Informačná bezpečnosť (4)

Informačná bezpečnosť na globálnej úrovni (prehľad a legislatíva)

Obsah

- Prečo globálna úroveň a čo sa na nej má a dá riešiť
- Štát a jeho úlohy v informačnej bezpečnosti
  - Prevencia
  - Riešenie bezpečnostných incidentov
  - Rozvoj

Formulácia problému

- Bezpečnosť IKT sa nedá obmedziť len na lokálne technické riešenia (každý sa stará sám o seba a svoj systém), lebo
  - Sú prepojené a navzájom sa ovplyvňujú (interoperabilita a bezpečnosť)
  - Nie sú izolované od ostatného sveta (zákony, pravidlá, záväzky z reálneho sveta)
  - Ich bezpečnosť závisí od faktorov, ktoré nemôžu ovplyvniť technické/logické riešenia, ani majitelia IKT systémov
- Viacúrovňová ochrana
- Na najvyššej (globálnej úrovni – štát a medzinárodné organizácie)

Čo treba/čo sa dá spraviť na globálnej úrovni?

- Stav:
  - Neexistuje globálna autorita, schopná prikazovať, presadzovať, kontrolovať a postihovať
  - Štandardy, normy a niekedy medzinárodné dohody
  - Zapojenie medzinárodných organizácií (OSN, OECD, WTO, WIPO, G8,...)
  - Štandardizačné organizácie (ISO, CEN, ITU, ETSI,...)
  - Odborné nevládne organizácie (IETF, W3C, IEEE, ISACA,...)
  - ENISA, FIRST, FESA
- Čo by bolo treba: koordinovať riešenie globálnych problémov
  - Štandardizácia
  - Zosúlaďovanie národných legislatív
  - Zvyšovanie bezpečnostného povedomia
  - Spolupráca pri riešení bezpečnostných problémov/incidentov

Úloha štátu v informačnej bezpečnosti

- Štát
  - Partner na medzinárodnej úrovni
  - Legislatíva a prostriedky na jej presadzovanie
  - Vlastná IKT infraštruktúra
  - veľký poskytovateľ služieb využívajúcich IKT
  - Veľký obstarávateľ
  - Vzdelávanie
- Úlohy štátu
  - Stratégia (priority, riešenia, zdroje, realizácia)
  - Vytváranie podmienok pre ochranu digitálneho priestoru štátu (legislatíva, štandardy, vzdelávanie, formovanie povedomia)
  - Bezpečnostné služby pre neštátnu časť digitálneho priestoru
  - Koordinácia ochrany celého priestoru (spolupráca so súkromným, akademickým sektorom a občanmi)
  - Medzinárodná spolupráca

Ako zorganizovať spoľahlivú ochranu národného digitálneho priestoru?

- Najprv delenie: dôležité a menej dôležité systémy, chránime len tie dôležité (dôvody)
- Neskôr
  - zmena chápania informačnej bezpečnosti
    - od zaistenia izolovaných systémov ku ochrane celého priestoru
    - Od striktných požiadaviek k dynamickým riešeniam
    - Nielen špecialisti, ale všetci používatelia IKT
    - Primeranosť ochrany (aspoň baseline všade)
    - Údržba a postupné zvyšovanie úrovne
  - Integrácia čiastkových riešení do ucelených koncepcií
  - USA, Nemecko, Austrália, Japonsko, Fínsko, Česká republika, EÚ – ucelené štátne koncepcie IB

Základné oblasti

- Koncepcie sú rôzne, ale v podstate sa sústreďujú na tri oblasti
  - Prevencia
  - Efektívna reakcia na bezpečnostné incidenty
  - Trvalo udržateľná úroveň
- Rozoberieme ich všeobecne (svet + Slovensko), potom sa ešte raz pozrieme na situáciu na Slovensku

1. Prevencia

- Cieľ: zabrániť vzniku bezpečnostných incidentov v (národnom) digitálnom priestore
- Nástroje/spôsoby prevencie
  - Legislatíva
  - Vytváranie bezpečnostného povedomia
  - Budovanie know-how (normy, štandardy, best-practices)
  - Zavádzanie bezpečných systémov (certifikované systémy)
  - Riadenie informačnej bezpečnosti (zavádzanie systémov riadenia informačnej bezpečnosti ISMS)
  - CERT a CSIRT
- Posledné dve riešenia (zavádzanie ISMS a CERT a CSIRT) patria skôr do oblasti riešenia bezpečnostných incidentov

1.1. Legislatíva

- Dva prístupy
  - Informačná bezpečnosť zakomponovaná v jednotlivých zákonoch
  - Špeciálne zákony
- Uplatňujú sa oba prístupy
- „Obyčajné“ zákony (Slovensko)
  - Trestný zákon, Trestný poriadok, Občiansky zákonník, Obchodný zákonník, Telekomunikačný zákon, Zákon o poskytovaní zdravotnej starostlivosti, Zákon o archívnictve a i.
- Špeciálne zákony (Slovensko)
  - Ochrana utajovaných skutočností
  - Ochrana osobných údajov
  - Elektronický podpis
  - Elektronický obchod
  - Ochrana kritickej infraštruktúry
  - Zákon o e-Gov
  - Zákon o IB

Základný problém legislatívy

- Súčasné legislatívne systémy sú výsledkom dlhého vývoja a snažia sa regulovať fungovanie spoločnosti v podmienkach reálneho fyzického sveta
- Rozvojom IKT vznikol duálny virtuálny svet (cyberspace, digitálny priestor), pre ktorý
  - Neexistujú hranice
  - Prenášajú sa doň dôležité spoločenské a ekonomické aktivity
  - Nedajú sa naň uplatniť tradičné zákony a pravidlá
  - Nie sú známe účinné spôsoby na presadzovanie práva
  - Má veľký dopad na reálny svet
  - Kriminálne aktivity v ňom prebiehajú v masovom rozsahu
- Potrebujeme rozumný právny rámec a etiku pre fungovanie virtuálneho sveta

„Bezpečnostná“ legislatíva vo svete

- Nasledujúci prehľad ukazuje, ako na informatizáciu reaguje legislatíva v informačne vyspelých krajinách; aké problémy štáty považujú za potrebné riešiť prostredníctvom zákonov

Legislatíva – Nemecko *)

- Federal Data Protection Act of December 20, 1990 (Bundesdatenschutzgesetz-BGBl.I 1990 S.2954), amended by law of September 14, 1994 (BGBl. I S. 2325), law of December 16, 1997 (BGBl. I S. 2325) and December 17, 1997 (BGBl. I S. 2325), last amendment 14.01.2003
- Act on Digital Signature (Gesetz zur digitalen Signatur) Federal Law Gazette (Bundesgesetzblatt) 1997 I 1872
- Act on the Protection of Personal Data used in Teleservices (Gesetz über den Datenschutz bei Telediensten). The Act was adopted on 22 July 1997 and entered into force on 1 August 1997.
- Act for the Establishment of the BSI (dated 17 December 1990, Federal Law Gazette I p. 2834 et seq.)
- Penal Code (1871) last amended 24.03.2005 (Strafgesetzbuch-StGB)
- Code of Criminal Procedure (1950) last amended 22.03.2005 (Strafprozessordnung-StPO)
- Telecommunications Act (2004) last amended 14.03.2005 (Telekommunikations-gesetz-TKG)
- Teleservices Act (1997) last amended 14.12.2001 (Gesetz für die Nutzungvon Telediensten-TDG)
- Unfair Competition Act (2004) (Gesetz gegen den unlauteren Wettbewerb-UWG)
- Protection of Minors in the Media Treaty (2004) (Jugendmedienschutz-Staatsvertrag-JMStV)

- *) takto označené slides majú len ilustrovať problematiku

Legislatíva – USA (1) *)

- (Vybrané zákony a prezidentské smernice týkajúce sa informačnej bezpečnosti)
- The National Security Act of 1947, Pub. L. No. 235, 80 Cong., 61 Stat. 496 (July 26, 1947)
- the National Security Council Intelligence Directive (NSCID) No. 9 on 24 October 1952, ktorou bola založená NSA on 4 November 1952.
- Privacy Act of 1974, Public Law 93-579 93rd Congress, Title 54 .S.C Sec. 552a U.S. Code -CITE- 5 USC Sec. 552a 01/16/96
- Computer Security Act of 1987 Public Law 100-235 (H.R. 145) January 8, 1988
  - NIST poverený vypracovaním štandardov pre minimálnu úroveň bezpečnosti
  - Vyžaduje bezpečnostné politiky pre systémy pracujúce s citlivou informáciou
  - Povinné školenia pracovníkov pracujúcich s týmito systémami

- http://en.wikipedia.org/wiki/Category:Computer_law

Legislatíva – USA (2) *)

- Presidential Decision Directive/NSC – 29 on Security Policy Coordination (1994)
- Paperwork Reduction Act of 1995
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001
- Homeland Security Act of 2002
- The E-Government Act of 2002. (H.R. 2458/S. 803)
- The Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, et seq.) is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.L. 107-347, 116 Stat. 2899).
- Cyber Security Research and Development Act of 2002. PUBLIC LAW 107–305—NOV. 27, 2002
- Help America Vote Act of 2002

Legislatíva – USA (3) *)

- Cyber Security Research and Development Act of 2002

  A Department of Defense Joint Task Force concluded after a 1997 United States information warfare exercise that the results ‘‘clearly demonstrated our lack of preparation for a coordinated cyber and physical attack on our critical military and civilian infrastructure’’.
- Computer security technology and systems implementation lack—

  (A) sufficient long term research funding;

  (B) adequate coordination across Federal and State government agencies and among government, academia, and industry; and

  (C) sufficient numbers of outstanding researchers in the field.

Legislatíva – USA (4) *)

- Federal investment in computer and network security research and development must be significantly increased to—

  (A) improve vulnerability assessment and technological and systems solutions;

  (B) expand and improve the pool of information security professionals, including researchers, in the United States workforce; and

  (C) better coordinate information sharing and collaboration among industry, government, and academic research projects.

- http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ305.107.pdf

Legislatíva EÚ (1)

- Najdôležitejšie dokumenty Európskej únie pre oblasť informačnej bezpečnosti sú
- Council Directive 1991/250/EEC on the legal protection of computer programmes.
- Directive 1995/46/EC on personal data protection.
- Directive 1997/66/EC on data protection in the telecommunications sector.
- Directive 1999/93/EC on community framework for electronic signatures.
- Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)
- Regulation 2001/45/EC on personal protection in personal data processing by authorities and institutions.
- Council Directive 2001/264/EC on the protection of classified information.

Legislatíva EÚ (2) *)

- Directive 2002/58/EC on privacy and electronic communications.
- Directive 2002/58/EC on the processing of personal data and privacy protection.
- Regulation (EC) No 460/2004 of the European parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency)
- Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
- Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions On Fighting spam, spyware and malicious software
- Communication From The Commission To The European Parliament, The Council, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime

Legislatíva EÚ (3) *)

- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union ?

	Regulation	Directive	Decision	Resolution	Recommendation or Communication	Framework Decision	Directive Proposal	Regulation Proposal
Network and Information Security	Yes		Yes	Yes	Yes			
Attacks against Information Systems			Yes	Yes	Yes	Yes		
Corporate Governance / IT Governance		Yes			Yes		Yes	
Data Authentication and Security	Yes	Yes						Yes
Data Protection and Data Retention		Yes			Yes			
Provision of Electronic Communications Networks and Services	Yes	Yes			Yes			
Intellectual Property rights and Protection of Technical Mechanisms designed to prevent copying and counterfeiting	Yes	Yes						
Security and financial Services		Yes			Yes		Yes	

Legislatíva EÚ (4)

- EU je pri vytváraní legislatívy aktívna, ale problémy informačnej bezpečnosti nerieši systematicky
- ENISA ad hoc working group on regulatory aspects of network and information security (RANIS) *Inventory and assessment of EU regulatory activity on network and information security* (NIS) December 2006
- Právne a regulatívne prostredie NIS (sieťová a informačná bezpečnosť) je charakterizované
  - neúplnými a zavádzajúcimi zákonmi a reguláciami, ktoré tvoria ovzdušie neistoty pre implementáciu celoeurópskej NIS,
  - hoci sú zákony a regulácie dobre mienené a sú v zhode s dlhodobou víziou elektronickej fakturácie (e-billing), zavádzajú neprimeranú záťaž pre výrobcov, podnikateľov a obchodníkov,
  - je príliš veľa (otvorených) otázok okolo interoperability, najmä cezhraničnej NIS, hoci štandardy NIS sú dostupné a nejaký čas sa používajú.
- http://www.enisa.europa.eu/Pages/ENISA_Working_group_RANIS.htm

Legislatíva EÚ (5)

- Dve zaujímavosti:
  - Ochrana počítačových programov
  - ACTA

Council Directive 1991/250/EEC on the legal protection of computer programs *)

- **Article 1 Object of protection** 1. In accordance with the provisions of this Directive, Member States shall protect computer programs, by copyright, as literary works within the meaning of the Berne Convention for the Protection of Literary and Artistic Works. For the purposes of this Directive, the term 'computer programs` shall include their preparatory design material.
- 2. Protection in accordance with this Directive shall apply to the expression in any form of a computer program. Ideas and principles which underlie any element of a computer program, including those which underlie its interfaces, are not protected by copyright under this Directive.
- 3. A computer program shall be protected if it is original in the sense that it is the author's own intellectual creation. No other criteria shall be applied to determine its eligibility for protection.
- **Article 7 Special measures of protection** 1. (c) any act of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate the unauthorized removal or circumvention of any technical device which may have been applied to protect a computer program.

ACTA (1)

- The Anti-Counterfeiting Trade Agreement (ACTA)
- Multilaterálna medzinárodná dohoda o ochrane intelektuálnych práv
- Vytvorená mimo medzinárodných organizácií World Intellectual Property Organization (WIPO) and the World Trade Organization (WTO),
- Pokus zaviesť v medzinárodnom meradle maximalistické štandardy na ochranu intelektuálneho vlastníctva nad rámec existujúcich kontrol a opatrení
- ACTA je prvotne dohoda o ochrane autorských práv (copyright), ktorá sa tvári ako zmluva o ochrane pred nebezpečnými liekmi a dovozom pochybného tovaru
- Ak by bola ACTA prijatá, stala by sa novým medzinárodnýmn štandardom pre presadzovanie intelektuálnych práv a ovlyvnila by legislatívu v celosvetovom rozsahu.

ACTA (2)

- Oproti existujúcemu právu ACTA prináša/mení

  (1) rozširuje pokrytie viacerých druhov intelektuálneho vlastníctva a mení definície používané vo WTO Agreement on Trade Related Aspects of Intellectual Property Law (TRIPS Agreement);

  (2) rozširuje to, čo sa považuje za trestné porušenie autorských práva

  (3) zavádza omnoho prísnejšie opatrenia na hraniciach

  (4) zavádza povinnú užšiu spoluprácu medzi štátnymi orgánmi a držiteľmi práv ohrozujúcu súkromie a zapája štátne zdroje pre zisk súkromného sektora

  (5) vytvára novú medzinárodnú inštitúciu – výbor ACTA – na presadzovanie práv duševného vlastníctva

  - Podozrivé metódy pri príprave a schvaľovaní
  - Výhrady odbornej verejnosti
  - Zamietnutá v roku 2012

Legislatíva SR – 1

- Zákon č. 483/2001 Z.z. o bankách a o zmene a doplnení niektorých zákonov a naň naväzujúce
- Metodické usmernenie Úseku bankového dohľadu NBS č. 7/2004 k overeniu bezpečnosti informačného systému banky a pobočky zahraničnej banky
- Zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov
- Výnos Ministerstva dopravy, pôšt a telekomunikácií SR č. 1706/M-2006 o štandardoch pre informačné systémy verejnej správy (obsahujúci aj bezpečnostné štandardy)
- Zákon č. 618/2003 Z.z. o autorskom práve a o právach súvisiacich s autorským právom
- Zákon č. 610/2003 Z.z. o elektronických komunikáciách v znení neskorších predpisov
- Zákon č. 211/2000 Z.z. o slobodnom prístupe k informáciám v znení neskorších predpisov
- Zákon č. 22/2004 Z. z. o elektronickom obchode

Legislatíva SR – 2

- ústavný zákon č. 254/2006 Z.z. o zriadení a činnosti výboru Národnej rady Slovenskej republiky na preskúmavanie rozhodnutí Národného bezpečnostného úradu
- Nariadenie vlády č. 216/2004 Z.z. ktorým sa ustanovujú oblasti utajovaných skutočností
- Zákon 300/2005 Z.z, z 20. mája 2005,Trestný zákon
- Zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov.
- Zákon č. 428/2002 Z.z. o ochrane osobných údajov v znení neskorších predpisov
- Zákon č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov
- Zákon č. 215/2004 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov
- Zákon č. 45/2011 Z.z. o kritickej infraštruktúre

Trestný zákon

- Pozrieme sa na trestný zákon
- Dva typy zmien:
  - Rozšírenie „tradičných“ trestných činov aj na oblasť digitálneho priestoru (počítače ako nástroj na páchanie tradičnej trestnej činnosti, ako je falšovanie dokumentov, peňazí a pod.)
  - Nová počítačová kriminalita (prieniky do systémov, odpočúvanie, elektromagnetické vyžarovanie)
- Odporúčam si pozrieť aj iné zákony, minimálne zákony o ochrane utajovaných skutočností, elektronickom podpise, ochrane osobných údajov a informačných systémoch verejnej správy.

Trestný zákon *)

§ 196
Porušovanie tajomstva prepravovaných správ

(1) Kto úmyselne poruší
a) listové tajomstvo vyzvedaním alebo otvorením uzavretého listu alebo inej písomnosti prepravovanej poštovým podnikom alebo iným obvyklým spôsobom,
b) tajomstvo informácie prenášanej prostredníctvom elektronickej komunikačnej služby, alebo
c) tajomstvo neverejného prenosu počítačových dát do počítačového systému, z neho alebo v jeho rámci, vrátane elektromagnetického vyžarovania z počítačového systému, prenášajúceho takéto počítačové dáta,
potrestá sa odňatím slobody až na tri roky.

Trestný zákon *)

§ 219
Neoprávnené vyrobenie a používanie elektronického platobného prostriedku a inej platobnej karty

(1) Kto neoprávnene vyrobí, pozmení, napodobní, falšuje alebo si obstará elektronický platobný prostriedok alebo inú platobnú kartu vrátane telefónnej karty alebo predmet spôsobilý plniť takú funkciu na účel použiť ho ako pravý alebo na taký účel ho prechováva, prepravuje, použije alebo poskytne inému, potrestá sa odňatím slobody na jeden rok až päť rokov.

(2) Kto neoprávnene vyrobí, prechováva, obstará si alebo inak zadováži alebo poskytne inému nástroj, počítačový program alebo iný prostriedok špeciálne prispôsobený na spáchanie činu uvedeného v odseku 1, potrestá sa odňatím slobody až na tri roky.

Trestný zákon *)

§ 226
Neoprávnené obohatenie

(1) Kto na škodu cudzieho majetku seba alebo iného obohatí tým, že neoprávneným zásahom do technického alebo programového vybavenia počítača, automatu alebo iného podobného prístroja alebo technického zariadenia slúžiaceho na automatizované uskutočňovanie predaja tovaru, zmenu alebo výber peňazí alebo na poskytovanie platených výkonov, služieb, informácií či iných plnení dosiahne, že tovar, služby alebo informácie získa bez požadovanej úhrady alebo peniaze získa neoprávnene, a spôsobí tým na cudzom majetku malú škodu, potrestá sa odňatím slobody až na dva roky.

Trestný zákon *)

§ 247
Poškodenie a zneužitie záznamu na nosiči informácií

(1) Kto v úmysle spôsobiť inému škodu alebo inú ujmu alebo zadovážiť sebe alebo inému neoprávnený prospech získa neoprávnený prístup do počítačového systému, k inému nosiču informácií alebo jeho časti a

a) jeho informácie neoprávnene použije,

b) také informácie neoprávnene zničí, poškodí, vymaže, pozmení alebo zníži ich kvalitu,

c) urobí zásah do technického alebo programového vybavenia počítača, alebo

d) vkladaním, prenášaním, poškodením, vymazaním, znížením kvality, pozmenením alebo potlačením počítačových dát marí funkčnosť počítačového systému alebo vytvára neautentické dáta s úmyslom, aby sa považovali za autentické alebo aby sa s nimi takto na právne účely nakladalo,potrestá sa odňatím slobody na šesť mesiacov až tri roky.

Trestný zákon *)

§ 283
Porušovanie autorského práva

(1) Kto neoprávnene zasiahne do zákonom chránených práv k dielu, umeleckému výkonu, zvukovému záznamu alebo zvukovo-obrazovému záznamu, rozhlasovému vysielaniu alebo televíznemu vysielaniu alebo databáze, potrestá sa odňatím slobody až na dva roky.

(2) Odňatím slobody na šesť mesiacov až tri roky sa páchateľ potrestá, ak spácha čin uvedený v odseku 1

a) a spôsobí ním väčšiu škodu,

b) závažnejším spôsobom konania,

c) z osobitného motívu, alebo

d) prostredníctvom počítačového systému.

Trestný zákon *)

§ 283
Porušovanie autorského práva

(2) Rovnako ako v odseku 1 sa potrestá, kto na účel spáchania činu uvedeného v odseku 1

a) neoprávnene sleduje prostredníctvom technických prostriedkov neverejný prenos počítačových dát do počítačového systému, z neho alebo v rámci počítačového systému, alebo

b) zaobstará alebo sprístupní počítačový program a iné zariadenia alebo počítačové heslo, prístupový kód alebo podobné údaje umožňujúce prístup do celého počítačového systému alebo do jeho časti.

(3) Odňatím slobody na jeden rok až päť rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 alebo 2 a spôsobí ním značnú škodu.

(4) Odňatím slobody na tri roky až osem rokov sa páchateľ potrestá, ak spácha čin uvedený v odseku 1 alebo 2

a) a spôsobí ním škodu veľkého rozsahu, alebo

b) ako člen nebezpečného zoskupenia.

Trestný zákon *)

§ 376

Kto neoprávnene poruší tajomstvo listiny alebo inej písomnosti, zvukového záznamu, obrazového záznamualebo iného záznamu, počítačových dát alebo iného dokumentu uchovávaného v súkromí iného tým, že ich zverejní alebo sprístupní tretej osobe alebo iným spôsobom použije a inému tým spôsobí vážnu ujmu na právach, potrestá sa odňatím slobody až na dva roky.

Legislatíva SR – 3

- Vyhlášky NBÚ upravujúce ochranu utajovaných skutočností
- Vyhláška NBÚ č. 314/2006 Z. z. z 23., ktorou sa mení a dopĺňa vyhláška Národného bezpečnostného úradu č. 337/2004 Z. z., ktorou sa upravujú podrobnosti o certifikácii mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov a o ich používaní
- Vyhláška NBÚ č. 315/2006 Z. z., ktorou sa mení a dopĺňa vyhláška Národného bezpečnostného úradu č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti
- Vyhláška NBÚ č. 325/2004 Z. z. o priemyselnej bezpečnosti
- Vyhláška NBÚ č. 331/2004 Z. z. o personálnej bezpečnosti a o skúške bezpečnostného zamestnanca
- Vyhláška NBÚ č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti
- Vyhláška NBÚ č. 337/2004 Z. z., ktorou sa upravujú podrobnosti o certifikácii mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov a o ich používaní
- Vyhláška NBÚ č. 338/2004 Z. z. o administratívnej bezpečnosti
- Vyhláška NBÚ č. 339/2004 Z. z. o bezpečnosti technických prostriedkov
- Vvyhláška NBÚ č. 340/2004 Z. z., ktorou sa ustanovujú podrobnosti o šifrovej ochrane informácií

Legislatíva SR – 4

- Zmena kompetenčného zákona (NBÚ – autorita pre kybernetickú bezpečnosť)
- Koncepcia kybernetickej bezpečnosti
- Akčné plány kybernetickej bezpečnosti
- EIDAS
- Direktíva o NIS
- Pripravovaná legislatíva
  - Novely zákonov
  - Zákon o IB
  - Zákon o kybernetickej bezpečnosti
  - Zákon o ochrane utajovaných skutočností a kybernetického priestoru
  - A zrejme aj ďalšie (v dôsledku zmien európskej legislatívy)