Appendiks 11. Ordliste – eksempler på udvalgte ord og begreber inden for cybersikkerhed

Active Directory (AD): Er den centrale bruger- og rettighedsdatabase i et Windows netværk der bl.a. indeholder informationer om computere, ressourcer, brugere og password og godkender login til systemerne. Ved et angreb vil hackerne gå målrettet efter at få administrator rettigheder til Active Directory (AD). Derfor er det vigtigt at overvåge.

Botnet: Et botnet er et netværk af kompromitterede computere, der styres af en tredjepart. Et botnet bliver skabt ved, at computere med internetadgang bliver inficeret med malware, hvorefter den, der kontrollerer botnettet, kan anvende det til f.eks. at udføre DDoS-angreb, phishing-angreb (spam), distribuere malware, mine bitcoins osv.

CEO fraud: "Direktørbedrageri" der går ud på at franarre en virksomhed oplysninger eller udbetale penge ved at udgive sig som direktør af virksomheden. Anvender ofte (spear)phishing-teknikker (f.eks. e-mail) og social engineering.

DDoS-angreb: Står for Distributed Denial of Service og er et overbelastningsangreb. Hackere udnytter kompromitterede computere (et botnet) til at generere usædvanligt store mængder datatrafik mod en hjemmeside (webserver) eller et netværk, så hjemmesiden eller netværket ikke er tilgængeligt for legitim trafik, mens angrebet står på.

Drive-by exploits: Et udtryk for, at den ramte virksomhed ikke var målet for kampagnen, men blot blev ramt ved et hændeligt uheld.

Logs: De informationer som IT-systemer kan konfigureres til at opsamle om forskellige former for aktiviteter, herunder sikkerhedshændelser. Som udgangspunkt gemmes logs lokalt på systemet, hvilket er problematisk da en angriber som det første vil søge at slette loggen for at skjule deres spor.

Log-management system: En centraliseret teknisk løsning som opsamler og sikre logs fra mange forskellige IT-systemer. Virksomheden kan enten selv have et log-management system eller købe det som en service der leveres via Internettet.

Malware: Malware betyder malicious software og er en betegnelse for computerprogrammer, der gør ondsindede, skadelige eller uønskede ting der, hvor de er installeret. Begrebet dækker over alle kategorier af skadelige programmer herunder virus og orme som f.eks. spyware, ransomware, botnets og trojanske heste. Antivirusprogrammer bekæmper som oftest ikke kun vira, men flere forskellige typer malware.

Man-in-the-middle: Angreb, hvor en skadelig enhed eller person placerer sig mellem to enheder, eksempelvis mellem brugeren og routeren. Dermed får mellemmanden adgang til al data, brugeren afsender.

Mass interception: Massiv overvågning af tele- og internetaktivitet, eksempelvis gennem logning af internetsessioner. Udføres af stater, men kan også ved hjælp af en ekstensive netværk af overvågningsprogrammer bruges af it-kriminelle til at indhente enorme mængder data om adfærd.

MSSP: En forkortelse for en Managed Security Service Provider, der er er en leverandør af sikkerhedsservices, typisk leveret over Internettet. I forbindelse med logning og overvågning vil en MSSP kunne levere en Managed SIEM og SOC-løsning, samt hjælpe med at reagere på hændelser.

Phishing/spear phishing: Phishing er forsøg på via social engineering at manipulere en person til i god tro at videregive personlige oplysninger eller klikke på inficerede filer eller links til falske hjemmesider. Phishing-mails sendes ofte bredt ud til mange modtagere. Spear phishing adskiller sig særligt ved at være målrettet den enkelte modtager og anvende teknikker fra social engineering. E-mails er typisk udformet, så de virker særligt relevante, overbeisende og troværdige for modtageren ved f.eks. at anvende navn, personspecifikke informationer eller relevante filer, der er opdaget ved forudgående rekognoscering.

Ransomware: Ved et ransomware-angreb bliver data og systemer på offerets computer holdt som gidsel, da de krypteres og derved bliver utilgængelige. Den ansvarelige bag angrebet kræver en løsesum typisk i form af kryptovaluta (f.eks. Bitcoin), for at give adgang til data igen. Som regel vil den ansvarlige bag angrebet installere malware ved hjælp af phishingmails. De fleste ransomware-angreb lykkes, fordi brugeren snydes til at klikke på et link eller en vedhæftet fil i en e-mail, men ransomware-angreb kan også ske via sms eller et reklamebanner på en hjemmeside. Der findes mange varianter af ransomware. Målrettede ransomwareangreb forsøger at ramme f.eks. administrative netværk i specifikke virksomheder og myndigheder.

SIEM: En forkortelse for et "Security Information and Event Management" system, der er en teknisk løsning, som udover opsamling af logs også sammenholder og analyserer logdata og sende alarmer ved mistænkelige aktiviteter. Virksomheden kan enten selv have en SIEM løsning eller købe det som en service der leveres via Internettet. Når et SIEM-system finder mistænkelige aktiviteter i logdata, bliver der genereret en alarm som derefter skal kvalificeres og analyseres dvs. det skal undersøges hvorvidt der er tale om en sikkerhedshændelse eller en falsk alarm.

SOC: En forkortelse for "Security Operation Center", der er en centraliseret funktion eller organisation der ved hjælp af mennesker, processer og teknologi overvåger og reagerer på sikkerhedshændelser. Dette kan bl.a. ske ved at overvåge og analyserer alarmer fra et SIEM systemer. Denne funktion kendes også under navne som Security Analytics Center (SAC) og Cyber Defense Center (CDC).

Social engineering: Et udtryk for, at man udnytter sociale interaktioner og psykiske kneb til at narre en person eller en virksomhed til at udlevere informationer, give adgang til systemer eller overføre penge til dem.

SQL injection: Angreb rettet mod databaselaget i software, som udnytter en sårbarhed i håndtering af input og databasekald. Databasekaldet manipuleres gennem inputtet (typisk ved brug af specialtegn) til at opnå en anden effekt end den tilsigtede - for eksempel at afsløre, hvem der har administratorrettigheder.

Se flere ordforklaringer på CFCS' hjemmeside: Ordforklaringer af begreber i cybersikkerhed (cfcs.dk)