# Predavanje 1 - Upravljanje ranjivostima

**- 0-day ranjivost:**

- sigurnosni propust u računalnoj aplikaciji koji je otkriven i poznat je napadačima prije nego što za njega zna proizvođač i javnost
- za takvu ranjivost proizvođač još nije objavio zakrpe koje uklanjaju problem (pošto za nju još ne zna)
- izraz „zero day“ nastao je kao vremenska oznaka ranjivosti - napad se obično javlja prije prvog ili nultog dana svjesnosti proizvođača o ranjivosti

**- ranjivost - svojstvo resursa:**

- slabost u sustavu, sigurnosnim procedurama, dizajnu ili implementaciji resursa
- ranjivosti nisu samo u tehničkim mjerama zaštite
    - iako su takve najčešće vidljive
    - propusti u konfiguraciji
    - brojne ranjivosti proizlaze iz loše definiranih procedura ili sigurnosnih politika
- npr. admin/admin, javno dostupna baza, izgubljeni USB…

**- Common Vulnerabilities and Exposures (CVE):**

- baza javno poznatih ranjivosti i izloženosti
- misija CVE programa je da identificira, definira i javno objavi katalog cybersecurity ranjivosti
- postoji jedan CVE zapis za svaku ranjivost u katalogu

**- Common Vulnerability Scoring System (CVSS):**

- to je način da se ocijene i rangiraju prijavljene ranjivosti u standardiziranom i ponovljivom načinu
- CVSS generira ocjenu od 0 do 10 na temelju ozbiljnosti ranjivosti (0 - manje značajna, 10 - najveća ranjivost)
- CVSS rezultat kombinira puno čimbenika kako bi mogao generirati rezultat:
    - vektor napada
    - kompleksnost napada
    - interakcija korisnika

**- životni ciklus ranjivosti:**

- **period kritične izloženosti** - vremensko razdoblje od trenutka kada je ranjivost otkrivena do trenutka kada je objavljena sigurnosna zakrpa
- životni ciklus izravno je povezan sa sigurnosnim rizikom
- **1. otkrivanje ranjivosti** - trenutak u kojem je ranjivost otkrivena:
    - slijedi razdoblje u kojem razina rizika ovisi o dinamici širenja informacije
- **2.** trenutak pojave **exploit** programa:
    - **exploit** - specijalizirani program koji iskorištava ranjivost
    - 0-day exploit -> iskorištava 0-day ranjivost
    - vrijeme potrebno za izradu exploita ovisi o složenosti i tipu ranjivosti
    - pojavljivanje exploit programa značajno povećava sigurnosni rizik -> pogotovo ako je exploit javno dostupan
- **3.** trenutak javne objave informacija o ranjivosti:
    - trenutak u kojem informacije postaju dostupne široj javnosti
    - službeno se smatra objava proizvođača ranjivog softvera/hardvera
- **4.** trenutak izdavanja sigurnosne zakrpe
    - proizvođač službeno objavljuje zakrpu
        - uklanjanje ranjivosti može se temeljiti i na konfiguracijskim promjenama
- **5.** instalacija sigurnosne zakrpe

**- upravljanje ranjivostima:**

- 0-day napadi - puno pozornosti, vrlo rijetki
- iskorištavanje poznatih ranjivosti predstavlja daleko realniji scenarij
- SANS (SysAdmin, Audit, Network, and Security Institute) - preko 80% sigurnosnih incidenata odnosi se na iskorištavanje poznatih ranjivosti

**- proces upravljanja ranjivostima:**

- jedan od temeljnih procesa upravljanja informacijskom sigurnošću (eng. *Vulnerability management*)
- sistematizirani proces identifikacije i uklanjanja sigurnosnih ranjivosti
    - minimiziranje, tj. spuštanje na prihvatljive razine
    - cilj je proaktivna zaštita informacijskog sustava
- sve aktivnosti moraju biti formalno definirane
    - s pripadajućim ulogama i odgovornostima
    - omogućava konzistentno i jednoznačno provođenje svih aktivnosti

**- otkrivanje i analiza ranjivosti:**

- korištenje alata za redovito automatsko skeniranje ranjivosti
- skeniranje s admin pravima (agent ili eksterno skeniranje)
- Tenable Nessus, Nexpose Rapid 7, Qualys - najpoznatiji alati
- alati su u principu bazirani na potpisima
- definiranje prioriteta za uklanjanje ranjivosti (izazov)
- inovativni pristupi (korištenje threat intelligence)
- omogućuju i automatizaciju nekih drugih postupaka:
    - identifikacija aktivnih sustava
    - pregledavanje TCP i UDP portova
    - identifikacija operacijskih sustava
    - enumeracija korisničkih računa i grupa
    - provjera instaliranih sigurnosnih zakrpi
    - pregledavanje web poslužitelja
    - provjera sigurnosnih postavki

**- procjena rizika:**

- svaka organizacija treba znati koji su to najvažniji resursi
- izloženost resursa jako važna
    - sustavi javno dostupni
    - interni sustavi
    - sustavi u izoliranom okruženju

**- evaluacija otkrivenih ranjivosti:**

- nema svaka ranjivost jednaku težinu
- najvažnije su one za koje postoje gotovi exploiti koji se koriste
- ranjivosti bez exploita ne predstavljaju ozbiljnu prijetnju - međutim, exploit se može pojaviti naknadno
- navedeno znači da se ranjivosti moraju kontinuirano evaluirati

**- evaluacija / što patchirati?**

- otprilike svaka dva od tri CVE-a korištena u napadu su imali već objavljen exploit
- kada je exploit objavljen, šansa da se vidi ciljana ranjivost „in the wild“ je sedam puta veća nego bez exploita
- strategija da se postave prioriteti prema „jako lošim“ CVE-ima kao što su oni s CVSS-om od 10 bi se podrazumijevala vrlo učinkovitom, ali ima slabu pokrivenost zbog mnogih ranjivosti koje je lako iskoristiti s nižim CVSS-om te bi takve ranjivosti izostale
- strategija da se poveća pokrivenost tako da se saniraju sve ranjivosti s CVSS-om većim ili jednakim 6 bi bile manje učinkovite jer bi se vrijeme trošilo na rješavanje ranjivosti koje nikada ne bi bile iskorištene

**- Vulnerability Prioritization Technology:**

- pojednostavnjuje analizu ranjivosti i sanaciju fokusiranjem napora na identificiranje i određivanje prioriteta ranjivosti koji predstavljaju najveći rizik za organizaciju
- iskorištavanje ranjivosti
- kritičnost imovine ili poslovanja
- ozbiljnost ranjivosti

**- Exploit Prediction Scoring System (EPSS):**

- EPSS je dnevna procjena vjerojatnosti exploita promatranih aktivnosti u sljedećih 30 dana

**- uklanjanje ranjivosti:**

- korištenje specijaliziranih alata za automatiziranu instalaciju
- vrlo rijetko manualna instalacija (npr. DMZ)

**- dobri hakeri i ranjivosti:**

- **Bug Bounty** - ponuda koju nude mnoge web-stranice i software developeri za koje pojedinci mogu dobiti priznanje i naknadu za prijavu bugova, posebno onih koji se odnose na exploite i ranjivosti

**- Google Project Zero:**

- tim sigurnosnih istraživača u Googleu koji proučavaju 0-day ranjivosti u softverskim i hardverskim sustavima o kojima ovise korisnici diljem svijeta
- njihova je misija napraviti otkrivanje i exploit sigurnosnih ranjivosti težima te značajno unaprijediti sigurnost interneta za sve
- koriste rezultate istraživanja kako bi patchirali ozbiljne sigurnosne ranjivosti, poboljšali razumijevanje kako exploit napadi funkcioniraju i potaknuli dugoročna strukturna poboljšanja sigurnosti
- kada Googleovi hacker-huntersi pronađu bug kažu da upozore tvrtku odgovornu za popravak i daju joj između 60 i 90 dana za izdavanje patcha prije javnog otkrivanja greške na Google Project Zero blogu

**- penetracijsko testiranje:**

- najsofisticiraniji i najtemeljitiji postupak ispitivanja sigurnosti
- sustav se u kontroliranim uvjetima podvrgava stvarnim pokušajima napada korištenjem svih onih tehnika i alata koje napadači inače koriste prilikom provođenja neovlaštenih aktivnosti
- svrha - pronaći ozbiljne slabosti u informacijskom sustavu
- ugovara se s vanjskim partnerima
- **goal-oriented / objective-oriented penetration testing:**
    - ovu vrstu penetracijskog testiranja pokreću ciljevi
    - definirani su ciljevi penetracijskog testiranja umjesto definiranja opsega ciljeva
    - cilj penetracijskog testiranja je definiran prije nego ono počne
    - posao pentestera je da provjeri može li postići cilj i utvrditi različite načine za postizanje cilja
    - primjeri: ostvarivanje remote pristupa internom networku, informacijama o kreditnim karticama, dobivanje admin ovlasti na domeni…
- **compliance-oriented penetration testing:**
    - ovu vrstu penetracijskog testiranja pokreću zahtjevi usklađenosti (compliance requirements)
    - uključuje provođenje procjene prema zahtjevima usklađenosti cybersecurity standarada, okvira, zakona, akata…
    - primjeri: organizacija može tražiti da se provede sigurnosna procjena protiv PCI-DSS zahtjeva
- **red-team-based penetration testing:**
    - u ovoj vrsti testiranja pentester mora oponašati ponašanje pravog napadača i ciljane okoline
    - nema posebnog motiva

    - npr. organizacija može tražiti provedbu sigurnosne procjene za vrednovanje njegove cjelokupne sigurnosti, može uključivati procjenu ljudi, mreža, aplikacija, fizičku sigurnost...
- **podjela prema načinu provođenja:**
    - bez prethodnog poznavanja testiranog sustava
        - eng. „black box, zero knowledge“
        - jedine informacije koje može imati su javno dostupne informacije
    - s prethodnim poznavanjem testiranog sustava
        - eng. „white box“
        - provoditelju se ustupaju sve potrebne informacije o ciljanom sustavu
    - s djelomičnim poznavanjem testiranog sustava
        - eng. „gray box“

**- postupak provođenja penetracijskog testiranja:**

- budući da simulira stvarni pokušaj napada na tehničkoj razini je praktički jednak stvarnom napadu
    - koriste se tehnike i alati koji su dostupni i napadačima
- razlika u cilju
    - napadač želi ukrasti podatke ili nanijeti štetu
    - provoditelj želi identificirati i ukloniti ranjivost
- razlika u cijeni
- postupak potrebno sistematizirati i kontrolirati
- pravno-formalni aspekt - penetracijski test je ugovorom definirana radnja koja obvezuje pravnu ili fizičku osobu zaduženu za njezino obavljanje na visokoj razini tajnosti prikupljenih podataka o slabostima testiranog sustava

**- BAS (Breach and Attack Simulation):**

- alati za simulaciju prodora i napada omogućuju organizacijama stjecanje dubljeg razumijevanja sigurnosnog položaja ranjivosti automatiziranjem testiranja vektora prijetnji kao što su external, internal, lateral movement i data exfiltration
- BAS nadopunjuje red teaming i penetracijsko testiranje, ali ih ne može u potpunosti zamijeniti
- BAS provjerava sigurnosno stanje organizacije testiranjem njezine sposobnosti otkrivanja portfelja simuliranih napada koje izvode SaaS platforme, software agenti i virtualni strojevi

**- Zaključak:**

- 0-day ranjivosti privlače pozornost
- pravovremeno patchiranje je izazov
- prioritizacija ranjivosti
- penetracijsko testiranje
- BAS

# Predavanje 2 - Malware

**- NotPetya:**

- napad na Ukrajinu
- Maersk - svi domain controlleri izbrisani u isto vrijeme (oko 150 komada), jedini preživjeli domain controller je ostao u Ghani - šteta od 300 milijuna dolara
- FedEx - šteta od 400 milijuna dolara
- Pharmaceutical company Merck - šteta od 870 milijuna dolara

**- fokus stavljen na krajnjeg korisnika, vanjske partnere i vanjsku infrastrukturu:**

- drive-by compromise
- exploit public-facing application
- external remote services
- hardware additions
- phishing
- valid accounts
- replication through removable media
- supply chain compromise / trusted relationship

**- vrste malicioznih programa:**

- vrsta malicioznog programa ovisi o dvije karakteristike:
  - metoda širenja
  - aktivnosti na inficiranom računalu
- četiri glavne vrste malicioznih programa:
  - virusi
  - crvi
  - trojanski konji
  - potencijalno neželjene aplikacije (eng. PUA)
- spyware, ransomware, fileless malware

**- Virusi:**

- najstarija vrsta malicioznih programa
- virus se „priljepljuje“ na legitiman program i izvršava prilikom pokretanja
- prema načinu inficiranja:
    - virusi koji inficiraju datoteke (eng. *file infectors*)
        - batch datoteke i shell skripte
    - boot sector virusi
        - inficiraju sektor na mediju koji se prvi čita
    - macro virusi
        - koriste macro jezik aplikacije
        - Microsoft Office (Word, Excel)
    - kombinirane kategorije (eng. *multipartite*)
        - npr. boot sector i file infector u jednom
        - otežavaju uklanjanje virusa (nije dovoljno ukloniti samo jedan izvor zaraze)

**- Crvi:**

- glavne karakteristike:
    - šire se putem računalnih mreža
    - **NE** inficiraju druge datoteke
- kako se crvi šire putem mreže:
    - iskorištavaju protokole za udaljeno spajanje/administraciju (npr. RDP, SSH)
    - iskorištavaju slabosti u lozinkama (npr. Stuxnet je koristio defaultne lozinke za Siemens PLC, pogađaju lozinke)
    - iskorištavaju sigurnosne ranjivosti u mrežnim servisima (npr. SQL Slammer, Blaster, Code Red, Nimda…)
    - iskorištavaju sigurnosne ranjivosti u aplikacijama

**- Trojanski konji:**

- glavne karakteristike:
    - nisu se u stanju sami širiti
    - ne inficiraju druge datoteke
- ponekad trebaju drugi maliciozni program za samu instalaciju i/ili socijalni inženjering
- napadaču omogućavaju kontrolu preko interneta
    - danas najčešći maliciozni programi
    - kradu osjetljive informacije ili koriste lokalne resurse
    - omogućuju potpunu kontrolu računala od strane napadača

**- Dridex:**

- upload files
- download files
- execute files
- monitor network traffic
- browser screenshot taking
- add the compromised computer to a botnet

**- potencijalno neželjene aplikacije:**

- aplikacije koje mogu imati neželjeni utjecaj na sigurnost i privatnost korisnika (eng. *grayware*)
- aplikacije koje instaliraju druge tijekom instalacije
    - Toolbar u web pregledniku, mijenja postavke (npr. tražilica)
- Adware - neželjene reklame
- Spyware - preveliko prikupljanje podataka

**- mreže malicioznih programa (Botneti):**

- autori malicioznih programa žele kontrolirati inficirana računala
    - mreže inficiranih računala nazivaju se *botneti*
- trojanski programi s komponentom udaljene kontrole
- centralni poslužitelji nazivaju se Command & Control (C&C)
- jednostavno davanje naredbi velikom broju inficiranih računala
- DDOS napadi, slanje spam poruka i sl.

**- napredne mogućnosti malicioznih programa:**

- cilj napadača - otežati detekciju i/ili analizu malicioznog programa
- napredne mogućnosti:
    - **polimorfizam:**
        - promjena tijela programa uz zadržavanje iste funkcionalnosti
        - detekcija temeljena na potpisima promatra tijelo programa -> promjena tijela -> potpis neučinkovit
        - kriptiranje ili komprimiranje tijela pomoću specijalnih programa (eng. *packer*) - njihov kod jedino vidljiv u memoriji računala, dekriptiraju/dekomprimiraju izvorni maliciozni program
        - promjena enkripcijskog ključa - promjena tijela programa

- **rootkit tehnologije:**
  - integriranje malicioznog programa s ključnim funkcijama i strukturama jezgre OS-a
    - postalo popularno u 2007.
  - presreće pozive jezgri (eng. *function hooking*)
    - npr. kada želi otvoriti neku datoteku ili direktorij
      - provjerava se ime željene datoteke te ako je na popisu vraća se lažni ili modificirani rezultat -> javlja AV softveru da ne postoji
      - u protivnom se izvršava legitimni dio koda
  - primjer Stuxneta:
    - worm dio - odgovoran za širenje malwarea
    - izvršni dio - izvođenje malwarea
    - rootkit dio - skrivanje malwarea
- kriptiranje koda
- emulacija korištenjem virtualnih strojeva
- **fileless:**
  - postojanost:
    - kada se isključi računalo svi aktivni procesi se zatvaraju, a kada se računalo ponovno pokrene tada se oni ponovno pokreću
    - fileless malware zapisuje svoju skriptu u Windows registar - to je funkcija OS-a koja pokreće programe na startupu sustava ili na raspored
    - kod koji pokreće fileless malware je zapravo skripta (obična tekstualna lista naredbi, a ne kompajlirana .exe datoteka)
    - kratka lista naredbi ne mora biti pohranjena u datoteci (fileless), ali duže i kompleksnije skripte se pohranjuju za „relaunch“ kod system starupa te zapravo tada postoji datoteka
  - ostaje rezistentan na računalu temeljem promjena registry postavki
  - nemoguće detektirati s tradicionalnim AV rješenjima
  - analiza anomalija -> strojno učenje
  - EDR funkcionalnosti u antivirusnom softwareu

**- defense evasion:**

- protivnik pokušava izbjeći da bude otkriven
- tehnike koje se koriste za izbjegavanje obrane uključuju deinstaliranje/onemogućavanje sigurnosnog softwarea ili (eng. *obfuscating*) zamagljivanje/šifriranje podataka i skripti
- protivnici također iskorištavaju i zlorabe pouzdane kako bi sakrili i maskirali svoj malware

**- anti-virusni programi:**

- osnovna zaštita od malicioznih programa
- korištenje AV programa propisuju razni standardi
    - CIS Top 18, ISO 27001, PCI DSS…
- integriraju se s operacijskim sustavom kako bi presreli rizične operacije
    - pokretanje programa
    - otvaranje datoteka
    - komunikacija preko interneta

**- platforme za analizu malicioznog softvera:**

- ReversingLabs
- VirusTotal

**- antivirusna rješenja nove generacije:**

- leaderi koji su kupili, dodali su nove funkcionalnosti
- izazivači koji su promijenili koncept zaštite na klijentu
- AV rješenja nove generacije moraju biti u stanju osigurati primjerenu:
    - prevenciju
    - detekciju
    - forenziku

**- Sandbox tehnike:**

- dinamička analiza - promatra datoteke dok „detoniraju“ u namjenski izgrađenom virtualnom okruženju otpornom na izbjegavanje (*evasion-resistant*)
- statička analiza - učinkovito otkrivanje malwarea i exploita koji nadopunjuju dinamičku analizu
- machine learning - izvlači tisuće jedinstvenih značajki iz svake datoteke trenirajući model strojnog učenja da prepoznaje novi malware što nije moguće samo sa statičkom ili dinamičkom analizom
- bare metal analysis - prijetnje izbjegavanja (*evasive threats*) se automatski šalju u stvarno hardversko okruženje za detonaciju kako bi se u cijelosti uklonila sposobnost da implementira anti-VM tehnike analize

**- strojno učenje:**

- nadzirano učenje
- nenadzirano učenje
- prevladava nadzirano učenje jer se temelji na analizi ogromne količine strukturiranih podataka
- izazov lažne pozitivne detekcije

**- MITRE evaluacija:**

- postoji šest glavnih kategorija otkrivanja koje predstavljaju količinu konteksta koji se daje analitičaru i tri glavne kategorije zaštite

**- Zaključak:**

- malware je bio, je i bit će ozbiljna prijetnja
- tvrtke moraju ulagati u prevenciju, detekciju i forenziku
- nova i stara rješenja -> nova generacija antivirusnih rješenja
- MITRE evaluacija - izvrstan okvir za testiranje
- napredne funkcionalnosti
    - strojno učenje
    - automatska analiza malwarea u sandbox okruženju

# Predavanje 3 - Napredna sigurnosna analitika

**- regulatorni zahtjevi:**

- DORA
- NIS2
- PCI DSS 4.0

**- upravljanje log zapisima:**

- propisati procedure i politike za upravljanje log zapisima
- **prikupljanje log zapisa:**
  - logovi imaju širu primjenu
  - rekonstrukcija događaja (što se dogodilo, kako…)
  - identifikacija problema (zašto ovaj upit troši resurse?)
  - utvrđivanje odgovornosti za aktivnosti ostvarene na informacijskom sustavu (tko je kriv?)
  - otkrivanje sumnjivih aktivnosti (tko je kriv?)
  - forenzika (kako su ušli u sustav?)
- što sve čini log zapis?
  - operativni i sistemski zapisi su bilješke o aktivnostima na resursima informacijskog sustava nastale onim slijedom kako su se te aktivnosti ostvarivale
  - **sistemski zapisi:**
    - zapisi operacijskih sustava, vatrozida, usmjernika, antivirusa…
    - start/stop, greške u sustavu i sl.
    - jednostavno podešavanje
  - **audit zapisi:**
    - korisničke aktivnosti (prijava/odjava, pristup datotekama i sl.)
    - zahtjeva planiranje prilikom podešavanja
  - **zapisi od bilo kud**
- **generiranje i slanje log zapisa:**
  - osnovni zahtjev pred operacijske sustave, aplikacije i uređaje
    - određeni log zapisi standardizirani, još uvijek velik broj nestandardiziranih log zapisa
  - nekonzistentnost između proizvođača
    - npr. autentikacijski log na Windowsima je drugačiji od onoga na Linuxu
    - potrebna normalizacija prije pohranjivanja

- **pohranjivanje log zapisa:**
  - odnosi se na metodu pohranjivanja na jednom ili više centralnih poslužitelja
  - klasično se logovi pohranjuju u tekstualne datoteke
  - na Windowsima Event Log
  - na Unixima /var/log
  - centralni poslužitelji su obično specijalizirane aplikacije
    - npr. Splunk, ELK…
  - pojedini sustavi ujedno i normaliziraju log zapise
- **analiza log zapisa:**
  - automatsko pregledavanje primljenih logova
    - izvještavanje
    - uzbunjivanje
  - vrlo kompleksni sustavi
    - SIEM (eng. *Security Information and Event Management*)
    - zadavanje kompleksnih pravila
    - korelacija logova iz različitih izvora
    - strojno učenje
- **arhiviranje i uklanjanje log zapisa:**
  - resursi sustava za pohranjivanje su ograničeni
    - cijena brzih diskova
    - centralni sustavi obično troše još prostora na dodatne informacije
  - potrebno odrediti periode arhiviranja/brisanja
    - u nekim slučajevima ovise o zakonskim odredbama
      - PCI DSS 10.5.1.
    - logovi se obično rotiraju

**- tipovi log zapisa:**

- dijelimo u tri osnovne kategorije:
  - **sigurnosni log zapisi**
    - zapisi koji bilježe sigurnosne događaje sustava
    - generiraju praktički svi uređaji i operacijski sustavi
    - zapisi prilikom prijave korisnika na sustav
      - autentikacijski logovi koji sadrže podatke o provjeri identiteta korisnika
      - autorizacijski logovi
    - OS-ovi često zapisuju i druge bitne informacije
    - log zapisi vatrozida
      - više kategorija, sve do aktivnosti administratora
    - IDS/IPS sustavi
      - detektiraju i sprječavaju neovlaštene aktivnosti

        - antivirusni programi
        - VPN sustavi
        - mrežni uređaji
    - audit zapisi:
        - Windowsi
    - sistemski zapisi:
        - zapisuju događaje sustava vezane uz općenitu funkcionalnost sustava
            - npr. informacije o pokretanju sustava, instalaciji programa i zakrpi
            - često pomažu prilikom analize incidenta
            - otkrivanje uzroka problema u radu
    - **operacijski log zapisi**
    - **aplikacijski log zapisi:**
        - praktički nema standarda
            - posebice za „custom made“ aplikacije
            - „off the shelf“ standardizirani
        - vrlo često se moraju dodatno procesirati
        - standardne aplikacije nisu problematične
        - pr. Apache

**- izvori podataka koji se moraju obavezno analizirati u svakoj organizaciji:**

- računala, poslužitelji
- mrežne aktivnosti
- vatrozid
- imenički servis (Active Directory, Azure AD)
- email
- surfanje (Web gateway, URL filtering, CASB)

**- Syslog:**

- jedan od najstarijih formata za slanje log zapisa preko IP mreža
- klijentsko-poslužiteljski protokol
    - razvio još 80-ih godina Eric Allman (autor Sendmaila)
    - definiran RFC 3164 dokumentom
        - klijent (eng. *Originator*)
        - poslužitelj (eng. *Collector*)
        - prijenosni poslužitelj (eng. *Relay*)
- koristi određeni format poruka
- vrsta log zapisa (Message facility), određuje izvor log zapisa, postoje 23 predefinirane vrijednosti
    - neke se koriste za zastarjele protokole

    - dozvoljeno 8 razina za proizvoljne protokole (tzv. local poruke)
    - u pravilu mrežni uređaji koriste local poruke
- prioritet pojedinog događaja se određuje prema kritičnosti log zapisa (eng. *severity*)
- severity - decimalna vrijednost od 0 do 7
- koriste se za određivanje metode uzbunjivanja

**- SIEM sustavi:**

- SIEM (Security Information and Event Management) - aplikacije koje omogućavaju centralno prikupljanje log zapisa te analizu, korelaciju, pretraživanje i uzbunjivanje
- dvije funkcionalnosti:
    - **SIM (Security Information Management)** - upravljanje logovima, analitika i izvješćivanje o sukladnosti (compliance reporting)
    - **SEM (Security Event Management)** - praćenje u stvarnom vremenu i upravljanje incidentima za sigurnosne događaje iz mreža, sigurnosnih uređaja, sustava i aplikacija
- tri scenarija korištenja:
    - napredna sigurnosna analitika u svrhu otkrivanja sigurnosnih anomalija/događaja odnosno pravovremenog otkrivanja incidenata
    - odgovor na incidente - automatizacija i forenzika
    - osnovno nadziranje sigurnosti - log management (uskladivost)

**- korelacija događaja:**

- omogućava pronalazak povezanosti između dva ili više sigurnosna događaja
    - najčešće se provodi kroz pravila koja definiraju uvjete povezivanja
- primjer: korelacija između otkrivenih ranjivosti na sustavu i detektiranih pokušaja upada u sustav
- nedostatci:
    - iznimno kompleksno za podešavanje
    - unaprijed se definiraju pravila
    - vrlo statično
- **machine learning jedino rješenje**

**- open source alternative:**

- ELK
- Graylog
- Wazuh

**- nedostatci SIEM rješenja:**

- implementacija istih često vrlo **kompleksna** i **skupa** te **zahtjevna** prema resursima -> različiti modeli licenciranja
- nepreciznost
- odvojena obrada i korelacija podataka
- ogroman broj događaja -> korelacija nije više učinkovita -> ML neophodan

**- otvoreno pitanje:**

- unatoč ovoj centralnoj ulozi, SOC (Security Operations Center) timovi sada okružuju SIEM s dodatnim alatima za detekciju/odgovor na prijetnje, istraživanje, analizu i automatizaciju procesa
- to postavlja pitanje: Je li SIEM bitan za sigurnosnu analitiku i operacije, zašto je organizacijama potrebno mnogo alata?

**- EDR (Endpoint Detection and Response):**

- sastavni dio EPP (Endpoint Protection Platforms) rješenja
- detaljno bilježenje svih aktivnosti na osobnim računalima/poslužiteljima (npr. izmjene na registry, URL, IP, pokrenuti proces)
- fokus na učinkovitu detekciju sigurnosnih incidenata
- uskladivost s MITRE ATT&CK okvirom
- izolacija računala/procesa/aplikacija u svrhu rješavanja sigurnosnih incidenata
- učinkovite istrage (eng. *threat hunting*)
- automatizacija

**- XDR (Extended Detection and Response):**

- omogućuje prikupljanje, tijesnu integraciju te naprednu analitiku podataka
- izvori podataka: osobna računala/poslužitelji, mrežni promet (NTA), email/web, imenički servisi, cloud…
- napredna analitika na machine learning načelima
- automatizacija odgovora na incidente (SOAR funkcionalnosti)
- naprednija detekcija kroz tijesnu integraciju događaja s različitih izvora -> kreiranje incidenata koji bi inače bili zanemareni
- smanjenje broja sigurnosnih događaja uslijed naprednije analitike/konteksta (npr. analiza mrežnih i endpoint događaja)
- XDR je zapravo što je SIEM trebao biti
- XDR pokriva prva dva SIEM scenarija

    - napredna sigurnosna analitika u svrhu otkrivanja sigurnosnih anomalija/događaja odnosno pravovremenog otkrivanja incidenata
    - odgovor na incidente - automatizacija i forenzika
- SIEM = XDR + Log management
- naravno da se neka SIEM rješenja reklamiraju kao XDR

**- zaključak:**

- primjereno upravljanje logovima je izuzetno važno
- osnovni cilj je čim prije detektirati zlonamjerne aktivnosti
- u velikoj količini podataka detekcija je veliki izazov
- machine learning je neophodan
- pojašnjenje pojmova XDR, EDR, SIEM

# Predavanje 4 - Mrežna sigurnost

**- najveći DDoS napad ikad:**

- dosegao 398 milijuna requestova po sekundi (rps)
- za osjećaj razmjera, taj dvominutni napad generirao je više requestova od ukupnog broja pregleda članaka na Wikipediji tijekom cijelog 9. mj. 2023.

**- vatrozidi (osnovne informacije):**

- filtriranje mrežnog prometa jedan je od temeljnih koncepata mrežne sigurnosti (i jedan od najstarijih - prvi vatrozidi pojavljuju se 1989.)
- uređaji koji omogućavaju filtriranje (eng. *firewall*)
    - ovisno o načinu rada mogu biti osobni, mrežni ili aplikacijski
    - „jednostavno“ filtriranje mogu provoditi i drugi mrežni uređaji
        - npr. usmjerivači s pristupnim listama (ACL-ovi)
    - mogu biti hardverski i softverski
- osnovna funkcija vatrozida je zaštita računala od napada na mrežnoj razini
- moderni vatrozidi implementiraju čitav niz funkcionalnosti
- povijesno su se stavljali samo na vezu prema internetu
- koriste se za segmentaciju interne mreže
- sigurnosna politika vatrozida definira njegovo ponašanje
    - vrlo osjetljiva konfiguracija
    - izbjegavati pravila s prevelikim dopuštenjima
    - redovita provjera pravila
- danas gotovo svi vatrozidi implementiraju tzv. **nulto pravilo**
    - nulto pravilo kaže: odbaci sav mrežni promet
    - administrator mora definirati promet koji dozvoljava, sve ostalo vatrozid blokira
    - ovo se zove **whitelisting** pristup
- vatrozidi mogu filtrirati promet na svim ISO/OSI razinama

**- paketni filtri (eng. *packet filter*):**

- prva generacija vatrozida
- jednostavan uređaj koji primjenjuje određena pravila na mrežni promet
- sastavni dio usmjerivača
- sigurnosna politika se određuje prema sljedećim parametrima:
    - izvorišna IP adresa
    - ciljna IP adresa

    - vrsta mrežnog prometa
    - izvorišni i ciljni mrežni port
- obično se postavljaju na granične točke računalnih mreža
- uspostavlja osnovnu razinu informacijske sigurnosti
    - cilj je odbaciti „smeće“
- glavna prednost fleksibilnost i brzina
- imaju neke velike nedostatke
    - ne provjeravaju više ISO/OSI razine
    - ne analiziraju mrežni promet pa nisu u stanju pratiti detaljno stanje komunikacijskih veza

**- proxy/circuit vatrozidi:**

- klijentsko računalo zapravo uspostavlja vezu s vatrozidom
    - može biti vidljivo, ali i transparentno
- vatrozid uspostavlja vezu s ciljnim računalom
    - nadgleda promet i u slučaju enkripcije
    - može prekinuti vezu prema obje strane
- striktno nadgledaju mrežni promet i sukladnost standardima
- integrirani s antivirusnim programima
- generiraju detaljne log zapise
    - imaju više informacija o kontekstu veze
- za svaku aplikaciju potrebno kreirati proxy
- nedostatak su zahtjevi na resurse
    - unošenje latencije
    - za nadgledanje SSL-a koriste se „lažni“ certifikati
    - rijetko se postavljaju na kritične sustave (u stvarnom vremenu)

**- detaljna analiza mrežnih protokola:**

- eng. *stateful inspection -> Checkpoint*
- čuvaju informacije o uspostavljenim vezama
    - neće dozvoliti prolaz paketa koji nema uspostavljenu vezu
    - informacije se čuvaju u internoj tablici
    - razumiju kontekst komunikacije
- nije potreban proxy za svaku aplikaciju
- prednost je brzina rada

**- vatrozidi nove generacije (NGFW):**

- tradicionalni vatrozidi ne ispituju detaljno mrežni promet
- nemaju sposobnost razlikovanja web prometa (koji predstavlja većinu komunikacije) -> rade na principu sve ili ništa
- najveća razlika između tradicionalnih i NGFW je svjesnost aplikacija -> mogu definirati korisnička pravila prema aplikacijama koje se koriste -> „safe application enablement“
- **funkcionalnosti:**
    - detaljno ispitivanje mrežnog prometa
    - IPS funkcionalnost
    - svjesnost aplikacija i detaljna kontrola pristupa
    - integracija s imeničkim servisima (pristup prema korisniku)
    - implementacija black lista i white lista
    - integracija s Threat Intelligence
    - analiza malwarea -> sandboxing
    - dekripcija prometa
    - inline machine learning

**- Three-leg implementacija:**

- cilj je odvojiti tri segmenta mreže:
    - javni dio - Internet
    - DMZ - demilitarizirana zona
        - segment mreže u kojoj se nalaze javni servisi tvrtke
        - samo je ovaj segment dostupan s javnog dijela (interneta)
        - dostupan je, po potrebi, s interne mreže
    - interna mreža
        - interni poslužitelji i računala
        - može biti dodatno segmentirana
- može postojati jedan ili više DMZ-ova zbog različitih zahtjeva sigurnosti

**- SASE (Security Access Service Edge):**

- odnosi se na cijeli okvir, a ne specifičnu tehnologiju
- Gartner je 2019. definirao SASE okvir kao cloud-based cybersecurity rješenje koje nudi sveobuhvatni WAN s opsežnim sigurnosnim funkcijama mreže (kao što su SWG, CASB, FWaaS i ZTNA) za podršku potrebe dinamičkog sigurnog pristupa digitalnih poduzeća
- naslijeđeni pristupi inspekciji i provjeri kao što je to prosljeđivanje prometa putem usluge MPLS (Multiprocotol Label Switching) na vatrozide u podatkovnom centru učinkovito je ako je to mjesto gdje su korisnici

- danas s mnogo korisnika na udaljenim lokacijama, kućnim uredima i sličnom prosljeđivanje udaljenog korisničkog prometa na podatkovni centar, pregled i ponovno slanje sklono je smanjenju produktivnosti i naštetiti korisničko iskustvo krajnjeg korisnika
- ono po čemu se SASE ističe od drugih sigurnosnih strategija i rješenja je to da je siguran i izravan
- umjesto da se oslanja na sigurnost podatkovnog centra, promet iz uređaja korisnika pregledava se na obližnjoj točki prisutnosti (eng. *the enforcement point*) i od tamo se šalje na odredište
- to znači učinkovitiji pristup aplikacijama i podatcima što ga čini daleko boljom opcijom za zaštitu distribuirane radne snage i podataka u cloudu

**- aplikacijski vatrozidi:**

- specijalizirani vatrozidi za zaštitu pojedine aplikacije/protokola
- danas su vrlo popularni web, email i DNS aplikacijski vatrozidi

**- DNS security:**

- sastavni dio vatrozida
- zasebna rješenja
- threat intelligence, machine learning primijenjeni na DNS upite

**- email security:**

- i Google i Microsoft pružaju osnovnu higijenu emailova uključujući:
    - blokiranje emailova od poznatih loših pošiljatelja
    - skeniranje privitaka antivirusom
    - blokiranje emailova s poznatim lošim URL-ovima
    - analiza sadržaja za prepoznavanje spam pošte

**- SEG (Secure Email Gateway) ili ICES (Integrated Cloud Email Security):**

- malware i spam zaštita
- integracija threat intelligencea
- sandboxing
- URL rewriting
- BEC zaštita

**- web aplikacijski vatrozidi:**

- softversko ili hardversko rješenje koje štiti web aplikacije od prijetnji napada
- rješenje mora razumjeti zaštitu weba na aplikacijskoj razini (npr. HTTP i HTTPS komunikaciju, XML/SOAP i web servise)
- detektira/sprječava OWASP Top Ten prijetnje
- učenje anomalija (ML/AI)

**- CDN (Content Delivery Network):**

- odnosi se na geografsku distribuiranu grupu poslužitelja koja radi zajedno kako bi brzo isporučili internetski sadržaj
- prednosti korištenja:
    - brzina učitavanja web stranica
    - dostupnost web stranica
    - sigurnost web stranica (DDos)
- CDN-ovi su dizajnirani tako da rukuju velikim količinama podataka pa ako tvrtka doživi veliki porast u broju requestova tipičan za DDoS napad, može odgovoriti redistribucijom tog prometa osiguravajući da ne dođe do izvornih poslužitelja i renderira stranicu offline

**- analiza mrežnog prometa:**

- analiza mrežnog prometa koristi kombinaciju ML/AI, napredne analitike te detekcije temeljem pravila u svrhu otkrivanja sumnjivih aktivnosti na korporativnoj mreži
- analiza kompletnog prometa ili slike protoka i volumena mrežnog prometa (NetFlow) u stvarnom vremenu
- analiza sjever/jug prometa (parametar) i istok/zapad (lateralni promet)
- modeliranje normalnog prometa te definiranje alerta za anomalije
- rješenja koja rade analizu na kompletnom prometu puno su preciznija
- izazov -> analiza kriptiranog prometa

**- analiza kriptiranog prometa:**

- JA3 je metoda za stvaranje SSL/TLS fingerprintsa klijenta koja bi se trebala lako proizvesti na bilo kojoj platformi i može se lako dijeliti za threat intelligence
    - To initiate a SSL session, a client will send a SSL Client Hello packet following the TCP 3-way handshake
    - This packet and the way in which it is generated is dependant on packages and methods used when building the client application. The server, if accepting SSL connections, will respond with a SSL Server Hello packet that is formulated based on server-side libraries and configurations as well as details in the Client Hello

    - Because SSL negotiations are transmitted in the clear, it's possible to fingerprint and identify client applications using the details in the SSL Client Hello packet

**- Cyber Threat Intelligence:**

- SANS: „Prikupljanje, klasifikacija i iskorištavanje znanja o protivnicima"
- Gartner: „Znanje temeljeno na dokazima, uključujući kontekst, mehanizme, pokazatelje, implikacije i savjete usmjerene na djelovanje o postojećoj ili novonastaloj prijetnji ili opasnosti za imovinu"
- djelotvorna inteligencija o akterima prijetnji
- **definicija:**
    - strateška:
        - prijetnje za organizaciju
        - okruženje
        - sektor
        - trendovi
        - regulatorne promjene
    - taktička:
        - metodologija napadača
        - alati
        - tehnike (TTP)
    - tehnička:
        - indikatori kompromitacije
    - operacijska:
        - detalji napada

**- IOC (Indicators of Compromise):**

- indikatori kompromitacije
- digitalni artefakt koji s velikom sigurnošću označava računalnu kompromitiranost:
    - MD5 hash
    - IP adrese
    - URL
    - domene

**- IOA (Indicators of Attack):**

- indikatori napada
- fokusiraju se na detekciju namjera napadača -> ponašanje, proaktivni (npr. sumnjivi PowerShell)

**- WannaCry IOC/IOA:**

- različiti MD5 hashevi

**- threat intel analiza:**

- analiza:
  - interni intel
  - threat podatci (forumi, društvene mreže, dark web…)
  - externi intel
- automatizacija i ažurnost može značajno povećati učinkovitost
- security analitičari

**- threat intel platforma:**

- organizacija threat podataka
- davanje konteksta threat podacima
- automatizacija s ostalim alatima
- machine learning
- open source:
  - Alien Vault OTX
  - Cymon
  - ThreatMiner
- komercijalne:
  - ThreatConnect
  - Anomali
  - RecordedFuture

**- security integracija:**

- SIEM
  - jednostavna integracija
  - veliki broj događaja
- vatrozid
  - preventivno djelovanje
  - false positive (npr. IOC za hosting poslužitelj)

**- Zaključak:**

- pregled različitih vrsta vatrozida, vatrozidi nove generacije, aplikacijski vatrozidi
- SASE
- analiza mrežnog prometa rastuće je područje
- pojašnjeni pojmovi za TI

# Predavanje 5 - Sigurnost web aplikacija

**- MOVEit napadi:**

- 0-day ranjivost na MOVEit poslužitelju (SQL injection)
- napadi su bili brzi i koordinirani
- napad je započeo na američki Dan sjećanja kada je bio produženi vikend
- iskoristili su ranjivost za izvođenje proizvoljno učitane datoteke putem usluge moveitsvc
    - povezali su se s određenim SQL bazama
    - eksfiltrirali su sadržaj datoteka koje je hostao MOVEit Transfer
    - kada je MOVEit Transfer bio spojen na Azure blob storage, eksfiltrirali su sadržaj određenih datoteka u Azure servis za blob storage
- broj napadnutih organizacija: 2771
- broj napadnutih individualaca: 95 788 491
- većinom organizacijski računi koji su bili smješteni u USA (78,9%)

**- napadi na web aplikacije:**

- web aplikacije predstavljaju osnovu elektroničkog poslovanja
    - jednostavno dostupne velikom broju korisnika
- web aplikacije - pogled iz perspektive sigurnosti
    - najizloženiji dio informacijskog sustava
    - vrlo zahtjevne za monitoring
- rezultat
    - iznimno velik broj napada

**- tehničke i logičke ranjivosti:**

- **tehničke ranjivosti**
    - relativno jednostavno ih je moguće otkriti automatiziranim alatima za provjeru ranjivosti
    - problemi u konfiguraciji, loše filtriranje korisničkog unosa i prikaza…
- **logičke ranjivosti**
    - ranjivosti u logici poslovne aplikacije
    - praktički nemoguće otkriti automatiziranim alatima

**- OWASP project:**

- **O**pen **W**eb **A**pplication **S**ecurity **P**roject
- projekti -> skup dokumenata i alata koji imaju za cilj:
    - spriječiti propuste
    - detektirati propuste
    - integrirati sigurnost u SDLC

**- OWASP top 10 web aplikacijskih rizika:**

- najvažniji projekt vezano za sigurnost web aplikacija
- rizici su određeni prema njihovoj metodologiji
- rizik = vjerojatnost * utjecaj
    - vjerojatnost
    - znanje potrebno za iskorištavanje
    - motivacija
- lakoća otkrivanja i iskorištavanja propusta
- tehnički i poslovni utjecaj

**- A1 - Broken Access Control:**

- kontrola pristupa provodi politiku tako da korisnici ne mogu djelovati izvan predviđenih dopuštenja
- greške obično dovode do neautoriziranog otkrivanja informacija, modifikacije, uništenja svih podataka ili obavljanja djelatnosti izvan korisničkih dopuštenja
- kršenje „least privilege“ ili „deny by default“ principa gdje se pristup treba odobriti samo za određene mogućnosti, role ili korisnike, ali je dostupan svima
- zaobilaženje kontrolnih provjera izmjenom URL-a, interne aplikacije, HTML stranice ili korištenjem alata za modificiranje API zahtjeva
- pristup API-ju s nedostatkom access controlsa za POST, PUT i DELETE
- EoP (Elevation of Privilege) - ponašanje kao korisnik bez prijave ili ponašanje kao admin dok je ulogiran zapravo user
- primjer: Yahoo - napadači su pronašli način kako da krivotvore authentication cookiese koji su im dali pristup računima bez potrebe za lozinkom, ti cookiesi su im dopustili da ostanu logirani u hakiranim računima nekoliko tjedana ili neodređeno
- što učiniti:
    - defaultno zabraniti pristup prema svim privatnim resursima
    - minimizirati Cross-Origin Resource Sharing (CORS)
    - implementirati mehanizam kontrole pristupa i koristiti ga za svaki zahtjev koji obrađuje privatne podatke

**- Optus data breach:**

- podatci o 11,2 milijuna korisnika
- tražili su 1 milijun dolara da ne prodaju te podatke
- imali su jednostavan API endpoint za koji su napadači napisali skriptu koja je uvećavala ID za 1 i tako uzimala podatke o svakom useru
- nije implementirana nikakva zaštita za API pristup:
    - autentikacija
    - teško pogodivi ID
    - rate limiting
- Optus se ispričao za data breach i osigurao 140 milijuna dolara za pomoć klijentima kako bi obnovili osobne dokumente te su obećali kako će investirati više u zaštitu sustava i ponovnu izgradnju povjerenja kod kupaca

**- A2 - Cryptographic Failures:**

- osjetljive podatke potrebno je prvo identificirati
- ne pohranjivati osjetljive podatke nepotrebno
- primjena kriptografije u gibanju i mirovanju
- identificirati sva mjesta na koja se isti pohranjuju:
    - računalni resursi u cloudu
    - baze podataka, datoteke, direktoriji, log datoteke…
    - backup datoteke
- korištenje jakih kriptografskih algoritama (npr. *salting*)
- primjereno upravljanje ključevima
- kako se zaštititi?
    - detaljna provjera arhitekture
    - identificiranje mjesta gdje se pohranjuju osjetljivi podatci
    - osiguravanje pohranjenih podataka
        - enkripcija podataka
    - koristiti odgovarajuće mehanizme zaštite
        - enkripcija datoteka, baze podataka, stupaca u bazi podataka
        - korištenje poznatih, snažnih algoritama za enkripciju
            - posebnu pažnju posvetiti rukovanju ključevima

**- zaboravljeni web server:**

- za potrebe konferencije napravljena je web stranica koja je uključivala prostor za uploadanje dokumenata anonimno putem URL-a
- nitko se nije sjetio (ili nije imao posao) ugasiti tu stranicu nakon što je konferencija završila te je tako ostala godinama
- dobili su kaznu od 160 000 dolara od Britain's Information Commissionera (ICO)
- baza je sadržavala osobne podatke od 19 500 studenata, zaposlenika, alumnija i gostujućih predavača na konferencijama Sveučilišta
- u podatcima je bilo navedeno također 3500 intimnih podataka o ljudima kao što su poteškoće u učenju, bolesti osoblja, alergije na hranu…
- prvotni upad u bazu dogodio se 2013. godine, a do najosjetljivijih podataka se došlo 2016. godine kada je jedan od napadača to i objavio na Pastebinu

**- A3 - Injection:**

- injection ranjivosti nastaju kada aplikacija pošalje korisnikov unos interpreteru
    - korisnikovom unosu ne možemo vjerovati
    - sukladno tome ga i treba tretirati
- što je interpreter?
    - bilo koji dio aplikacije koji prima ulazni niz znakova i interpretira ih kao naredbe
        - klasično SQL, ali može biti i ljuska sustava, LDAP, Xpath…
- najčešći primjer je SQL injection
    - veliki broj ranjivih aplikacija
    - obično kritične ranjivosti
- koraci:
    - aplikacija predstavlja formu napadaču
    - napadač šalje napad u podatcima obrasca
    - aplikacija prosljeđuje napad na bazu podataka u SQL upitu
    - baza podataka pokreće upit koji sadrži napad i šalje šifrirane rezultate natrag do aplikacije
    - aplikacija dekriptira podatke kao normalno i šalje rezultate do usera
- kako se obraniti?
    - korijen problema sa SQL injectionom je miješanje koda i podataka
    - upit i podatke treba slati SQL serveru zasebno:
        - 1. Prepared statements (with Parameterized Queries)
            - In a prepared statement, the values that will be inserted into a SQL query are sent to the SQL server after the actual query is sent to the server data input by a hacker can’t be interpreted as SQL

        - 2. Stored procedures
            - The difference between prepared statements and stored procedures is that the SQL code for a stored procedure is defined and stored in the database itself, and then called from the application
- **Cross Site Scripting (XSS):**
    - XSS je script injection
    - uzroci: nedovoljno filtriranje podataka (ulaznih/izlaznih podataka)
    - izvršavanje malicioznog koda unutar web preglednika korisnika koji posjećuje ranjivu web stranicu
        - JavaScript (AJAX), VBScript, ActiveX, HTML, Flash
    - vrlo česta i podcijenjena ranjivost
    - napad uključuje tri strane:
        - napadač, ranjiva web stranica, klijent (web browser)
        - meta napada je korisnik, ne web aplikacija
    - XSS posljedice napada:
        - krađa cookiea/preuzimanje sessiona
        - lažiranje sadržaja web stranice
            - prikaz lažnih informacija
            - web defacement
            - phishing
        - krađa identiteta
        - napadi na internu računalnu mrežu

**- A4 - Nesigurni dizajn:**

- novi rizik koji se odnosi na loš dizajn i arhitekturu
- razlika između nesigurnog dizajna i nesigurne implementacije
- implementirati najbolju praksu za siguran razvoj softvera

**- A5 - Nesigurna konfiguracija:**

- web aplikacije baziraju se na sigurnoj infrastrukturi
    - web poslužitelj
    - framework (ASP, PHP…)
    - operacijski sustav
- vrlo često framework „štiti“ programera od grešaka
    - moderni framework štiti od SQL injectiona, XSS-a i slično
    - no i dalje trebamo biti upoznati s ovim ranjivostima
- defaultne postavke
    - administratorska sučelja dostupna svima

    - defaultni korisnički računi
- kako se zaštititi?
    - standardne preporuke za hardening
    - potrebno zaštititi cijelu platformu
        - OS, web poslužitelj, framework
        - ne ignorirati lokalne ranjivosti
    - redovito instalirati zakrpe
    - provjera sa automatiziranim alatima
        - dobri u pronalaženju problema u konfiguraciji

**- A6 - Ranjive i zastarjele komponente:**

- korištenje ranjivih/zastarjelih komponenti (OS, baza, web poslužitelj, aplikacije, programski okvir…)
- neprimjereno/neučinkovito upravljanje ranjivostima
- ne testiranje kompatibilnosti ažuriranih komponenti

**- A7 - Identifikacijske/autentifikacijske pogreške:**

- automatski autentifikacijski napadi
- korištenje slabih i/ili inicijalnih lozinki
- NIST preporuke se ne slijede
- nezaštićena pohrana lozinki
- nekorištenje MFA

**- A8 - Software and Data Integrity Failures:**

- pogreške u integritetu softvera i podataka odnose se na kod i infrastrukturu koja ne štiti od povrede integriteta
- primjer: kada se aplikacija oslanja na plugin-ove, library-eve ili module iz nepouzdanih izvora, repozitorija i mreža za isporuku sadržaja (content delivery network)
- nesiguran CI/CD pipeline može predstavljati potencijal za neovlašteni pristup, maliciozan kod ili ugrožavanje sustava
- potrebno uspostaviti procesne i softverske kontrole (korištenje specijaliziranih alata) nad vanjskim komponentama

**- A9 - Nedovoljno logiranje i nadziranje:**

- iskorištavanje nedovoljnog logiranja i monitoringa je temelj skoro svakog većeg incidenta
- napadači se oslanjaju na nedostatak monitoringa i pravovremene reakcije kako bi postigli svoje ciljeve bez da budu otkriveni

**- A10 - Server-Side Request Forgery (SSRF):**

- napad gdje poslužitelj može biti prevaren da se poveže s poslužiteljem s kojim se nije namjeravao
- SSRF nedostatci se javljaju svaki put kada web aplikacija dohvaća remote resurs bez validacije URL-a koji je naveo korisnik

**- DevSecOps:**

- predstavlja Development, Security and Operations
- okvir je koji integrira sigurnost u sve faze životnog ciklusa razvoja softvera
- to je način automatizacije procesa razvoja, testiranja, deploymenta i održavanja aplikacija uz osiguravanje da su sigurnosni i sukladnosni zahtjevi ispunjeni

**- Alati za provjeru sigurnosti web aplikacija:**

- **Static AST (SAST)** - this technology analyzes an application's source and binary code for security vulnerabilities, typically at the programming or testing phases of the software lifecycle
- **Dynamic AST (DAST)** - this testing method analyzes applications while they're running. It simulates attacks against an application, analyzes the application's reactions to the attack, and then determines whether it's vulnerable or not

**- Zaključak:**

- Sigurnost Web aplikacija je uvijek aktualna tema
- OWASP Top 10 predstavlja izvrstan okvir
- DevSecOps

# Predavanje 6 - Napredni napadi i kontrole

**- Banco de Chile:**

- 9000 računala zaraženo ransomwareom (KillDisk wiper malware)
- oštećuje MBR i reboota računalo
- zašto?
    - ukradeno 11 milijuna dolara kroz sumnjive SWIFT transakcije

**- Bangladeš napad:**

- veljača 2016. - pokušali isprazniti financijske rezerve centralne banke u Bangladešu u iznosu od milijarde dolara
- godinu dana neprimijećeni na internoj mreži
- kompromitirali SWIFT, onemogućili rad ključnog printera
- planirali napad tako da su imali 4 dana za prebacivanje sredstava
- pokušali prebaciti sredstva na banku u Filipinima
- 35 transfera na RCBC banku u Jupiter ulici Manila
- nisu prošle sve transakcije zbog ključne riječi „Jupiter“ koja je naziv sankcioniranog iranskog broda
- prošlo je 5 transakcija u vrijednosti od 101 milijuna dolara

**- Lazarus grupa:**

- koriste različite tehnike i malware familije (više od 45)
- povezuju se sa Sjevernom Korejom
- vrlo moguće da je Lazarus grupa bila iza WannaCry napada
- Sony Pictures:
    - studeni 2014.
    - izašli su osobni podatci o Sonyjevim zaposlenicima i njihovim obiteljima, e-mailovi između zaposlenika, informacije o plaćama u firmi, kopije do tada neobjavljenih filmova
    - obrisana infrastruktura
    - prijetnja terorističkim napadima na kina koja se odluče na prikazivanje filma „Intervju“, komedije o ubojstvu sjevernokorejskog predsjednika Kim Jong-Una
    - film pušten na mala vrata

**- APT (Advanced Persistent Threat):**

- termin su 2006. skovale Američke zračne snage (US Air Force) kako bi olakšale komunikaciju s medijima u slučaju napada kojeg nisu smjele klasificirati
- kasnije je preuzet od strane stručnjaka za računalnu sigurnost
- zahtijeva izrazito velike ljudske i novčane resurse
- mogu ga izvesti vlade ili velike organizacije
- **napredan** - široki spektar tehnologija, tehnika i metodologija upada u računalne sustave
- **perzistentan** - neprestano praćenje i interakcija s metom
- **prijetnja** - koordinirana skupina ljudi, a ne automatizirani programski kod
- APT napadi često koriste dotad nepoznate propuste u računalnim sustavima, programima ili operacijskim sustavima (eng. *zero-day exploits*)
- upotreba „zero-day" exploit programa svojstvena je za APT napade pošto je razvoj takvih programa skup, složen i dugotrajan, a rijetki imaju dovoljno resursa za razvoj

**- Napredne kontrole za umanjenje rizika od APT-a:**

- **CIS Top 18 IG3:**
  - sastoji se od dodatne 23 mjere zaštite
- **Threat Hunting:**
  - aktivna potraga za anomalijama na poslužiteljima, osobnim računalima… koje mogu biti znakovi kompromitacije, neovlaštenih upada i sl.
  - nije reakcija na alerte u sustavima za detekciju već aktivna potraga:
    - **procesi:**
      - lovci traže procese s određenim imenima, file pathovima, mrežnom aktivnošću… kako bi pronašli procese koji mijenjaju unose u registru, imaju specifične child procese, pristup određenim softverskim libraryjevima, imaju određene MD5 hasheve, uključuju poznate loše datoteke
    - **izvršne datoteke:**
      - lovci traže binarne datoteke s određenom checksumom, file nameovima, pathovima, određene modifikacijske registre
    - **mrežne postavke:**
      - mrežna aktivnost po specifičnim nazivima domene i IP adresama
    - **izmjene sistemskih postavki** (npr. Windows registry):
      - lovci mogu tražiti specifične dodatke i modifikacije registry keyeva
  - vještine huntera:
    - lovci su znatiželjni, strastveni, vješti u korištenju više alata i razumijevanju te izvlačenju maksimuma iz tih alata
    - što je najvažnije, lovci su inovativni analitičari koji dobro razumiju njihovo okruženje i njihovu organizaciju da znaju postaviti prava pitanja i pronaći odgovore

- **Deception:**
  - svrha:
    - može dodati nasumičnost i nepredvidivost arhitektura, mrežnog prometa, usluga ili stvaranje izazovnije protivnikove okoline
    - zbuniti i zavesti protivnike
    - utjecaj na protivnikov proces donošenja odluka
    - umanjiti sposobnost protivnika da se miče lateralno
    - ne razlikuje se pravo od lažnog -> prave se pogreške
    - povećanje troškova napadača -> trošenje više vremena/ponovni početak
    - nepoželjna ekonomija -> traži lakšu metu
- **Simulacija napada:**
  - simuliranje „pravih“ napada u stvarnom okruženju
  - red teams
    - internal or external entities dedicated to testing the effectiveness of a security program by emulating the tools and techniques of likely attackers in the most realistic way possible
  - blue teams
    - internal security team that defends against both real attackers and Red Teams
  - purple teams
    - ensure and maximize the effectiveness of the Red and Blue teams. They do this by integrating the defensive tactics and controls from the Blue Team with the threats and vulnerabilities found by the Red Team into a single narrative that maximizes both. Ideally Purple shouldn’t be a team at all, but rather a permanent dynamic between Red and Blue

**- MITRE ATT&CK:**

- javno dostupna baza taktika i tehnika napadača temeljena na analizama napada
- ATT&CK baza znanja iznimno je korisna u detekciji napada
- radi poduzimanja primjerenog sigurnosnog odgovora važno je identificirati u kojoj smo fazi napada
- sigurnosni alati integrirani s MITTRE ATT&CK

**- Zaključak:**

- APT napadi su rijetki, ali iznimno moćni
- povrh standardnih sigurnosnih kontrola potrebno implementirati dodatne kontrole koje su fokusirane na detekciju
- istaknute su: deception, threat hunting i simulacija napada

# Predavanje 7 - Kontinuitet poslovanja

**- kontinuitet poslovanja:**

- odnosi se na dvije stvari koje su ključne da poslovanje dostigne svoje ciljeve:
  - isporuka otpornog (elastičnog) poslovanja
  - zaštita reputacije (ugleda, brenda)

**- ISO 22301:**

- puni naziv: Societal security - Business continuity management systems - Requiremenst
- definira zahtjeve za Sustav upravljanja kontinuitetom poslovanja (eng. *Business Continuity Management System - BCMS*)
  - dio ukupnog sustava upravljanja uz pomoću kojeg se planira, implementira, održava i poboljšava kontinuitet poslovanja
- **kontinuitet poslovanja** = sposobnost organizacije da nastavi s isporukom proizvoda i usluga unutar prihvatljivih vremenskih okvira s unaprijed definiranim kapacitetom tijekom prekida
- **prekid** = incident, očekivan ili neočekivan, koji uzrokuje neplanirano, negativno odstupanje od očekivane isporuke proizvoda i usluga u skladu s ciljevima organizacije

**- najvažnije aktivnosti:**

- **Plan kontinuiteta poslovanja**
  - dokumentirane informacije koje omogućuju organizaciji da odgovori na prekid i nastavi, obnovi i oporavi isporuku proizvoda i usluga u skladu s njezinim ciljevima kontinuiteta poslovanja
- **Disaster Recovery**
- **Analiza utjecaja na poslovanje i Procjena rizika** -> određuju strategiju kontinuiteta poslovanja
- **Upravljanje incidentnim/kriznim situacijama**

**- BIA (Business Impact Analysis):**

- definicija:
  - Proces analize poslovnih aktivnosti koje podržavaju produkte i usluge organizacije te učinka koji poslovni prekid može imati na njih
- zašto je BIA važna?
  - bitno je saznati koliko brzo organizacija treba reagirati nakon prekida
  - temeljem toga se definira D/R strategija i rješenja (definira se RTO i RPO)

- bez BIA analize imamo dva scenarija:
  - podcijenjenost učinka incidenta -> prevelika šteta, učinak incidenta na organizaciju
  - precijenjenost učinka incidenta -> previše plaćamo za DR rješenje

**- RPO (Recovery Point Objective):**

- ciljana točka oporavka - maksimalno dozvoljena veličina gubitka podataka u vremenskim jedinicama
- definira maksimalni gubitak podataka
- određuje se tijekom BIA analize
- definira backup politiku

**- određivanje MTPD-a (Maximum Tolerable Period of Disruption):**

- maksimalno dozvoljeno vrijeme prekida poslovanja, prije značajnih (neprihvatljivih) gubitaka za organizaciju
- zapravo vrijeme nakon kojeg nema povratka

**- RTO (Recovery Time Objective):**

- ciljano vrijeme oporavka sustava
- vremensko razdoblje nakon incidenta unutar kojeg:
  - proizvod ili usluga moraju se nastaviti
  - ili aktivnost mora biti nastavljena
  - ili se resursi moraju povratiti
- RTO mora biti manji od MTPD-a
- u praksi se organizacije fokusiraju na RTO

**- RTO, MTPD od poslovnih aktivnosti:**

- identificirati koje aktivnosti podržavaju kritične proizvode/usluge
- koliko dugo može korisnik čekati da isporučimo proizvod/uslugu?
- kontinuirane aktivnosti (kratko trajanje) -> Internet bankarstvo (uplate/isplate), telekomunikacijske usluge
- periodičke aktivnosti (dugo trajanje) -> proizvodnja, projekti
- periodičke aktivnosti zahtjevnije za procjenu

**- definiranje RPO i RTO:**

- RPO - How recent is the point in time for your recovery?
- RTO - How fast can you restart a failed application?

} RPO + RTO = Acceptable Business Risk

**- Upravljanje rizikom:**

- ista metodologija
- fokus na rizike koji utječu na kontinuitet poslovanja

**- Upravljanje krizom:**

- upravljanje krizom = proces kojim organizacija upravlja neželjenim događajem koji prijeti uništenju organizacije, njenih interesnih skupina, odnosno njenog ugleda
- tri elementa su zajednička za krizu:
    - 1. prijetnja organizaciji
    - 2. element iznenađenja
    - 3. kratko vrijeme za donošenje odluke

**- Krizna komunikacija:**

- Budite proaktivni i spremni: nemojte čekati da se kriza dogodi prije nego što izradite plan komunikacije u kriznim situacijama. Identificirajte potencijalne rizike i unaprijed razvijte sveobuhvatnu strategiju kriznog komuniciranja
- Dajte prioritet transparentnosti i autentičnosti: tijekom krize transparentnost je ključna. Pružite točne informacije, čak i ako su detalji u početku ograničeni
- Komunicirajte dosljedno i pravovremeno: dosljednost i pravovremenost ključni su u kriznom komuniciranju. Osigurajte da su sve poruke usklađene preko svih komunikacijskih kanala i glasnogovornika
- **Krizna komunikacija i društvene mreže:**
    - društvene mreže ubrzale su brzinu širenja informacija
    - testiranja i vježbe temeljene na dobrom planu krizne komunikacije kao i „dobri alati“ za praćenje (nadzor) društvenih mreža mogu na vrijeme uočiti pokušaje razbijanja „upravljanja krizom“
    - prednost i nedostatak

**- Zaključak:**

- svaka organizacija želi nastaviti s poslovanjem i nakon neke havarije
- u tu svrhu potrebno je dobro planirati
- identificirati kritične aktivnosti i resurse potrebne za njihovo izvođenje
- imati u vidu financijske aspekte
- krizna komunikacija je vrlo važna

# Sretno na ispitu!