RP#80

RESEARCH PROJECT

PREVENTING MOST COMMON ATTACKS ON CRITICAL INFRASTRUCTURES

Wouter Miltenburg & Koen Veelenturf
University of Amsterdam
Students Master System and Network Engineering

Supervisors:
Jaya Baloo & Oscar Koeroo
KPN

RESEARCH QUESTIONS

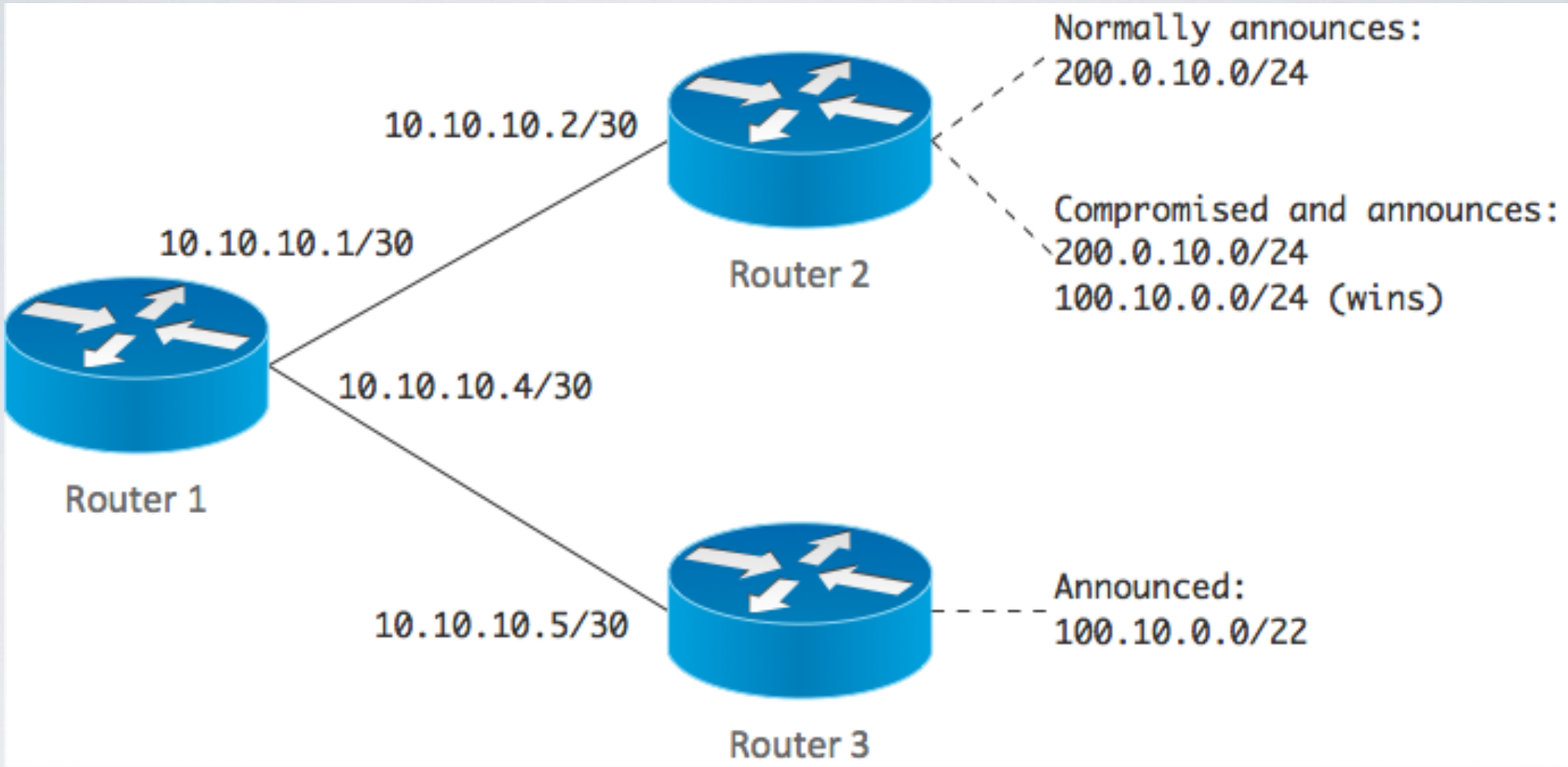
- *Which techniques are available today that could be used to mitigate common attacks?*
- What kind of attacks are critical infrastructures suffering from?
- What kind of techniques can be used?
- Why are these techniques not common practices?

INTERVIEWED COMPANIES

- KPN
- A2B Internet (Erik Bais)
- NLnet (Marc Gauw)
- A multinational company

COMMON ATTACKS

- BGP Hijacking
- DDoS
- Email Abuse (e.g. Phishing)



EXAMPLE: BGP PREFIX HIJACKING

MEASURES: BGP HIJACKING (I)

- Peer Policies
- Detailed route filtering per neighbour
- Prefix
- AS_PATH filtering
- IRR

MEASURES: BGP HIJACKING (II)

- Securing BGP sessions

- BGP Origin Validation/BGPsec

MEASURES: DDoS ATTACKS

- Scrubbing
- Ingress / egress / uRPF
- BGP FlowSpec
- Trusted Networks Initiative

TRUSTED NETWORKS INITIATIVE

- Last-resort solution for DDoS mitigation
- “Raising the Internet bridges”
- AMS-IX / NL-IX
- Foreign equivalent: The FENIX Project (Czech)

MEASURES: EMAIL ABUSE (I)

- SPF
- DKIM
- DMARC

```
<record>
  <row>
    <source_ip>213.75.39.6</source_ip>
    <count>1</count>
    <policy_evaluated>
      <disposition>none</disposition>
      <dkim>pass</dkim>
      <spf>fail</spf>
    </policy_evaluated>
  </row>
  <identifiers>
    <header_from>veelenturf.email</header_from>
  </identifiers>
  <auth_results>
    <dkim>
      <domain>veelenturf.email</domain>
      <result>pass</result>
    </dkim>
    <spf>
      <domain>veelenturf.email</domain>
      <result>softfail</result>
    </spf>
  </auth_results>
</record>
```

MEASURES: BUSINESS

- Creating awareness
- Creating business cases for security measures
- Possible reputation damage
- CERT

CONCLUSION

- Identified common attacks
- Techniques are not the problem
- Awareness
  - "Get Hacked!"
- Balance between Business & Security
- Implement suggested security measures

REMARKS

- More mitigation techniques

- Configuration examples

THANK YOU FOR YOUR TIME

QUESTIONS?