Безбедносни аспекти информатизације на примерима Словачке и Србије

Зоран Чекеревац и Zdeněk Dvořák[1]

Резиме

Чланак описује неке принципе информационих стратегија Словачке Републике и Републике Србије. Акценат је стављен на заједничке проблеме везане за безбедност, дефинисање ризика, претњи и сл.

Summary

The article describes some principles of Informatization Strategy of Slovak Republic and Serbia. The main attention is oriented on problems about security, define of risk, threat etc.

Увод

Сарадња између наставника и сарадника Факултета специјалног инжењерства Универзитета у Жилини и Више железничке школе из Београда прешла је са нивоа упознавања на припремним састанцима и учествовања на конференцијама, на ниво научне и стручне сарадње. Као једна од веома важних тема, од заједничког интереса, јавила се тема везана за проблематику информационе безбедности, информатизације друштва и с тим повезаних проблема.

Заједнички принципи стратегије информатизације

Политика информатизације друштва произилази из усвојених националних стратегија информатизације у Републици Словачкој и у Републици Србији. У обе земље се развијају одговарајући системи управљања безбедношћу – развијају политике безбедности информационих технологија, идентификују задаци и одговорности у унутрашњој организацији. Препоручена је следећа структура активности:

- управљање развојем мреже информационих система,
- управљање говором,
- упознавање свих запослених са безбедношћу информационих система,
- хаваријски план и планови обнове рада система и података после хаварије,
- управљање ризиком, укључујући идентификације, прорачуне и предвиђања везана за:
  - акта која треба чувати,
  - опасности,
  - рањивост,
  - могуће нападе,
  - ризике,
  - мере заштите,
  - остале ризике,
  - ограничења.

[1] Зоран Чекеревац, проф. др, Виша железничка школа, Здравка Челара 14, Београд, Србија, Тел: ++381 11 27 68 095, факс: ++381 11 27 68 095

Zdeněk Dvořák, doc. PhD., Fakulta špeciálneho inžinierstva, Žilinská univerzita v Žiline, 1.mája 32, Žilina, Slovenská republika, Tel: ++421 513 6854, Fax: ++421 513 6620.

У оквиру припремних активности при улажењу у проблематику потребно је обратити пажњу и на дефинисање циљева, стратегије и безбедносне политике информационог система. Веома битан, суштински, фактор при анализи и решавању проблема безбедности је комплексан приступ проблему. Примењена решења нису увек у потпуности избалансирана и дешава се да не одговарају стварним потребама и захтевима. Неизбалансираност може да буде последица и тога што се мера заштите везују искључиво за техничко обезбеђење, што је данас основни тренд, а да се при томе потпуно заборавља на људски фактор у заштити. Ретко ко је свестан да људски фактор мора да буде укључен и у најситнијим детаљима информационог система да би се он заштитио. Другим речима, ако желимо да обезбедимо информациони систем од напада споља потребно је да имамо напредну технику и осмишљен систем заштите. Неопходно је паралелно решити и проблеме који се тичу напада изнутра. То што гарантује успех или га знатно умањи нису само техничка решења, већ и поштовања организацијских правила. Те проблеме треба стално решавати у оквиру животног циклуса информационог система.

Систем за управљање безбедношћу може се поделити у два дела:

1. **Избор и имплементација одговарајућих техничких мера заштите**

Под овим се може подразумевати нпр. увођење приступних шифара, ограничавање права приступа корисника подацима и ресурсима у складу са њиховим стварним потребама и овлашћењима, дефинисање правила и процедура за комуницирање преко интернета, антивирусна и остале мере заштите у оба смера, од напада споља и од унутрашњих напада. Обезбеђење техничке заштите може се постићи правилним избором и постављањем баријера, firewall-a, као и избором одговарајуће унутрашње архитектуре мреже.

2. **Упознавање свих запослених са безбедношћу информационих система**

Исправно функционисање система заштите захтева придржавање постављених правила при раду са рачунарским системима. То значи, пре свега, да корисници не објављују приступна имена, лозинке и приступне кодове. Ти подаци су записани на папиру и држе се у сефу, а отварају се само у случајевима кризних ситуација. Поред тога је нужно придржавати се правила о забрани пријема и слања одређених врста прилога, инсталирању непознатих апликација или самоактивирајућих фајлова, неприступању одређеним ризичним www страницама и сл. Правилно постављање firewall-a на прокси серверу може знатно умањити ризике.

Користи од формирања безбедносне политике

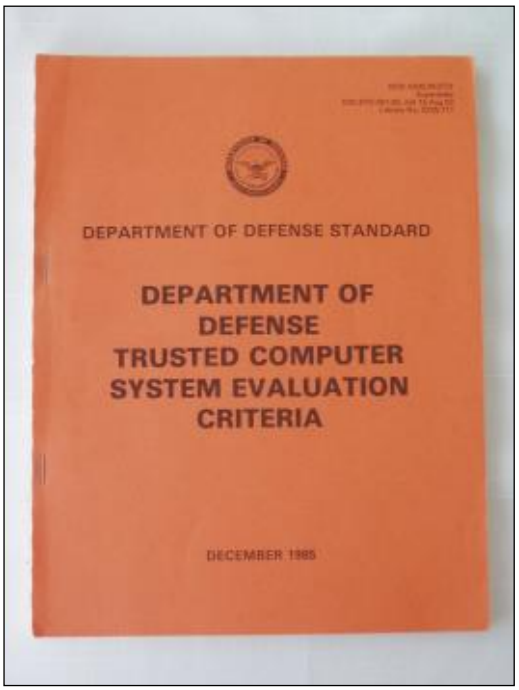
- израђена студија сигнализира најважније захтеве везане за организацију информатичке безбедности,
- комплексни приступ свим аспектима безбедности указаће и на унутрашњу повезаност система,
- поглед „из вана“ често може да открије и укаже на грешке о којима сви знају, али које нико не помиње.

Метод рада при предузимању корака ка формирању безбедносне политике базира се на томе да организација формира неформалну радну групу састављену од одговорних лица из области којих се тиче безбедност и екстерног сарадника, експерта за

безбедносну политику. Информације се прикупљају у форми разговора са екстерним експертом према претходно формираним листама питања.

Безбедносна политика тиче се следећих области

- безбедност IT,
- физичка заштита,
- легислатива,
- логичка заштита,
- персонална заштита.



Сл. 1 Наранџаста књига

Циљеви IT заштите

- минимизирање штета насталих безбедносним инцидентима и грешкама, њихово изучавање и учење на њима,
- обезбедити да корисници буду свесни угрожавања безбедности и да буду припремљени за рад на својим радним местима у складу са усвојеном безбедносном политиком,
- снизити ризике везане за људске грешке, крађу, непоштовање правила усвојене организације.

Дефинисање потенцијала

Потенцијали су оно што организациона јединица има на располагању. Потенцијали организације обухватају:

- физичка, материјална, средства (нпр. рачунарски хардвер, комуникациона опрема итд),
- информације (документа, базе података, ...),
- нематеријална средства (нпр. апстрактна вредност фирме, имиџ, добре везе итд),
- радна снага, обученост, стручност и искуство радника,
- способност за стварање сопствених производа или за давање услуга,
- софтвер.

Сваки од наведених потенцијала има своју цену која је толика да заслужује висок степен заштите.

Предвиђање претњи

Потенцијали су предмет разних претњи. Претње имају природно или људско порекло. Могу да буду случајне природе, инциденти, или осмишљене. Штета настала инцидентом може да буде привремена или трајна са различитим градацијама у интензитету.

Анализа рањивости

Рањивости доприносе слабе тачке у систему које су и најчешћи предмет угрожавања. Слабости система воде ка нежељеним последицама. Оне представљају могућност за

настанак штете. Пример рањивости је одсуство механизма контроле приступа. Анализа рањивости обухвата преиспитивање и проналажење слабих тачака система које могу да буду предмет угрожавања познатим претњама.

Предвиђање пада система

Пад система је последица нежељених осмишљених инцидената или инцидената случајне природе. Последице могу да имају негативан утицај на неке специфичне активности и потенцијале као што су: оштећење ИТ система, губитак веза, интегритета, доступности, веродостојности, индивидуалног губитка података и резултата рада пре настанка инцидента итд. Анализа и предвиђање пада доприноси успостављању равнотеже између последица нежељених инцидената и мера и трошкова везаних за заштиту система. Такође, анализом и прорачунима могуће је предвиђање учесталости падова система и интервала између падова што омогућава и предузимање одговарајућих мера заштите.

Квантитативно и квалитативно вредновање падова система врши се:

- применом придева према унапред дефинисаним категоријама, нпр. ниски средњи, високи, ...
- применом емпиријски дефинисане бројне скале, нпр. 1 – 10,
- специфицирањем финансијских трошкова изазваних падом система.

Анализа ризика

Под појмом ризик у информатици се подразумева потенцијална могућност да дато угрожавање изазове рањивост или евентуално губитак појединих потенцијала или чак скупине потенцијала. Ризик се карактерише као комбинација два фактора: вероватноће настанка нежељеног инцидента и самог његовог настанка.

Прихватање последичних ризика

Од ризика се брани обично предузимањем мера заштите од ризика, чиме се доприноси њиховом смањењу. Последичним ризицима се називају ризици од последица. О прихватању последичних ризика води се посебна анализа у складу са потребама организације за коју се информациони систем користи.

Утврђивање ограничења

Ограничења су повезана са радом и могућностима организације и могу да буду:

- финансијска,
- организациона,
- персонална,
- правна,
- техничка.

Надзор и вредновање

Процеси надзирања и вредновања су основне компоненте одржавања и развоја ИТ система. Суштинска разлика између ова два процеса лежи у задацима које извршавају и проблемима на које се односе. У *Националној стратегију за информационо друштво у Србији* предвиђају се стални надзор и процена оствареног напретка у развоју

информационог друштва што такође представља и значајан део одрживости развојног процеса. Ради се о два различита типа надзора и процене: једним се обухвата процес имплементације Стратегије и Акционог плана а другим целокупни развој информационог друштва у Републици Србији.
За спровођење оба типа надзора и процене потребно је утврдити и дефинисати следеће:

- Мерне показатеље напретка;
- Методологију праћења напретка (коришћење методологија које се примењују у другим земљама);
- Периоде процене напретка (годишње);
- Овластити установу која ће бити надлежна да разматра и усваја процене напретка и извештаје.

Надзор над имплементацијом Стратегије за информационо друштo у Србији је процес који се остварује у три фазе:

- Утврђивање показатеља;
- Мерење и анализа;
- Ажурирање развојне политике и стратегије.

Редовни извештаји о напретку пружају најбољу основу за усвајање нових развојних политика, док систем мерних показатеља представља квантитативну основу за ажурирање и исправљање циљева стратегије. Спровођење ових мера у Србији отпочело је одмах након усвајања стратегије.

Закључак

На основу рада сагледани су многи фактори коју указују на сличност погледа у односу на безбедносне аспекте информатизације Србије и Словачке. Узајамна сарадња у овој стручној области може донети читав низ нових открића и корисних резултата. У првој фази, први корак сарадње може да буде усаглашавање наставних планова и програма у овој специфичној проблематици. После тога могло би да следи усаглашавање уџбеничке литературе и њено унапређење кроз размену материјала за предавања и вежбања. Интензивна свакодневна сарадња чак и на растојању од 600km данас се лако може остварити захваљујући модерним ИТ технологијама. Читав низ стручних проблема на којима се заједнички ради и из којих се развијају заједнички пројекти говоре о квалитету узајамне комуникације. Верујемо да ће даљи кораци бити усмерени ка размени наставника и студената у оквиру разних програма сарадње и грантова.

♦♦♦

Литература

[1] ESEE. *Agenda for the Development of the Information Society.* Stability Pact. 4 June, 2002
[2] EU. *eEurope 2002: eEurope Benchmarking Report.* Brussels: Commission of the European Communities, 2002
[3] *eEurope e 2002: Impacts and Priorities*. Brussels: Commission of the European Communities, 2001
[4] *eEurope 2005: Benchmarking Indicators*. Brussels: Commission of the European Communities, 2002

[5] *eEurope: An Information Society for All.* Brussels: Commission of the European Communities, 2002
[6] *Национална стратегија за информационо друштво у Србији*, Република Србија Министарство науке и заштите животне средине, 2006