Sigurnost računalnih sustava

Pregled ostalih područja sigurnosti

doc. dr. sc. Ante Đerek
izv. prof. dr. sc. Stjepan Groš
izv. prof. dr. sc. Miljenko Mikuc
izv. prof. dr. sc. Marin Vuković

Jesmo li obradili sva područja sigurnosti?

- Dosta toga smo obradili tijekom ovog predavanja
  - Naglasak je bio na nekim bitnijim područjima sigurnosti
  - Međutim, tek smo „grebali po površini” svake teme
- Ali ima još područja sigurnost s kojima smatramo da se trebate upoznati
  - S obzirom na raspoloživo vrijeme ne možemo ići u detalje, ali u ovom predavanju ćemo napraviti kratki pregled tih tema
    - Cilj je da vam skrenemo pozornost na njihovo postojanje, a oni koji žele imat će prilike na višim godinama neke od tih tema dublje proučavati

Teme

- Digitalna forenzika
- Upravljanje sigurnošću
- Rukovanje incidentima
- Obavještajni rad u kibernetičkom prostoru
- Sigurnost strojnog učenja
- Privatnost i anonimnost

Pregled ostalih područja sigurnosti

Digitalna forenzika

Motivacija za digitalnu forenziku (1)

- Pretpostavimo da je učinjeno nekakvo kriminalno djelo
  - Recimo da je provaljeno na neko računalo unutar organizacije te je potom to računalo iskorišteno da se obavljaju razne kriminalne aktivnosti
    - Napadi na druge organizacije sa značajnom štetom, širenje poruke čiji sadržaj vrijeđa, maltretira, širi govor mržnje, prijeti, itd.
- Protiv vlasnika računala (organizacija) prijeti se tužbama
- Sistem administrator u organizaciji otkriva da je navedenom računalu pristupio bivši djelatnik te zloupotrijebio to računalo

Motivacija za digitalnu forenziku (2)

- Na temelju rezultata istrage sistemskog administratora Organizacija podiže tužbu protiv bivšeg djelatnika i javno ga proziva za počinjenje kaznenog djela
- Sud oslobađa bivšeg djelatnika optužbi
  - **Prihvaćen je argument obrane da dokazi nisu ispravno prikupljeni, pohranjeni i analizirani!**
- Bivši djelatnik podiže kontratužbu i traži obeštećenje

Motivacija za digitalnu forenziku (3)

- Pitanje je kako prikupiti dolaze kojima se dokazuje počinjenje kriminalnog djela
  - Spriječiti sumnju da je onaj tko je pregledavao računalo manipulirao podacima (dokazima)?
    - Primjerice, kao u filmovima kada policija podmeće dokaze…
  - Spriječiti sumnju da su izostavljeni relevantni podaci koji idu u prilog opovrgavanja teze da je učinjeno kriminalno djelo?
- Inače se istragom kriminalnih djela bavi kriminalistika, a prikupljanjem dokaza forenzika i forenzičke znanosti
  - Kada su digitalni uređaji u pitanju, koristi se **digitalna forenzika** za prikupljanje podataka

Što je digitalna forenzika

- **Digitalna forenzika** je grana forenzičkih znanosti koja

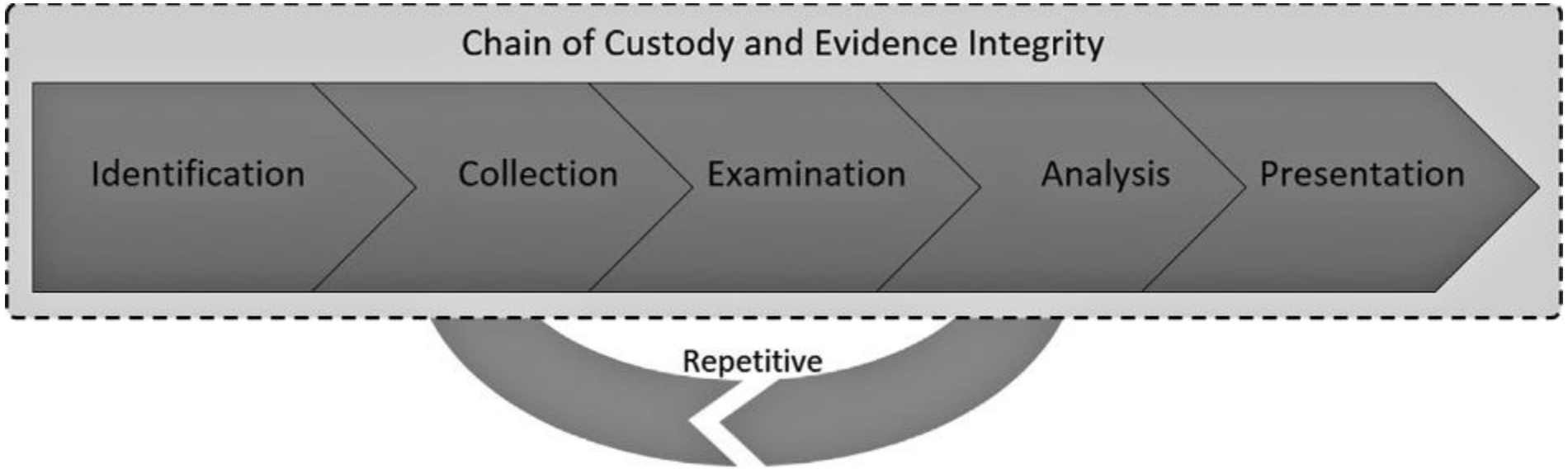
  koristi znanstveno izvedene i dokazane metode za očuvanje, prikupljanje, provjeru valjanosti, identifikaciju, analizu, tumačenje, dokumentiranje i iznošenje digitalnih dokaza izvedenih iz digitalnih izvora u svrhu objašnjavanja ili daljnje rekonstrukcije događaja za koje se utvrdi da su kriminalni, ili pomažući u predviđanju neovlaštenih radnji koje mogu remetiti planirane operacije
- **Digitalni dokaz** je bilo koji digitalni podatak koji pruža pouzdanu informaciju koja podržava ili opovrgava hipotezu o incidentu ili kriminalu
- **Računalna forenzika** – forenzika samo računala

Tko koristi digitalnu forenziku?

- Najčešće digitalnu forenziku koriste policije
  - Kriminalci koriste različite računalne uređaje (mobiteli, računala) te se tijekom istraga javlja potreba za analizom sadržaja tih uređaja u potrazi za mogućim dokazima počinjenja kriminalnih djela
  - Kibernetički kriminalci (engl. cyber criminals) kaznena djela čine u kibernetičkom prostoru („unutar računala”) te je u tim slučajevima digitalna forenzika temeljni izvor dokaza o počinjenju kaznenih djela
- Digitalna forenzika se koristi i u tvrtkama i institucijama
  - Tijekom istrage incidenata kada je potrebno utvrditi što se desilo pri čemu može ali i ne mora postojati mogućnost korištenja utvrđenih činjenica na sudu

Proces provođenja digitalne forenzike

- Proces digitalne forenzike sastoji se od niza koraka
  - Tijekom provođenja svih koraka mora se paziti na podatke kako bi se u svakom trenutku moglo jamčiti integritet i autentičnost digitalnih dokaza



Tehnički aspekti digitalne forenzike

- Digitalna forenzika u tehničkog dijelu značajno koristi elemente drugih područja sigurnosti
  - Analiza logova, kriptoanaliza, analiza mrežnog prometa, pogađanje lozinki, …
- U digitalnoj forenzici velik naglasak se stavlja na otkrivanje mjesta gdje su pohranjeni podaci s digitalnim dokazima koji mogu pomoći u istragama
  - Reverzanje različitih formata pohrane, unutarnjeg načina rada aplikacija i operacijskih sustava („internals”)
  - Mjesta za pohranu nisu samo statička već i dinamička (radna memorija)

Izazovi za digitalnu forenziku

- Privatnost i sigurnost
  - Kriptografska zaštita podataka
- Sve veći memorijski kapaciteti uređaja
  - Znači veliku količinu podataka koju je potrebno analizirati
- Sve veći raspon raznih uređaja
- Računarstvo u oblaku

Pregled ostalih područja sigurnosti

Upravljanje sigurnošću

Motivacija

- U dosadašnjim predavanjima vrlo površinski smo se dotaknuli sigurnosti – i vidljivo je kako tu ima puno detalja
- Pretpostavimo da ste se zaposlili u nekoj tvrtci ili instituciji kao osoba zadužena za sigurnost te tvrtke ili institucije.
  - Kako bi ste pristupili tom poslu? Što bi ste prvo napravili? Kako i kakve si prioritete posložili?
  - **Upravljanje sigurnošću** (engl. security management) je odgovor na navedena pitanja

Upravljanje sigurnošću

- Postizanje i održavanje sigurnosti organizacija je složena aktivnost
  - direktno ovisan o složenosti organizacija i njenom okruženju
- Nužan je ciljan, sustavan i kontinuiran pristup
  - Pokušaj rješavanja taktičkih problema bez poznavanja stanja i cilja sigurno dovodi do neuspjeha
- Upravljanje sigurnošću mora biti sastavni dio upravljanja organizacijom
  - O sigurnosti se brine *Voditelju sigurnosti informacijskog sustava* (engl. Chief Information Security Officer, CISO)
    - Titula, organizacijski položaj i ovlasti i odgovornosti ovise o konkretnoj organizaciji, području i povijesti razvoja organizacije!

Uspostava upravljanja sigurnošću

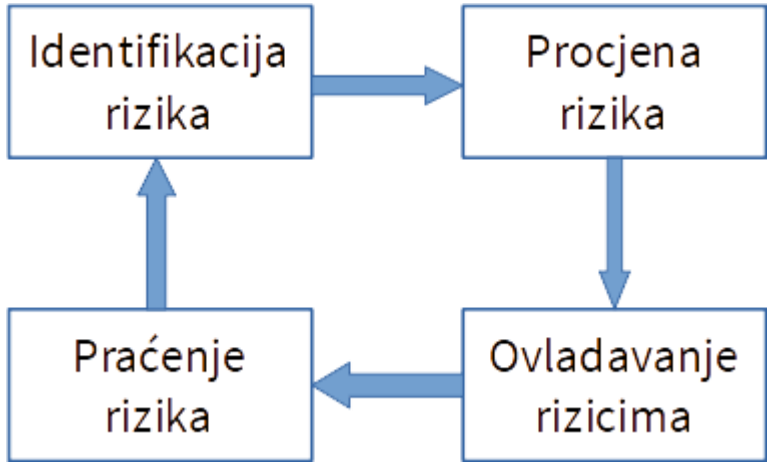
- Upravljanje sigurnošću dio je upravljačke (engl. governance) strukture organizacije
- Ne može se upravljati sigurnošću bez upravljačkog okvira
  - Pravilnici i politike usvojeni od strane Uprave (ili ekvivalentnog upravljačkog tijela) koji definiraju što znači biti siguran, tko je zadužen za sigurnost, koje su ovlasti i odgovornosti te osobe, kako se sigurnost postiže i održava, kako se provjerava stanje sigurnosti, koje su ovlasti i odgovornosti zaposlenika, ...

Upravljanje rizicima

- Osnovni alat za upravljanje sigurnošću su rizici i upravljanje rizicima (engl. risk management)
  - S pojmom rizika smo se upoznali na početku predmeta kada smo uvodili osnovne pojmove
- Upravljanje rizicima omogućava
  - Uvid u stanje sigurnosti u organizaciji
  - Prioritizaciju problema (rizika) s kojima se treba pozabaviti
    - Na koje treba usmjeriti ograničene resurse
  - Praćenje promjene stanja sigurnosti u organizaciji
  - Balansiranje uloženih sredstava i moguće štete po organizaciju

Proces upravljanja rizicima

- Upravljanje rizicima je proces identificiranja, mjerenja i kontroliranja rizika u informacijskim sustavima tako da se rizici reduciraju na vrijednosti odgovarajuće vrijednostima resursa koji se štite.
  - Upravljanje rizicima može se opisati sljedećim dijagramom



Upravljanje rizicima (2)

- Identifikacija rizika
  - Zadaća je identificirati rizike pri čemu se svaki rizik sastoji od prijetnje, ranjivosti i štete.
  - Izlaz ovog koraka je popis svih potencijalnih rizika koji prijete sustavu za koji upravljamo rizicima.
  - Umijeće je identificirati odgovarajuće rizike, a da se pri tome ne ide u prevelike detalje ili se radi o preopćenitim rizicima.
- Procjena (mjerenje) rizika
  - Svaki rizik potrebno je ocijeniti (mjeriti) prema nekom unaprijed zadanom kriteriju i ocjenama
  - Primjer mjere je skala od 1 (gotovo nikakav rizik) do 5 (vrlo visok rizik)

Ovladavanje rizicima

- Četiri pristupa za svaki identificirani rizik
  - Uklanjanje rizika – uklanjanje rizika tako što se uklanja prijetnja ili ranjivost
  - Prijenos rizika – prijenos rizika na treću stranu, primjerice kupovinom osiguranja
  - Umanjenje rizika – uvođenje kontrola koje će umanjiti vjerojatnost djelovanja prijetnje ili koje će umanjiti štetu u slučaju da se rizik realizira
  - Prihvaćanje rizika – rizik se prihvaća te se ne djeluje na njega
- Odluku o pristupu za pojedini rizik donosi isključivo uprava
- Praćenje rizika
  - Praćenje promjena u sustavu ili njegovoj okolini koji utječu na procjenu rizika i ovladavanje rizicima

Revizije sigurnost informacijskog sustava

- Vrlo bitna komponenta upravljanja sigurnošću
  - Povratna veza kojom se nadzire upravljačka komponenta informacijske sigurnosti
  - Reviziju provode ovlašteni revizori
- Elementi provedbe revizije
  - Intervjui sa ključnim dionicima, pregled internih akata i dokumentacije, uvid u stanje informacijskog sustava i provođenje aktivnosti propisane internim aktima
  - Na temelju provedene revizije slaže se izvješće koje se prezentira upravi, nadzornom odboru, i regulatoru

Norme i upravljanje sigurnošću

- Norme su vrlo značajne u procesu upravljanja sigurnošću
  - ISO 27000 serija normi
    - ISO 27000 serija sastoji se od više od 40 zasebnih dokumenata koji propisuju ili daju smjernice za različite aspekte informacijske sigurnosti
  - Neke češće korištene
    - ISO 27000 – terminologija i rječnik
    - ISO 27001 – smjernice za upravljanje informacijskom sigurnošću
    - ISO 27002 – popis kontrola
    - ISO 27003 – upute za implementaciju 27001 norme
    - ISO 27005 – upravljanje rizicima

Međunarodne i nacionalne norme (2)

- National Institute of Standards and Technology (NIST)
  - Vrlo utjecajna agencija Američke vlade vrlo aktivna u području informacijske i kibernetičke sigurnosti
    - Primjerice, AES kripto-algoritam standardizirao je NIST
  - Jako puno uputa za različita područja prvenstveno orijentirano prema institucijama i agencijama američke Vlade
  - Svi dokumenti su slobodno dostupni

Međunarodne i nacionalne norme (3)

- Payment Card Industry Data Security Standard (PCI DSS)
  - Standard koji se primjenjuje na sve koji u svom radu koriste brojeve kreditnih kartica (banke, procesori)
  - Njegovi kreatori su kartičarske kuće (Visa, Mastercard, Diners)
  - Propisuje minimalnu razinu sigurnosti koji je potrebno implementirati
- CIS kontrole
  - Odabir 20 kontrola za koje se smatra da sprečavaju najveći broj napada
    - https://www.cisecurity.org/controls/
- ITIL, COBIT, …

Pregled ostalih područja sigurnosti

Rukovanje incidentima

Motivacija

- Općeprihvaćen stav je kako će se incident sigurno desiti
  - Nije pitanje AKO već KADA (nekada je bilo obratno!)
- Incidenti mogu varirati od vrlo jednostavnih do vrlo složenih
  - Jednostavan incident je, primjerice, zlućudni kod kojega je AV uspješno uklonio
- U općem slučaju, po otkrivanju incidenta nije nimalo lako otkriti što se desilo

Što kada se desi incident?

- Kada se desi neki značajniji incident incident nužno je reagirati na odgovarajući način
  - Neispravnim ili zakašnjelim odgovorom šteta može biti veća nego što bi trebala, može se onemogućiti istraga i utvrđivanje činjenica
- Neki mogući problemi u reakciji na incident
  - Što ako se incident desio usred noći, za vikend i slično?
  - Što ako vam direktor informatike kaže da ga ne zanima?
    - Slično ako vam administratori sustava kažu da ne žele raditi ništa što vi kažete?
  - Što ako ne možete angažirati vanjsku pomoć/suradnike?
- **Kako bi se ispravno reagiralo na incident nužno je planiranje unaprijed!**

Definicije

- *Upravljanje incidentima* (engl. incident management) se bavi pitanjem kako će organizacija prepoznati, analizirati, spriječiti i odgovoriti na incident, bavi se budžetom i ostalim upravljačkim pitanjima.
- *Rukovanje incidentom* (engl. incident handling) je proces koji se aktivira nastankom incidenta
  - Sastoji se od četiri koraka: detekcija, trijaža, analiza, odgovor na incident (engl. incident response)

Napomena: Terminologija nije standardizirana, ove definicije su preuzete iz ENISA dokumenta „Good Practice Guide for Incident Management”.

Svrha rukovanja incidentima

- Umanjenje štete
  - Djelovanjem na incident što više umanjiti štetu
- Brz i efikasan oporavak
  - Nakon što se razriješi uzrok incidenta što prije treba vratiti sustave u normalu
- Osiguranje sustava
  - Utvrditi uzroke koji su doveli do incidenta te spriječiti njegovo ponavljanje
- Follow-up
  - Pohraniti sve informacije o incidentu, podijeliti naučene lekcije

Upravljanje i rukovanje incidentima

- Priprema
  - Uspostavljanje politike i procedure za upravljanje incidentima, formiranje tima, uvježbavanje
- Detekcija i analiza
  - Detekcija incidenta, trijaža, prioritizacija, obavještavanje zainteresiranih strana
- Ograničavanje, uklanjanje i oporavak
  - Odabir strategije zaštite, prikupljanje i upravljanje dokazima, uklanjanje uzroka incidenta, oporavak od incidenta
- Aktivnosti nakon incidenta
  - Naučene lekcije, pohranjivanje dokaza incidenta

CERT/CSIRT

- *Computer Emergency Response Team* (CERT) je zaštićeno ime pa se paralelno upotrebljava naziv *Computer Security Incident Response Team* (CSIRT)
  - CERT je zaštićeno ime sveučilišta CMU koja je i uspostavila prvi CERT 1988. godine
- Organizacije čija zadaća je
  - zaštita, detekcija i odgovor na incidente,
  - pomoć u rješavanju incidenata (ako se radi o javnim CERT-ovima)
- Podjela
  - Samostalni ili u sklopu neke organizacije, javni ili privatni

CSIRT u Hrvatskoj

- U Hrvatskoj postoje dva javna CERT-a
  - Zavod za sigurnost informacijskih sustava (ZSIS) – vladin CERT zadužen za državne institucije
    - https://zsis.hr/default.aspx?id=15
  - Nacionalni CERT (NCERT) – dio CARNet-a zadužen za sve ostale institucije
    - https://www.cert.hr/csirt_specifikacija/
- Oba CSIRT-a su uspostavljena Zakonom o informacijskoj sigurnosti (NN 79/2007)
  - Nacionalni CERT je proizašao iz CARNet-ovog privatnog CERT-a

Sigurnosni operacijski centar

- Security Operations Center (SOC)
  - Ne treba miješati sa Network Operations Center – različite svrhe, NOC je puno stariji
  - Proistekao iz Security Information and Event Management (SIEM)
  - SIEM je u osnovi centralizirani sustav za prikupljanje sistemskih i operativnih zapisa
- Centralno mjesto na kojemu se prikupljaju svi podaci relevantni za sigurnost te se obrađuju
- U SOC-u rade analitičari različitih razina koji u osnovi slijede proces rukovanja incidentima

Primjeri reakcija i rješavanja incidenata

- RSA incident iz 2011. godine
  - https://www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told/
- FireEye incident iz 12. mjeseca 2020. godine
  - https://www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html
  - https://www.bloomberg.com/news/articles/2020-12-15/fireeye-stumbled-across-solarwinds-breach-while-probing-own-hack

Pregled ostalih područja sigurnosti

Obavještajni rad u kibernetičkom prostoru

Motivacija

- Neka pitanja s kojima se mnogi susreću
  - Koje prijetnje mogu djelovati na moj informacijski sustav?
    - Koje su sposobnosti, motivi tih prijetnji, način djelovanja?
  - Kako prepoznati prijetnje u mom informacijskom sustavu?
- Do odgovora se može doći na razne načine
  - I uglavnom nisu temeljeni na strukturiranim procesima
- Obavještajna zajednica bavi se strukturiranjem tih aktivnosti desetljećima
  - I tijekom tog perioda razvila je razne metode kako bi rezultati bili što objektivniji i potpuniji

Što je CTI?

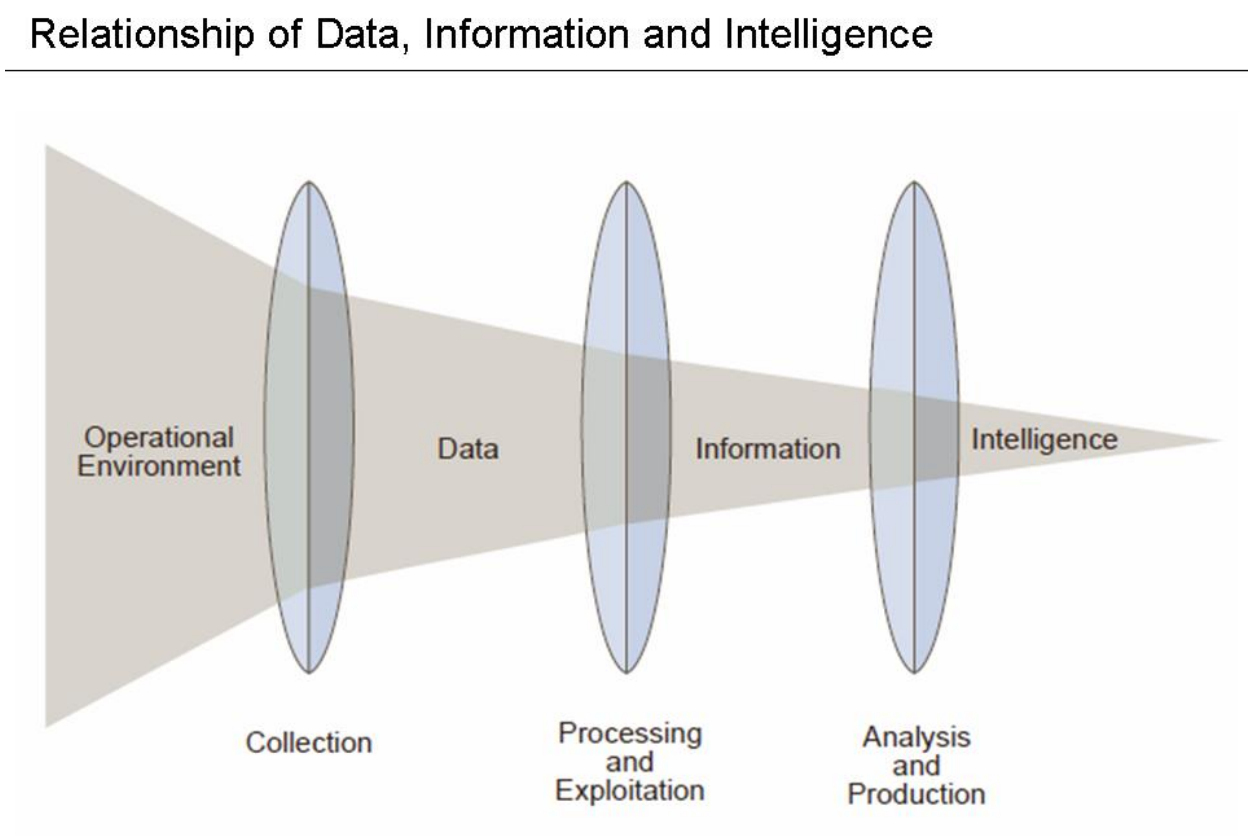
- Cyber Threat Intelligence (CTI), obavještajni rad u kibernetičkom prostoru
  - U EN se pojam „intelligence” odnosi i na ljudsku inteligenciju, ali i na obavještajni rad.
  - Obavještajni rad i „inteligencija” su povezani!
- Teško je definirati obavještajni rad, ali primjer jedne definicije je

  „Intelligence” znači poznavanje cilja. „Intelligence” prikuplja informacije o cilju i na temelju toga razvija ekspertno znanje o njemu koristeći dokaze iz svih dostupnih izvora […] „Intelligence” je o znanju, ali i o predviđanju. Ono mora doći pravovremeno do korisnika

Karakteristike CTI-ja

- Na temelju definicije slijede neke ključne karakteristike CTI-ja
  - CTI je proces i rezultat tog procesa
  - Rezultat nisu podaci (engl. data) niti informacije (engl. information) već znanje (engl. knowledge)
  - Vrlo je bitno znanje pravovremeno isporučiti korisniku jer je u suprotnom beskorisno.

Odnos podataka, informacije i znanja



Source: Joint Intelligence / Joint Publication 2-0 (Joint Chiefs of Staff)

Primjeri podataka, informacija i znanja

- Primjer odnosa podatak-informacija-znanje za slike
  - Snimljena slika je podatak
  - Identificirani objekti na slici su informacije
  - Namjena objekata je znanje
- Primjer odnosa podatak-informacija-znanje za zlćudni kod (engl. Malware)
  - Binarni kod je podatak
  - Nakon reverzanja dobija se informacija o karakteristikama zlćudnog koda
  - Analiza karakteristika napadača i njihova korištenja zlćudnog koda predstavlja znanje

Razine CTI-ja

- Nije svejedno kome su namijenjena izvješća
  - Primjerice, CEO ne treba tehničke izvještaje
  - S druge strane IDS/IPS/AV ne mogu ništa s narativnim opisima
- CTI se zato razvrstava u razine
  - strateška, operativna, taktička i tehnička.
- Neki kriteriji za razvrstavanje:
  - Tko je korisnik izvješća (znanja, rezultata CTI-ja);
  - Vremenski okvir u kojemu korisnik izvješća djeluje;
  - Odluke koje će se na temelju izvješća donositi;
  - Opseg prikupljanja podataka;

Izvori obavještajnih podataka

- Obavještajne službe prikupljaju informacije na razne načine
  - HUMINT – Human Intelligence
    - Prikupljanje informacija od osoba s terena – primjerice izbjeglica, tajni nadzor osoba, …
  - SIGINT – Signals Intelligence
    - Analiza i prisluškivanje radio-komunikacijskih kanala (ELINT) i ljudske komunikacije (COMINT)
- Od svih izvora najpopularniji i najdostupniji je OSINT
  - Ali ne nužno i najkvalitetniji

Open source intelligence (OSINT)

- Od svih načina prikupljanja informacija tvrtkama i pojedincima je zakonski dozvoljen samo OSINT
  - Obavještajna djelatnost regulirana je Zakonom o sigurnosno–obavještajnom sustavu Republike Hrvatske (NN 79/06)
- Primjeri OSINT izvora
  - Društvene mreže – LinkedIn, Twitter, Facebook, …
  - Javne baze podataka – Whois, Poslovna Hrvatska
  - Dnevne novine, Web stranica tvrtke
  - Razni forumi – StackOverflow, Reddit, …
  - …

Zaključno za CTI

- Postoje i drugi pojmovi, terminologija nije sređena
  - Cyber intelligence, Threat intelligence
- Tvrtke već koriste obavještajni rad dugo vremena
  - Business intelligence, Competitive intelligence
- Postoji određeno preklapanje između znanstvenog rada, digitalne forenzike i CTI-ja u metodama
- CTI koriste vojske, policije, organizacije
- „Najrazvikaniji” je tehnički CTI (IoC) ali i najviše automatiziran i najmanje zanimljiv (IMHO)

Pregled ostalih područja sigurnosti

Sigurnost strojnog učenja

Primjena strojnog učenja

- Strojno učenje danas je sveprisutno
  - Strojno učenje, i općenito AI, su značajno poboljšali kvalitetu života
- Stalno se eksperimentira s novim primjenama
- MEĐUTIM, strojno učenje nije savršeno i događaju se pogreške
  - Posljedice pogreški ovise o primjeni, a mogu varirati od neugodnih do fatalnih
    - Automatsko prepoznavanje ljudi s tjeralica (neugodno), autonomna vozila (fatalno)
- Zato se postavlja pitanje, **je li primjena strojnog učenje sigurna (safe & secure)?**

Sigurnosni problemi strojnog učenja

- Postoji niz istraživanja koja ukazuju na ranjivosti aplikacija strojnog učenja
  - Napadi na samovozeća vozila (primjerice, manipulacija znakova)
  - Napadi na Amazon Alexa, Google Home, Siri (naredbe koje čovjek ne čuje)
  - Rasizam, neprimjereni riječnik, …
- Problem je da se tehnologija upotrebljava na mjestima gdje to nije primjereno
  - Zbog „hypea” se tehnologija „gura” gdje ima i nema smisla

Umjesto zaključka

- Preporuka pogledati „keynote” s konferencije USENIX Security 2018, „*Why Do Keynote Speakers Keep Suggesting That Improving Security Is Possible?*”

https://www.usenix.org/conference/usenixsecurity18/presentation/mickens

Pregled ostalih područja sigurnosti

Privatnost i anonimnost

Privatnost vs. anonimnost

- Privatnost
  - Želimo prikriti podatke
    - Ne želimo objaviti naše osobne podatke, medicinske podatke, i sve ostalo što smatramo osjetljivim.
  - Želimo kontrolirati tko ima uvid u naše podatke i način kako se oni koriste
  - Privatnost je društveno, pravno i tehničko pitanje
- Anonimnost
  - Želimo prikriti tko je objavio informacije
    - Ne želimo se razlikovati u grupi nekakvih korisnika
  - Anonimnost nije moguća kada se radi o samo jednom korisniku

Štete od narušavanja privatnosti

- Krađa identiteta
- Ucjena
- Javno sramoćenje

Anonimnost na Internetu

- Internet je zamišljen i ostvaren kao **javna** mreža
  - Na Internetu **niste anonimni**
- Kad se koristi neka usluga postoje razne informacije koje vode do vas
- Najčešće metode koje omogućavaju narušavanje anonimnosti su IP adrese i Web kolačići
- Anonimnost je bitna u mnogim slučajevima: disidenti, zviždači, borci za ljudska prava, …

IP adrese

- Bilo tko tko vam omogućava pristup Internetu može pratiti što radite
  - ISP, vlasnik „besplatnog pristupa Internetu”, napadač koji je preuzeo kontrolu nad „besplatnim pristupom Internetu”
- Kada pristupate nekoj usluzi u sistemskim i operativnim zapisima bilježi se vaša IP adresa
  - ISP zapisuje koju IP adresu vam je dodijelio u kojem periodu
  - Policija na temelju sudskog naloga može dobiti informaciju od ISP-a

Kako se otkrivaju počinitelji?

- Počinitelj u istoj državi kao i kazneno djelo
  - Policija traži sudski nalog kojim se nalaže pružatelju usluge pristupa Internetu (ISP) da otkrije tko je koristio neku IP adresu u nekom točno određenom trenutku
  - Relativno brz proces
- Počinitelj u drugoj državi
  - Putem Europola/Interpola traži se pomoć organa gonjenja druge države
  - Relativno spor do nemoguć proces
- Društvene mreže imaju poseban mehanizam
  - Primjer Facebooka, https://www.facebook.com/records/login/

Inkognito način rada Web preglednika

- Omogućava novu sjednicu
  - Podaci iz „običnog” načina rada se ne prebacuju u inkognito način
- Ne pamti ništa u inkognito sjednici, sve se briše
  - Upisane lozinke, Web kolačići, podaci koje je poslala Web stranica
- Problemi
  - Još uvijek ostaje IP adresa
  - Ne smijete se prijavljivati (ili se morati prijavljivati isključivo u inkognito načinu rada)

Anonimizirajući Web posrednici

- Jedna vrsta usluge su i Web posrednici (proxy)
  - Umjesto korisnika upućuju zahtjev prema usluzi
  - Nije svaki posrednik istovremeno i anonimizirajući
    - Posrednici proslijeđuju IP adresu klijenta u HTTP zahtjevu
- Problemi
  - Kao i VPN-ovi, ne smiju se bilježiti IP adrese
  - Ne pročišćavaju sadržaj – IP adrese, kolačići i drugi podaci mogu „curiti”
  - Radi isključivo za HTTP protokol
    - Primjerice, preko DNS-a mogu curiti informacije

Pružatelji usluge VPN

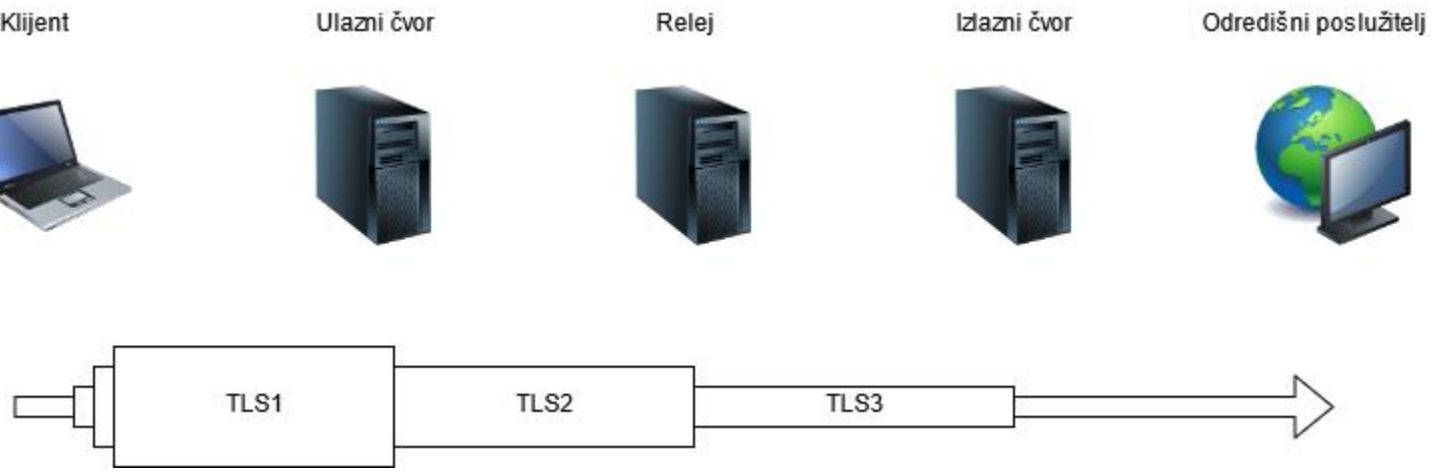
- Postoje VPN-ovi uz pomoć kojih je moguće sakriti IP adresu
  - Pružatelj usluge VPN zna vašu IP adresu, a usluga kojoj pristupate vidi IP adresu pružatelja usluge
  - Najčešće se ipak koristi za zaobilaženje ograničenja temeljem IP adresa
- Ključni dio je da pružatelj usluge VPN ne čuva podatke tko je koristio koju IP adresu
  - **Problem je da li pružatelj VPN usluge čuva sistemske i operativne zapise ili ne**
  - Bilo je situacija u kojima se ispostavilo da pružatelji usluge VPN čuvaju sistemske i operativne zapise bez obzira što su tvrdili drugačije

Anonimizacijska mreža Tor

- Najbolji način postizanja anonimnosti
  - Postoje alternative, primjerice I2P (Invisible Internet Project)
- Temelji se na tri vrste čvorova kako bi se omogućila anonimizacija
  - Ulazni čvorovi (guard node), releji (middle), izlazni čvorovi
- Kada korisnik pristupa resursu putem Tor mreže tada se
  - Uspostavlja put (engl. circuit) kroz anonimizacijsku mrežu
  - Pristupa se resursu
    - Ovdje je jako bitno paziti da se ne odaju informacije s klijentske strane!

Uspostava puta u mreži Tor

- Iz skupa svih raspoloživih čvorova slučajno se biraju po jedan ulazni čvor, relej i izlazni čvor
  - Moguće je imati i dulje puteve, ali ovo se smatra dovoljnim



Skrivene usluge

- Do sada smo htjeli da je klijent anoniman, **ali što ako želimo da i poslužitelj bude anoniman?**
- Tor nudi skrivene usluge
  - Poslužitelj izgrađuje put kroz mrežu te odabire jedan Tor čvor kako mjesto sastanka (engl. rendezvous point)
  - U direktoriju objavljuje mjesto sastanka (obavezno koristeći drugi Tor put)
  - Klijent na temelju adrese skrivene usluge u direktoriju pronalazi mjesto sastanka te se spaja na njega (sve ide preko Tor puteva!)
- Primjer adrese skrivene usluge:

http://3g2upl4pq6kufc4m.onion/

Problemi mreže Tor

- Visoka latencija
- Kriminalne aktivnosti se jako puno provode zahvaljujući mreži Tor
  - Prodaja i kupovina ilegalnih proizvoda, dječja pornografija, …
- Ako „vrtite” izlazni čvor možete imati problema
  - ISP vas može blokirati, policija vas može tražiti

Tamni Web (engl. dark web)

- Ime za skrivene usluge općenito, a specifično za različita Web sjedišta sa ilegalnim sadržajem
  - Prodaja razno-robe, forumi s nedozvoljenim i uvredljivim sadržajima
- Bitcoin (i druge kripto-valute) su dodatno omogućile takva sjedišta
- Za priču o jednom popularnom ilegalnom Webu koji je policija uspješno ugasila pročitajte

https://en.wikipedia.org/wiki/Silk_Road_(marketplace)

https://en.wikipedia.org/wiki/Ross_Ulbricht

Kako koristiti mrežu Tor?

- Najjednostavnije je skidanjem i instalacijom Tor Browsera
  - Firefox LTS sa Tor podrškom te postavkama kako bi se spriječilo curenje informacija – ne dirati postavke, čak ni veličinu prozora(!)
- Za skrivene usluge također postoji programska podrška
- ALI UPOZORENJE – ništa nije savršeno(!)
  - U programskoj podršci za Tor mrežu se s vremena na vrijeme nađu ranjivosti
  - Jako je puno detalja preko kojih mogu curiti informacije uz pomoć kojih možete biti deanonimizirani
  - U konačnici, sve ovisi tko vas pokušava deanonimizirati!

Hvala!