Prehľad

Bezpečnosť informačných systémov a sietí

Smerom ku kultúre bezpečnosti

Overview

OECD Guidelines for the Security of Information Systems and Networks:

Towards a Culture of Security

Slovak translation

Prehľady sú preložené výňatky z publikácií OECD.
Možno ich získať bezplatne cez internetové kníhkupectvo
www.oecd.org/bookshop/
Tento Prehľad nie je oficiálnym prekladom OECD.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

ORGANIZÁCIA PRE HOSPODÁRSKU SPOLUPRÁCU A ROZVOJ

Úvod

Od roku 1992, kedy OECD prvýkrát prezentovala *Smernice pre bezpečnosť informačných systémov*, sa používanie informačných systémov, sietí a celej informačnej technológie dramaticky zmenilo. Tieto neustále zmeny ponúkajú značné výhody, avšak zároveň kladú oveľa vyššie bezpečnostné nároky na vlády, obchodné a iné spoločnosti, ako aj na jednotlivcov, ktorí vyvíjajú, vlastnia, poskytujú, riadia služby a ktorí používajú informačné systémy a siete („účastníci“).

Kedysi prevládajúce lokálne a uzatvorené siete nahradili stále výkonnejšie počítače, vzájomne prepájajúce technológie a stále všestrannejšie využívanie Internetu. V súčasnej dobe sú účastníci stále vo väčšej miere vzájomne prepojení a prepojenia presahujú hranice štátov. Navyše, Internet podporuje kritické odvetvia ako napríklad energetiku, dopravu a financie a v značnej miere ovplyvňuje štýl obchodovania spoločností, štýl, ktorým vlády poskytujú služby občanom a podnikom a štýl komunikácie a výmeny informácií medzi jednotlivcami. Takisto došlo ku zmenám podstaty a typu technológií, ktoré vytvárajú komunikačnú a informačnú infraštruktúru. Mnohonásobne sa zvýšil počet a charakter prípojných zariadení, pričom tieto zahŕňajú pevné, bezdrôtové a mobilné zariadenia. Takisto sa rapídne zvyšuje počet nepretržite pripojených zariadení. Uvedené má za následok podstatné zvýšenie objemu a citlivosti vymieňaných informácií.

Stále väčšie prepojenie má za následok zvyšujúci sa počet a rôznorodosť ohrození a vyššiu zraniteľnosť informačných systémov a sietí. Táto situácia vyžaduje zavedenie nových bezpečnostných opatrení. Z týchto dôvodov sa tieto Smernice vzťahujú na všetkých účastníkov novej informačnej spoločnosti a navrhujú potrebu vyššieho povedomia a pochopenia bezpečnostných otázok a potrieb vývoja „kultúry bezpečnosti“.

I. Smerom ku kultúre bezpečnosti

Tieto Smernice reagujú na stále sa meniace bezpečnostné prostredie podporou rozvoja kultúry bezpečnosti – to znamená zameranie sa na bezpečnosť informačných systémov a sietí a prijatie nových spôsobov myslenia a správania sa pri používaní a styku s informačnými systémami a sieťami. Smernice naznačujú jasný zlom v čase, keď bezpečnostný dizajn a používanie sietí a systémov predstavovali len dodatočný nápad. Účastníci sa stávajú omnoho viacej závislými na informačných systémoch, sieťach a ich službách, čo vyžaduje vyššiu spoľahlivosť a bezpečnosť. Iba ten prístup, ktorý berie do úvahy záujem všetkých účastníkov a charakter systémov a sietí a príslušných služieb, môže poskytovať efektívnu bezpečnosť.

Každý účastník je dôležitým prvkom zaistenia bezpečnosti. Účastníci by si mali uvedomovať náležité bezpečnostné riziká a preventívne opatrenia, mali by prijať určitú mieru zodpovednosti a učiniť potrebné kroky na zvýšenie bezpečnosti informačných systémov a sietí.

Podpora kultúry bezpečnosti bude vyžadovať vodcovský prístup a širokú zainteresovanosť a mala by vyústiť do posilnenia priorít plánovania a manažmentu bezpečnosti, ako aj do akceptovania potrieb bezpečnosti všetkými účastníkmi. Otázka bezpečnosti mala by byť predmetom záujmu a zodpovednosti na všetkých úrovniach štátnej administrácie a súkromného podnikania ako aj pre všetkých účastníkov. Tieto Smernice tvoria základ pre dosiahnutie kultúry bezpečnosti prostredníctvom spoločnosti. Toto umožní účastníkom zakomponovať prvok bezpečnosti do dizajnu a používania všetkých informačných systémov a sietí. Smernice navrhujú, aby si všetci účastníci osvojili kultúru bezpečnosti a podporovali ju ako spôsob myslenia, hodnotenia a svojej aktivity v rámci informačných systémov a sietí.

II. Ciele

Hlavným cieľom týchto Smerníc je:

- Podpora kultúry bezpečnosti ako spôsobu ochrany informačných systémov a sietí medzi všetkými účastníkmi.
- Zvýšenie povedomia o rizikách, vzťahujúcich sa na informačné systémy a siete; o opatreniach, postupoch a procedúrach, dostupných na čelenie týmto rizikám a zvýšenie povedomia o potrebe prijatia a implementácie týchto opatrení.
- Podpora širšej dôveryhodnosti informačných systémov a sietí a spôsobov ich používania medzi všetkými účastníkmi.

- Vytvorenie všeobecného referenčného rámca, ktorý pomôže účastníkom pochopiť bezpečnostné opatrenia a rešpektovať etické hodnoty rozvoja a implementácie koherentných praktík, opatrení a procedúr, potrebných pre bezpečnosť informačných systémov a sietí.
- Podpora spolupráce a výmeny informácií (do prípustného rozsahu) medzi všetkými účastníkmi pri rozvoji a implementácii bezpečnostných opatrení, praktík a procedúr.
- Podpora vnímania bezpečnosti ako dôležitého nástroja medzi všetkými účastníkmi, ktorí sa podieľajú na vývoji alebo zavádzaní štandardov.

III. Pravidlá

Nasledujúcich deväť pravidiel sa navzájom dopĺňa a mali by sa posudzovať ako celok. Pravidlá sa týkajú účastníkov na všetkých úrovniach, vrátane úrovní politických a výkonných. V rámci týchto Smerníc sa zodpovednosť účastníkov líši v závislosti od ich postavenia. Všetci účastníci budú upovedomení, bude im poskytnuté vzdelávanie, zdieľanie informácií a školenie, čo by malo viesť k lepšiemu vnímaniu a pochopeniu bezpečnosti. Snaha o zvýšenie bezpečnosti informačných systémov a sietí by mala byť konzistentná s hodnotami demokratickej spoločnosti, najmä pokiaľ ide o otvorený a voľný tok informácií a o osobnú informačnú bezpečnosť[1].

1) Povedomie

Účastníci by si mali byť vedomí potreby bezpečnosti informačných systémov a sietí a krokov, ktoré môžu vykonať na zlepšenie úrovne bezpečnosti.

Uvedomovanie si rizík a znalosť dostupných zabezpečovacích prostriedkov je prvým krokom pri ochrane bezpečnosti informačných systémov a sietí. Riziká, ktoré môžu ovplyvniť bezpečnosť informačných systémov a sietí, sú rizikami internými a externými. Účastníci by si mali uvedomiť, že zlyhanie bezpečnosti môže vážnym spôsobom ohroziť systémy a siete, ktoré sú pod ich kontrolou. Takisto by si mali uvedomiť, že v dôsledku prepojenia a vzájomnej závislosti sa ohrozenie týka aj ostatných. Účastníci by preto mali dokonale poznať konfiguráciu svojho systému, možnosti dostupných aktualizácií svojho systému, jeho miesto v sieti, mali by poznať kroky, ktoré prispievajú k zvýšeniu bezpečnosti a takisto by mali poznať potreby ostatných účastníkov.

[1] Okrem týchto Bezpečnostných smerníc vydala OECD ďalšie odporúčania, týkajúce sa ostatných oblastí, dôležitých pre svetovú informačnú spoločnosť. Tieto opatrenia sa týkajú súkromia (*Smernice OECD o ochrane súkromia a cezhraničného toku osobných údajov*, vydané v roku 1980), a kryptografie (*Smernice OECD pre kryptografiu*, vydané v roku 1997). Tieto Bezpečnostné smernice by sa mali posudzovať a vnímať v súvislosti s vyššie uvedenými odporúčaniami.

2) Zodpovednosť

Všetci účastníci sú zodpovední za bezpečnosť informačných systémov a sietí.

Účastníci sú závislí na prepojených miestnych a globálnych informačných systémoch a sieťach a mali by chápať svoju zodpovednosť za bezpečnosť týchto informačných systémov a sietí. Ich zodpovednosť by mala odrážať ich individuálnu pozíciu. Účastníci by mali pravidelne prehodnocovať svoje vlastné spôsoby konania, metódy, opatrenia, nariadenia a postupy a posudzovať ich vhodnosť vo vzťahu k ich okoliu. Tvorcovia produktov a služieb by mali brať do úvahy systémovú a sieťovú bezpečnosť a pravidelne a včas distribuovať relevantné informácie a aktualizácie tak, aby účastníci dokonale pochopili bezpečnostnú funkčnosť produktov a služieb a svoju zodpovednosť vo vzťahu k bezpečnosti.

3) Odozvy

Účastníci by mali spolupracovať v oblasti prevencie, detekcie a odoziev na prípadné bezpečnostné incidenty.

Vzhľadom na prepojenie informačných systémov a sietí a z toho vyplývajúcej existencie rozsiahleho potenciálu zdrojov škôd by mali všetci účastníci vzájomne spolupracovať pri odhaľovaní a odstraňovaní bezpečnostných incidentov. Mali by si vzájomne vymieňať informácie o rôznych formách hrozieb a zraniteľných miestach systémov a sietí (do prípustného rozsahu), a zaviesť rýchlu a efektívnu spoluprácu, zameranú na ochranu a detekciu bezpečnostných incidentov. Tam, kde je to možné, by táto spolupráca mala zahŕňať cezhraničnú spoluprácu a vzájomnú výmenu informácií.

4)Etika

Účastníci by mali plne rešpektovať legitímne záujmy ostatných.

Vzhľadom na prienik informačných systémov a sietí do našich spoločností by si mali účastníci uvedomiť, že ich činnosť, resp. nečinnosť môže poškodiť druhých. Etické chovanie je preto zásadným pravidlom a účastníci by sa mali snažiť o zavedenie „najlepších postupov“ a podporovať chovanie, ktoré odráža potreby bezpečnosti a plne rešpektuje legitímne záujmy ostatných.

5) Demokracia

Bezpečnosť informačných systémov a sietí by mala byť v súlade so základnými hodnotami demokratickej spoločnosti.

Implementácia bezpečnosti by mala plne odrážať hodnoty, vyznávané demokratickými spoločnosťami, vrátane voľnej výmeny myšlienok a nápadov, voľného toku informácií, dôvernosti informácií a komunikácie, primeranej ochrany osobných informácií, otvorenosti a transparentnosti.

6) Hodnotenie rizika

Účastníci by nemali zanedbávať hodnotenie rizika.

Hodnotenie rizika pomáha identifikovať prípadné hrozby a zraniteľné miesta a malo by predstavovať rozsiahlu základňu, ktorá by obsiahla hlavné interné a externé faktory, ako napr. technológiu, fyzikálne a ľudské faktory, politiku a služby tretích strán, ktoré majú vplyv na bezpečnosť. Hodnotenie rizika umožní stanoviť prijateľnú mieru rizika a pomôže pri výbere kontrolných činností, zabezpečujúcich správnu a patričnú ochranu informačných systémov a sietí. Vzhľadom na narastajúci objem prepojení by hodnotenie rizika malo zahŕňať aj zhodnotenie potenciálneho nebezpečenstva, ktoré môže byť spôsobené ostatnými účastníkmi, alebo ktoré môže byť spôsobené im.

7) Návrh a implementácia bezpečnosti

Účastníci by mali zaviesť a vnímať bezpečnosť ako jeden zo základných prvkov informačných systémov a sietí.

Za účelom optimalizácie bezpečnosti by systémy, siete a relevantná politika mali byť správne navrhnuté, zavedené a koordinované. Jedným z hlavných, avšak nie výlučných ohnísk pozornosti v tomto smere je návrh a zavedenie vhodných prostriedkov zabezpečenia, ako aj návrh a implementácia riešení, ktoré by mali vylúčiť, alebo aspoň obmedziť potenciálne škody, vyplývajúce z identifikovaných hrozieb a zraniteľných miest. Základným predpokladom sú technické a netechnické spôsoby zabezpečenia a tieto by sa mali zaviesť proporcionálne vzhľadom na hodnotu informácií o systémoch a sieťach príslušnej organizácie. Bezpečnosť by mala zohrávať hlavnú úlohu pri všetkých produktoch, službách, systémoch a sieťach a mala by predstavovať integrálnu súčasť návrhu a architektúry systému. Pre konečných používateľov znamená návrh a implementácia zabezpečenia najmä výber a konfiguráciu produktov a služieb, ktoré sú poskytované pre ich systém.

8) Manažment bezpečnosti

Účastníci by si mali osvojiť komplexné ponímanie manažmentu bezpečnosti.

Manažment bezpečnosti by mal predstavovať nadstavbu hodnotenia rizík a mal by byť dynamickým prvkom, zahŕňajúcim všetky úrovne a aspekty činnosti účastníkov. Mal by zahŕňať prezieravé odozvy na vznikajúce hrozby a ochranu pred nimi, detekciu a odozvu na incidenty, obnovenie systému, trvalú údržbu systému, dôkladnú prehliadku systému a jeho audit. Všetky opatrenia, nariadenia a procedúry, týkajúce sa informačných systémov a sietí, by mali byť koordinované a integrované tak, aby vytvárali koherentný systém bezpečnosti. Požiadavky manažmentu bezpečnosti závisia od úrovne angažovanosti, úlohy jednotlivých účastníkov, obsiahnutého rizika a od systémových požiadaviek.

9) Potreba prehodnocovania

Účastníci by mali prehodnocovať úroveň bezpečnosti informačných systémov a sietí a následne by mali vhodne upravovať svoje bezpečnostné opatrenia, nariadenia a procedúry.

Neustále sa objavujú nové a meniace sa hrozby a tým aj nové zraniteľné miesta systémov a sietí. Účastníci by mali pravidelne prehodnocovať a modifikovať všetky aspekty bezpečnosti, aby tak zabránili potenciálnym rizikám a škodám.

Odporúčania Rady týkajúce sa Smerníc o informačných systémoch a sietiach

Smerom ku kultúre bezpečnosti

RADA,

Vzhľadom na konvenciu OECD zo dňa 14.12. 1960 a jej články 1 b), 1 c), 3 a) a 5 b);

vzhľadom na odporúčanie Rady, týkajúce sa Ochrany súkromia a cezhraničného toku osobných údajov zo dňa 23.9. 1980 [C(80)58(FINAL)];

vzhľadom na odporúčanie Rady, týkajúce sa Deklarácie o cezhraničných tokoch údajov, ktorá bola prijatá vládami členských krajín OECD dňa 11.04. 1985 [Príloha k C(85)139];

vzhľadom na odporúčanie Rady, týkajúce sa kryptografií zo dňa 27.03. 1997 [C(97)62/FINAL];

vzhľadom na Ministerskú deklaráciu o Ochrane súkromia v globálnych sieťach zo dňa 7.-9.12. 1998 [Príloha k C(98)177/FINAL];

vzhľadom na Ministerskú deklaráciu o Overení elektronického obchodu zo dňa 7. – 9.12. 1998 [Príloha k C(98)177/FINAL]

berúc do úvahy, že používanie informačných systémov a sietí a ich hodnota pre vlády, obchodné a iné organizácie a pre jednotlivcov narastajú;

berúc do úvahy, že rastúca dôležitosť informačných systémov a sietí, ako aj závislosť stabilného a efektívneho rastu národných hospodárstiev, medzinárodného obchodu a sociálnej, kultúrnej a politickej sféry na týchto systémoch vyžadujú špeciálne snahy, ktoré by zvýšili ochranu a dôveryhodnosť týchto systémov;

berúc do úvahy, že informačné systémy a siete a ich celosvetové rozšírenie prinášajú nové a narastajúce riziká;

berúc do úvahy, že údaje a informácie, uložené v informačných systémoch a sieťach, alebo ktoré sú nimi rozširované, podliehajú rôznym ohrozeniam, ako napríklad neoprávnenému prístupu k nim, ich neoprávnenému použitiu, ich sprenevere, zmenám, prenosu zlomyseľných kódov, odmietnutiu služby alebo ich zničeniu, a preto vyžadujú adekvátne formy zabezpečenia;

berúc do úvahy, že je nevyhnutné zvýšiť povedomie o rizikách, vzťahujúcich sa na informačné systémy a siete a povedomie o taktike, opatreniach a postupoch, ktoré tieto riziká obmedzujú, a že je nevyhnutné podporovať vhodné správanie ako základný prvok smerom ku kultúre bezpečnosti;

berúc do úvahy, že je nevyhnutné pravidelne prehodnocovať existujúcu bezpečnostnú taktiku, opatrenia, a postupy tak, aby plne zodpovedali meniacemu sa prostrediu informačných systémov a sietí a potenciálnym zdrojom ohrození týchto systémov a sietí;

berúc do úvahy spoločný záujem o podporu bezpečnosti informačných systémov a sietí prostredníctvom kultúry bezpečnosti, ktorá podporuje medzinárodnú koordináciu a spoluprácu za účelom eliminácie prípadných škôd, ktoré by prípadné zlyhanie bezpečnosti spôsobilo národným ekonomikám, medzinárodnému obchodu a účasti na sociálnom, kultúrnom a politickom živote;

a ďalej berúc do úvahy, že *Smernice pre bezpečnosť informačných systémov a sietí: Smerom ku kultúre bezpečnosti*, ktoré tvoria prílohu tohto odporúčania, sú materiálom dobrovoľným a neovplyvňujú žiadnym spôsobom suverenitu národov;

a berúc do úvahy, že tieto Smernice nenaznačujú, že existuje len jedno bezpečnostné riešenie, a ani nenaznačujú, aká taktika opatrenia, alebo postupy sú tými vhodnými pre riešenie danej situácie, ale rámcovo uvádzajú pravidlá pre lepšie pochopenie prínosov pre používateľov a možnosti ich prispetia k rozvoju kultúry bezpečnosti;

ODPORÚČA tieto *Smernice pre bezpečnosť informačných systémov a sietí: Smerom ku kultúre bezpečnosti* vládam, obchodným a iným spoločnostiam a jednotlivcom, ktorí sa podieľajú na vývoji, vlastnia, poskytujú, riadia, obsluhujú a používajú informačné systémy a siete;

ODPORÚČA členským krajinám:

prispôsobiť existujúce, alebo zaviesť novú taktiku, opatrenia a postupy tak, aby odrážali ustanovenia *Smerníc pre bezpečnosť informačných systémov a sietí: Smerom ku kultúre bezpečnosti* a to osvojením si a podporou kultúry bezpečnosti, ako je uvedená v týchto Smerniciach;

konzultovať, koordinovať a spolupracovať na národnej a medzinárodnej úrovni pri zavádzaní Smerníc;

rozšíriť Smernice medzi verejnosťou a v rámci súkromného sektoru vrátane vlád, obchodných a iných organizácií a jednotlivcov za účelom podpory kultúry bezpečnosti, a podporovať všetky zainteresované strany v ich zodpovednosti a snahe učiniť všetky nevyhnutné kroky na zavádzanie Smerníc v súlade s ich individuálnym postavením;

včas a vhodným spôsobom sprístupniť tieto Smernice krajinám, ktoré nie sú členmi OECD;

každých 5 rokov prehodnocovať tieto Smernice tak, aby sa podporila medzinárodná spolupráca v oblasti bezpečnosti informačných systémov a sietí;

NARIAĎUJE Komisii OECD pre informačnú, počítačovú a komunikačnú politiku (Committee for Information, Computer and Communications Policy) podporovať zavádzanie týchto Smerníc.

Toto Odporúčanie nahrádza Odporúčanie Rady, týkajúce sa Smerníc pre bezpečnosť informačných systémov zo dňa 26.11. 1992 [C(92)188/FINAL].

História procedúry

Smernice pre bezpečnosť boli prvýkrát opublikované v roku 1992 a revidované v roku 1997. Súčasnú aktualizáciu dokonala Pracovná skupina pre bezpečnosť informácií a osobných údajov (Working Party on Information Security and Privacy- WPISP) na základe splnomocnenia Komisií OECD pre informačnú, počítačovú a komunikačnú politiku, a po tragédii z 11. septembra 2001. tieto práce boli urýchlené.

Odborná skupina WPISP, ktorá sa stretla 10-11 marca 2001 vo Washingtone, 12-13 februára 2002 v Sydney a 4,6 marca 2002 v Paríži podniknula práce nad náčrtom. Členovia WPISP stretli sa v Paríži 5-6 marca 2002, 22-23 apríla 2002 a 25-26 júna 2002.

Tieto *Smernice OECD pre bezpečnosť informačných systémov a sietí: Smerom ku kultúre bezpečnosti* ostali prijaté ako Odporúčania Rady OECD na 1037. zhromaždení, 25. júla 2002.

Obsah pôvodnej anglickej verzie publikácie

(bez príloh, zoznamu rámčekov, tabuliek a grafov):

Tento prehľad je prekladom výňatkov z publikácie OECD vydanej pod anglickým a francúzskym názvom:

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information: Vers une culture de la sécurité

Publikácie OECD a *Prehľady* možno získať bezplatne cez internetové bezplatne cez internetové kníhkupectvo OECD na www.oecd.org/bookshop

Napíšte „overview"(prehľad) v poli „Title search" na stranie internetového kníhkupectva alebo napíšte názov anglickej publikácie

(Prehľady sú spojené s pôvodnými publikáciami v angličtine)

Prehľady pripravuje

Divízia autorských práv a prekladov riaditeľstva verejných záležitostí a komunikácie.

email : rights@oecd.org / Fax: +33 1 45 24 13 91