BITPRO

IT-sikkerhetsordbok

A

Aksesskontroll	Regler og mekanismer som styrer hvilke brukere som har tilgang til hva.
Angrep	Uautorisert eller ondsinnet forsøk på å få tilgang til datasystemer, nettverk, applikasjoner eller digital informasjon.
Autentisering	Kontroll av at bruker er den de hevder å være før de gis tilgang til bestemte ressurser, tjenester eller informasjon.
Autentiserte identiteter	Brukere og enheter som allerede har blitt autentisert/identifisert som gyldige i systemet.
Autorisasjon	Tillatelsene en bruker/enhet har til å få tilgang til bestemte ressurser, tjenester eller informasjon.

B

Biometrisk autentisering	Bruk av fingeravtrykk, ansiktsgjenkjenning, øyescanning eller stemmegjenkjenning for å bekrefte en brukerens identitet.
Bluejacking	Uautorisert kommunikasjon som utnytter Bluetooth for å sende meldinger eller kontaktforespørsler til Bluetooth-enheter.
Botnet	Et nettverk av enheter som er infisert med ondsinnet programvare og dermed kan kontrolleres av ondsinnede aktører.
Brannmur	Sikkerhetsteknologi som overvåker og blokkere uønsket trafikk inn og ut av en bedrifts lokalt nettverk.
Brute Force Attack	Automatisert angrep som systematisk prøver alle mulige kombinasjoner av tegn og tall til den finner rett passord.

C

Cyber sikkerhet	Beskyttelse av enheter, nettverk, systemer, applikasjoner og data mot uautorisert tilgang, skade, tyveri eller misbruk.

D

Denial of Service (DoS)	Angrep med mål om å overvelde en tjeneste eller et nettverk, slik at det blir utilgjengelig for legitime brukere.

E

Eiendomsbasert autentisering	Bruk av fysiske gjenstander for å bekrefte identiteten til en bruker eller enhet.

BITPRO

F

Flerfaktor-autentisering	Benytter mer enn en faktor for å bekrefte identiteten og videre få tilgang til system, applikasjon eller tjeneste.

H

Hacking	Uautorisert tilgang til systemer, applikasjoner og enheter for å stjele eller forårsake forstyrrelser.
Hvitelisting	Sikkerhetspraksis der bare godkjente elementer eller enheter får tilgang til et system, et nettverk eller en resurs.

I

IKT-system	Enheter, programvarer og nettverk som brukes til å håndtere, lagre, overføre og behandle informasjon.
Incident Response Plan (IRP)	Plan som beskriver de nødvendige trinnene og prosedyrene for å håndtere og svare på sikkerhetsbrudd.
Informasjonssikkerhet	Beskyttelse av informasjon fra uautorisert tilgang, uønskede endringer, avsløringer, ødeleggelser eller forstyrrelser.
Inntrengingsdeteksjonssystem	Sikkerhetsteknologi som overvåker nettverkstrafikk og systemaktivitet for å identifisere mistenkelig aktivitet.
IT-sikkerhet	Beskyttelse av systemer, data, nettverk og digital informasjon mot uautorisert tilgang, skade eller uønskede hendelser.

K

Kunnskapsbasert autentisering	Informasjon som bare brukeren kjenne til, f.eks. passord, PIN-kode, svar på spørsmål eller annen informasjon.

L

Logic Bomb	Skadelige programvarer eller koder som aktiviseres når visse betingelser eller kriterier blir oppfylt.
Løsepengekrav	Filene er kryptert/utilgjengelig og offeret får et pengekrav fra angriperen for å gi tilbake kontrollen.
Løsepengevirus	En type malware som krypterer filene og gjør dem utilgjengelige, etterfulgt av et krav om løsepenger.

M

Malware	Virus, ormer, trojanere og ransomware utviklet for å infiltrere eller skade et datasystem.
Man-in-the-Middle	Uautorisert tredjepart posisjonerer seg mellom to parter i en kommunikasjon uten at partene har kjennskap til det.

BITPRO

O

Open Source Intelligence	Metode for innsamling, analyse og bruk av informasjon som er fritt tilgjengelig på offentlige kilder.

P

Packet Injection	Elementer som sendes inn i et nettverk for testing, overvåking eller angrepsformål.
Patch	Oppdatering av programvare/operativsystem for å løse utfordringer, feil, sårbarheter eller forbedre funksjonaliteten.
Pentesting	Kontrollert simulering av et angrep for å identifisere sårbarheter.
Phishing	Forsøk på å lure brukere til å gi fra seg sensitive data som passord, kredittkortinformasjon eller andre personopplysninger.
Policyer	Regler og retningslinjer som bestemmer hvilke aksjoner som er tillatt eller forbudt for ulike typer brukere.

R

Ransomware	En type malware som krypterer filene og gjør dem utilgjengelige, etterfulgt av et krav om løsepenger.
Replay Attack	Angriper gjenopptar eller "replayer" tidligere fanget kommunikasjon eller autentiseringsdata mellom toparter i et nettverk.
Ressurser	Alt som er relevant for aksesskontroll, inkludert filer, mapper, databaser, applikasjoner og nettverkstjenester.
Rettigheter	Spesifikke tillatelser som gir en bruker mulighet til å utføre bestemte handlinger eller aksessere ressurser.
Rootkit	Skadelig programvare som skjuler seg og skaper vedvarende og uoppdaget tilgang til et system eller et nettverk.
Rouge Access Point	Uautorisert og ondsinnet WiFi-punkt som er satt opp i et datanettverk.

S

Sikkerhetsbevissthet	Kunnskapen, forståelsen og oppmerksomheten enkeltpersoner og organisasjoner har rundt digital sikkerhet.
Sikkerhetsbrudd	Et vellykket forsøk på å omgå sikkerhetsmekanismer for å få uautorisert tilgang til systemer eller informasjon.
Sikkerhetsevaluering	Systematisk vurdering og analyse av et system, applikasjon, nettverk eller en organisasjons sikkerhetstilstand.
Sikkerhetshendelseshåndtering	Prosessen med å identifisere, evaluere og håndtere sikkerhetshendelser i en organisasjon.
Sikkerhetspolicy	Retningslinjer, regler og prosedyrer som beskriver rammeverket for digital sikkerhet i en organisasjon.
Security Operations Center (SOC)	Kontrollsenter/driftssenter som har ansvaret for overvåking, deteksjon, analyse og respons på trusler i sanntid.
Sosial manipulering	Utnyttelse av psykologiske sårbarheter hos menneskelige for å få tilgang til systemer og informasjon.
Spoofing	Manipulasjon av data eller identitet for å skjule sin egentlige opprinnelse eller fremstå som noen andre.
SQL-injeksjon	Angrep som utnytter sårbarheter i webapplikasjoner for å injisere skadelige koder i databaser.

BITPRO

Svartelisting	Sikkerhetspraksis der enheter, IP-adresser, eller programmer nektes adgang/handling basert på definerte regler/kriterier.
Sårbarhet	Svakheter i programvare, operativsystemer, applikasjoner, enheter eller prosedyrer som kan utnyttes av en angriper.

T

To-faktor-autentisering	To separate autentiseringsfaktorer for å bekrefte identiteten før det gis til et system, applikasjon eller tjeneste.
Trussel	Hendelse, handling, programvare eller tilstand som kan utnytte sårbarheter, påføre skade eller tap.

U

Uautorisert	Handlinger, tilgang, bruk eller annen aktivitet som ikke er godkjent av rettmessige eiere eller administratorer.
Uautorisert tilgang	Forsøk på å få tilgang til systemer eller data uten tillatelse fra rettmessige eiere eller administratorer.

V

VPN (Virtual Private Network)	En sikker og kryptert forbindelse fra et offentlig nettverk og til et lukket nettverk.

Z

Zero-Day angrep	Angrep som utnytter sikkerhetshull i programvarer/systemer som utviklerne ikke kjenner til eller har rukket å tette.