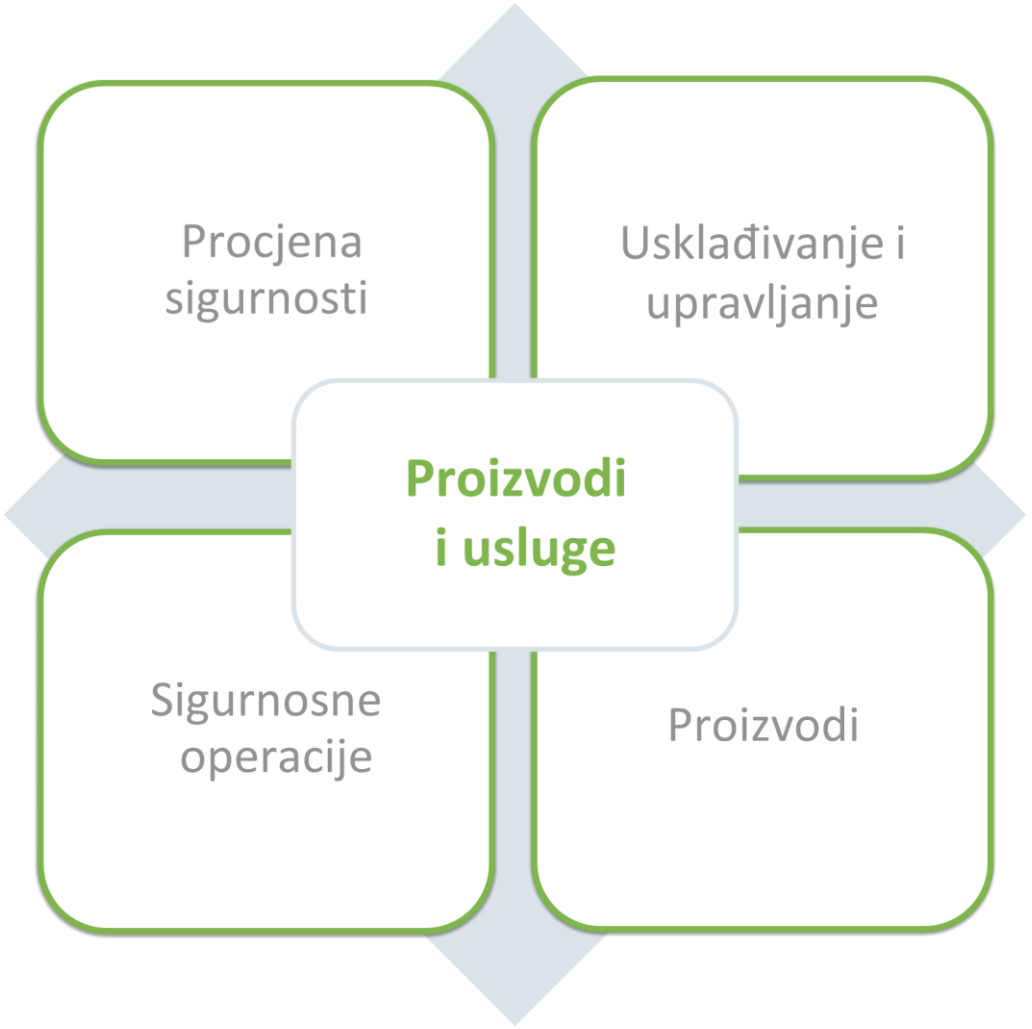
# „Praktični savjeti za obnovu nakon kibernetičkih napada”

M.Sc. Berislav Crkvenac

# O Divertu

- **Informacijska sigurnost** je od početka osnovna djelatnost poduzeća (2007)
- Zapošljavamo **visoko kvalificirane i motivirane stručnjake** koji posjeduju brojne stručne certifikate, kao i certifikate Tajno i Vrlo tajno na nacionalnoj razini
- Imamo široku bazu klijenata: financije, osiguranja, telekomi, razne industrije, vlada, energetski sektor
- Naše temeljne vrijednosti:


# Diverto portfelj



## Nije mi cilj…

- Plašiti vas
- Prodavati
- Ići u detalje
- Učiti vas standardima
- Objašnjavati razliku IT i OT

- Podsjećati vas da trebate:
  - aktivno upravljati rizicima
  - uključiti visoki management
  - educirati zaposlenike
  - ulagati u tehnologiju i imati dostatan budget
  - na vrijeme uskladiti poslovanje s regulativom i standardima

# Kvar ili sigurnosni incident?

## U slučaju sigurnosnog incidenta…

1. Stvorite konstruktivno okruženje
2. Ne žurite sa zaključcima, ne preskačite nužne korake, slušajte struku
3. Ne zaboravite na važnost komunikacije
4. IT i OT se ponekad „ne razumiju”
5. Oslonite se na partnere koji razmišljaju „e2e”
6. Imajte jasan odgovor na pitanje „što je nama zaista važno?”

# Proces

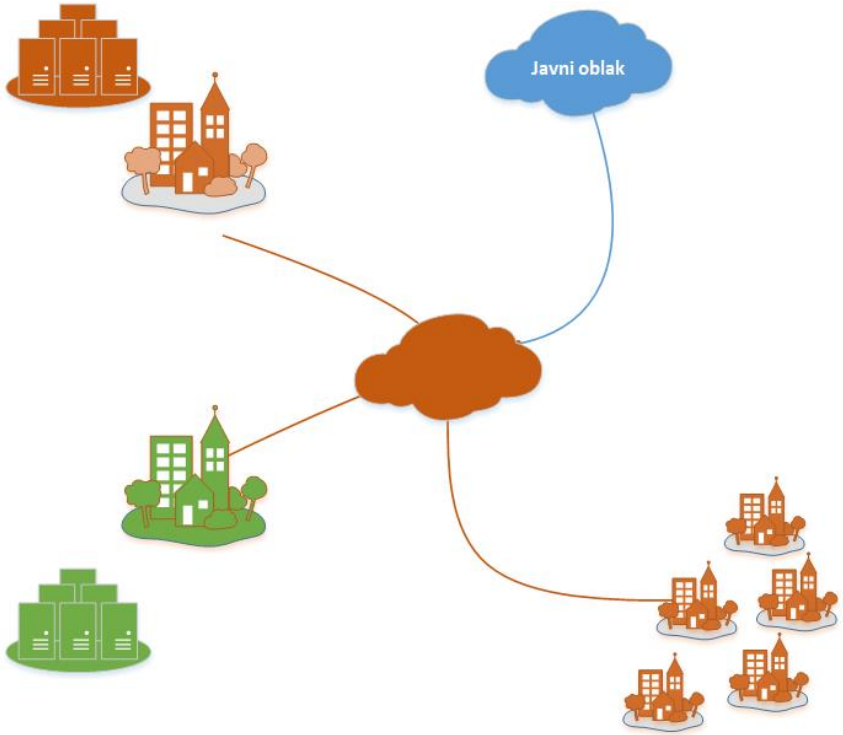
1. Detekcija incidenta
2. Obavještavanje o incidentu
3. Trijaža i analiza incidenta
4. Preporuke za ograničavanje incidenta, uklanjanje prijetnji i ranjivosti, oporavak
5. Izvještavanje o incidentu
6. Preporuke

- Incident response director
- Incident responder
- Analitičar
- Reversing ekspert
- Forenzički ekspert
- ...

# SOC usluga

| | | |
|---|---|---|
| Zaštita ključnih informacija i procesa | Sprječavanje incidenata | Pravovremeno otkrivanje prijetnji i zlouporaba unutarnjih i vanjskih aktera |
| Poboljšanje sposobnosti otkrivanja i reagiranja na incidente | Poboljšanje sposobnosti forenzičke istrage | Usklađivanje s regulativom |

# „Praktični savjeti za obnovu nakon kibernetičkih napada”





## TEHNOLOGIJA 01

- SIEM, Threat Intel
- Network Security Monitoring, IDS/IPS
- DNS, DHCP
- EDR, DLP, AV, HIPS
- Proxy, Firewall, Honeypot
- ...

## LJUDI 02

- T1: Trijaža alarma i inicijalni odaziv
- T2: Dubinska analiza
- T3: Stručnjaci raznih „Cyber” područja
- SOC Menadžer
- SOC Inženjer

## PROCESI 03

- Upravljanje Incidentima
- Procedura nadzora
- Procedura obrade alarma
- Procedura obavještavanja
- Proces eskalacije


# Inicijative nakon incidenta

- Unaprijeđeni asset management i praćenje ranjivosti
- Širenje pokrivanja SOC-a
- Dodatna *zonifikacija*
- Dodatni *honeypot*
- *Purple teaming*
- Edukacija
- Testiranje vanjskih sustava
- Pomoć u sveobuhvatnom pristupu upravljanju rizicima

## Sažetak

- Priprema zlata vrijedi
- Sigurnost smatrajte poslovnom, ne tehničkom temom
- Vježbajte, educirajte, simulirajte…
- Analizirajte opskrbni lanac
- Ljudi/procesi/tehnologija
- „Trust, but verify”
- Krenite na vrijeme (odmah)
- Dodijelite ljude, stvorite timove
- Nemojte sve raditi sami
- Komunikacija je jako važna
- ISA/IEC 62443…
- Iskoristite NIS2 kao priliku

# Hvala na pažnji

- Uskoro će i peti godišnji izvještaj
- Četvrto izdanje, slobodno dostupan
  - https://diverto.hr/hr/report/
- Fokus
  - Stanje informacijske i kibernetičke sigurnosti u organizacijama u RH, SLO i BiH