

KONFERENCA

# Informacijska varnost

Zaupanje v človeka in tehnologijo

8. november 2022 \ Hotel Slovenija, Portorož



## > Offline Backups - čemu in kako?

Speaker: **Urh Srečnik** <[urh.srecnik@abakus.si](mailto:urh.srecnik@abakus.si)>

DBA, sistem & razvoj

14:45 – 15:00



ORACLE®

Gold  
Partner

# Abakus Plus d.o.o.

- Infrastructure Team

- Services

- OS & NET admin
    - DBA, Programming

- Applications

- APPM
    - **Backup Server** & Deja Vu
    - Arbiter

- Development Team

- Custom Enterprise Applications

- Document Management

- Newspaper Distribution

- Flight Information System

# Abakus Customers

Gorenjska Banka

GENERALI  
Zavarovalnica

Ljubljana Airport

EKDIS  
Ekspresno. Ekonomično.

REPUBLIKA SLOVENIJA  
MINISTRSTVO ZA OBRAMBO

NOVA  
BANKA

MILENIJUM  
OSIGURANJE

KONTROLA  
ZRAČNEGA  
PROMETA  
SLOVENIJE

Iskra

hidria

Mestna občina  
Ljubljana

LON

triglav

ANDRITZ

jata emona  
LJUBLJANA

UNIVERZITETNA PSIHIATRIČNA  
KLINIKA LJUBLJANA  
University Psychiatric Clinic Ljubljana

skbbanka  
otp group

SAVARe

MERKUR

TRELLEBORG

SODO  
SISTEMSKI OPERATER  
DISTRIBUCIJSKEGA OMREŽJA Z  
ELEKTRIČNO ENERGIJO

BANKA  
SLOVENIJE

PRVA

MAGNETIK d.o.o.  
TSS PEST MANAGEMENT SOLUTIONS

Trelleborg Slovenija, d.o.o.

NLB Vita  
Življenjska zavarovalnica

Mercator

GOODYEAR DUNLOP  
SAVA TIRES

MM  
KARTON

studio ritem

Blubit  
TikO  
TOVARNA KOVINSKE OPREME

ZAVOD ZA  
ŠPORT RS  
PLANICA

PH  
Primorska  
hranilnica

CENTROSINERGIJA  
PANTEON  
GROUP

Lonia

PRONET  
CHOOSE THE FUTURE

hit alpinea  
Kranjska Gora

SAVA  
HOTELS & RESORTS

LASERLINE

ORACLE

ROS d.o.o.

NFOTRANS

PARK  
POSTOJSKA  
JAMA



ADRIA ANKARAN  
HOTEL & RESORT

TUJINA

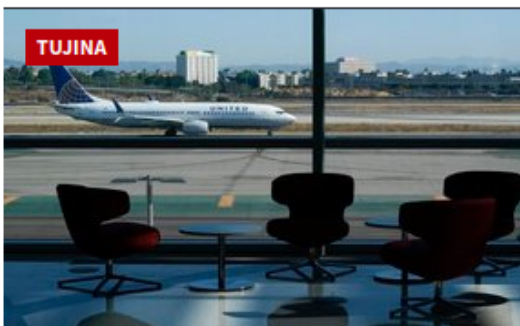


## Je hrvaška policija izsledila hekerja, ki je napadel A1?

14.02.2022, 18:34

Hrvaška policija za hekerski napad na mobilnega operaterja A1 Hrvaška, zaradi katerega so potencialno ogroženi osebni podatki okoli 150.000 ljudi, sumi mladoletnika. Med preiskavo njegovega doma v ...

TUJINA

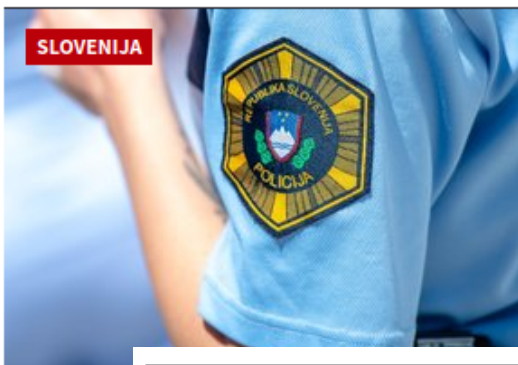


## Proruski hekerji napadli ameriška letališča

11.10.2022, 10:16

Proruski hekerji so napadli spletne strani ameriških letališč, vključno s tistimi v Atlanti, Chicagu, New Yorku in Los Angelesu. Zaradi napada je bil dostop do njihovih spletnih strani nekaj časa ...

SLOVENIJA



## Trojanski virus vdrl v Policijo, na MORS-u napad preprečili

03.09.2022, 11:25

Ministrstvo za obrambo in ministrstvo za notranje zadeve sta bili v četrtek zjutraj tarči hekerskega napada. Preko elektronske pošte z domeno @policija.si je po naših podatkih okoli 90 uporabnikov ...

TUJINA



## Hakerji napadli digitalno infrastrukturo Črne gore

27.08.2022, 8:48

Črna gora je bila žrtev najhujšega kibernetkega napada doslej, so sporočile črnogorske oblasti. Tarča napada je bila digitalna infrastruktura države. Kot zagotavljajo pristojni, so pravočasno ...

# Preventiva

- Redni varnostni pregledi
- Redne nadgradnje
- Upoštevanje dobrih praks
  - npr: redno menjavanje gesel ipd
- Investicije v varnostno infrastrukturo
  - Firewall, Antivirus, IDS, ...

# Zero Day Exploits

VARNOŠTNA OBVESTILA / 10. 12. 2021

## SI-CERT 2021-06 / Kritična ranljivost Java knjižnice Apache Log4j

*Objavljeno: 10.12.2021*

*Zadnja posodobitev: 2.2.2022*

### **Povzetek**

Kritična ranljivost knjižnice Log4j omogoča napadalcu izvedbo poljubne programske kode na ranljivem sistemu (RCE – Remote Code Execution). Ranljivost se proži ob zapisu podatka v dnevnik in se lahko izrablja tudi na sistemih, ki niso javno dostopni na internetu, vendar do njih vodi ustrezna podatkovna pot. Ranljivost najdemo tako v odprtokodnih aplikacijah, lastnih rešitvah in številnih komercialnih produktih. Identifikacija vseh ranljivih komponent je zahtevna, univerzalne rešitve za različne postavitve sistemov ni.



**UNTIL FILES**  
**0D 02:45:10**  
**PUBLICATION**

11 Mar, 2022 23:59:00

**ALL AVAILABLE DATA WILL BE PUBLISHED !**

# Offline Backup

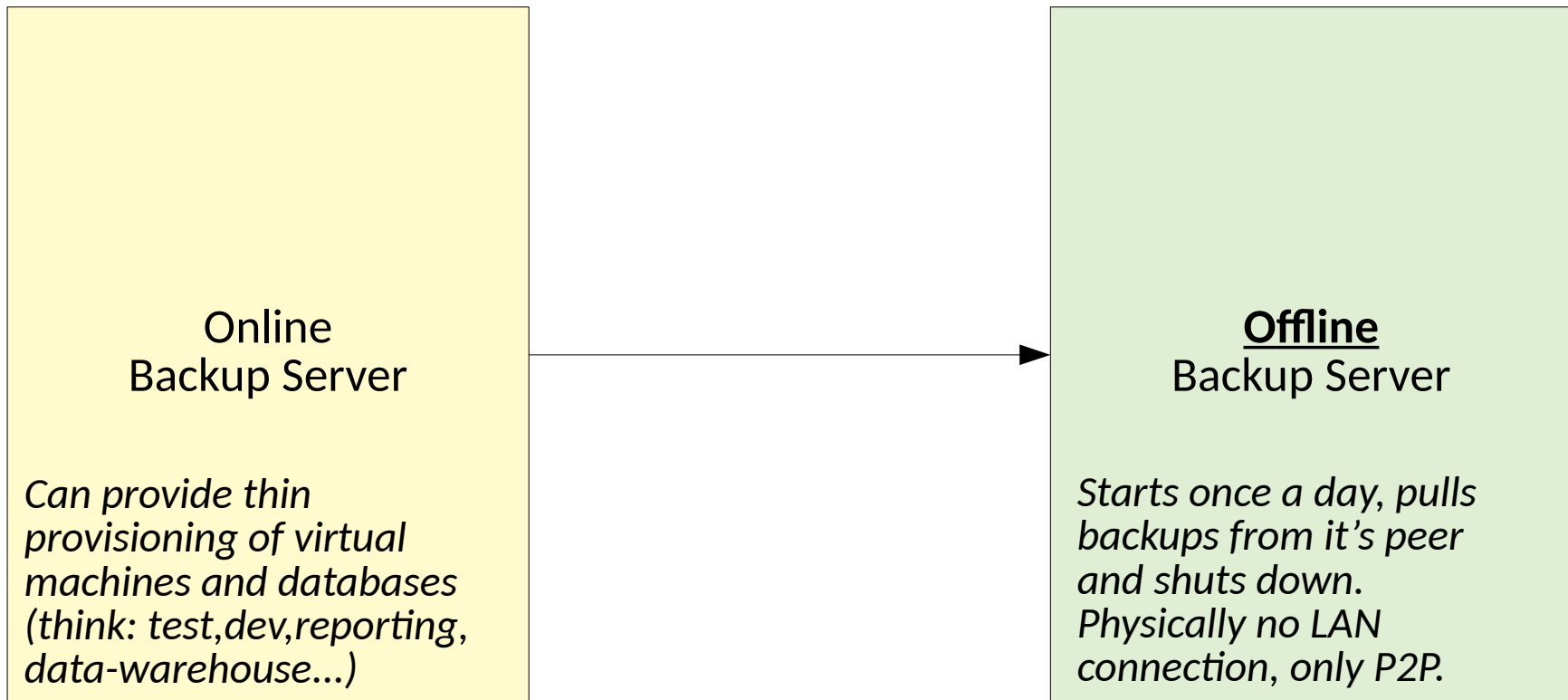
- Ne bo preprečil morebitnega razkritja podatkov
- Lahko pa prepreči izgubo podatkov
  
- Izvedba je lahko relativno enostavna (t.j. poceni)



# Možnosti izvedbe

- Kasete
- Zunanji USB diski, ki jih nekdo dnevno preklaplja
- Dedicirane naprave (primer sledi)
- Zanimive in-house rešitve
  - e.g. fizični odklop dela diskov s skripto :)
- ...

# Abakus Pristop



# Tehnični namigi

- (paralelna) **kompresija** ali deduplikacija
- **Enkripcija**  
(privatni ključ shranjen ločen v fizičnem sefu)
- Digitalno podpisani **checksum**
- **Monitoring**

*& that is way it's important to have a backup media  
collecting dust somewhere :)*



**<http://www.abakus.si/>**