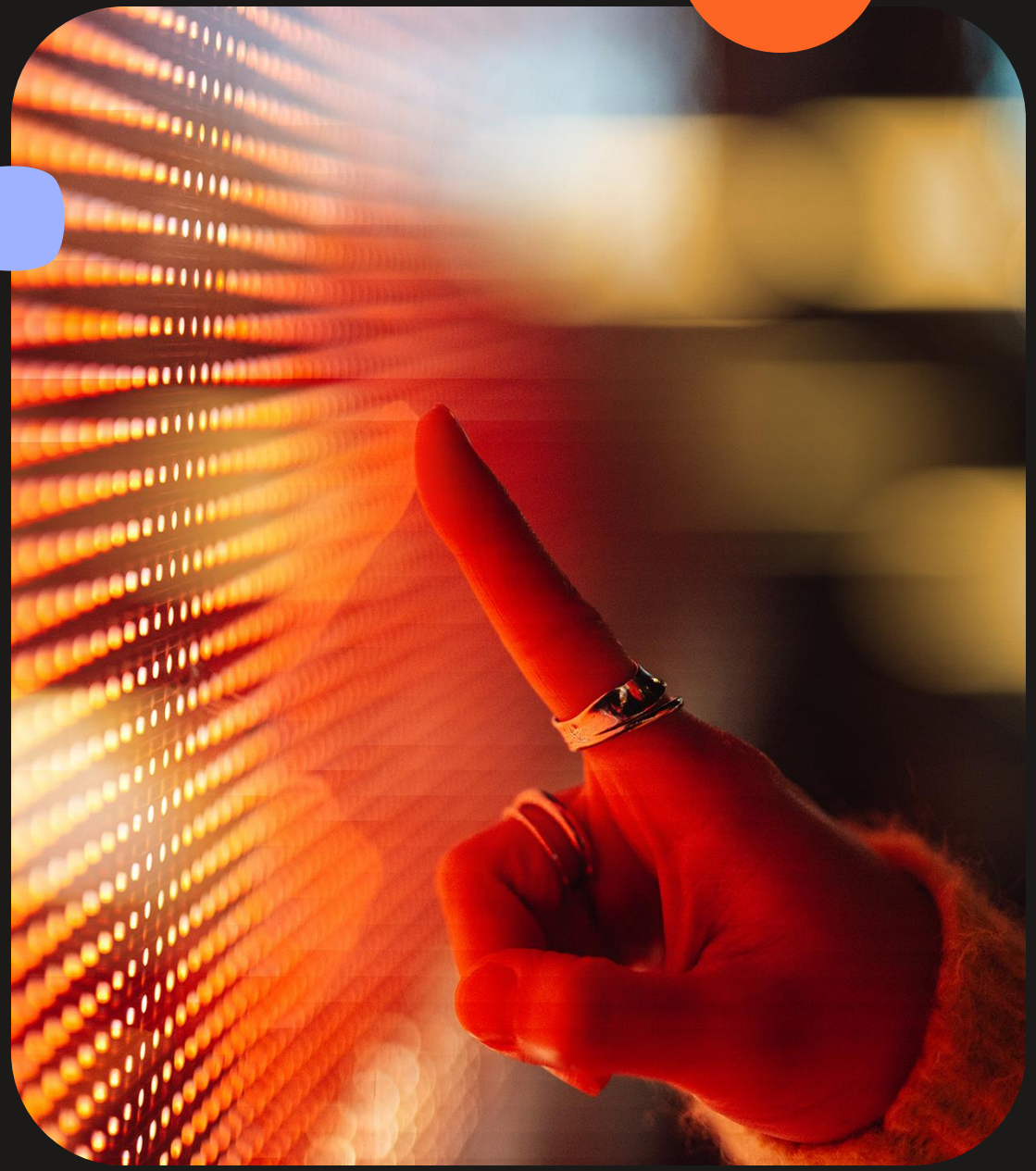
Put implementacije kibernetičke sigurnosti

- iskustva i lekcije



Andro Galinović, CISO
Jurica Čular, Security Governance and Resilience manager

07.10.2025

Danas na meniju

1. Mapiranje implikacije zakona na poslove u organizaciji
2. Stvarna cijena sigurnosti i regulative

Što znači imati *in house sigurnost ?*

- Koliko je to kompleksno i ***da li to pokriva sve zahtjeve Zakona i Uredbe***?
  - mi vjerujemo da pokriva

- **Na primjeru Infobipa** (koji već 6-7 godina gradi i investira u sigurnost)
  - koji su to minimalno potrebni procesi po ZKS/UKS
  - kako je to složeno kod nas

- Koliko bi to **moglo koštati prosječnu srednju firmu**?

A što točno trebamo raditi?

Upute za korištenje Početna stranica

NARODNE NOVINE

SLUŽBENI LIST REPUBLIKE HRVATSKE

Uredba o kibernetičkoj sigurnosti

VLADA REPUBLIKE HRVATSKE

2217

Na temelju članka 24. Zakona o kibernetičkoj sigurnosti (»Narodne novine«, broj 14/24.), Vlada Republike Hrvatske je na sjednici održanoj 21. studenoga 2024. donijela

UREDBU

O KIBERNETIČKOJ SIGURNOSTI

Dio NN: Službeni

Vrsta dokumenta: Uredba

Izdanje: NN 135/2024

Broj dokumenta u izdanju: 2217

Stranica tiskanog izdanja: 3

Donositelj: Vlada Republike Hrvatske

Kibernetički mozak

Domena:

Politike

UKS

- Svaka od 13 mjera (M) zahtjeva high level policy dokument / izjave
- M1 - "*...definirati i usvojiti na upravljačkom tijelu subjekta strateški akt kibernetičke sigurnosne politike koji definira ciljeve subjekta u pitanjima kibernetičke sigurnosti, mjere upravljanja kibernetičkim sigurnosnim rizicima koje će subjekt primjenjivati, organizacijski sustav i raspodjelu uloga...*"
- M3 - "*...Subjekt mora dokumentirati, komunicirati i zaposlenicima subjekta, koji su odgovorni za segmente poslovanja subjekta povezane s rizicima, učiniti dostupnim kibernetičke sigurnosne politike i upute o osnovnim procedurama za identifikaciju, analizu, procjenu i obradu rizika...*"

Infobip

- Nekoć imali po jednu detaljnu politiku po ISO 27k poglavljima danas big high level ISMS policy za sve
- Niz operativnih procedura, SOP, PlayBooks

Domena:

Podizanje svijesti

UKS

- **M4 - Sigurnost ljudskih potencijala i digitalnih identiteta**
- "*...osigurati redovnu obuku o osnovnim praksama kibernetičke higijene i podizanje svijesti o rizicima i kibernetičkim prijetnjama za sve zaposlenike, neposredno nakon stupanja osobe u radni odnos u subjektu te kasnije redovito tijekom radnog odnosa. Subjekt mora uspostaviti program podizanja svijesti u skladu s kibernetičkom sigurnosnom politikom, tematski specifičnim politikama i relevantnim procedurama kibernetičke sigurnosti u okviru mrežnog i informacijskog sustava subjekta...*"

Infobip

- Inicijalni trening za sve tijekom onboarding akademije + sigurno kodiranje za inženjere + phish simulacija
- Mjesečni interno razvijani kratki i tematski seminari do 10min – interni **BipSecBites** brand (e.g na kraju)
- Dodatni interno razvijani seminari za prodaju, podršku, razvoj,..
- Kupljeni awarenss materijali e.g ***The Inside Man*** (2019-2024) https://www.imdb.com/title/tt11847918/

Domena:

Upravljanje imovinom

UKS

- **M2 - Upravljanje programskom i sklopovskom imovinom**
- "*Cilj mjere je uspostaviti strukturirani pristup identifikaciji i klasifikaciji programske i sklopovske imovine subjekta te uspostaviti potpunu kontrolu i zaštitu programske i sklopovske imovine subjekta prilikom njezina korištenja, skladištenja, prijevoza i u konačnici brisanja ili uništavanja, odnosno upravljanja životnim ciklusom programske i sklopovske imovine.*"

Infobip

- Potpuno automatizirani asset inventory (CD/CI, automatizirani deployment, platform agenti, MDM ...)
- By policy rule based klasifikacija asseta
- Specifični standardi zaštite ovisno o vrsti imovine (WorkStations, Servers, Network,...)

Domena:

Upravljanje rizicima

UKS

- **M3 - Upravljanje rizicima**
- "...*Cilj mjere je uspostaviti odgovarajući organizacijski okvir za upravljanje rizikom kako bi subjekt utvrdio i odgovorio na sve rizike koji prijete sigurnosti njegovih mrežnih i informacijskih sustava i pri tome predstavljaju rizik za poslovanje subjekta...*"

Infobip

- Sveobuhvatni framework upravljanja rizicima
- Asset based & event based
- Rizici redovno komunicirani Upravi
- Posebne vrste rizika – rizici korištenja trećih strana, rizici mogućih nesukladnosti

Domena:

Upravljanje identitetima

UKS

- **M4 - Sigurnost ljudskih potencijala i digitalnih identiteta**
- "*...osigurati da svaki korisnik mrežnog i informacijskog sustava (neovisno o tome je li ili nije zaposlenik subjekta), gdje god je to tehnički moguće i sustav dozvoljava, posjeduje jedan ili više digitalnih identiteta koji su samo njegovi te ih koristi tijekom rada na mrežnim i informacijskim sustavima subjekta...*"

Infobip

- Implementiran (ongoing) ID(e)M sustav
- Role i atribute based pristup
- Automatsko oduzimanje prava
- Redovna certifikacija – access review

Domena:

Lanac opskrbe

UKS

- **M8 - Sigurnost lanca opskrbe**
- "*Cilj mjere je uspostaviti jasnu i sveobuhvatnu politiku za izravne dobavljače ili pružatelje usluga, osobito ključnih lanaca opskrbe IKT uslugama, IKT sustavima ili IKT proizvodima, u svrhu smanjenja identificiranih rizika i minimiziranja ranjivosti te optimiziranja lanca opskrbe subjekta, što će rezultirati stabilnijim poslovanjem i većom pouzdanosti isporuke svojih proizvoda i usluga.*"

Infobip

- Procjena rizika/kritičnosti trećih strana
- Ocjena zrelosti security i privacy praksi
- Peridička ponovljena procjena

Domena:

Kontinuitet poslovanja

UKS

- **M8 - Kontinuitet poslovanja i upravljanje kibernetičkim krizama**
- "*Cilj mjere je osigurati postojanje unaprijed pripremljenih planove za minimiziranje prekida u poslovanju i osiguravanje kontinuiteta ključnih poslovnih aktivnosti subjekta za slučajeve incidenata i kibernetičkih kriza.*"

Infobip

- BIA i RA kao temelj decission making procesa
- Različiti DR modeli: active-active, active-passive...
- Redovno testiranje svih vrsta: TTX, Crisis managament EX, restore, failover...na produkscijskim sustavima!

Domena:

Izvještavanje

UKS

- **M1 - Predanost i odgovornost osoba odgovornih za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima**
- "*...osigurati godišnje izvještavanje osoba odgovornih za provedbu mjera o stanju kibernetičke sigurnosti. Ovi izvještaji trebaju sadržavati analizu uspostavljenih mjera upravljanja kibernetičkim sigurnosnim rizicima, identificirane kibernetičke prijetnje i rizike, te preporuke za unapređenje razine kibernetičke sigurnosti. Redovito izvještavanje treba osigurati informiranost osoba odgovornih za provedbu mjera i omogućiti donošenje strateških odluka za podizanje razine kibernetičke sigurnosti....*"

Infobip

- Infobip Security Steering (ISS) 7-member Committee
- Weekly CISO – CTO, beweekly CISO – CIO aligements, monthly CISO - Chief Legal Officer
- Risk Committee

Domena:

Sigurnosna testiranja

UKS

- **M5 - Osnovne prakse kibernetičke higijene**
- "*...implementirati mehanizme za periodičnu ili redovitu provjeru ranjivosti svih mrežnih i informacijskih sustava kako bi se pravovremeno otkrio manjak primjene sigurnosnih zakrpi ili nepravilna konfiguracija sustava. Subjekti su dužni, na temelju procjene rizika, utvrditi potrebu i učestalost te vrste sigurnosnog testiranja (penetracijski testovi, red teaming, purple teaming, i dr.) kako bi otkrili ranjivosti u implementaciji mrežnog i informacijskog sustava....*"

Infobip

- Dnevno / tjedno skeniranje poznatih ranjivosti (VA)
- Interna penetracijska testiranja (33x u 2024) / Threat modeling
- Vanjska pentracijska testiranja, red/purple teaming, 24x7/365 Bug Bounty
- Tabletop za provjeru postojanja novih ranjivosti

Domena:

Sigurni razvoj

UKS

- **M9 - Sigurnost u razvoju i održavanju mrežnih i informacijskih sustava**
- "*Cilj mjere je osigurati da subjekti uspostave, dokumentiraju, provode i kontinuirano nadziru konfiguraciju svojih mrežnih i informacijskih sustava, uključujući sigurnosne postavke sklopovske i programske imovine, kao i vanjske usluge i mreže koje koriste.*"

Infobip

- Security by desing, Security u ranim fazama razvoja (product tags) + threat modeling + testiranje prije GA
- SDLC – SCA + SAST
- Custom made security edukacija developera

Domena:

Kriptografija

UKS

- **M10 - Kriptografija**
- "*Cilj mjere je da subjekti, sukladno vlastitim poslovnim potrebama, uspostave sveobuhvatne kriptografske politike i postupke kako bi osigurali zaštitu podataka u prijenosu i mirovanju. Implementacija kriptografskih politika treba osigurati primjenu prikladne kriptografske tehnike i algoritama, u skladu s najboljim praksama i regulatornim zahtjevima.*"

Infobip

- Kriptiranje u prijenosu, kriptiranje u mirovanju / krito sažetci za loznike,
- Vlastita HSM i key vault arhitektura
- Istraživanje Post-quantum kriptogafije u tijeku

Domena:

Vidljivost i odziv

UKS

- **M5 - Osnovne prakse kibernetičke higijene**
- *"...osigurati, ukoliko je tehnički izvedivo, stvaranje zapisa o svakoj prijavi i aktivnosti na kritičnom mrežnom i informacijskom sustavu radi osiguravanja forenzičkog traga, a pri tome treba koristiti alate i procese za praćenje i bilježenje aktivnosti na mrežnom i informacijskom sustavu subjekta u svrhu otkrivanja sumnjivih događaja koji bi mogli predstavljati incident te postupanja kojim će se umanjiti potencijalni učinak incidenta..."*

Infobip

- Follow the sun SOC smjene
- Korišteni SIEM, EDR, DFIR alati
- SOAR automatizacija za brži onboarding i odziv na tipične slučajeve

Domena:

Upravljanje ranjivostima

UKS

- **M5 - Osnovne prakse kibernetičke higijene**
- "*...definirati i dokumentirati proces identifikacije i upravljanja ranjivostima na kritičnim mrežnim i informacijskim sustavima koje samostalno razvija. U tu svrhu, subjekt mora osigurati mehanizam identifikacije mogućih ranjivosti na mrežnim i informacijskim sustavima koje samostalno razvija....*"

Infobip

- Sveobuhvatna politika upravljanja ranjivosti
- Izvori informacija: OSINT, technology watch – u okviru SOC vulnerability "smjene", skeniranja, testovi...
- Prioritizacija i remedijacija u skladu s propisanim rokovima (based, environmental & temporal score)
- SOAR automatizacija remindera za reboot i patch (koristeći VA skener)

Domena:

Postupanje incidentima

UKS

- **M11 - Postupanje s incidentima**
- "*Cilj mjere je uspostaviti sveobuhvatan okvir za utvrđivanje uloga, odgovornosti i procedura koje će omogućiti subjektu učinkovito sprječavanje, otkrivanje, analizu, zaustavljanje i odgovor na incidente te oporavak od incidenata*"

Infobip

- Dedicirani IRT (SOC) Team
- Risk follow the sun smjene
- Trijaža - klasifikacija, procjena utjecaja, eskalacija
- Notifikacija / escalacija prem DEFCON razinama

Domena:

Higijena i mjere zašite

UKS

- **M5 - *Osnovne prakse kibernetičke higijene***
- "...razviti, dokumentirati, održavati i implementirati pravila osnovne prakse kibernetičke higijene..."
- **M6 - *Osiguravanje kibernetičke sigurnosti mreže***
- *"definirati i uspostaviti, sukladno svojoj mrežnoj arhitekturi i izloženosti javnim mrežama, obavezne mjere zaštite mreže te pritom razmotriti adekvatne mjere"*
- **M7 - Kontrola fizičkog i logičkog pristupa mrežnim i informacijskim sustavima**
- "razviti, dokumentirati održavati i implementirati pravila kontrole pristupa ..."

Infobip

- interni sigurnosni sistem integratorski tim od 7 inženjera
- rade istraživanje, PoC/PoV, razvoj, integraciju i održavanje
- npr: SIEM, PKI, ZTNA, kripto key management, password mng, VA, EPM, IAM, passwordless, WAF,...

Domena:

Tehnička zaštita

UKS

- **M13 - Fizička sigurnost**
- Cilj: Cilj je uspostaviti mjere za sprječavanje i nadziranje neovlaštenog fizičkog pristupa mrežnim i informacijskim sustavima subjekta, kako bi subjekt zaštitio te sustave od moguće štete i smetnji uzrokovanih fizičkim prijetnjama"

Infobip

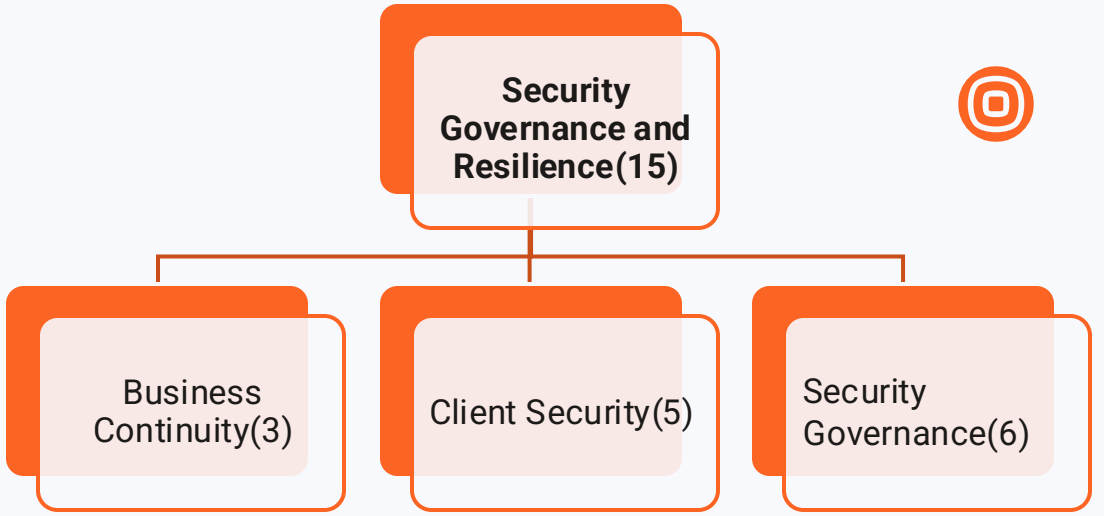
- Tim za "*korporativno upravljanje sigurnošću"* definira standarde fizičke zašite za podatkovne centre, kampuse, velike ured, male i dijeljene urede
- Tim korporativnog IT-u radi implementaciju onog što ne rade vanjski (npr video nadzor)
- Tim za "sigurno projektiranje" analizira razne zahtjeve, arhitekture i tehnologije
- Tim za "napadačku sigurnost" radi provjere sigurnosti

Korporativno upravljanje sigurnošću

aka Security Governace

Stvarni trošak sigurnosti

Korporativno upravljanje sigurnošću



opseg	period	~FTE	UKS ref	opaska
Politike	projektno i godišnje	1/8	M1-M13	Moguće je kupiti i samo održavati
Podizanje svijesti	1/g ili bolje 1/m	1/6	M1,	Uz kupljeni sadržaj samo administracija
Upravljanje rizicima	1-4 x / godišnje	1/4	M1, M3	Uz godišnju, treba i projektnu, te praćenje
Izvještavanje	1x godišnje	1/6	M1	Najčešće radi CISO dakle nije novi FTE
Upravljanje imovinom	stalno ručno/auto	1/4	M2	Ovisi o količini promjena, 1/g nije dovoljno
Upravljanje identitetima	stalno ručno/auto	1/4	M4, M7	Ovisi o migracijama
Lanac opskrbe	stalno ručno/auto	1/4	M8	~ ciklusi nabave
Kontinuitet poslovanja	barem godišnje	1/6	M12	Velika investicija vremena izvan sigurnosti

~FTE:	**1-2***	**TCO/g:**	**~100-120k€**

**jedan je CISO*

Aplikativna ili napadačka sigurnost

aka Application Security

Stvarni trošak sigurnosti

Aplikativna ili napadačka sigurnost

Application Security(7)

opseg	period	~FTE	UKS ref	opaska
Upravljanje rizicima	po projektu	1/12	M3	Event based RA + projekti
Sigurnosna testiranja	4 x godišnje	1/6	M5, M6	Authn, protokoli, SAST, SCA, DAST, BB, PT
Lanac opskrbe	stalno ručno/auto	1/4	M8	Ili će dobavljač dati PT izvještaj ili DIY
Sigurni razvoj	po projektu	1/6	M9	Ovisno o projektu te više za interne
Kripto pomoć i provjera	po projektu	1/6	M10	Samo u slučaju internog razvoja

~FTE:	0.5-1	TCO/g:	~50k€

Operativna sigurnost

aka SOC

Operativna sigurnost

SOC (8)

opseg	period	~FTE	UKS ref	opaska
Upravljanje imovinom	samo input	1/12	M2	Osiguravanje poveznice s stvarnošću
Upravljanje rizicima	projektno	1/12	M3	Cyber response plan – ne pisati bez SOC-a
Vidljivost i odziv	povremeno	1/6	M5	Inicijalno velik angažman
Upravljanje ranjivostima	svaki dan	1	M5	Praćenje novih ranjivosti je dnevna stvar
Sigurnosna testiranja	godišnje	1/6	M6, M7	Oni su predmet provjere kod Purple i Red
Lanac opskrbe	opcionalno		M8	Prava prilikom integracija
Postupanje incidentima	svaki dan	1	M9	Osnovni posao trijaže
Kontinuitet poslovanja	Tijekom	1/12	M12	Odgovor na velike cyber incidente

~FTE:	**2***	**TCO/g:**	**~80-100k€**

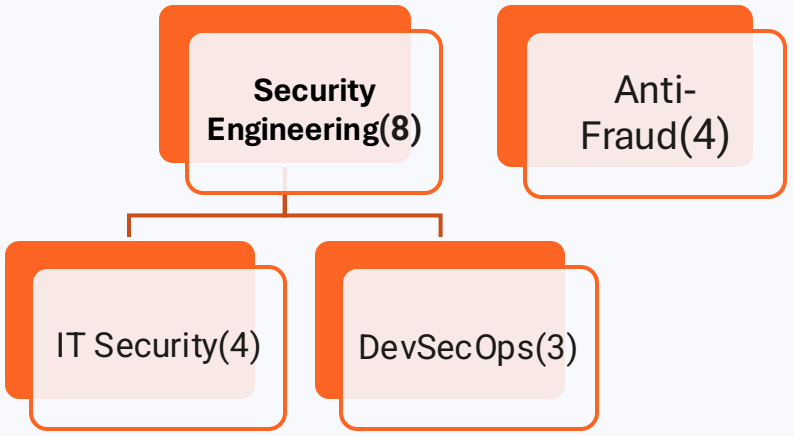
**smjenski rad i jedan uvijek mora biti*

Sigurno projektiranje

aka Security Enginering

Stvarni trošak sigurnosti

Sigurno projektiranje



opseg	period	~FTE	UKS ref	opaska
Upravljanje imovinom	projektno	1/8	M2	Sigurno zbrinjavanje opreme
Upravljanje rizicima	1-4 x / godišnje	1/4	M3	Godišnje i projektni input
Upravljanje identitetima	Projektno i održavanje	1/8	M4	Podizanje i održavanje IAM-a
Higijena i mjere zašite	Projektno i održavanje	1/8	M5, M6, M7	Tehnički
Sigurni razvoj	Projektno i održavanje	1/8	M9	Ako postoji razvoj: CI/CD i IaC
Kriptografija i PKI	Projektno i održavanje	1/8	M10	Dobra praksa traži "su ključarstvo"
Tehnička zasitite	Projektno i održavanje	1/8	M13	Kontrola prolaza i video nadzor

~FTE:	0.5-1	TCO/g:	~50-70k€

Minimalni broj ljudi

4

- *minimalni broj za ovaj opseg*
- *barem jedna je "heroj"*

Realnije broj ljudi

6

- *Veća specijalizacija*
- *Lakše zapošljavanje*
- *Nema heroja*

Realna cijena minimalnog tima srednje zrelosti

280,000.00 €
Bruto 2 godišnje

Realna cijena dobrog tima srednje zrelosti

340,000.00 €
Bruto 2 godišnje

Koliko dobro može izgledati in house sigurnost ?

Prilično dobro

Hvala

Andro Galinović
CISO

Jurica Čular
Security Governance
& Reliance Manager

www.infobip.com