

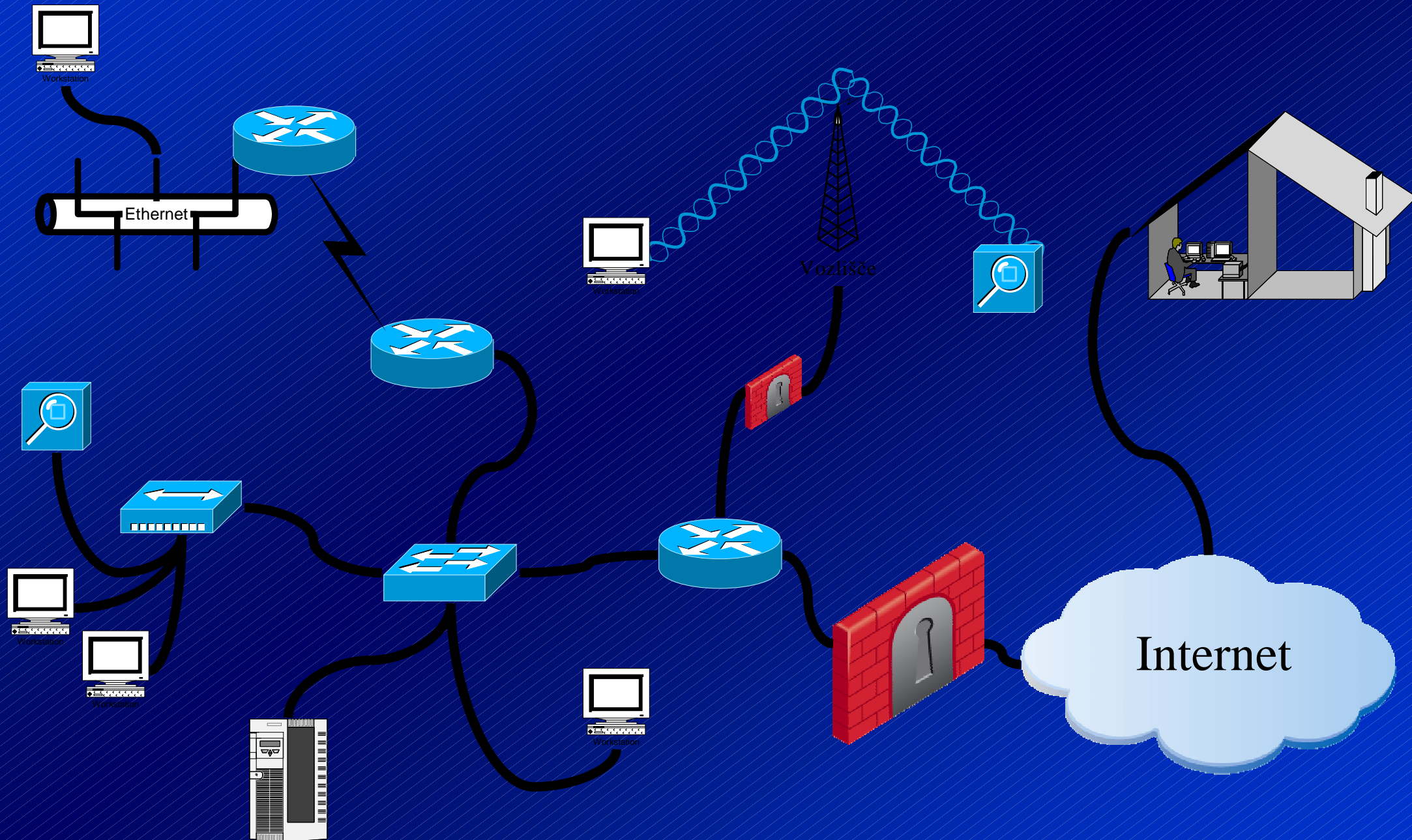
Varovanje informacijske infrastrukture

Andrej Zimšek

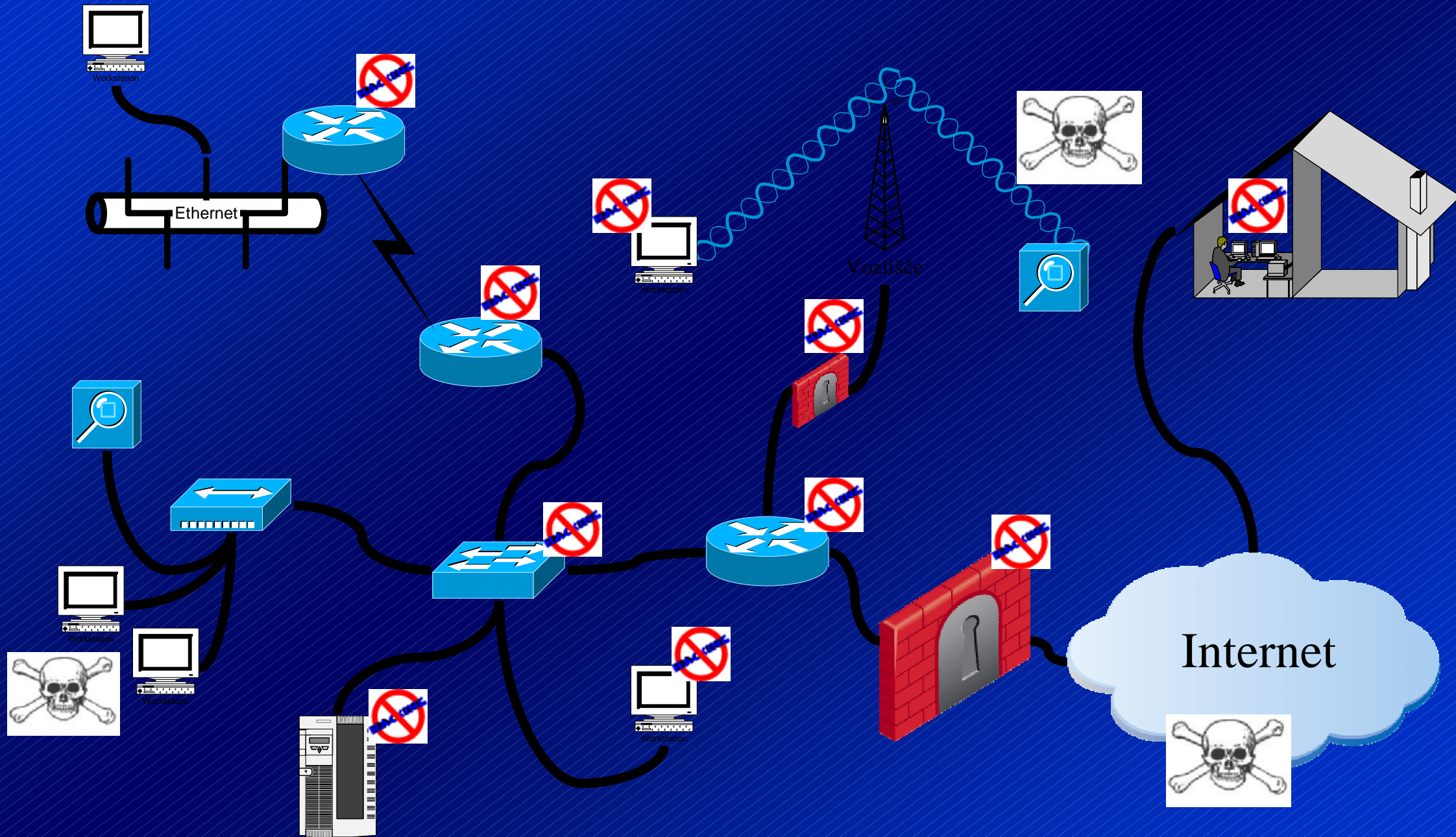
Varovanje informacijske infrastrukture

- Elementi informacijske infrastrukture
- Nevarnosti, ki se pojavljajo na informacijski infrastrukturi
- Varnostno testiranje
- Varnostni incidenti in ukrepanje
 - Primer zlonamerne programske opreme
 - CodeRed
 - Večnivojska zaščita pred zlonamerno programsko opremo

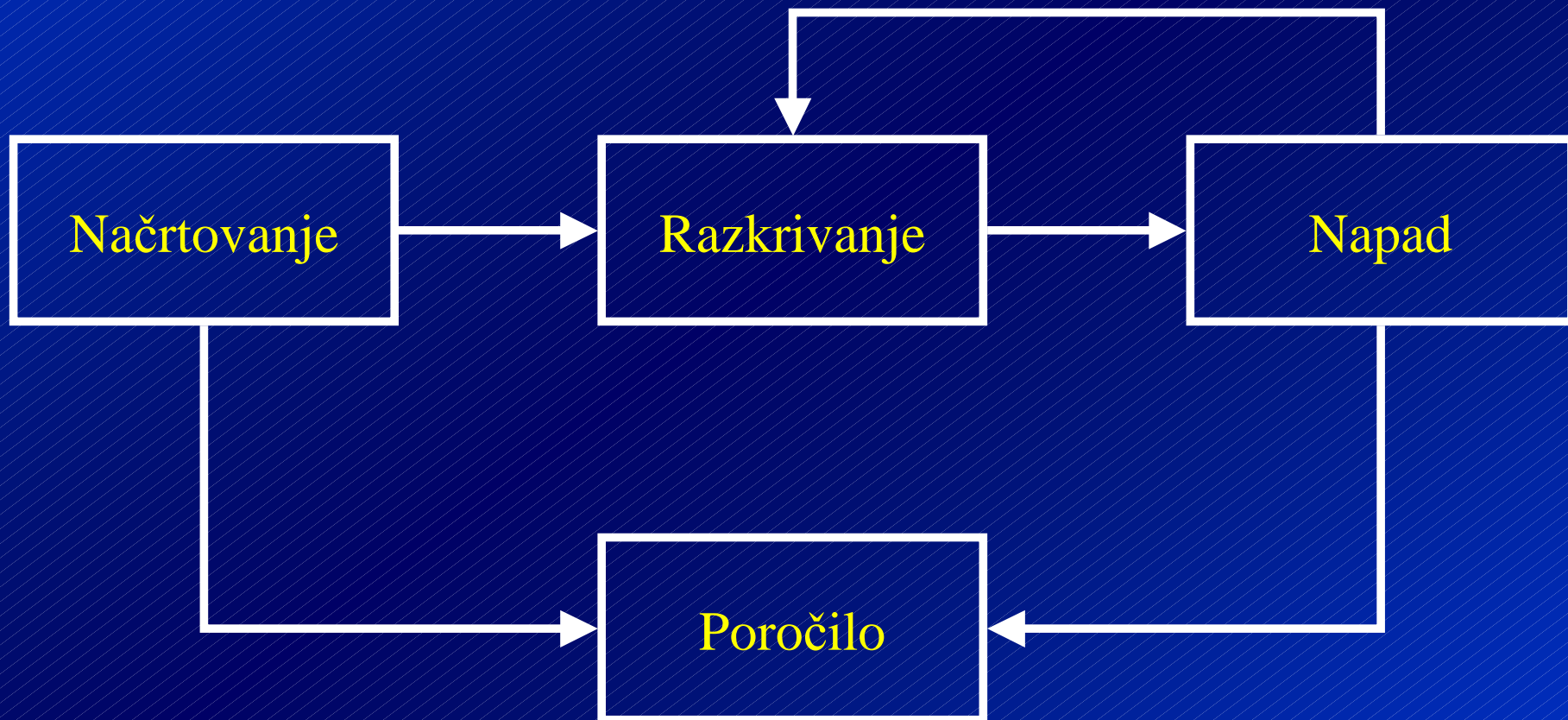
Osnovni elementi informacijske infrastrukture



Zaščita informacijske infrastrukture



Varnostno testiranje



Varnostni incidenti

- Onemogočanje delovanja določenega servisa
- Zlonamerna programska oprema
- Neavtoriziran dostop do sistema in datotek na sistemu
- Nedovoljeno pridobivanje informacij
- Uporaba nedovoljene programske opreme
- Uporaba programske opreme za nedovoljene storitve

Zaščita pred zlonamerno programsko opremo

- Ali obstajajo kontrole proti uporabi zlonamerne programske opreme?
- Ali varnostna politika vsebuje določilo o prepovedani uporabi neavtorizirane programske opreme?
- Ali obstajajo postopki za preverjanje točnosti informacij o zlonamerni programski opremi pridobljenih preko različnih virov (internet, obvestila, protivirusni programi...)?

Zaščita pred zlonamerno programsko opremo

- Ali je na računalnikih instalirana protivirusna zaščita?
- Ali se podatki o novi zlonamerni programski opremi obnavljajo v rednih časovnih intervalih?
- Ali se preverja ves promet iz omrežij in virov, ki jim ne zaupamo? Preverjanje elektronske pošte in priponk, promet iz internet omrežja, diskete,...

Primer CodeRed

1. Ali obstajajo kontrole proti uporabi zlonamerne programske opreme?

Redna kontrola operacijskega sistema in instalacija vseh potrebnih popravkov, spremljanje nenavadnega obnašanja strežnikov in delovnih postaj s stališča mrežnega prometa, itd.

Primer CodeRed

2. Ali varnostna politika vsebuje določilo o prepovedani uporabi neavtorizirane programske opreme?

Nevarnost vnosa nezaželene kode na računalniški sistem

Primer CodeRed

3. Ali obstajajo postopki za preverjanje točnosti informacij o zlonamerni programski opremi pridobljenih preko različnih virov (internet, obvestila, protivirusni programi...)?

Vrsta zlonamerne programske opreme, način za odstranitev neželene kode.

Primer CodeRed

4. Ali je na računalnikih instalirana protivirusna zaščita?

Avtomatske kontrole, preverjanje osveževanja podatkov, problemi pri pojavu nove vrste zlonamerne programske opreme, analiza vzorcev napadov ali analiza delovanja kode.

Primer CodeRed

5. Ali se podatki o novi zlonamerni programski opremi obnavljajo v rednih časovnih intervalih?

Avtomatska kontrola – obveščanje o obnavljanju podatkov

Primer CodeRed

6. Ali se preverja ves promet iz omrežij in virov, ki jim ne zaupamo?

Preprečimo lahko samo širjenje, ki poteka preko točke na kateri vršimo pregled. Širjenje v lokalnem omrežju je še vedno mogoče, če ni dodatnih kontrol.

Primer CodeRed

- Učinkovita zaščita je mogoča samo s kombinacijo različnih metod
- Ukrepi morajo biti zapisani kratko in jasno
- Izobraževanje osebja
- Nenavadni dogodki (povečan promet na omrežju)

Večnivojska protivirusna zaščita

- Strežniki, delovne postaje
- Strežniki elektronske pošte
- Prehodi med omrežji, npr. na požarnem zidu

- Omogoča dobro zaščito omrežja pred znanimi virusi in drugo zlonamerno programsko opremo

Standardi in priporočila



- **ISO17799**

Prej BS7799

- **Computer security incident handling**

http://csrc.nist.gov/publications/drafts/draft_sp800-61.pdf

- **COBIT**

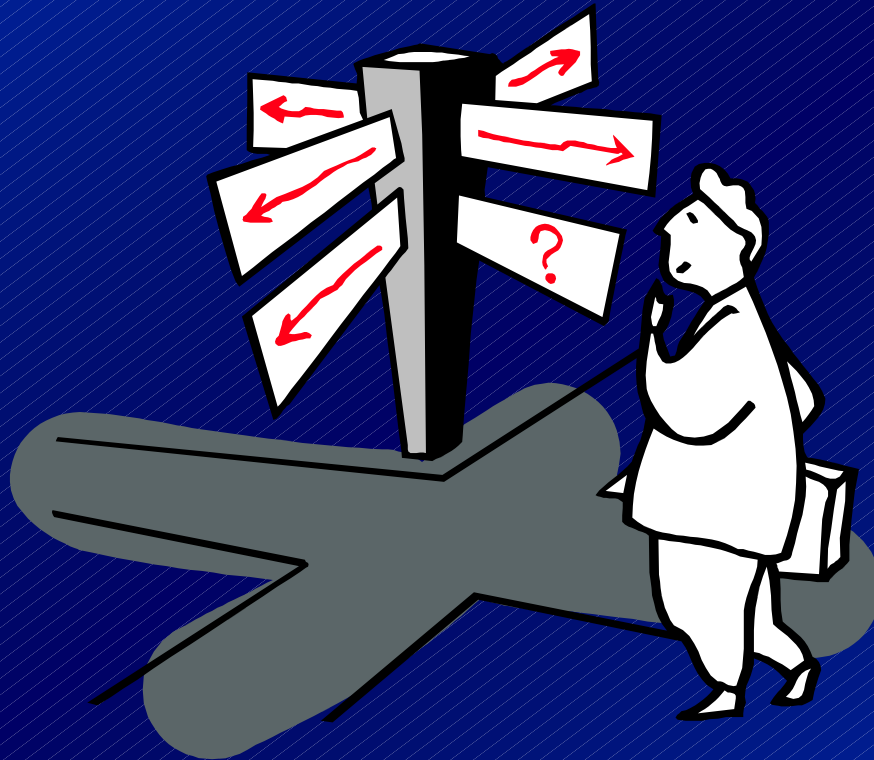
<http://www.isaca.org/cobit.htm>

- **Handbook of international auditing, assurance, and ethics pronouncements**

<http://www.ifac.org/Guidance/>

Vprašanja ...

Izmenjava mnenj ...



Andrej.Zimsek@snt.si

Nekaj “literature” na spletu

8 steps to protect your Cisco router, *Daniel B. Cid*,
<http://www.ossec.net/docs/cisco/8Steps-secure-Cisco.pdf>

Corporate Anti-Virus Protection – A Layered Approach, *Elizabeth Peyton*,
http://www.giac.org/practical/GSEC/Elizabeth_Peyton_GSEC.pdf

Corporate Incident Handling Guidelines, *David Theunissen*,
<http://www.sans.org/rr/papers/27/645.pdf>

Guideline on Network Security Testing, *John Wack, Miles Tracy, Murugiah Souppaya*,
<http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf>