

Best practices z oblasti informačnej a kybernetickej bezpečnosti

Ivan Makatura

Konferencia eFocus:
Informačná a kybernetická bezpečnosť prakticky

23.5.2019, Austria Trend Hotel, Bratislava

„U ľudí z pamäti vzniká skúsenosť;
pretože mnohokrát opakovaný a
pamäťou uchovaný vnem tej istej veci
nadobúda význam jednej skúsenosti.“

(Aristoteles, Metafyzika I, 1, 980b-981a)

Je potrebné znova vynaliezať koleso...?

Prax

Podľa definície:

- z lat. praxis = konanie

V prenesenom význame:

- Cieľavedomá činnosť, ktorá zodpovedá teórii
- Opakované vykonávanie lekcií pre získanie alebo vylepšenie zručností
- Zaužívaný obvyklý spôsob konania
- Zavedený postup
- Skúsenosti získané praktickou činnosťou

Od zvyčajnej praxe ku najlepšej praxi...

Dobrá prax – Good Practice

„Dobrá skúsenosť“:

- Pozitívna alebo žiaduca
- Lepšia ako priemerná
- Majúca vlastnosti, ktoré sú rozlišujúce v konkrétnej veci
- Slúžiaca na požadovaný účel

Najlepšia prax – Best Practice

„Najlepšia skúsenosť“:

- Vynikajúca, ktorá vo výslednej kvalite prekračuje všetkých ostatné skúsenosti
- Kvalifikovane osvedčená
- Majúca vlastnosti, ktoré sú v konkrétnej veci už mnohokrát overené
- Najvhodnejšia, najužitočnejšia pre požadovaný účel

Čo je to „Best practice“ v technických odvetviach?

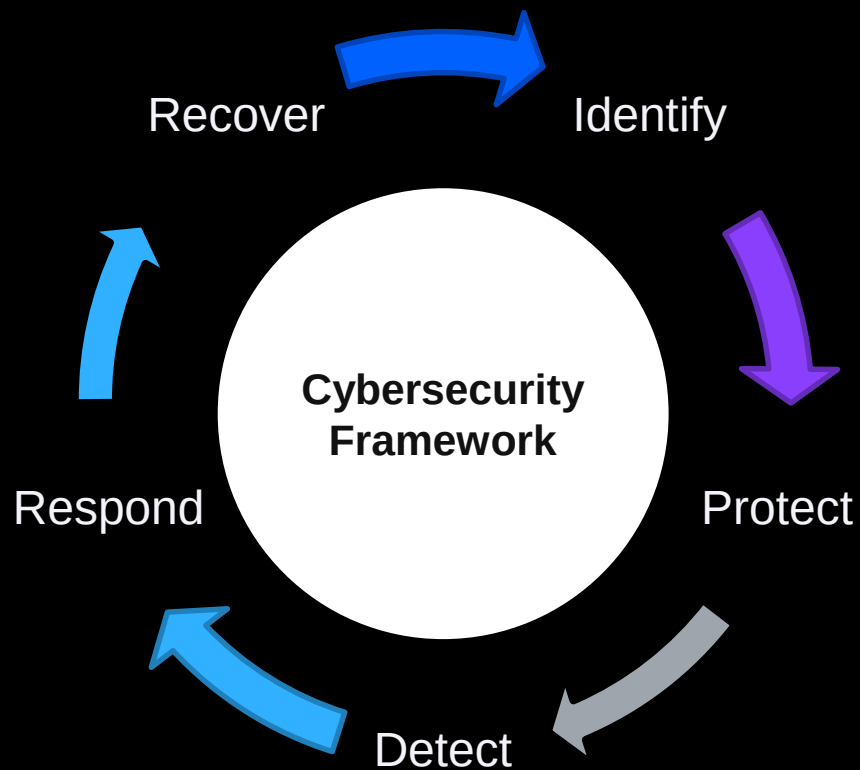
- Technika, metóda, proces, aktivita, alebo motivácia, ktorá je efektívnejšia pri dosahovaní konkrétneho výsledku ako ktorákoľvek iná
- Best practice je podpora osvedčených postupov:
 - najefektívnejšie (t.j. s vynaložením najmenšieho úsilia)
 - s najlepším výsledkom
 - založená na opakovateľných činnostiach, ktoré časom v praxi overilo väčšie množstvo profesionálov, vrátane konkurencie

O akú formalizovanú prax sa oprieť
v informačnej a kybernetickej bezpečnosti?

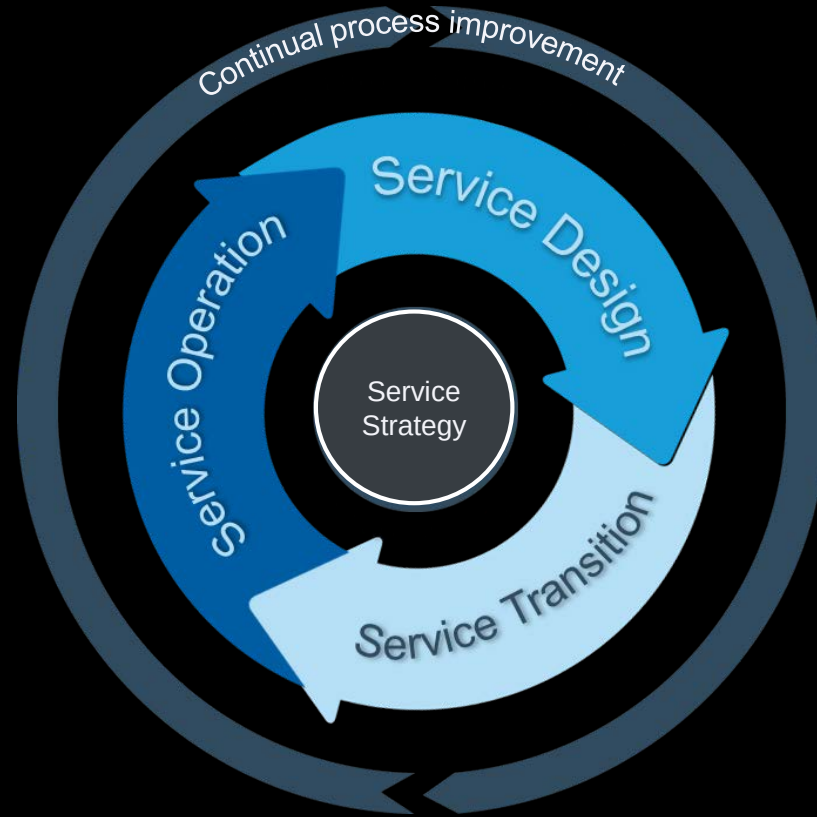
Systém riadenia informačnej bezpečnosti podľa ISO 27001



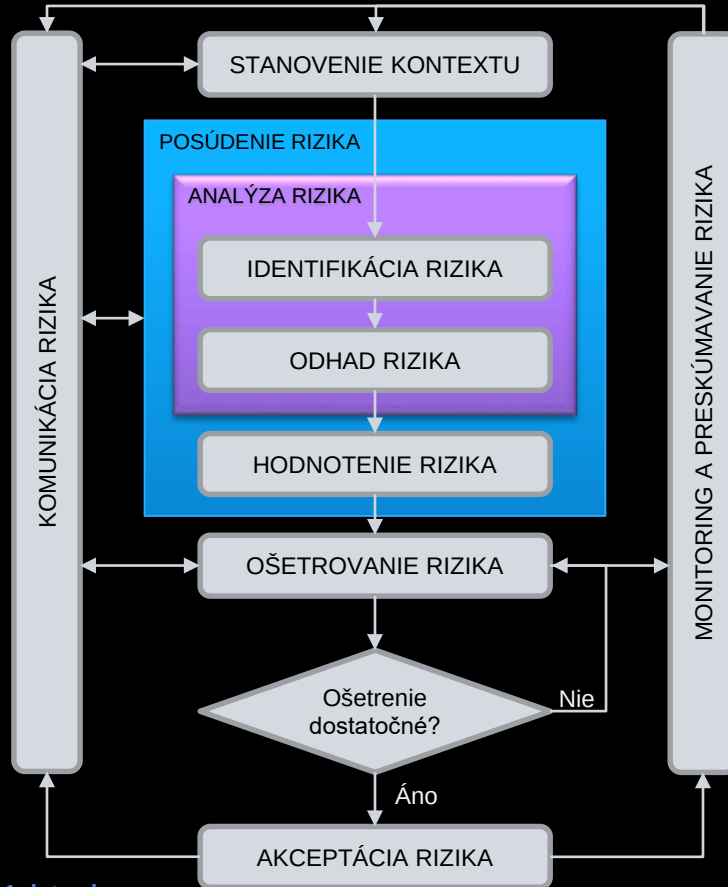
Rámec kybernetickej bezpečnosti podľa NIST



Rámec kybernetickej odolnosti RESILIA[®] podľa Axelos



Riadenie rizík informačnej bezpečnosti podľa ISO 27005

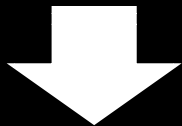


Akým spôsobom je možné
sformalizovať osvedčené skúsenosti?
...Legislatíva vs. štandardizácia

Rôzne ciele legislatívy a štandardizácie

Legislatíva:

- Cieľom je najmä regulácia, t.j. dosiahnutie žiaduceho správania zúčastnených subjektov
- Štátna moc si legislatívou vyhradzuje oprávnenie rozhodovať o právach a povinnostiach dozorovaných subjektov



- Nízka úroveň detailu
- Všeobecné právne definície
- Typicky široký dosah (celý štát, celé odvetvie)

Štandardizácia (normalizácia):

- Zjednotenie definícií a názvoslovia
- Zjednotenie rámcov
- Zaručenie kompatibility metód



- Vysoká úroveň detailu
- Odborné definície
- Špecifický dosah (konkrétny odbor a odvetvie)

Legislatíva v kotexte bezpečnosti

Výhody legislatívy

- Všeobecná právna záväznosť (vynucuje sa ňou žiaduce správanie zúčastnených subjektov)
- Dostatočné nástroje regulačného, kontrolného a sankčného charakteru vo vzťahu k povinným osobám

Nevýhody legislatívy

- Právnou úpravou nie je efektívne možné navrhnúť konkrétne návody a stanoviť univerzálne pravidlá, platné naprieč všetkými odvetvami
- Legislatíva vo svojej väčšine popisuje iba „ČO“ je potrebné vykonať, nie však „AKO“ to vykonať
- Pokuty vytvárajú novú hrozbu a odvádzajú pozornosť od pôvodných rizík

Štandardizácia v informačnej bezpečnosti

Výhody štandardizácie

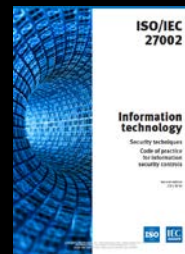
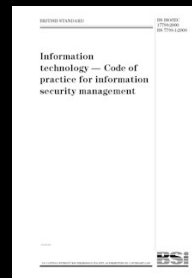
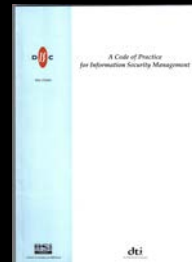
- Zjednotenie definícií, názvoslovia a rámcov
- Zaručenie kompatibility metód
- Možnosť benchmarkingu
- Najekonomickejší spôsob získania informácií o riešeniach, ktoré sú so zreteľom na najnovšie poznatky pre tú-ktorú oblasť vhodné, osvedčené a medzinárodne akceptované

Nevýhody štandardizácie

- Zhoda so slovenskou technickou normou je od 1.1.2001 dobrovoľná a STN nie sú právne záväzné
- V zmysle legislatívnych pravidiel vlády nemožno v právnom predpise uvádzať predpisy, ktoré neboli vyhlásené v Zbierke zákonov. t.j. ak text z normy nie je súčasťou právneho predpisu, má citácia normy iba informatívny charakter.

Stručná história medzinárodnej štandardizácie v informačnej bezpečnosti

- 1992 Department of Trade and Industry (DTI) publikoval 'Code of Practice for Information Security Management'
- 1995 Tento dokument bol vydaný cez British Standards Institute (BSI) ako BS7799
- 1996 David Lilburn Watson sa stáva prvým certifikovaným audítorom informačnej bezpečnosti
- 1999 Prvá majoritná revízia BS7799. Navrhnuté sú akreditačné a certifikačné schémy. LRQA a BSI sa stávajú prvými certifikačnými orgánmi
- 2000 BS7799 je vydaná ako ISO norma, mení názov na ISO/IEC 17799
- 2005 Publikovaná je norma ISO 27001, nahrádza BS7799-2. Špecifikuje prístup podľa ISMS (kompatibilná s normami riadenia kvality (ISO 9001 a ISO 14001))
- 2007 ISO17799 je premenovaná na ISO 27002 a zaradená do rodiny noriem Informačnej bezpečnosti ISO27k



Posudzovanie zhody, posudzovanie súladu

Certifikácia, certifikačné schémy

Certifikácia



- atestácia treťou stranou týkajúca sa produktov, procesov, systémov alebo osôb. (STN EN ISO/IEC 17000: 2005, čl. 5.5).
- nezávislé, nestranné a odborné posúdenie a oficiálne uznanie zhody, (t.j. určených znakov a vlastností) pre:
 - výrobok
 - systém
 - službu (proces)
 - fyzickú osobuso špecifickými požiadavkami deklarovanými v príslušných predpisoch (napr. v norme, alebo v zákone)
- Certifikáciu môže vykonávať výhradne orgán, ktorý je na takúto činnosť akreditovaný

Posudzovanie zhody

Aby vôbec mohla byť vykonávaná akákoľvek „certifikácia“, sú nutné tri podmienky:

existencia všeobecne uznanej odbornej authority

t.j. certifikačného orgánu, ktorý navrhuje mechanizmus posudzovania, vykonáva posudzovanie, prípadne poveruje posudzovaním tretie strany

existencia certifikačnej schémy

t.j. všeobecne prijatého a akceptovaného mechanizmu a požiadaviek posudzovania

**existencia
certifikačného
systému**

t.j. súhrnu poznatkov a zdrojov realizácie certifikačného procesu podľa certifikačnej schémy (ktoré vedú k vydaniu certifikátu a k udržaniu spôsobilosti certifikovanej osoby / systému / produktu / procesu)

Akreditácia

Akreditácia



- atestácia treťou stranou týkajúca sa orgánu posudzovania zhody, ktorá slúži ako oficiálny dôkaz kompetentnosti plniť špecifické úlohy posudzovania zhody.
- Orgánom povereným vydávať osvedčenia o tom, že organizácia, alebo osoba je spôsobilý/á vykonávať deklarované činnosti a jediná autorizovaná akreditujúca právnická osoba na vykonávanie akreditácie v Slovenskej republike je Slovenská národná akreditačná služba (SNAS).

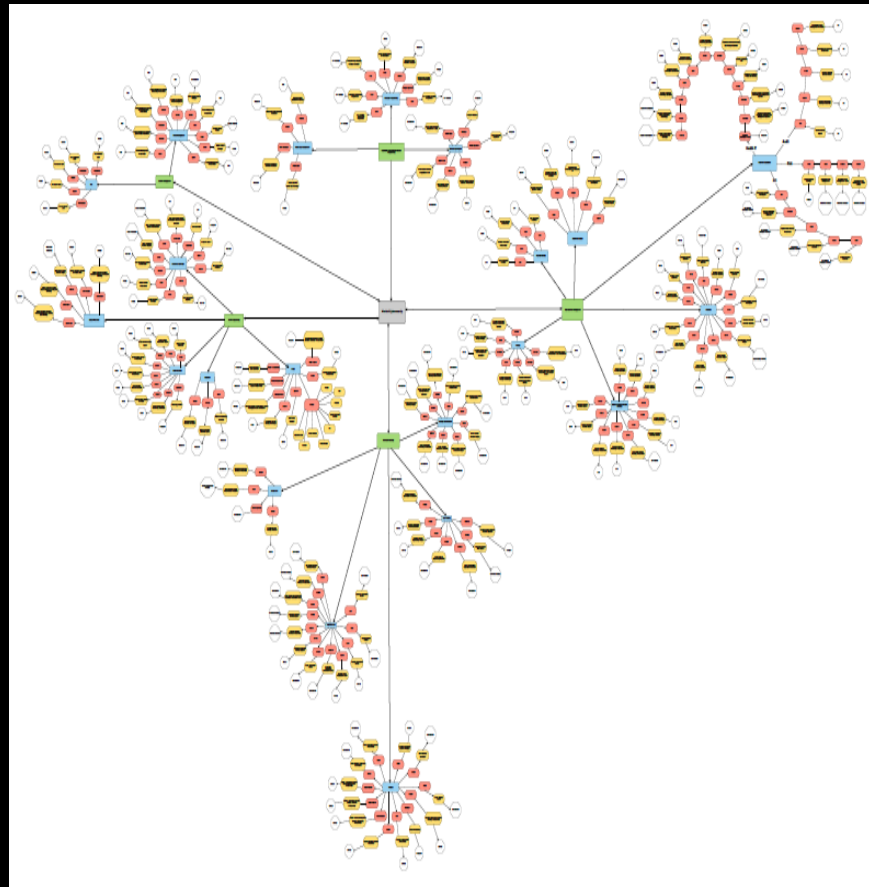
Generický certifikačný proces

Certifikačný proces je činnosť, v rámci ktorej akreditovaný certifikačný orgán určí, že predmet certifikácie spĺňa špecifikované požiadavky



Certifikačné schémy v oblasti bezpečnosti

- Rozhodnúť o existencii primeraných záruk kvality (dodávateľa, konzultanta, produktu) je možné napríklad na základe vyžiadania relevantných certifikátov
- Počet a komplexita certifikačných schém je vysoká...
- Ako sa v tom vyznať?
 - » Pochopiť princíp certifikácií
 - » Vyberať cielene vlastníctvo certifikátov podľa predmetu obstarávania
 - » Opierať sa o uznávané certifikačné schémy



Záver

Výhody prístupu k informačnej a kybernetickej bezpečnosti podľa najlepšej praxe

„Opakovaný a pamäťou uchovaný vnem tej istej veci nadobúda význam jednej skúsenosti“

- Využitie historických skúseností je výhodné (poučenie z cudzích chýb...)
- Kvalita je skôr akceptovaná, ak sa porovnáva ku všeobecne uznanej špecifikácii
- Priebežne zaručí, že predmet certifikácie spĺňa špecifikované požiadavky
- Posudzovanie súladu bude jednoduchšie s vopred stanovenou metrikou, s jednotným názvoslovím
- Rýchlejšia reakcia bezpečnosti na zmeny alebo inovácie
- Získate možnosť priebežného porovnávania s trhom (benchmarking)
- Umožňuje vám zvyšovať efektívnosť bezpečnostných procesov

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube/user/ibmsecuritysolutions

@makatura

IBM Security

© Copyright IBM Corporation 2019. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

