CYBERVEILIGHEID
WOORDENLIJST

100 Essentiële Cyberveiligheidstermen

Erasmus+ KA210-ADU Project
2023-1-TR01-KA210-ADU-000165733

BEDREIGINGEN - Schadelijke Software

1. **Virus** - Schadelijke software die computers infecteert en zichzelf vermenigvuldigt.
2. **Worm** - Zelfvermenigvuldigende malware die automatisch via netwerken verspreidt.
3. **Trojaans Paard** - Malware vermomd als legitieme software die schadelijke acties uitvoert.
4. **Ransomware** - Malware die bestanden versleutelt en betaling eist voor ontsleuteling.
5. **Spyware** - Software die stiekem gebruikersinformatie en activiteiten verzamelt.
6. **Adware** - Software die ongewenste advertenties toont en browsers vertraagt.
7. **Rootkit** - Malware die diep in het systeem verborgen is voor volledige controle.
8. **Keylogger** - Software die toetsaanslagen registreert om wachtwoorden te stelen.
9. **Botnet** - Netwerk van geïnfecteerde computers op afstand bestuurd door hackers.
10. **Malware** - Algemene term voor schadelijke software zoals virussen, wormen, trojans.
11. **Zero-Day** - Nieuw ontdekte beveiligingskwetsbaarheid zonder beschikbare patch.
12. **Exploit** - Code of techniek die misbruik maakt van beveiligingskwetsbaarheden.
13. **Backdoor** - Verborgen toegangspunt voor ongeautoriseerde toegang tot een systeem.
14. **RAT** - Remote Access Trojan. Maakt volledige afstandsbediening mogelijk.
15. **Cryptojacking** - Ongeautoriseerd gebruik van computers voor cryptocurrency mining.
16. **Scareware** - Valse beveiligingswaarschuwingen om gebruikers bang te maken.
17. **Logic Bomb** - Schadelijke code die activeert bij specifieke voorwaarden.
18. **Fileless Malware** - Malware die in geheugen werkt zonder bestanden achter te laten.
19. **Dropper** - Programma ontworpen om andere malware te downloaden en installeren.

20 **Wiper** - Malware die gegevens permanent vernietigt zonder herstelmogelijkheid.

AANVALLEN - Cyberaanvaltechnieken

21 **Phishing** - Frauduleuze pogingen om informatie te stelen via valse e-mails of sites.

22 **Smishing** - Phishing-aanval uitgevoerd via SMS-tekstberichten.

23 **Vishing** - Voice phishing-aanval uitgevoerd via telefoongesprekken.

24 **Spear Phishing** - Gerichte phishing-aanval op specifieke personen of organisaties.

25 **Whaling** - Phishing-aanval specifiek gericht op topmanagers.

26 **DDoS** - Distributed Denial of Service. Aanval van meerdere bronnen.

27 **DoS** - Denial of Service. Aanval die een systeem onbeschikbaar maakt.

28 **Man-in-the-Middle** - Aanval die stiekem communicatie tussen twee partijen onderschept.

29 **SQL Injection** - Aanval die schadelijke SQL-code in databasequery's invoegt.

30 **XSS** - Cross-Site Scripting. Schadelijke scripts injecteren in websites.

31 **Brute Force** - Aanval die alle mogelijke wachtwoordcombinaties systematisch probeert.

32 **Dictionary Attack** - Aanval met een lijst van veelvoorkomende wachtwoorden.

33 **Credential Stuffing** - Gestolen inloggegevens gebruiken op andere sites.

34 **Session Hijacking** - Een actieve sessie overnemen voor ongeautoriseerde toegang.

35 **DNS Spoofing** - DNS-records manipuleren om gebruikers naar valse sites te leiden.

36 **ARP Spoofing** - ARP-tabellen manipuleren om netwerkverkeer te onderscheppen.

37 **Pharming** - Gebruikers omleiden naar frauduleuze websites via DNS-manipulatie.

38 **Social Engineering** - Mensen psychologisch manipuleren om informatie te onthullen.

39 **Baiting** - Slachtoffers lokken met beloftes van gratis items of beloningen.

40 **Pretexting** - Een vals scenario creëren om vertrouwen te winnen en info te krijgen.

BESCHERMING - Beveiligingsmaatregelen

41 **Antivirus** - Beveiligingssoftware die schadelijke programma's detecteert en verwijdert.

42 **Firewall** - Beveiligingssysteem dat netwerkverkeer bewaakt en controleert.

43 **2FA** - Tweefactorauthenticatie. Extra beveiligingsverificatielaag.

44 **MFA** - Multi-Factor Authenticatie. Meerdere verificatiemethoden.

45 **Versleuteling** - Gegevens omzetten in onleesbare code ter bescherming. Encryption.

46 **SSL/TLS** - Protocollen die internetverkeer versleutelen voor veilige verbindingen.

47 **HTTPS** - Veilig HTTP-protocol met versleutelde webverbindingen.

48 **VPN** - Virtual Private Network. Versleutelt en anonimiseert internetverkeer.

49 **Back-up** - Kopieën van gegevens maken ter bescherming tegen verlies.

50 **Update** - Software actueel houden om beveiligingslekken te dichten.

51 **Wachtwoordbeheerder** - Applicatie die wachtwoorden veilig opslaat en beheert.

52 **Sandbox** - Geïsoleerde omgeving voor veilig testen van verdachte bestanden.

53 **IDS** - Intrusion Detection System. Bewaakt op verdachte activiteiten.

54 **IPS** - Intrusion Prevention System. Detecteert en blokkeert aanvallen.

55 **WAF** - Web Application Firewall. Beschermt webapplicaties.

56 **Endpoint Security** - Bescherming voor computers en apparaten op een netwerk.

57 **Zero Trust** - Beveiligingsaanpak: nooit vertrouwen, altijd verifiëren.

58 **Patch** - Software-update die bugs en beveiligingsfouten repareert.

59 **Whitelist** - Alleen goedgekeurde applicaties of adressen toestaan.

60 **Blacklist** - Bekende schadelijke sites of software blokkeren.

TOOLS - Technologie & Infrastructuur

61 **IP-adres** - Unieke numerieke identificatie voor apparaten op internet.

62 **MAC-adres** - Uniek fysiek adres van een netwerkinterfacekaart.

63 **DNS** - Domain Name System. Vertaalt domeinnamen naar IP-adressen.

64 **Router** - Apparaat dat netwerkverkeer tussen netwerken stuurt.

65 **Proxy** - Tussenliggende server die internetverzoeken doorstuurt.

66 **Poort** - Virtueel verbindingspunt voor netwerkcommunicatie.

67 **Protocol** - Regels voor communicatie tussen apparaten. HTTP, FTP, TCP.

68 **Cookie** - Kleine gegevensbestanden opgeslagen door websites in uw browser.

69 **Cache** - Tijdelijke opslag van gegevens voor snellere toegang.

70 **Token** - Digitale sleutel gebruikt voor authenticatiedoeleinden.

71 **Hash** - Vaste-lengte waarde gegenereerd uit gegevens. Digitale vingerafdruk.

72 **API** - Application Programming Interface. Maakt softwarecommunicatie mogelijk.

73 **Cloud** - Externe serverdiensten toegankelijk via internet.

74 **Metadata** - Gegevens die informatie over andere gegevens verstrekken.

75 **Bandbreedte** - Gegevensoverdrachtskapaciteit van een netwerkverbinding.

76 **Latency** - Vertragingstijd bij gegevensoverdracht.

77 **Ping** - Commando om netwerkconnectiviteit te testen.

78 **Traceroute** - Tool die het pad toont dat datapakketten afleggen.

79 **Tor** - Netwerk dat anoniem internetten mogelijk maakt.

80 **Dark Web** - Verborgen deel van internet toegankelijk met speciale software.

CONCEPTEN - Fundamentele Kennis

81 **Cyberveiligheid** - Praktijk van het beschermen van digitale systemen en gegevens.

82 **Datalek** - Ongeautoriseerde toegang tot gevoelige of vertrouwelijke gegevens.

83 **Identiteitsdiefstal** - Iemands persoonlijke informatie stelen voor frauduleus gebruik.

84 **Spam** - Ongewenste bulk-e-mails of berichten.

85 **CAPTCHA** - Test om mensen van geautomatiseerde bots te onderscheiden.

86 **Privacy** - Bescherming van persoonlijke informatie tegen ongeautoriseerde toegang.

87 **Anoniem** - Een onbekende of verborgen identiteit online hebben.

88 **Open Source** - Software met publiekelijk beschikbare broncode.

89 **Penetratietest** - Geautoriseerde gesimuleerde aanval om beveiliging te testen.

90 **Kwetsbaarheid** - Zwakte in een systeem die kan worden misbruikt.

91 **Risico** - Beoordeling van potentiële bedreigingen en hun impact.

92 **Compliance** - Naleving van beveiligingsstandaarden en regelgeving.

93 **GDPR** - Algemene Verordening Gegevensbescherming. EU-privacywetgeving.

94 **Cyberaanval** - Opzettelijke poging om digitale systemen te beschadigen.

95 **Hacker** - Persoon die inbreekt in computersystemen. Ethisch of kwaadaardig.

96 **White Hat** - Ethische hacker die beveiliging test met toestemming.

97 **Black Hat** - Kwaadaardige hacker die illegaal systemen binnendringt.

98 **Bug Bounty** - Programma dat mensen beloont voor het vinden van kwetsbaarheden.

99 **Digitale Voetafdruk** - Sporen en gegevens achtergelaten door internetactiviteiten.

100 **Cyberhygiëne** - Best practices voor het handhaven van digitale beveiliging.

De steun van de Europese Commissie voor de productie van deze publicatie houdt geen goedkeuring van de inhoud in, die alleen de mening van de auteurs weergeeft, en de Commissie kan niet verantwoordelijk worden gehouden voor enig gebruik van de informatie die erin is vervat.