Ne budi i ti hrvatski naivac

#SurfajSigurnije

Mali pojmovnik kibernetičke sigurnosti

CERT.hr
surfaj sigurnije

Sufinancirano instrumentom Europske unije za povezivanje Europe

OSNOVNI POJMOVI KIBERNETIČKE SIGURNOSTI

Asimetrični kriptografski algoritmi	Algoritmi koji za šifriranje i dešifriranje koriste dva ključa, javni i privatni.
Bandwidth	Količina podataka koja u definiranom vremenskom roku može proći kroz mrežu.
Bug	Greška ili nedostatak u programskom kodu koja uzrokuje neispravan ili neočekivan rad softvera.
BYOD (Bring Your Own Device)	Korištenje vlastitih korisničkih uređaja (prijenosno računalo, pametni telefon, tablet i sl.) u korporativnom okruženju.
Cjelovitost	Načelo informacijske sigurnosti koje podrazumijeva zaštitu informacija od namjerne ili slučajne neovlaštene modifikacije uzrokovane ljudskim utjecajem ili pogreške u radu sustava.
CERT (Computer Emergency Response Team)	Skupina stručnjaka odgovornih za rješavanje računalno-sigurnosnih incidenata i odgovorna za koordinaciju, prevenciju i zaštitu od računalnih ugroza sigurnosti informacijskih sustava. U međunarodnoj praksi koristi se i kratica CSIRT (Computer Security Incident Response Team).
Curenje podataka (engl. Data Breach)	Slučajni ili namjerni prijenos i distribucija privatnih i povjerljivih informacija neke organizacije bez njenog znanja i privole.
Dešifriranje	Proces pretvorbe šifriranih podataka u njihov primarni oblik.
Digitalni certifikat	Informacija koja jamči da je pošiljatelj provjeren, izvoran te da je njegov identitet stvaran.
Digitalni trag	Trag u digitalnom svijetu kojeg je, za razliku od stvarnog svijeta, gotovo nemoguće obrisati, a sastoji se od svih informacija koje ostavljamo prilikom korištenja interneta.
Dostupnost	Načelo informacijske sigurnosti koje podrazumijeva dostupnost informacije ovlaštenim korisnicima u određenom trenutku i u skladu sa zadanim uvjetima.
End-to-End šifriranje	Komunikacija u kojoj se razmjenjuju šifrirani podaci koji imaju vidljive informacije o putanji.

Haker	1. a. Onaj koji je obuzet programiranjem i računalnom tehnologijom. 1. b. Onaj koji se ne zadovoljava programiranjem, već želi proučavati jezgru nekog operativnog sustava ili programa. 2. Onaj koji potajno i neovlašteno upada u tuđa računala ili u mreže, provjeravajući ili mijenjajući programe i podatke pohranjene u njima.
Hardver (engl. Hardware)	Fizički dijelovi računalnog sustava, uključujući sve vanjske uređaje.
Internet	Mreža koja povezuje mnogobrojne računalne sustave i mreže, zasnovana na zajedničkom adresnom sustavu i komunikacijskim protokolima.
Internetska tražilica	Digitalna usluga koja korisniku omogućuje da pretražuje u načelu sve internetske stranice ili internetske stranice na određenom jeziku na temelju upita o bilo kojoj temi u obliku ključne riječi, rečenice ili nekog drugog unosa, a rezultat su poveznice na kojima se mogu pronaći informacije koje su povezane sa zatraženim sadržajem.
Internetsko tržište	Digitalna usluga koja potrošačima i/ili trgovcima, kako su oni definirani zakonom kojim se uređuje alternativno rješavanje potrošačkih sporova, omogućuje da na internetu sklapaju kupoprodajne ugovore i ugovore o uslugama s trgovcima na mrežnoj stranici tog internetskog tržišta ili na mrežnoj stranici tog trgovca koji se služi računalnim uslugama koje pruža internetsko tržište.
IoT (Internet of Things)	"Internet stvari" odnosi se na povezivanje svakodnevnih objekata, uređaja i stvari na internet i s drugim uređajima s ciljem pružanja jednostavnijeg, preciznijeg i pametnijeg iskustva u njihovu korištenju.
Kibernetička sigurnost	Sustav organizacijskih i tehničkih aktivnosti i mjera kojima se postiže autentičnost, povjerljivost, cjelovitost i dostupnost podataka, kao i mrežnih i informacijskih sustava u kibernetičkom prostoru.
Kibernetički kriminalitet	Činjenje kaznenih djela protiv računalnih sustava, programa i podataka unutar kibernetičkog prostora uporabom informacijskih i komunikacijskih tehnologija.
Kibernetički prostor	Virtualni prostor unutar kojeg se odvija komunikacija između mrežnih i informacijskih sustava te obuhvaća sve mrežne i informacijske sustave neovisno o tome jesu li povezani na internet.
Kompromitacija sustava	Zlonamjerno ostvarivanje pristupa sustavu bez znanja korisnika.
Kriptografija	Znanost koja se bavi proučavanjem metoda šifriranja podataka.
Kritična infrastruktura	Sustavi, mreže i objekti od nacionalne važnosti čiji prekid djelovanja ili prekid isporuke roba ili usluga može imati ozbiljne posljedice na nacionalnu sigurnost, zdravlje i živote ljudi, imovinu i okoliš, sigurnost i ekonomsku stabilnost i neprekidno funkcioniranje vlasti.
Lozinka (engl. Password)	Oblik tajnog podatka kojeg je potrebno poznavati kako bi se pristupilo određenim resursima. Snažna lozinka sastoji se od velikih i malih slova, brojki i simbola te ima 12 ili više znakova.

Mrežni i informacijski sustav	a. Elektronička komunikacijska mreža kako je ona definirana zakonom kojim se uređuje područje elektroničkih komunikacija; b. bilo koji uređaj ili grupa povezanih ili srodnih uređaja, od kojih jedan ili više njih programski izvršava automatsku obradu digitalnih podataka; c. digitalni podaci koji se pohranjuju, obrađuju, dobivaju ili prenose elementima opisanim u točkama a. i b. u svrhu njihova rada, uporabe, zaštite i održavanja.
Povjerljivost	Načelo informacijske sigurnosti koje podrazumijeva niz pravila koja ograničavaju pristup informacijama ili onemogućavaju dijeljenje informacija neovlaštenim osobama u svrhu očuvanja i zaštite privatnosti informacija.
Prava pristupa	Pravo ili dozvola za pristup koja se dodjeljuju pojedincu ili programu kako bi pristupio, izmijenio ili obrisao podatke koji se nalaze na mreži.
Privatnost	Pravo pojedinca da bude pušten na miru, da bude van javnog pogleda te da kontrolira informacije o sebi. "Nitko ne smije biti podvrgnut samovoljnom miješanju u njegov privatni život, obitelj, dom ili dopisivanje, niti napadima na njegovu čast i ugled. Svatko ima pravo na zakonsku zaštitu protiv takvog miješanja ili napada."
Ranjivost	Slabost nekog računalnog sustava čijim iskorištavanjem zlonamjerni napadač može narušiti sigurnost informacija na tom sustavu.
Računalno-sigurnosni incident	Jedan ili više računalno-sigurnosnih događaja koji su narušili odnosno narušavaju sigurnost informacijskog sustava ili računalne mreže te ugrožavaju povjerljivost, cjelovitost i dostupnost informacija koje se korištenjem informacijskog sustava ili računalne mreže stvaraju, obrađuju, pohranjuju ili prenose.
Rizik	Bilo koja razumno prepoznatljiva okolnost ili događaj koji ima potencijalno negativni učinak na sigurnost mrežnih i informacijskih sustava.
Root ovlasti	Korisničko ime ili račun koji ima ovlasti za pristup svim naredbama i datotekama.
Šifriranje	Proces pretvorbe podataka u šifrirani oblik.
Simetrični kriptografski algoritmi	Algoritmi koji za šifriranje i dešifriranje koriste isti tajni ključ.
Softver (engl. Software)	Opći naziv za programe i njima pripadne podatke namijenjene za rad na računalima.
Steganografija	Znanstvena disciplina koja proučava metode skrivanja informacija u naizgled bezazlene objekte.
TCP/IP (Transmission Control Protocol/Internet Protocol)	Skupina temeljnih protokola poznatih i pod imenom IP skupina protokola koji omogućavaju komunikaciju raznih međusobno povezanih mreža.
Usluga računalstva u oblaku	Digitalna usluga kojom se pruža pristup nadogradivom i elastičnom skupu djeljivih računalnih resursa, usluga i aplikacija.
Zaglavlje (engl. E-mail Header)	Zapis kojeg sadrži svaka poruka elektroničke pošte, a u tom se zapisu nalaze podaci o pošiljatelju, primatelju, informacije o poslužiteljima preko kojih je poruka poslana, odnosno primljena, te još niz informacija.

ZLONAMJERNI SADRŽAJ I PRIJETNJE

Adware	Reklamni ili oglašivački softver koji automatski prikazuje ili preuzima oglase na računala nakon što je instaliran neki softver ili nakon korištenja neke aplikacije.
APT (Advanced Persistent Threat)	Složeni i ciljani napad na određenu žrtvu uz korištenje većeg broja naprednih tehnika i tehnologija.
Backdoor	Zlonamjerni sadržaj instaliran bez znanja korisnika koji napadaču omogućuje pristup sustavu.
Bot	Pojedino zaraženo računalo koje je dio botnet mreže.
Botnet	Mreža računala koja su zaražena zlonamjernim programom koji omogućava osobi koja ga je stvorila određenu kontrolu nad zaraženim računalima.
C&C (Command and Control Server)	Komandni i kontrolni poslužitelj za nadzor i upravljanje računalima koja su dio botneta. Također može služiti kao točka prikupljanja ukradenih podataka s različitih botova.
CEO fraud ili BEC (Bussiness Email Compromise)	Pokušaj prijevare u kojem napadač lažnim predstavljanjem pokušava steći financijsku korist od ciljane žrtve. Kako bi elektronička poruka izgledala što uvjerljivije, prevaranti koriste stvarna imena visoko pozicioniranih osoba u tvrtki/instituciji.
Crv (engl. Worm)	Zlonamjerni ili nepoželjni računalni program koji sam sebe umnožava i širi se putem računalne mreže.
Dictionary napad	Pogađanje lozinke korisnika služeći se složenim rječničkim bazama u koje je napadač upisao poznate lozinke, poznate kombinacije riječi ili nizova riječi.
DoS (Denial of Service)	Napad u kojem napadač slanjem velikog broja upita prema uređaju, servisu ili usluzi legitimnom korisniku uskraćuje pristup.
Exploit	Zlonamjerno iskorištavanje ranjivosti u sustavu.
Hoax	Poruka elektroničke pošte neistinitog sadržaja, poslana s ciljem zastrašivanja ili dezinformiranja primatelja.
Keylogger	Zlonamjerni programski alat namijenjen tajnom praćenju i snimanju korisničke aktivnosti bilježenjem (svih) pritisnutih tipki na računalu.
Malver (engl. Malware)	Zlonamjerni softver namijenjen ostvarivanju pristupa računalu bez znanja njegovog vlasnika, odnosno korisnika.
Malware URL (Uniform Resource Locator)	Poveznica do postavljenog zlonamjernog programskog koda na kompromitiranom web sjedištu.
Pametno pogađanje lozinke	Pogađanje lozinke na temelju prikupljenih informacija o korisniku.

Phishing	Masovno zasipanje velikog broja osoba porukama u kojima se na prijevaru traži odavanje tajnih podataka.
Phishing URL	Poveznica do lažne internet stranice na kompromitiranom web sjedištu čija je svrha krađa povjerljivih podataka.
Ransomware	Naziv za skup zlonamjernih programa koji korisniku onemogućuju korištenje računala. Nakon zaraze ransomware može šifrirati datoteke ili onemogućiti korištenje tako da se pojavi početni ekran s određenom porukom koju nije moguće maknuti. Od korisnika čije je računalo zaraženo traži se otkupnina u zamjenu za daljnje normalno korištenje računala.
Rootkit	Vrsta zlonamjernog sadržaja koji se aktivira prilikom svakog pokretanja računala.
Scam	Pokušaji vještog navođenja potencijalne žrtve na djelovanje u korist prevaranta (najčešće putem elektroničke pošte). Najpoznatiji oblik je „nigerian scam“ ili „419 fraud“.
Skeniranje	Neovlašteno automatizirano prikupljanje informacija o računalnim mrežama i sustavima.
Sniffing	Neovlašteno presretanje mrežnog prometa.
Socijalni inženjering	Niz tehnika pomoću kojih pojedinac, iskorištavanjem ljudskih pogrešaka i slabosti, utječe na drugog pojedinca kako bi ga naveo da učini nešto što nije u njegovom interesu. Najčešće se koristi u svrhu otkrivanja povjerljivih informacija ili dobivanja pristupa nekim resursima do kojih napadač inače ne bi mogao doći.
Spam	Neželjena elektronička poruka poslana u svrhu izravne promidžbe i prodaje bez prethodno pribavljene privole primatelja poruke.
Spam URL	Poveznica do kompromitiranog web sjedišta na web poslužitelju s neovlašteno postavljenim reklamnim sadržajem.
Spear phishing	Pokušaj ciljanog navođenja specifičnog korisnika na odavanje povjerljivih podataka ili pokretanje zlonamjernog programa putem raznih komunikacijskih kanala.
Sustav zaražen zlonamjernim kodom	Računalo (npr. PC, pametni telefon, IoT i sl.) zaraženo zlonamjernim kodom.
Trojanski konj	Oblik zlonamjernog softvera koji se lažno predstavlja kao neki koristan softver kako bi ga korisnik izvršio, odnosno dozvolio mu instalaciju.
Virus	Računalni program koji svojom reprodukcijom može zaraziti računala tako da bez dopuštenja ili znanja korisnika kopira samog sebe u datotečni sustav ili memoriju ciljanog računalnog sustava.
Web Defacement	Kompromitirano web sjedište s izmijenjenim izgledom ili sadržajem web stranice.
Zero Day ranjivost	Sigurnosni propust u računalnoj aplikaciji koji je otkriven i poznat je napadačima prije nego što je za njega izdana sigurnosna zakrpa.
Zlonamjerno rudarenje kriptovalute (engl. Cryptojacking)	Neovlašteno iskorištavanje resursa korisničkog računala ili mobilnog uređaja za rudarenje kriptovalute.

ZAŠTITA OD RAČUNALNO-SIGURNOSNIH INCIDENATA

Antivirus/ Antispyware / Antimalware	Sigurnosna rješenja za prepoznavanje i zaustavljanje aktivnosti zlonamjernog sadržaja na uređaju.
Sigurnosna kopija	Kopija podataka koja se izrađuje u svrhu osiguranja u slučaju oštećenja ili gubitka izvornih podataka.
Upravitelj lozinkama (engl. Password Manager)	Alat koji omogućava generiranje i pohranu većeg broja složenih lozinki u šifriranom obliku. Do lozinki se dolazi poznavanjem samo jedne, glavne lozinke (engl. Master password) koja omogućava dešifriranje ostalih lozinki.
Vatrozid (engl. Firewall)	Sigurnosni uređaj ili alat koji nadzire mrežni promet te ga temeljem unaprijed definiranih pravila propušta ili odbacuje.
Višefaktorska autentifikacija	Proces u kojem se od korisnika iziskuje potvrda identiteta koristeći više različitih autentifikacijskih faktora.

CERT.hr

Hrvatska akademska i istraživačka mreža

CARNET

Zahvaljujemo nakladničkoj kući Znanje d.o.o. na dozvoli za korištenje nekih definicija preuzetih s Hrvatskog jezičnog portala (HJP) koji je zajednički projekt nakladničke kuće Znanje i Sveučilišnog računskog centra (Srce).

Projekt je sufinanciran sredstvima CEF - Connecting Europe Facility programa Europske komisije, broj ugovora: INEA/CEF/ICT/A2016/1334308 (Action No: 2016-HR-IA-0085)

Sufinancirano instrumentom Europske unije za povezivanje Europe