

# **Unutrašnje prijetnje - kako ih spriječiti, a kako liječiti?**

Goran Pizent  
minus5 d.o.o

# Mudrost

“Znanje o rasporedu neprijateljskih snaga se može dobiti jedino od drugog čovjeka”

Sun Tzu 500. p.n.e.

# Sadržaj

- Motivi
- Tko su insideri?
- Unutrašnje prijetnje
- Tko otkriva insidere?
- Kako spriječiti/liječiti?
- Primjeri iz prakse

# Motivi

- Osveta
- Novac
- Poslovna prednost na tržištu
- Ego
- Nacionalno/vjersko uvjerenje

# Tko su insideri?

- Trenutni ili bivši zaposlenici
- Zaposlenici u otkaznom roku
- Honorarni djelatnici
- Poslovni partneri/firme
- Manje firme kupljene od većih

# Tko su insideri?

- Administratori (45%) - sabotaza/osveta
- Netehničke niske pozicije s pristupom osjetljivim informacijama (44%) - novac
- Rukovoditelji sektora, odjela, marketniški suradnici, programeri, znanstvenici (14%) - krađa za poslovnu prednost na tržištu

# Unutrašnje prijetnje

- Neadekvatni poslovni procesi
- Maliciozni napadi/sabotaža
- Socijalni inženjering
- Slučajni događaji
- Curenje informacija
- Ilegalne aktivnosti

# Tko i kako otkriva insidere?

- Otkriveni od strane osoba koje nisu zadužene za sigurnost (61%)
- Otkriveni manuelnim metodama (pritužbe klijenata, notifikacije partnera itd.)
- 74% - nakon detekcije identitet utvrđen kroz systemske logove

# Kako spriječiti?

- Adekvatni poslovni procesi/rizici
- Ugovorno/provjera novih zaposlenika
- Centralno logiranje/nadzor mrežnog prometa
- Preventivni pregled logova/nenajavljene sigurnosne revizije
- SDLC - razvoj softvera

# Kako spriječiti?

- Ciljano nadgledanje (u suradnji s HR)
- EXTRA pažljivo s administratorima
- IDS/IPS (OSSEC, Snort, NitroView...)
- Fizička sigurnost
- Tehnička i organizacijska podjela dužnosti
- Periodička sigurnosna edukacija
- VPN

# Kako liječiti?

- Naveći pokretač u svemiru su pogreške
- Dio BC/DC
- Analizom logova
- Djelovati sukladno zakonima

# Primjeri iz prakse

- Outsourcing
- Tim testera
- Dio Botneta
- Izdaja tehnologije
- Zaporku molim!
- Banka ima otvoreni WiFi?!?!?
- Reboot servera?

Pitanja!