ccTLD Security Practices

Iliya Bazlyankov, EDOMS

vTechDay
ICANN 70
22.03.2021

Importance of ccTLD Security Practices

Database integrity

ccTLD Reliability

Avoiding leaks

Public Infrastructure

Avoiding DDOS

Categories

Software

Backups

Hardware

Personnel

Software

Security Levels

green

yellow

red

Server Security

ssh
vpn
database
web services

Software Components

balance between updates and stability

diversity

Registry Components

whois
rdap
epp
database
dnssec
registrar panel
billing software
zone generator

Registry Components

open to public	firewall	internal IP
whois	epp	database
rdap	registrar panel	zone generator
billing	DAS	DNSSEC

Backups

Remote data center backup

Escrow

Hot-cold standby and replication

Hardware

Access to machines and datacenter (the best with ISO)

Restrict physical access to DC

Personnel

Phishing attack

Stealing access to email

Stealing server credentials

Ex staff

Removing of access

Thank you for your attention!

iliya@edoms.com