Úvod do informačnej bezpečnosti (3)

Štát – organizácia - jednotlivec

Agenda

- Informačná bezpečnosť na úrovni štátu
- IB v organizácii - ISMS

Globálny pohľad na IB

- IB – nielen technický, resp. informatický problém
- Prečo potrebujeme, aby IKT spoľahlivo fungovali?
- Kto má záujem, aby nefungovali, resp. zneužiť ich
- Kto/čo môže ovplyvniť funkčnosť/nefunkčnosť IKT?
- Môžeme IB odignorovať?

IB a štát

- Globálny charakter IKT
- Prepojenie štátnych a súkromných systémov
- Využívanie spoločných prenosových kanálov
- Štátne systémy netvoria uzavretý systém
- Štát v IB:
  - Starostlivosť o celý priestor
  - Ochrana vlastných systémov

Úlohy štátu v IB

- Koncepcia ochrany (dôvody)
  - Veľký priestor
  - Zložité úlohy
  - Veľa zainteresovaných subjektov
  - Rôznorodé záujmy
  - Málo zdrojov
  - Spolupráca v globálnom meradle
- Koncepcia (obsah)
  - Popísať stav
  - Kľúčové priority
  - Zodpovednosť
  - Zdroje
  - Postup (Akčný plán)

Úlohy štátu v IB

- Zákony
- Priradenie zodpovednosti (štátne orgány, súkromné inštitúcie až jednotlivci)
- Stanovenie záväzných postupov
- Akreditácia a certifikácia
- Kontrola
- Sankcie
- Medzinárodné vzťahy

Legislatíva a normy

- Štátne orgány môžu robiť len to, čo stanovuje zákon
- Na IB musia participovať všetci - potrebujeme zákon, ktorý im to prikáže
- Ako koncipovať legislatívu:
  - Špeciálny zákon o IB/KB (FISMA v USA) - nevyrieši všetko
  - Zákony riešiace čiastkové oblasti
  - Úprava existujúcich zákonov
  - Európske zákony (nariadenia, direktívy, odporúčania)
  - Nadviazanie na technické normy
- Kombinácia vyššie uvedených riešení

Koncepcie IB na Slovensku

- Najprv len zmienka o IB v Stratégii informatizácii spoločnosti
- Čiastkové koncepcie (utajované skutočnosti, osobné údaje)
- Národná stratégia informatizácie spoločnosti (2008), Akčný plán
- Koncepcia Kybernetickej bezpečnosti (2015) a Akčný plán (2016)
- NATO a obrana kybernetického priestoru

Legislatíva

- **Utajované skutočnosti** – CIAA
- Zákon č. 215/2004 Z. z. Zákon o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov
  - Vyhlášky
  - Organizačné zabezpečenie
- **Osobné údaje**
- GDPR
- Zákon č. 122/2013 Z. z. Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (do mája 2018)
- **Kritická infraštruktúra**
- 45/2011 Z. z. - Zákon o kritickej infraštruktúre

Legislatíva

- **Elektronický podpis**
- Nariadenie EIDAS – NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (Nariadenie eIDAS).
- Zákon o e-Governmente
- 272/2016 Z. z. ZÁKON o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách)

Legislatíva

- Zákon o informačnej bezpečnosti >>> **Zákon o kybernetickej bezpečnosti**
- Podrobná analýza na https://uniba.sk/infosec/

IB v iných zákonoch

- Trestný zákon z Trestný poriadok
  - kriminalita s použitím počítačov
  - Aj špeciálne trestné činy zamerané na počítače
- Zákon o elektronickom obchode
- Zákon o slobodnom prístupe k informáciám
- Zákon o bankách
- Telekomunikačný zákon
- Zákon o ISVS
- Zákon o archívoch a registratúrach
  - Výnos č. 525/2011 Z. z.Výnos Ministerstva vnútra Slovenskej republiky o štandardoch pre elektronické informačné systémy na správu registratúry
- ...

Normy

- Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, odbor technickej normalizácie
- Predtým SÚTN
- Členstvo SR v ISO
- Vlastná štandardizačná činnosť
- Do pozornosti ISO/IEC 27xxx – séria ISO noriem venovaná manažmentu informačnej bezpečnosti
- Ale aj iné zdroje- NIST, BSI, IETF (RFC), FIPS, ...

Organizácia IB/KB

- Donedávna – distribuovaná
- MF SR – ISVS >>> v súčasnosti Úrad podpredsedu vlády pre informatizáciu a investície
- CSIRT.SK – Datacentrum >>>> ÚPVII
- Utajované skutočnosti – NBÚ
- Elektronický podpis – NBÚ
- Kybernetická bezpečnosť – NBÚ
- Telekomunikačná bezpečnosť, Internet – Telekomunikačný úrad a Ministerstvo dopravy...
- Osobné údaje – Úrad na ochranu osobných údajov
- Počítačová kriminalita – spravodlivosť, prokuratúra, polícia, súdy
- Kybernetická obrana – Ministerstvo obrany

Čo chýba?

- Realistická koncepcia a koordinácia
- Nemecko, USA
  - Ústredný koncepčný, metodický a kontrolný orgán
  - Rezorty
    - špecifické činnosti
    - Ochrana vlastnej infraštruktúry (CSIRT, bezpečnostné útvary)
  - Bezpečnostní manažéri a správcovia systémov in situ
  - Systematická príprava odborníkov
  - Vysokoškolské vzdelávanie
  - Výskum – základný aj aplikovaný
  - Spolupráca štátu s Univerzitami
  - Kvalifikovaní ľudia v súkromných spoločnostiach

Aktuálna situácia

- Trápime sa so zákonom o e-Gov (ÚPVS, ale najmä informatizácia v organizáciách)
- GDPR a zákon o ochrane osobných údajov
- Zákon o kybernetickej bezpečnosti

Informačná bezpečnosť v organizácii

- Štandardy ISO/IEC 27001 a 27002
- Kde začať?
- Popis stavu (čo sa v IB v organizácii robilo – bezpečnostné projekty, politiky, audity, kto mal v organizácii na starosti IB,...)
- Pozrieť sa na zavedenie IB v organizácii ako na projekt
  - Najprv poverenie vedenia organizácie
  - Inventarizácia stavu
  - Identifikácia hlavných aktív organizácie, ako sú podporované IKT, hrozby, dopady, riziká
  - Stanovenie cieľov
  - Zodpovednosti zainteresovaných (vedenie, vedúci na nižších úrovniach, zamestnanci, externisti, tretie strany)
  - Vytvorenie bezpečnostného manažmentu
  - Bezpečnostná politika organizácie

Politika informačnej bezpečnosti

- Začnime Politikou informačnej bezpečnosti, skrátene Bezpečnostnou politikou
- Obsah BP - ISO/IEC normy 27001 a 2
- Základný koncepčný dokument IB v organizácii
- Vytvára rámec pre budovanie IB v organizácii
  - Čo organizácia potrebuje chrániť
  - Na akej úrovni
  - Povinnosti jednotlivých ľudí
  - Organizačné zaistenie IB
  - Kde sa ciele IB rozpracujú podrobnejšie
  - Kontrola plnenia úloh v IB
  - Revízie politiky IB
- Politika IB je určená všetkým zamestnancom aj návštevníkom a externým spolupracovníkom

Čo dať do Bezpečnostnej politiky?

- Úvod politiky IB
  - Čo je IB
  - Význam IB pre organizáciu
  - Čo organizácia hodlá spraviť pre zaistenie IB
  - Význam politiky IB
  - Deklarácia vedenia organizácie (povinná) v ktorej vedenie

    (a) deklaruje význam informačnej bezpečnosti pre organizáciu,

    (b) stotožní sa s cieľmi stanovenými v bezpečnostnej politike,

    (c) dá prísľub, že bude presadzovať realizáciu bezpečnostnej politiky a vytvárať na to podmienky.
- Príklad Management IB, Bezpečnostná politika, str. 57
- Deklarácia vedenia organizácie, aj ako samostatný dokument, Bezpečnostný zámer

Obsah Bezpečnostnej politiky

- Pôsobnosť politiky IB (celá organizácia, nejaká oblasť, systém)
- Aj hlavné aktíva organizácie
- Na koho sa vzťahuje (domáci zamestnanci a externisti)
- Čo s externistami
  - Nemáme bezprostredný dopad, ale
  - Politika riadenia prístupu a
  - Klasifikačná schéma a pravidlá pre narábanie s klasifikovanými informáciami
- Špeciálne podsystémy – potrebujeme vyššiu úroveň IB – vyčlenenie z pôsobnosti „obyčajnej“ politiky IB
- Elektronická, alebo aj papierová forma?
- Viac politík – problém s koordináciou

Obsah Bezpečnostnej politiky

- Roly a povinnosti
- Politika IB sa týka všetkých ale primerane ich postaveniu. Všeobecná deklarácia
- Konkretizácia buď ešte v samotnej politike, alebo v dokumentoch nižšej úrovne
- Aké roly treba rozlišovať a aké povinnosti sú na ne viazané?
- Štandardy definujú príliš veľa rolí, v našich podmienkach na to nemáme dosť ľudí
- Ale úlohy ostávajú

Obsah Bezpečnostnej politiky

- Analýza rizík – kvantitatívna alebo kvalitatívna, hranica akceptovateľného rizika
- Riešenie bezpečnostných incidentov, vrátane disciplinárnych postihov
- Plány kontinuity činnosti
- Audit
- Zodpovednosť za Bezpečnostnú politiku
- Revízie Bezpečnostnej politiky
  - Pravidelné
  - Veľké zmeny
  - Závažné bezpečnostné incidenty

Ďalší postup

- BP musí schváliť vedenie organizácie a vydať ako záväzný predpis (na UK smernica rektora)
- Zamestnanci sú povinní oboznámiť sa s BP a dodržiavať ju
- Povinnosť stanovená v pracovnej zmluve
- Školenia – ochrana osobných údajov, bezpečnosť pri práci + informačná bezpečnosť
- Aj externisti a dočasní pracovníci
- Rozpracovanie v podobe dokumentácie nižšej úrovne a kontrola dodržiavania

Personálne zabezpečenie

- Vedenie organizácie – podpora, zdroje, vydávanie vnútorných predpisov
- Bezpečnostný manažment – bezpečnostný manažér a podľa veľkosti organizácie – ľudia na plný alebo čiastočný úväzok
- Vedúci pracovníci (majitelia systémov)
- Informatici
- Vnútorná kontrola, audit
- Referent pre zvláštne úlohy (utajované skutočnosti)
- Zástupcovia právneho a osobného oddelenia
- Pracovník zodpovedný za ochranu osobných údajov
- Používatelia IKT
- externisti

Ďalej?

- Správa rizík
- Podrobnejší bezpečnostný projekt – tematicky zameraný (napr. osobné údaje), alebo na kľúčové systémy
- Analýza rizík, návrh, implementácia opatrení, monitorovanie systémov
- Takisto – konkretizácia bezpečnostnej politiky
- Vzdelávanie ľudí
- Podrobnosti – ďalšie prednášky, resp. prednáška Manažment IB