

# Insideri: T(r)ajna prijetnja vašim podacima

Sagena Security Day  
Zagreb, 22.9.2011.



# Sadržaj

- Što su “insiderski” napadi?
- Faktori koji utječu na pojavu insiderskih prijetnji
- Pregled insiderskih prijetnji
- Tehnike obrane
- Pitanja i odgovori

# O predavaču

- Damir Paladin, CISA, CISM
- Osnivač i direktor poduzeća Borea (1998.)
- Profesionalno se bavi informacijskim tehnologijama od 1985.
- Konzultant za informacijsku sigurnost, specijaliziran za sigurnosna testiranja, računalnu forenziku i IT reviziju
- Član Upravnog odbora hrvatskog ogranka ISACA-e

# Tko su “insideri”

- Tko su “insideri”?
  - osobe formalno povezane s određenom organizacijom
  - organizacija im je ukazala određenu razinu povjerenja, uključujući ovlasti i znanje za rad na informacijskom sustavu
  - postoji namjera zloupotrebe ukazanog povjerenja
- Primjeri:
  - zaposlenici (sadašnji, bivši, privremeni)
  - djelatnici pod ugovorom
  - vanjski suradnici
  - partneri (uslužne djelatnosti, outsourcing...)

# Insiderski događaji

- Prijevare i manipulacije (“Fraud”):
  - poslovna prijevara ili manipulacija podacima počinjena od osobe koja sudjeluje u poslovnom procesu a u cilju pribavljanja koristi
- Krađa informacija:
  - krađa povjerljivih informacija, osobnih podataka ili intelektualnog vlasništva neke organizacije
- Sabotaža i vandalizam:
  - djelovanje s namjerom izazivanja negativnih materijalnih posljedica prema podacima, informatičkoj infrastrukturi ili operativnom procesu neke organizacije

# Razlike između vanjskih i unutarnjih prijetnji

## Vanjske prijetnje

Ograničeno poznavanje žrtve

Napadači ostavljaju tragove

Visoki medijski publicitet

Vremenski ograničene

Obrana usmjerena  
infrastrukturno

Odgovornost IT odjela

## Unutarnje prijetnje

Odlično poznavanje žrtve

Napadači skrivaju tragove

Izbjegavanje medijske buke

Vrijeme je dostupan resurs

Infrastrukturna obrana je  
neučinkovita

Nedefinirana odgovornost

**Zaštita od prijetnji “insidera” zahtjeva  
promjenu uobičajenog pristupa  
informacijskoj sigurnosti**

# Faktori insiderskih prijetnji

1. Motivacija napadača
  - ✓ Doznati nedozvoljeno
  - ✓ Steći financijsku dobit
  - ✓ Nezadovoljstvo i osveta
  - ✓ Dokazati vlastitu sposobnost
  - ✓ Industrijska špijunaža
  - ✓ Ideološki razlozi i/ili patriotizam
  - ✓ Emocionalni problemi
2. Katalizatori
  - ✓ Javni događaji
  - ✓ Poslovne ili tehnološke promjene
  - ✓ Osobne promjene

# Faktori insiderskih prijetnji (nastavak)

## 3. Prilika za izvršenje prijetnje

- ✓ Redovite nadležnosti
- ✓ Izvanredne nadležnosti
- ✓ Posebne okolnosti

## 4. Sposobnost agenta prijetnje

- ✓ Resursi koje napadač ima na raspolaganju (tehnički, novčani, vrijeme, asistencija)
- ✓ Tehnička obrazovanost



# Faktori insiderskih prijetnji (nastavak)

## 5. Inhibitori

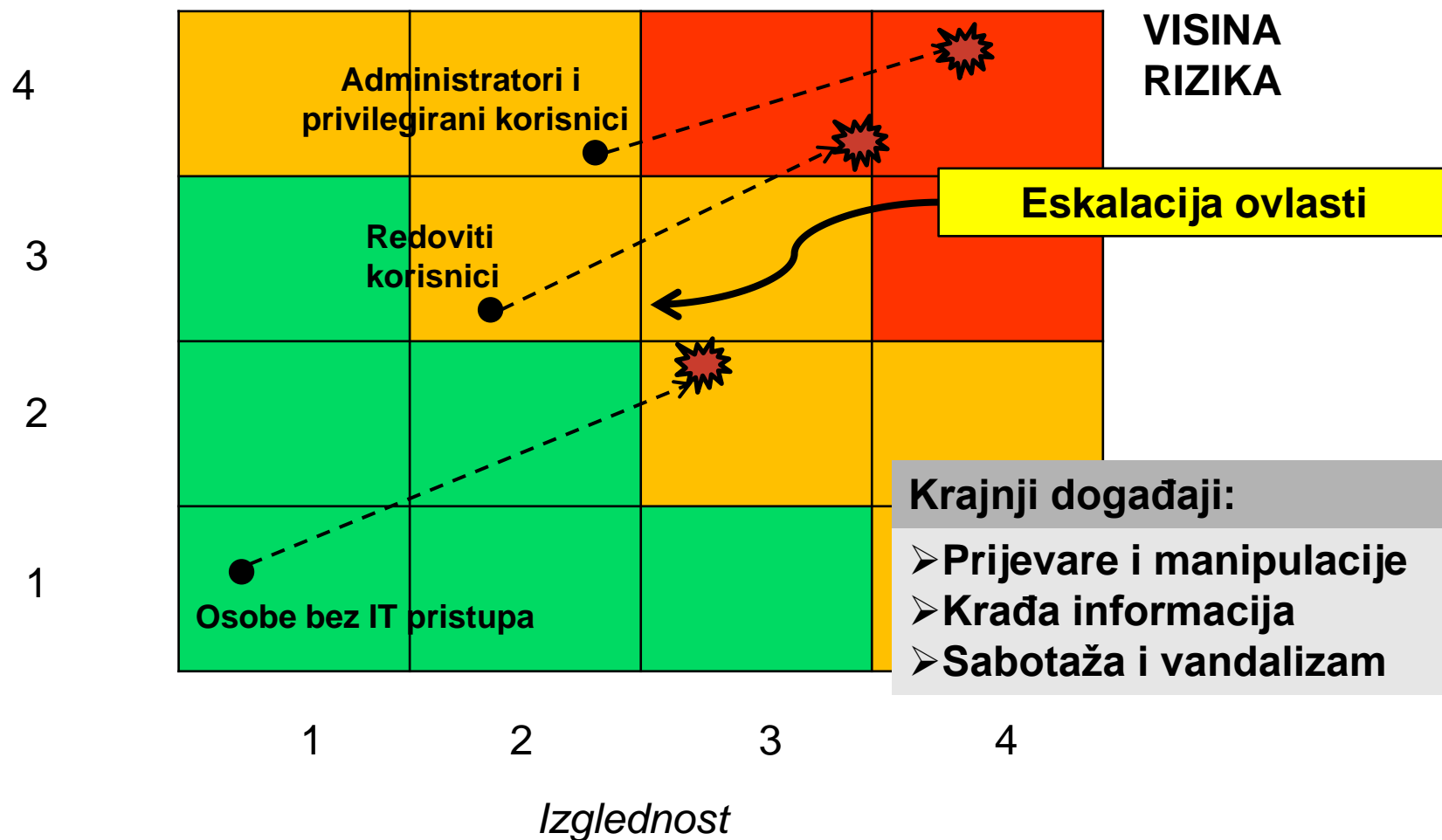
- ✓ Strah od posljedica
- ✓ Složenost
- ✓ Respekt u odnosu na vanjsku percepciju

## 6. Poticajni faktori

- ✓ Pristup informacijama
- ✓ Usmješno ovladavanje vještinama napadača
- ✓ Tehnološke promjene
- ✓ Slabe mjere zaštite sustava
- ✓ Loši međuljudski odnosi
- ✓ Slava

# Primjer: Procjene rizika insiderskih napada

Posljedice



# Metode eskalacije ovlasti

- Zloupotreba fizičkog pristupa
- Neovlašten logički pristup
- Neovlašten uvid u dokumente ili datoteke
- Socijalni inženjering
- Otkrivanje lozinki drugih osoba
- Neovlašteno korištenje sigurnosnih alata
- Prisluškivanje komunikacijskog tijeka
- Iskorištavanje programskih ranjivosti
- Pojava ili unošenje malicioznih programa
- Neovlaštene promjene programskog koda
- Prikrivanje podataka o nedozvoljenim aktivnostima

# 10 savjeta za efikasnu obranu

1. Napravite stvarnu inventuru svoje informacijske imovine
2. Budite “škrti” s pravima pristupa informacijske imovini
3. Na vrijeme se pripremite za insiderske incidenete
4. Primjereno upravljanje ljudskim resursima
5. Ne zanemarujte mjere fizičke zaštite

# 10 savjeta za efikasnu obranu

6. Redovito pratite i otklanjajte nedostatake interne mreže i sustava
7. Koristite sustave za prevenciju gubitaka podataka (DLP)
8. Uvedite enkripciju digitalne imovine
9. Provjerite kontrole u procesu razvoja aplikacija
10. Pojačajte nadzor nad događajima i informacijskim sustavom

# Nadzor kod insiderskih prijetnji

- Što pratiti:
  - Socijalni pokazatelji
  - Tehnički pokazatelji i anomalije
  - Log zapisi
  - Korištenje privilegiranih korisničkih računa
  - Drugi sigurnosni događaji
- Kako pratiti:
  - SIEM/"Log Management"
  - "Database Activity Monitoring"
  - DLP
  - Drugi sigurnosni sustavi

# McAfee protiv insidera

- McAfee Data Loss Prevention
- McAfee Device Control
- McAfee Endpoint Encryption
- McAfee Encrypted USB
- McAfee Data Protection Suite for Rights Management
- McAfee Total Protection for Data
- McAfee Database Activity Monitoring

# Što možemo očekivati u (skoroj) budućnosti?

- Porast vrijednost informacijske imovine pojačati će motivaciju insidera
- Management će ostati jednako (ne)zainteresiran
- Insideri će postati sve sposobniji
- Približavanje vanjskih i unutarnjih prijetnji



# Pitanja i odgovori