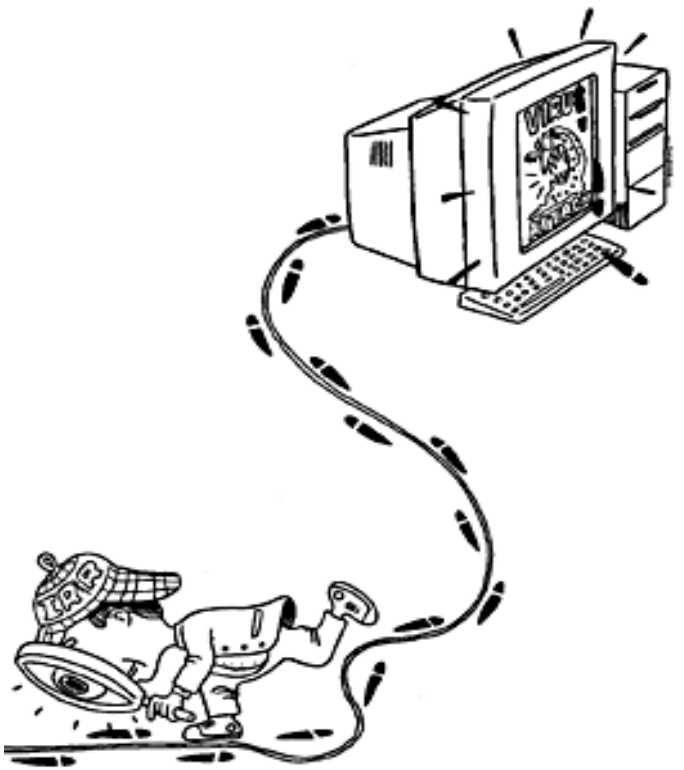
NIX·CZ

Dial Telecom

# SecVLAN@NIX.CZ from the customer perspective



**Zbyněk Pospíchal**
**Dial Telecom, a.s.**

# Secure VLAN: Why?

Response to massive DoS attacks to major Czech targets (online media, banks, mobile operators, Seznam.cz)

Attack through NIX.CZ and IP transit upstreams, source probably in Russia

No malicious traffic sourced from Czech Republic

Some of the victims used "island operation mode"
=> national IP traffic has been affected too

# Secure VLAN: What?

Create a club of trustworthy local companies, 6 members now

Last resort path to these trustworthy peering partners in "island mode" during massive (D)DoS attacks

"Czech users can still connect to Czech resources" (banks, newspapers, e-mail servers)

High entry threshold

# Secure VLAN: Who can?

An operator, who implements the following:

End user Terms & Conditions allowing an action in case of malicious traffic

24/7 NOC contact, no IVR

Terena-listed CSIRT team

More than 6 months in NIX.CZ

Impeccable reputation

Two members should guarrantee, right of veto

# Secure VLAN: What's necessary?

BCP38/SAC004 required and enforced

RTBH over RS

DNSSEC implemented

Fully redundant connection to NIX.CZ peering platform with no loss of traffic in case of an outage

Network monitoring with threshold alarms implemented

CoPP according to RFC6192

UDP amplification protection implemented

# Secure VLAN: What's new?

6 companies signed a memorandum:

Active24, CESNET (NREN), CZ.NIC (.cz TLD register), Dial Telecom, Seznam.cz ("czech Yandex") and Telefonica O2 (incumbent)

Technical setup almost prepared

# Secure VLAN: Eh?


**"Somebody broke into your computer, but it looks like the work of an inexperienced hacker."**