Informačná bezpečnosť (6)

Informačná bezpečnosť na globálnej úrovni (efektívne riešenie bezpečnostných incidentov, trvale udržateľná úroveň)

Obsah

- Riešenie bezpečnostných incidentov
  - CSIRT a CERT
  - ISMS
  - Ochrana kritickej infraštruktúry
- Trvale udržateľná úroveň
  - Vzdelávanie
  - Výskum
  - Medzinárodná spolupráca

2. Efektívne riešenie bezpečnostných incidentov

- Druhý veľký okruh (prvý bola prevencia)
- čo je bezpečnostný incident = udalosť narušujúca zásady bezpečnostnej politiky organizácie
- Preventívne opatrenia mali za cieľ zabrániť vzniku bezpečnostných incidentov, ale nemohli ich vylúčiť (znižovanie pravdepodobnosti a dopadov bezpečnostných incidentov)
- Bezpečnostné incidenty môžu nastať
- Ďalšia línia ochrany – efektívne riešenie bezpečnostných incidentov
- Ciele : minimalizovať dopad, urýchlene dosiahnuť návrat do normálneho stavu, zaistiť stopy, vyvodiť dôsledky
- Viaceré z už spomenutých úloh/riešení spadali tak do prevencie ako aj do riešenia bezpečnostných incidentov
- Incidenty – v konkrétnych inštitúciách – tak čo sa dá spraviť na globálnej úrovni?

Čo s bezpečnostnými incidentmi na globálnej úrovni?

- Vzrastá počet
- Bezpečnostné incidenty môžu mať veľký rozsah aj zahraničný pôvod
- Príklady: Estónsko, útoky na veľké servery, útoky na banky
- http://www.cybersecurity-review.com/
- Útoky/problémy toho istého typu v rôznych organizáciách
- Nedostatočné vedomosti a kapacity v organizáciách
- Špecializované inštitúcie (CSIRT, CERT, vyšetrovatelia, jednotky boja proti počítačovej kriminalite a pod.)
- Koordinácia obrany (národné a medzinárodné cvičenia)

CERT a CSIRT – história

- Morrisov červ 1988
- Stretnutie expertov – záver vytvoriť jeden kontaktný bod, v ktorom by sa sústreďovali informácie o bezpečnostných incidentoch
- krátko na to vznikol prvý CERT® (Computer Emergency Response Team), ktorého úlohou bolo poskytovať pomoc pri riešení bezpečnostných incidentov (na Internete).
- v Európe zaužíval širší pojem CSIRT (Computer Security and Incident Response Team)
- 1990 založená medzinárodná organizácia FIRST (Forum of Incident Response and Security Teams) združujúca v súčasnosti viac než 180 CSIRT a CERT tímov z celého sveta.
- Európa TF-CSIRT
- ENISA

Poslanie a úlohy CSIRT

- Analógia – hasičská stanica
- Pre verejnosť, alebo vybranú skupinu používateľov
- Úlohy
  - Riešenie akútnych problémov
  - Cvičenia, metodiky, školenia, posudzovanie úrovne ochrany konkrétnych systémov
  - Monitorovanie a varovné signály
  - Legislatíva a štandardy
  - Zaisťovanie stôp
  - Spolupráca s vyšetrovateľmi a políciou
  - Medzinárodná spolupráca
- http://www.csirt.gov.sk/ http://www.cert.org/

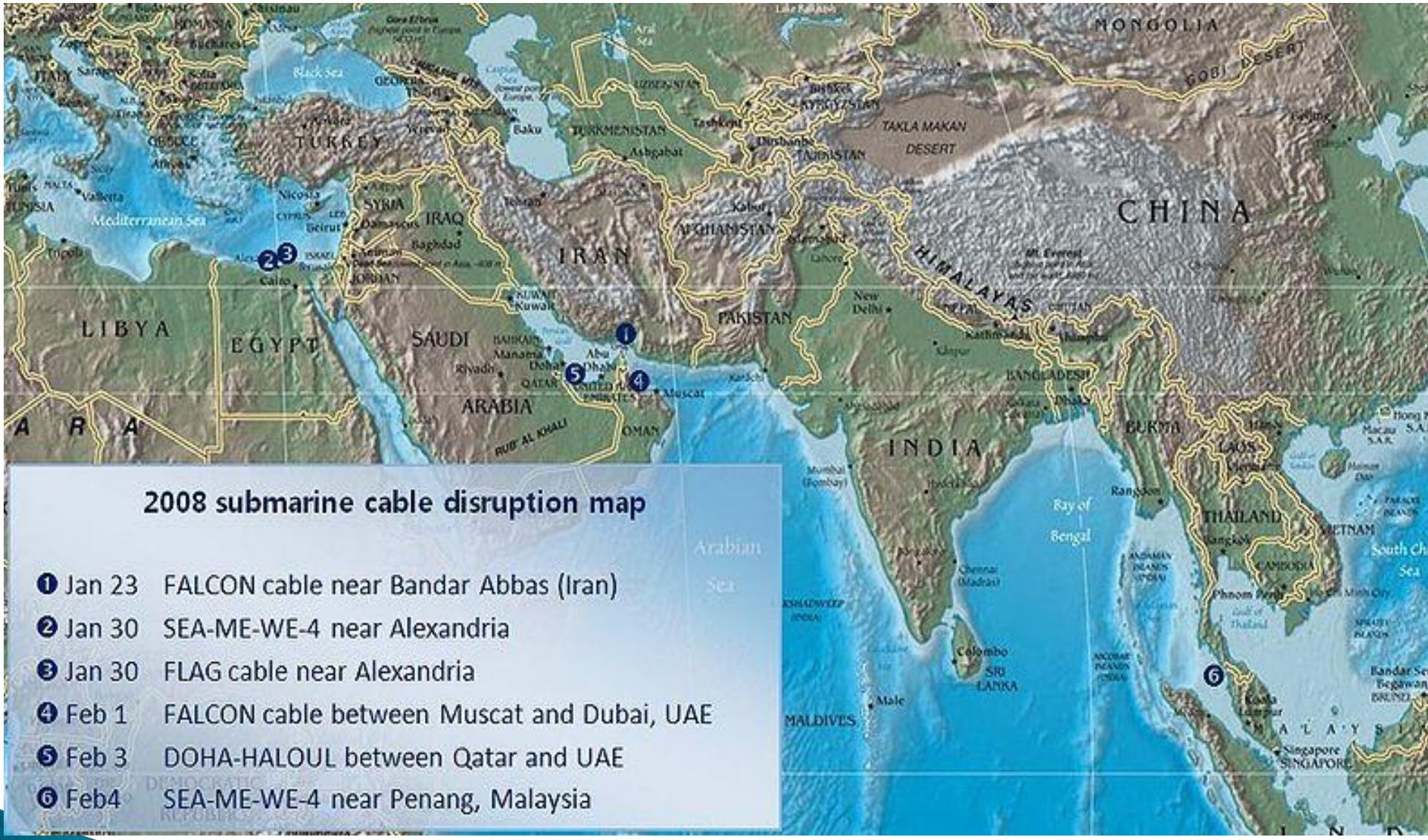
Systémy riadenia informačnej bezpečnosti

- ISMS = Information security management system, na Slovensku SMIB = Systém manažmentu informačnej bezpečnosti
- Systematický prístup na zistenie potrebnej úrovne informačnej bezpečnosti v organizácii; aj prevencia, aj riešenie bezpečnostných incidentov
- Špeciálne
  - Business continuity planning
  - Disaster recovery
- Bezpečnostné štandardy IS VS na Slovensku zavádzajú ISMS pre IS VS
- Komplexnejšie (pozri ISO/IEC 27001) – budeme sa ním zaoberať neskôr

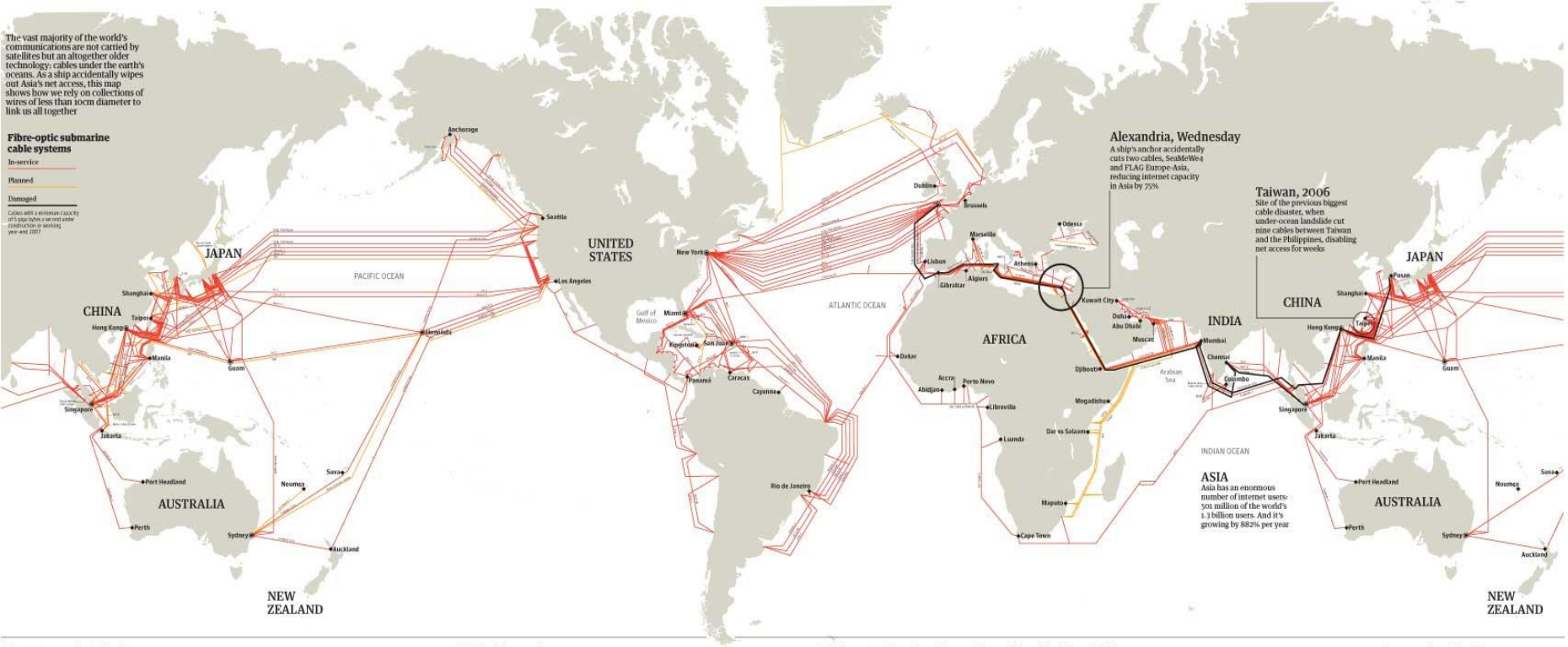
Kritická infraštruktúra

- IKT sú súčasťou kritickej infraštruktúry spoločnosti

  Revolutionary advancements in computing and communications technology have interconnected government, commercial, scientific, and educational infrastructures—including critical infrastructures for electric power, natural gas and petroleum production and distribution, telecommunications, transportation, water supply, banking and finance, and emergency and government services—in a vast, interdependent physical and electronic network.
- Terč potenciálnych útokov (zaujímavý príklad – prerušenie podmorských káblov na Blízkom východe, útoky čínskych a ruských hackerov)
- http://en.wikipedia.org/wiki/2008_submarine_cable_disruption
- http://image.guardian.co.uk/sys-images/Technology/Pix/pictures/2008/02/01/SeaCableHi.jpg

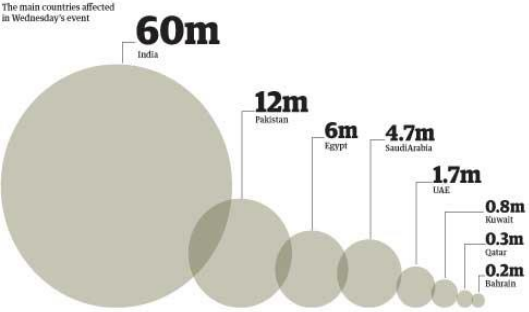

2008 submarine cable disruption map
1 Jan 23 FALCON cable near Bandar Abbas (Iran)
2 Jan 30 SEA-ME-WE-4 near Alexandria
3 Jan 30 FLAG cable near Alexandria
4 Feb 1 FALCON cable between Muscat and Dubai, UAE
5 Feb 3 DOHA-HALOUL between Qatar and UAE
6 Feb4 SEA-ME-WE-4 near Penang, Malaysia
MONGOLIA
CHINA
TURKEY
IRAN
IRAQ
SYRIA
LIBYA
EGYPT
SAUDI ARABIA
PAKISTAN
INDIA
Mediterranean Sea
Black Sea
Arabian Sea
Bay of Bengal
HIMALAYAS
GOBI DESERT
TAKLA MAKAN DESERT
Cairo
Baghdad
Tehran
Kabul
New Delhi
Mumbai (Bombay)
Colombo
SRI LANKA
MALDIVES
THAILAND
VIETNAM
CAMBODIA
Singapore
SINGAPORE

The internet's undersea world



Internet users affected by the Alexandria accident

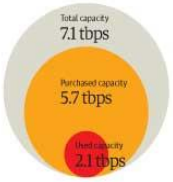
The main countries affected in Wednesday's event



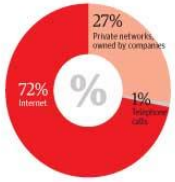
World cable capacity

Submarine cable operators light (turn on) capacity on their systems to sell bandwidth to other carriers. Carriers buy extra capacity, mainly to hold in reserve. On the trans-Atlantic route 80% of the bandwidth is purchased, but only 29% is used

Capacity in terabytes a second



What makes up "used capacity"?



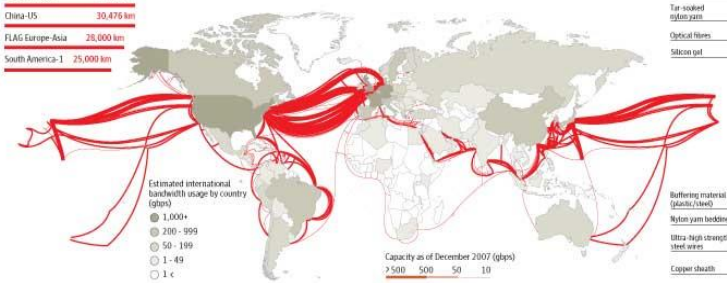
The longest submarine cables

The SeaMeWe-3 system from Norden in Germany to Keoje, South Korea connects 32 different countries with 39 landing points

SeaMeWe-3	39,000 km
Southern Cross	30,500 km
China-US	30,476 km
FLAG Europe-Asia	28,000 km
South America-1	25,000 km

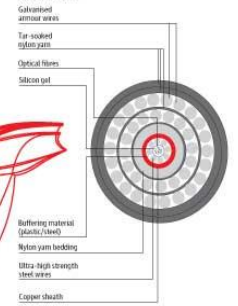
The world's cables in bandwidth

The first intercontinental telephony submarine cable system, TAT-1, connected North America to Europe in 1958 and had an initial capacity of 640,000 bytes per second. Since then, total trans-Atlantic cable capacity has soared to over 7 trillion bps



Cross-section of a cable

Cables of this strength are typically 69 mm in diameter and weigh over 10,000 kilograms a kilometer. In deeper waters, lighter and less insulated cables are used



Čo sa dá robiť s ochranou CRITIS?

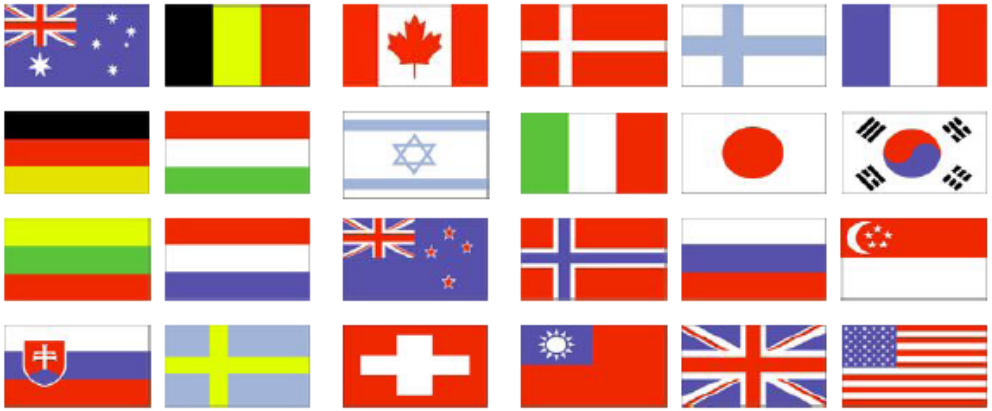
- Je to vážny problém, nepoznáme uspokojivé riešenia
- Nový veľmi rozsiahly front vojenských konfliktov (nielen potenciálny, ale horúci)
- Potenciálni útočníci – nielen nepriateľské štáty, ale aj teroristi, zločinci a nespokojní občania
- A samozrejme príroda, zlyhanie techniky, ľudské chyby, nedokonalosť systémov
- Ochrana: ako u IKT systémov, rozdiel v úrovni a rozsahu
- Špeciálna legislatíva (na ukážku USA)
  - The Protecting Cyberspace as a National Asset Act of 2010
- http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf

US cyberspace

http://www.mobiledia.com/news/images/101304-1.jpg

GREEN

FOR GOVERNMENT USE ONLY



INTERNATIONAL CIIP DIRECTORY

Top ten security guidelines *)

1. assess the risks to your business
2. consider security first when planning building works
3. establish a security culture in your business
4. keep premises clear and tidy
5. control access points and use staff and visitor passes
6. install physical measures e.g. locks, alarms, CCTV, lighting etc
7. establish good mail handling procedures
8. recruit carefully, checking identities and following up references
9. take proper IT security precautions
10. test your business continuity plans regularly

http://www.cpni.gov.uk/About/topTen.aspx

Panta Rhei (πάντα ῥεῖ všetko plynie) Trvale udržateľná úroveň

- Herakleitos *„zostupujeme i nezostupujeme do tých istých riek, sme to my i nie sme to my, lebo sa nedá dva razy vstúpiť do tej istej rieky“*
- Mení sa svet, IKT, hrozby aj požiadavky na informačnú bezpečnosť
- Ochranu musíme podľa potrieb prispôsobovať
- Na to potrebujeme
  - Know-how (výskum)
  - Kvalifikovaných ľudí (vzdelávanie)
  - Koordináciu (na lokálnej ale aj na globálnej úrovni)

Výskum v IB – na čo sa sústrediť?

Cyber Security Research Priorities (PITAC)

1. Authentication Technologies
2. Secure Fundamental Protocols
3. Secure Software Engineering and Software Assurance
4. Holistic System Security
5. Monitoring and Detection
6. Mitigation and Recovery Methodologies
7. Cyber Forensics: Catching Criminals and Deterring Criminal Activities
8. Modeling and Testbeds for New Technologies
9. Metrics, Benchmarks, and Best Practices
10. Non-Technology Issues That Can Compromise Cyber Security

Current Hard Problems in INFOSEC Research

INFOSEC Research Council USA, UK, CA

1. Global-Scale Identity Management
2. Insider Threat
3. Availability of Time-Critical Systems
4. Building Scalable Secure Systems
5. Situational Understanding and Attack Attribution
6. Information Provenance
7. Security with Privacy
8. Enterprise-Level Security Metrics

Výskum – príklady

- Kryptológia
- Projekt FIDIS (identifikácia a autentizácia vo virtuálnom priestore)
- Centrá pre IB (výskum a vzdelávanie) na univerzitách (MIT, Purdue, Carneggie Mellon, ETH Zürich, Royal Holloway College London, Bochum, ...)
- DHS S&T: A Roadmap for Cybersecurity Research

Nedostatok kvalifikovaných ľudí

- Niekto „to“ musí vedieť robiť
- Nedostatočné bezpečnostné povedomie (ľudia sa nevyznajú v IKT, IB obmedzuje)
- Nedostatok špecialistov
- Ako ich pripravovať?
  - USA (kvalifikačné štandardy, Centrá excelencie, zrovnoprávnenie s civilnými certifikátmi, Obamov program)
  - ISACA, SANS institute
  - Vysoké školy
  - Súkromné (firemné) vzdelávanie

Slovensko

- Vláda schválila Koncepciu vzdelávania v IB
- Zohľadnené medzinárodné poznatky, potreby a možnosti Slovenska
- Základný princíp: primeranosť
- Kategorizácia:
  - Laici (čo a ako majú robiť)
  - Manažéri (čo je IB, aký je jej význam a ako ju riadiť)
  - Informatici nešpecialisti
    - Správcovia systémov
    - Vývojári
  - Špecialisti v IB (vzdelávanie, prax, certifikácia, celoživotné vzdelávanie)
  - Učitelia a výskumníci

(Medzinárodná) spolupráca

- Široká a náročná oblasť
- Málo zdrojov
- Korektná spolupráca je výhodná pre všetky zúčastnené strany
- Formy (riešenie spoločných problémov, výmena operatívnych informácií, zvyšovanie povedomia, výmena know-how)
- Nielen štáty a inštitúcie, ale aj jednotlivci (Informačné zdroje: BSI, NIST, ENISA, OECD,....)

Čo treba vedieť

- Globálne bezpečnostné problémy a ich nositelia
- Kritická informačná infraštruktúra a jej ochrana
- Čo môže spraviť štát a ako
  - Legislatíva
  - Štandardizácia
  - Koordinácia
  - Vzdelávanie
  - Výskum
- Medzinárodné inštitúcie (CERT, CSIRT, ENISA)

Odporúčané čítanie/prelistovanie

1. Cyber Security: A Crisis of Prioritization, PITAC, 2005
2. Federal Plan For Cyber Security And Information Assurance Research And Development, NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, 2006
3. The National Strategy to Secure Cyberspace, 2003
4. Státní Informační Politika – Cesta k Informační Společnosti , 2006
5. Národná stratégia pre IB v SR
6. M.Královič: Štandardizácia v oblasti informačnej bezpečnosti, Diplomová práca, 2008