ethical hacking – etyczne hakowanie
European Cyber Security Organisation (ECSO) – Europejska Agencja ds. Cyberbezpieczeństwa
European Digital Single Market – europejski jednolity rynek cyfrowy
event – wydarzenie, zdarzenie
evidence – poświadczenie, dowód
exfiltration – przeniknięcie (wrogo nastawionej) osoby z zewnątrz do systemu lub organizacji
exploit – złośliwe oprogramowanie, które wykorzystuje błędy w oprogramowaniu
external audit – audyt zewnętrzny

F
Fear of Missing Out (FOMO) – lęk przed odłączenie od Internetu
fingerprinting – zdejmowanie odcisków palców, algorytm dopasowania wzorca
firewall – zapora sieciowa
firmware – mikrooprogramowanie, oprogramowanie wbudowane/ niskopoziomowe
forensic analysis – analiza śledcza
forensic copy – kopia na potrzeby zabezpieczenia dowodu
fraudulent sales online – fałszywe transakcje on-line

G
gap analysis – analiza luk
gateway – wejście, brama sieciowa
General Data Protection Regulation (GDPR) – ogólne rozporządzenie o ochronie danych (RODO)
Geospatial Intelligence (GEOINT) – rozpoznanie geoprzestrzenne

global threat landscape – globalny krajobraz zagrożeń
gray hat (hacker) – haker działający na granicy prawa

H
hacktivism – haktywizm
hard disk – dysk twardy
hardening – usztywnienie, wzmocnienie, łatanie podatności
hash function – funkcja haszująca, funkcja mieszająca, funkcja skrótu
honeypot – pułapka mająca na celu wykrycie prób nieautoryzowanego użycia systemu lub pozyskania danych
Host Intrusion Prevention System (HIPS) – system identyfikujący i blokujący próby włamania, które sforsowały firewall (element dogłębnej obrony)
hub – centrum, ośrodek, koncentrator, węzeł komunikacyjny
human factor – czynnik ludzki
Human Intelligence (HUMINT) – wywiad osobowy (działalność wywiadowcza, w ramach której informacje pozyskiwane są od osób)
hybrid – hybrydowy
Hypertext Markup Language (HTML) – język znaczników stosowany do tworzenia dokumentów hipertekstowych

I
identification – identyfikacja
Identity and Access Management (IAM) – zarządzanie tożsamością i dostępem
identity theft (also identity fraud) – kradzież tożsamości
impact – wpływ, konsekwencje
impact of technology – wpływ technologii
imprint – odcisk
incident – incydent
incident response – reakcja na incydenty
Incident Response Plan – plan reagowania na incydenty
incomplete and imperfect data – niekompletne i niedoskonałe dane
incremental backup – kopia przyrostowa (np. plików komputera)
independent communication – niezależna komunikacja
Indicators of Compromise (IOC) – wskaźnik narażenia
Industrial Control System (ICS) – przemysłowy system sterowania
industrial property – własność przemysłowa
industrial property right – prawo własności przemysłowej (przynależne podmiotowi)
information and communication technology system – system teleinformatyczny
information and communications technology (ICT) – teleinformatyka, technologie teleinformacyjne
information operations – operacje informacyjne
information owner – właściciel informacji, podmiot dysponujący informacjami
information security (infosec) – bezpieczeństwo informacji
information security architecture – architektura bezpieczeństwa informacji

information security incident – incydent bezpieczeństwa informacji
Information Security Management System (ISMS) – System Zarządzania Bezpieczeństwem Informacji
information security policy – polityka bezpieczeństwa informacji
information sharing – wymiana danych/informacji/wiedzy, dzielenie się informacjami
information technology (IT) – technologia informacyjna
information technology consulting – doradztwo informatyczne
Information Technology Infrastructure Library (ITIL) – zbiór publikacji zawierających najlepsze praktyki zarządzania usługami informatycznymi
information technology management – zarządzanie technologiami informatycznymi
Infrastructure-as-a-Service (IaaS) – infrastruktura jako usługa
insider threat – zagrożenie wewnętrzne
integrity – integralność
intellectual property protection – ochrona własności intelektualnej
intellectual property theft – kradzież własności intelektualnej
intellectual property – własność intelektualna
internal audit – audyt wewnętrzny
internal network – sieć wewnętrzna
International Organization for Standardization (ISO) – Międzynarodowa Organizacja Normalizacyjna
Internet Governance Forum (IGF) – Forum Zarządzania Internetem
Internet of Things (IoT) – internet rzeczy
Internet Protocol (IP) – protokół internetowy IP
Internet Protocol Security (IPsec) – zbiór protokołów służących implementacji bezpiecznych połączeń oraz wymiany kluczy szyfrowania pomiędzy komputerami
internet service provider – dostawca Internetu
interoperability – interoperacyjność, współdziałanie, efektywna współpraca (np. między systemami, usługami), kompatybilność
intrusion – wtargnięcie, włamanie
Intrusion Detection System (IDS) – system wykrywania włamań
Intrusion Prevention System (IPS) – system prewencji włamań
investigation – dochodzenie, śledztwo, badanie
IT Security Policy – polityka bezpieczeństwa systemów informatycznych

J

jamming – zagłuszanie (nadawanie na określonej częstotliwości przeszkadzające innym w odbiorze sygnału)
jump server – serwer przesiadkowy

K

keylogger – oprogramowanie śledzące aktywność użytkownika urządzenia
know-how – wiedza specjalistyczna, know-how
knowledge management – zarządzanie wiedzą

L

lack of crisis preparedness – brak przygotowania na wypadek kryzysu
lack of transparency – brak przejrzystości
layer – powłoka, warstwa (np. sieci)
leaked data – dane z wycieku
leaky – przeciekający, wyciekający
leased circuit – łącze telekomunikacyjne dzierżawione
least privilege – zasada najmniejszego uprzywilejowania/ najmniejszych uprawnień
legal and regulatory controls – prawne i regulacyjne środki bezpieczeństwa
legal protection of industrial property – ochrona prawna własności przemysłowej
lines of defense – linie obrony
Local Area Network (LAN) – Lokalna Sieć Komputerowa
log management – zarządzanie logami
logic bomb – bomba logiczna (rodzaj złośliwego oprogramowania)

M

machine learning – uczenie maszynowe
maintenance – utrzymanie, opieka, konserwacja, utrzymanie ruchu
malware – złośliwe oprogramowanie
man in the middle (MITM) – człowiek wewnątrz/pośrodku, atak podsłuchowy
management information system (MIS) – system zarządzania informacjami w ramach organizacji
masquerade attack – atak maskaradowy
metadata – metadane
microservice – mikroserwis
Military Deception (MILDEC) – dezinformacja wojskowa
mirroring – dyski lustrzane
monitoring – monitorowanie
Multi-Factor Authentication (MFA) – wieloczynnikowe uwierzytelnianie
Multilevel Security (MLS) – wielopoziomowe zabezpieczenia, wiele poziomów zabezpieczeń
mutual authentication – wzajemne potwierdzenie tożsamości

N

National Institute of Standards and Technology (NIST) – Narodowy Instytut Standardów i Technologii (USA)
NATO Cooperative Cyber Defence Center of Excellence (CCDCOE) – Centrum Doskonalenia Cyberobrony NATO
need to know principle – zasada wiedzy koniecznej
network – sieć
Network Address Translation (NAT) – translacja adresów sieciowych
network sniffing – węszenie w sieci, badanie sieci przez użytkownika, który nie powinien mieć do niej dostępu
node – węzeł

non-disclosure agreement (also nondisclosure agreement, confidentiality agreement, NDA) – umowa o zachowaniu poufności
non-repudiation – niezaprzeczalność

O

obfuscation – zamaskowanie, utajnienie, zaciemnianie
open source software – oprogramowanie o otwartym źródle
Open-Source Intelligence (OSINT) – wywiad jawnoźrodłowy
Operations Security (OpSec) – bezpieczeństwo operacyjne
outside threat (also external threat) – zagrożenie zewnętrzne
overload – przeładowanie, nadmiar informacji

P

packet filter – program typu zapora sieciowa
packet sniffer – oprogramowanie służące do podsłuchiwania w sieci
Pan European Game Information (PEGI) – ogólnoeuropejski system klasyfikacji gier
parental controls – środki kontroli rodzicielskiej
passive attack – atak pasywny (napastnik nie ingeruje w transmisję)
passphrase – hasło frazowe (hasło składające się z kilku słów)
password – hasło
password cracking – łamanie haseł
password generator – generator haseł
password manager – menadżer haseł
patch management – zarządzanie aktualizacjami
patch – potocznie łatka, poprawka/ulepszenie programu
Payment Initiation Services (PIS) – usługa inicjowania płatności
penetration test – test penetracyjny, kontrolowane włamanie mające na celu ujawnienie podatności i słabych punktów systemu
Personal Identifiable Information (PII) – informacje pozwalające zidentyfikować osobę fizyczną
Personal Identification Number (PIN) – osobisty numer identyfikacyjny
personnel security – bezpieczeństwo osobowe, bezpieczeństwo personelu
pharming – tworzenie fałszywych stron internetowych, podszywających się pod prawdziwe serwisy w celu kradzieży danych
phishing – potocznie łowienie ryb, rodzaj ataku socjotechnicznego dążącego do wyłudzenia danych bądź wymuszenia określonej aktywności ze strony ofiary
physical controls – fizyczne środki bezpieczeństwa
physical layer – warstwa fizyczna
Plan of Actions and Milestones (POA&M) – plan działań i kamienie milowe
Platform-as-a-Service (PaaS) – platforma jako usługa
policy management – zarządzanie politykami/procedurami (tworzenie, komunikacja, utrzymywanie polityk i procedur)
port scan – skanowanie portów
port scanner – oprogramowanie służące do skanowania portów

portable device – urządzenie przenośne/ podręczne
portal – portal (internetowy), strona internetowa
post-quantum cryptography – kryptografia postkwantowa
primary volumes – dyski źródłowe
privacy – prywatność
privilege – przywilej, uprawnienie
protection of industrial property – ochrona własności przemysłowej
protection profile – profil ochrony
proxy server – serwer pośredniczący
pseudonymous – pod pseudonimem
pseudonym – pseudonim
public data – publiczne dane (informacje skierowane do szerszego grona osób)
public domain software – oprogramowanie ogólnodostępne
public-key cryptography (asymmetric cryptography) – kryptografia klucza publicznego
Public-Private Partnership (cPPP) – partnerstwo publiczno-prywatne
quarantine – kwarantanna

R

Random Number Generator (RNG) – generator liczb losowych
ransomware – oprogramowanie, które blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych
read access – dostęp do danych obejmujący jedynie wgląd
Real-Time Monitoring – monitorowanie w czasie rzeczywistym
reconnaissance – rozpoznanie (np. rejonu), zwiad, rekonesans
records – archiwum, zapisy, rejestry, dokumentacja (czegoś)
Recovery Time Objective (RTO) – docelowy czas odzyskania
Red Team – zespół czerwony (jego celem jest kontrolowane atakowanie organizacji w celu identyfikacji słabych punktów)
redundancy – nadmiarowość, zdublowanie krytycznych elementów
registry – rejestr
reliability – wiarygodność
remediation – poprawa jakości, korekcja, wyrównanie
remote – zdalny, na odległość
remote access – zdalny dostęp
Remote Desktop Protocol (RDP) – protokół pulpitu zdalnego (pozwalający na komunikację z usługą terminala graficznego w Microsoft Windows)
remote maintenance – zdalna opieka i utrzymanie
remote work (also telecommuting, telework) – praca zdalna
reporting – raportowanie
resource access – dostęp do zasobów
responding – odpowiadanie, reagowanie
revalidation – rewalidacja, przedłużenie
reverse engineering – inżynieria wsteczna, metoda projektowania oparta na analizie konstrukcji

risk based approach – podejście oparte na ryzyku
rogue device – urządzenie znajdujące się poza kontrolą organizacji
Role-Based Access Control (RBAC) – kontrola dostępu oparta na rolach
Root Cause Analysis (RCA) – analiza przyczyn źródłowych
router – ruter

S

sandboxing – piaskownica, bezpieczne środowisko (mechanizm izolacji uruchamianych programów komputerowych od reszty systemu służący poprawie bezpieczeństwa)
sanitization – higiena, warunki sanitarne
scam – przekręt, oszustwo
scenario – scenariusz, przewidywany rozwój wypadków
screen scraper – narzędzie do wydobywania danych
script kiddie – skryptowy dzieciak (początkujący, domorosły haker)
secondary volumes – dyski docelowe
secret – tajemnica
secret know-how – poufna wiedza specjalistyczna
secure internet access – bezpieczny dostęp do Internetu
secure network engineering – bezpieczna architektura sieciowa
secure-by-default – domyślne bezpieczeństwo
secure-by-design – bezpieczeństwo wpisane w rozwój produktu lub usług
security assessment – ocena bezpieczeństwa
security audit – audyt bezpieczeństwa
security awareness training – szkolenia z zakresu świadomości w obszarze bezpieczeństwa
security control – środek bezpieczeństwa, środek mitygujący ryzyko, zabezpieczenie
security documentation – dokumentacja bezpieczeństwa
security incident – incydent bezpieczeństwa
Security Information and Event Management (SIEM) – Informacje Dotyczące Bezpieczeństwa i Zarządzanie Zdarzeniami
security information management (SIM) – zarządzanie bezpieczeństwem informacji
Security Operations Center (SOC) – (operacyjne) centrum bezpieczeństwa
security perimeter – strefa bezpieczeństwa
security policy – polityka bezpieczeństwa
security posture – stan zabezpieczeń (np. urządzeń, informacji przez atakami hakerskimi)
sensitive information – dane wrażliwe, informacje wymagające szczególnej ochrony
separation of duty – separacja obowiązków
Service-Oriented Architecture (SOA) – architektura zorientowana na usługi (koncepcja)
Short Message Service (SMS) – krótka wiadomość tekstowa
Signals Intelligence (SIGINT) – wywiad sygnałowy
situational awareness – świadomość sytuacyjna
smart cities – inteligentne miasta
social engineering – inżynieria społeczna, socjotechnika
social media (SM) – media społecznościowe
Software-as-a-Service (SaaS) – oprogramowanie jako usługa

source port – port źródłowy
spear phishing – ukierunkowany atak phishingowy
spyware – oprogramowanie szpiegujące
steganography – steganografia
Storage Area Network (SAN) – organizacja pamięci masowych w strukturę sieciową
strong customer authentication (SCA) – silne uwierzytelnianie klienta
Supervisory Control and Data Acquisition (SCADA) – system informatyczny nadzorujący przebieg procesu technologicznego lub produkcyjnego
supply chain – łańcuch dostaw
supply chain attacks – ataki na łańcuchy dostaw (np. producentów oprogramowania)
switch – przełącznik
synchronization – synchronizacja
system and services acquisition – pozyskiwanie systemów i usług
system hardening – wzmacnianie systemu (np. przez redukcję podatności)
system reliability – niezawodność systemu
System Security Officer (SSO) – inspektor zabezpieczenia systemu

T

Targeted Persistent Threats (TPT) – ukierunkowane trwałe zagrożenia
technical controls – techniczne środki bezpieczeństwa
telecommunications – telekomunikacja, łączność
test and evaluation – testowanie i ocena
The European Union Agency for Cybersecurity (ENISA) – Agencja Unii Europejskiej ds. Cyberbezpieczeństwa
threat – zagrożenie
threat actor – zagrażający podmiot/ aktor
threat analysis – analiza zagrożeń
threat hunting – polowanie na zagrożenia, tropienie zagrożeń (proaktywne podejście do zarządzania ryzykiem)
time bomb – tykająca bomba, bomba zegarowa
to abort – anulować, przerwać, zatrzymać
to archive – archiwizować
to audit – audytować
to caveat – zgłosić sprzeciw, zastrzeżenie
to investigate – prowadzić dochodzenie/postępowanie wyjaśniające
to overload –przeciążać, przeładowywać
to patch – łatać
to quarantine – poddawać kwarantannie
to restore – przywrócić, odbudować
trade secret – tajemnica przedsiębiorstwa
trojan horse – koń trojański
Two Factor Authenticaton (2FA) – uwierzytelnianie dwuskładnikowe
unauthorized access – nieautoryzowany dostęp

U

Uniform Resource Locator (URL) – jednolity lokalizator zasobów
user – użytkownik
user account – konto użytkownika
user authentication – uwierzytelnienie, potwierdzenie tożsamości użytkownika
user identifier (ID) – identyfikator użytkownika, login

V

virtual crime – przestępczość wirtualna
virtual machine – maszyna wirtualna
Virtual Private Network (VPN) – wirtualna sieć prywatna
virtualisation – wirtualizacja
virus – złośliwe oprogramowanie, wirus
vulnerability – podatność

W

watering hole attack – taktyka wodopoju (atak na najczęściej odwiedzane przez pracowników danej organizacji serwisy internetowe)
weak password – słabe hasło
Web Application Firewall (WAF) – zapora aplikacji sieci Web
whaling – forma phishingu ukierunkowana na wysoko postawione osoby
white hat (hacker) – haker kierujący się dobrymi intencjami (włamujący się do systemów i sieci celem doskonalenia ich bezpieczeństwa)
whitelist – biała lista, lista podmiotów/ elementów, które mają uprawnienia
Wide Area Network (WAN) – rozległa sieć komputerowa
Wireless Local Area Network (WLAN) – bezprzewodowa sieć lokalna
worm – robak

Z

Zachman Framework – Siatka Zachmana (siatka do opisu architektury systemów informatycznych)
zero day attack – atak dnia zerowego (rodzaj exploita)
zeroisation – zerowanie (w kryptografii usuwanie wrażliwych danych)
zombie – potocznie zainfekowane urządzenie wykonujące polecania osoby go kontrolującej