WISER
Wide-Impact cyber SEcurity Risk framework

Glosar Kibernetske Varnosti

Glede na raziskave vlade Združenega kraljestva je bilo v zadnjem letu 74% malih podjetij v Združenem kraljestvu žrtev vdora v podatkovno bazo, 90% velikih podjetij je bilo tarča kibernetskih napadov. Nekateri incidenti so povzročili večmiljonsko škodo.

Ta priročnik je namenjen ponudnikom digitalnih storitev in administratorjem v javni upravi kot prvi korak k razumevanju in obvladovanju kibernetskih tveganj.

Kibernetski napad (angl. cyber attack) – zlonamerno dejanje, ki škodljivo vpliva na delovanje informacijskega sistema, digitalno odvisnih podjetij in omrežij.

Kibernetski incident (angl. cyber incident) – grožnja in/ali uresničena grožnja, ki prekine delovanje računalnika, z internetom povezanimi napravami, internetno povezavo ali vdor v podatkovno bazo, zajem podatkov, ki so v obdelavi, med transferjem ali le shranjeni na ogroženi infrastrukturi. Zahteva usklajen odziv za blaženje posledic.

Kibernetska odpornost / obrambne zmogljivosti (angl. cyber resilience) – zmožnost neprekinjenega delovanja sistema IKT in organizacij v primeru kibernetskega incidenta, in, v primeru posledic, zmogljivost vzpostavitve prvotnega stanja

Kibernetska varnost (angl. cyber security) – stopnja varnosti z internetom povezanega informacijskega sistema, strojne opreme, programske opreme in pripadajoče infrastrukture, podatkov, shranjenih na le-tej in storitev pred nepooblaščenim dostopom, škodo ali zlorabo. Vključno s škodo, ki je bila povzročena namerno, ali nenamerno, zaradi neupoštevanja varnostnih predpisov in postopkov.

Ocena kibernetskega tveganja (angl. cyber security risk assessment) – ocena verjetnosti varnostnega incidenta in ovrednotenje škode, ki lahko nastane. Identifikacija šibkih točk, ki ogrožajo organizacijo, ter predlogi, kako povečati obrambne zmogljivosti, in ustrezne investicije.

Kibernetska grožnja (angl. cyber threat) – možnost, da se uresniči varnostni incident in povzroči škoda informacijskemu sistemu, z internetom povezanimi napravami, vključno s strojno opremo, programsko opremo in infrastrukturo, podatki, shranjenimi na le-tej, storitve, ki jih omogočajo.

Vrste napadov in ranljivosti

Splošna zlonamerna programska oprema (angl. commodity malware) – zlonamerna programska oprema, ki je na voljo proti plačilu ali brezplačno prenosljiv program, ki ni prilagojen za uporabnika, in ga lahko uporablja kdorkoli.

Zalezovanje v kibernetskem prostoru (angl. cyberstalking) – prikrito zalezovanje z uporabo elektronskih storitev npr. družbenih medijev.

Vdor v podatkovne baze/kršitev varnosti osebnih podatkov (angl. data breach) – nepooblaščen prenos podatkov ali razkritje informacij nepooblaščenim osebam.

Ohromitev storitve DDoS/napad tipa DDoS (angl. Distributed Denial of Service) – večje št. poslanih zahtevkov, ki presežejo zmogljivosti strežniške obdelave, kar lahko omogoči dostop nepooblaščenim uporabnikom.

Doxing, potvarjanje (angl. doxing) – sledenje in kraja osebnih podatkov posameznika (PII) na internetu in njihova (nepooblaščena) objava.

Zlonamerna programska oprema/programje (angl. malware, malicious software) – programska oprema ali koda, katere namen je škodljivo vplivati na delovanje informacijskega sistema, npr. virusi, črvi, trojanski konji, vohunsko programje.

Virusi (angl. viruses) – zlonamerni program s sposobnostjo samodejnega razmnoževanja in širjenja na druge datoteke.

Črv (angl. worm) – zlonamerni program, ki se razširja v računalniških omrežjih in se pri tem samodejno razmnožuje. Za razmnoževanje izkorišča pomanjkljivosti v varnostnih nastavitvah računalniškega sistema. Za razliko od virusa za širjenje ne potrebuje obstoječih programov, na katerega bi se vezal.

Trojanski konj, trojanec (angl. Trojan horse, Trojan) – zlonamerni program z navidezno koristno funkcijo.

Ribarjenje (angl. phishing) – zavajanje prejemnikov e-pošte, da s klikom na zlonamerne povezave ali priloge v e-sporočilu, kar aktivira zlonamerno programsko opremo, ali da deli občutljive podatke z neznano tretjo osebo. Pošiljateljev elektronski naslov je videti, kot da izvira iz zanesljivega vira.

Izsiljevalsko programje (angl. ransomware) – zlonamerna programska oprema, ki onemogoči uporabo sistema, storitve in za ponovno vzpostavitev uporabe zahteva plačilo

Zlonamerno predstavljanje s tujo identiteto v SMS (angl. SMS spoofing) – nepooblaščeno zlonamerno predstavljanje s tujo identiteto, tehnika, ki zakrije pošiljatelja (ID) sporočila SMS z alfanumeričnim besedilom. Uporaba je lahko zakonita, ko pošiljatelj nadomesti svojo tel. številko s svojim imenom, imenom podjetja, ali nezakonita, v primeru izdajanja za drugo osebo.

Socialni inženiring (angl. social engineering) – nagovarjanje uporabnikov, da razkrijejo tajne informacije, ki nepooblaščeni osebi omogočajo dostop do informacijskega sistema, tudi z manipulacijo. Navadno socialni inženiring vključuje obisk zlonamerne spletne strani ali odpiranje neželenih datotek v prilogi.

Ranljivost (angl. vulnerability) – občutljivost digitalnih naprav za zlorabe, šibke točke/hrošči varnostnega sistema, ki jih lahko hekerji izkoristijo in ogrozijo delovanje sistema

Preverjanje ranljivosti (angl. vulnerability testing) – testiranje programske opreme za identifikacijo ranljivosti sistema, in prednostno opredelitev okrepitev obrambnih ukrepov. Priporočljivo je teste ranljivosti izvajati redno, saj je stopnja ogroženosti in izpostavljenosti visoka tudi več kot leto po prvi objavi ranljivosti.