1. Disaster Recovery (Odzyskiwanie po Awarii): To proces przywracania danych i operacji informatycznych organizacji po poważnym zakłóceniu, takim jak katastrofa naturalna, atak hakerski lub awaria techniczna. Plan odzyskiwania po awarii obejmuje procedury i narzędzia niezbędne do szybkiego przywrócenia funkcjonalności systemów.
2. Security by Design (Bezpieczeństwo przez Projektowanie): To podejście do projektowania systemów i aplikacji, które uwzględnia bezpieczeństwo na każdym etapie procesu tworzenia, od początku aż do końca. Celem jest zbudowanie systemów odpornych na ataki i usterki już od podstaw.
3. Bezpieczeństwo Informacji: Jest to praktyka ochrony informacji przed nieautoryzowanym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zakłóceniem. Obejmuje zarówno bezpieczeństwo cyfrowe, jak i fizyczne.
4. Szyfrowanie: Metoda ochrony poufności danych poprzez ich konwersję z formatu zrozumiałego (tekst jawny) na format zakodowany (szyfrogram), który jest niezrozumiały bez odpowiedniego klucza do deszyfrowania.
5. Haker: Osoba posiadająca zaawansowaną wiedzę i umiejętności w dziedzinie technologii komputerowych i sieci, która może być wykorzystywana zarówno w legalnych (tzw. etyczny haker), jak i nielegalnych celach (haker atakujący systemy).
6. Złośliwe Oprogramowanie (Malware): Obejmuje wszelkiego rodzaju złośliwe programy, takie jak wirusy, trojany, robaki, spyware czy ransomware, które mają za zadanie uszkodzić system, kraść dane, zakłócać działanie lub uzyskać nieautoryzowany dostęp do systemów.
7. Phishing: Metoda cyberataków polegająca na podszywaniu się, często przez email, pod zaufaną osobę lub instytucję, w celu wyłudzenia poufnych informacji, takich jak hasła czy dane karty kredytowej.
8. DDoS (Distributed Denial of Service): Atak polegający na zalewaniu serwisu internetowego ogromną ilością ruchu z wielu źródeł jednocześnie, co prowadzi do przeciążenia i unieruchomienia serwisu.
9. Firewall (Zapora sieciowa): Urządzenie lub oprogramowanie służące do monitorowania i kontrolowania przychodzącego i wychodzącego ruchu sieciowego na podstawie zdefiniowanych zasad bezpieczeństwa, służące jako bariera między zaufaną siecią wewnętrzną a niezaufaną siecią zewnętrzną, jak Internet.
10. Uwierzytelnianie: Proces weryfikacji tożsamości użytkownika, zazwyczaj poprzez wymaganie od użytkownika podania nazwy użytkownika i hasła. Może także obejmować inne metody, takie jak uwierzytelnianie dwuskładnikowe lub biometria.
11. Wyciek Danych (Data Breach): Zdarzenie, w którym poufne, chronione lub wrażliwe dane są wydobywane, kopiowane, przekazywane lub używane przez osobę nieupoważnioną do tego.
12. VPN (Virtual Private Network): Technologia tworzenia wirtualnej sieci prywatnej poprzez połączenie z zaszyfrowanym kanałem komunikacyjnym w ramach publicznej sieci (takiej jak Internet), umożliwiająca bezpieczny transfer danych i anonimowość użytkownika.
13. Incident Bezpieczeństwa: To każde zdarzenie, które narusza zasady bezpieczeństwa lub powoduje nieautoryzowany dostęp do systemów informatycznych. Może to obejmować ataki hakerskie, wycieki danych, naruszenia integralności systemu lub wszelkie inne działania, które zagrażają bezpieczeństwu informacji.
14. Kryptografia: Jest to nauka i praktyka zabezpieczania komunikacji przez szyfrowanie informacji, czyli przekształcanie danych w taki sposób, aby tylko uprawnione strony mogły

je odczytać. Wykorzystuje algorytmy matematyczne do szyfrowania i deszyfrowania danych.

15. Polityka Bezpieczeństwa: Jest to zbiór zasad, procedur i standardów stosowanych w organizacji do zarządzania i ochrony informacji. Polityka ta określa, jakie informacje są ważne, jak powinny być chronione i jakie działania należy podjąć w przypadku naruszenia bezpieczeństwa.
16. Analiza Ryzyka: Proces identyfikowania, oceniania i priorytetyzowania ryzyk związanych z bezpieczeństwem informacji. Pomaga w określeniu potencjalnych zagrożeń dla zasobów informacyjnych i wdrażaniu odpowiednich środków zaradczych.
17. Testy Penetracyjne: Metoda oceny bezpieczeństwa systemu informatycznego poprzez symulowanie ataku z zewnątrz lub wewnątrz organizacji. Celem jest znalezienie słabości, które mogą być wykorzystane przez cyberprzestępców.
18. ISO/IEC 27001: Międzynarodowy standard określający wymagania dotyczące systemu zarządzania bezpieczeństwem informacji (ISMS). Pomaga organizacjom w zabezpieczaniu ich informacji w sposób systematyczny i ciągły.
19. CISSP (Certified Information Systems Security Professional): Jest to prestiżowe międzynarodowe świadectwo kompetencji w dziedzinie bezpieczeństwa informacji, oferujące potwierdzenie umiejętności i wiedzy w tej dziedzinie.
20. Atak Man-in-the-Middle (MitM): Rodzaj ataku cybernetycznego, w którym atakujący umieszcza się pomiędzy dwiema komunikującymi się stronami i przechwytuje lub manipuluje przesyłanymi danymi.
21. Social Engineering: Techniki manipulacyjne wykorzystywane przez cyberprzestępców do oszukania użytkowników i skłonienia ich do ujawnienia poufnych informacji, takich jak hasła lub dane bankowe.
22. Zero Trust: Model bezpieczeństwa, który zakłada, że żadnej jednostce wewnętrznej lub zewnętrznej nie można ufać domyślnie. Wszystkie próby dostępu do systemów i danych muszą być ściśle weryfikowane.
23. Multi-Factor Authentication (MFA): Metoda weryfikacji tożsamości użytkownika, która wymaga więcej niż jednego dowodu tożsamości, zwykle połączenia czegoś, co użytkownik wie (np. hasło), czegoś, co użytkownik ma (np. token lub telefon komórkowy), i/lub czegoś, czym użytkownik jest (biometria).
24. Kontrola Dostępu: Procesy i technologie używane do zarządzania dostępem do zasobów w organizacji, w tym do systemów informatycznych, aplikacji i danych.
25. Bezpieczeństwo Fizyczne: Odnosi się do ochrony fizycznych systemów informatycznych, urządzeń i infrastruktury przed uszkodzeniem, kradzieżą lub dostępem nieautoryzowanych osób.
26. Zarządzanie Ryzykiem (Risk Management): Proces identyfikowania, oceniania i kontroli ryzyka związanego z informacjami. Obejmuje identyfikację potencjalnych zagrożeń dla informacji i wdrażanie strategii mających na celu minimalizację negatywnego wpływu tych zagrożeń.
27. Compliance (Zgodność): Proces zapewnienia, że organizacja przestrzega obowiązujących przepisów, standardów i polityk, szczególnie tych dotyczących bezpieczeństwa danych i prywatności. Obejmuje zrozumienie i stosowanie się do wymogów prawnych i regulacyjnych.
28. Cyberhigiena: Praktyki i nawyki, które pomagają w utrzymaniu bezpieczeństwa danych i urządzeń. Obejmuje regularne aktualizacje oprogramowania, stosowanie silnych haseł,

regularne tworzenie kopii zapasowych danych i świadome korzystanie z zasobów internetowych.

29. SOC (Security Operations Center): Specjalistyczne centrum operacji, którego zadaniem jest monitorowanie, analiza i ochrona przed zagrożeniami cybernetycznymi w czasie rzeczywistym. SOC stanowi centralny punkt dla działań związanych z bezpieczeństwem informacji w organizacji.
30. Luka Bezpieczeństwa (Vulnerability): Słabość w systemie informatycznym, procedurach, projektowaniu lub wewnętrznych kontrolach, która może być wykorzystana przez zagrożenie do naruszenia bezpieczeństwa systemu.
31. SIEM (Security Information and Event Management): Rozwiązanie technologiczne służące do zbierania, analizowania i prezentowania danych związanych z bezpieczeństwem z różnych źródeł. Pomaga w szybkiej detekcji i reagowaniu na incydenty bezpieczeństwa.
32. End-point Security: Ochrona punktów końcowych sieci, takich jak komputery, smartfony i inne urządzenia, przed zagrożeniami i atakami. Obejmuje stosowanie antywirusów, zapor ogniowych, narzędzi do wykrywania i reagowania na zagrożenia.
33. Patch Management: Proces zarządzania aktualizacjami oprogramowania, w tym instalacją łatek bezpieczeństwa, które naprawiają znane luki i słabości w systemach i aplikacjach.
34. IDS (Intrusion Detection System): System wykrywający próby nieautoryzowanego dostępu lub naruszenia systemu informatycznego. Monitoruje ruch sieciowy i analizuje go pod kątem oznak naruszenia.
35. IPS (Intrusion Prevention System): Rozwiązanie służące nie tylko do wykrywania prób naruszenia, ale również do aktywnego zapobiegania tym próbom poprzez blokowanie potencjalnie szkodliwego ruchu.
36. Threat Intelligence (Wywiad w Zakresie Zagrożeń): Informacje wykorzystywane do identyfikowania, oceny i reagowania na cyberzagrożenia. Umożliwia lepsze zrozumienie natury zagrożeń i pomaga w ich efektywnym zwalczaniu.
37. Tokenization: Proces zamiany wrażliwych danych na unikalny identyfikator, czyli token, który nie ma eksploatacyjnej wartości. Jest to technika wykorzystywana do ochrony danych, szczególnie w transakcjach płatniczych.
38. Secure Code (Bezpieczny Kod): Praktyka pisania oprogramowania w taki sposób, aby było ono odporne na ataki. Obejmuje stosowanie technik programowania zapobiegających wadom bezpieczeństwa.
39. Incident Response (Reagowanie na Incydenty): Zorganizowany proces reagowania na incydenty bezpieczeństwa, obejmujący identyfikację, analizę, przeciwdziałanie i raportowanie incydentów, aby zminimalizować ich wpływ i zapobiec powtórzeniu się w przyszłości.
40. Cyber Resilience (Odporność Cybernetyczna): Zdolność organizacji do przygotowania się na, reagowania na oraz adaptowania się do zmian i wyzwań w środowisku cybernetycznym, w tym umiejętność skutecznego odzyskiwania po cyberatakach czy innych zakłóceniach.
41. Modelowanie Zagrożeń (Threat Modeling): To proces identyfikowania potencjalnych zagrożeń, które mogą wpłynąć na system informatyczny. Modelowanie zagrożeń pomaga zrozumieć, gdzie mogą wystąpić słabości systemu i jakie są potencjalne skutki ataków. Wykorzystuje się je do projektowania systemów odpornych na ataki poprzez zastosowanie odpowiednich środków obronnych.

42. Szkolenia z Świadomości Bezpieczeństwa (Security Awareness Training): To programy edukacyjne mające na celu zwiększenie świadomości pracowników na temat zagrożeń cybernetycznych oraz nauczenie ich, jak rozpoznawać i reagować na różne formy ataków, takie jak phishing, malware czy inżynieria społeczna.

43. Ocena Podatności (Vulnerability Assessment): Jest to proces identyfikacji, klasyfikacji i priorytetyzacji słabości w systemach informatycznych. Oceny te mają na celu znalezienie luk w zabezpieczeniach, które mogą być wykorzystane przez atakujących do uzyskania nieautoryzowanego dostępu do systemu lub danych.

44. Cyber Threat Intelligence (CTI): Odnosi się do informacji używanych do rozumienia zagrożeń cybernetycznych, które mogą mieć wpływ na organizację. CTI obejmuje analizę trendów, taktyk, technik i procedur stosowanych przez cyberprzestępców, co pomaga w przewidywaniu i zapobieganiu atakom.

45. Data Encryption Standard (DES): To szyfr blokowy, który był jednym z pierwszych standardów szyfrowania przyjętych na szeroką skalę. DES jest teraz uważany za przestarzały ze względu na krótki klucz (56-bitowy), co sprawia, że jest podatny na ataki brute-force.

46. Security Posture: To ogólny stan bezpieczeństwa organizacji, w tym jej zdolność do ochrony przed atakami oraz szybkiego reagowania na incydenty. Obejmuje to zarówno aspekty techniczne, jak i organizacyjne, takie jak polityki bezpieczeństwa, procedury, narzędzia obronne i świadomość personelu.

47. Intrusion Response Plan: Plan odpowiedzi na incydenty, który określa, jak organizacja będzie reagować na wykrycie nieautoryzowanego dostępu do swoich systemów. Plan ten powinien obejmować procedury identyfikacji, oceny, izolacji, usuwania zagrożeń oraz przywracania normalnej działalności.

48. Klasyfikacja Danych (Data Classification): To proces organizowania danych w kategorie na podstawie ich wrażliwości i znaczenia. Dzięki temu można zastosować odpowiednie środki ochrony dla różnych typów danych, takie jak dane osobowe, poufne informacje biznesowe czy dane publiczne.

49. Analiza Kryminalistyczna (Forensic Analysis): To proces badania cyfrowych dowodów po incydencie cybernetycznym. Analiza ta pomaga w ustaleniu, co dokładnie się stało, jak doszło do naruszenia bezpieczeństwa, kto jest odpowiedzialny oraz jakie mogą być długoterminowe skutki ataku.