

Prax informačnej bezpečnosti - alebo čo vám o reálnom procese legislatíva nepovie

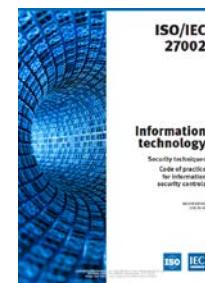
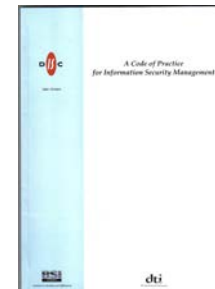
EFOCUS: KONFERENCIA IT PRÁVO „NOVÝ EURÓPSKY PRÁVNY RÁMEC V PODMIENKACH SR PRE GDPR, KYBERNETICKÚ BEZPEČNOSŤ A EIDAS”



Ivan Makatura
IBM Security Services

Stručná história technickej normalizácie 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 (Information Security Management System), 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



Požiadavky na ochranu informačných aktív v európskej legislatíve



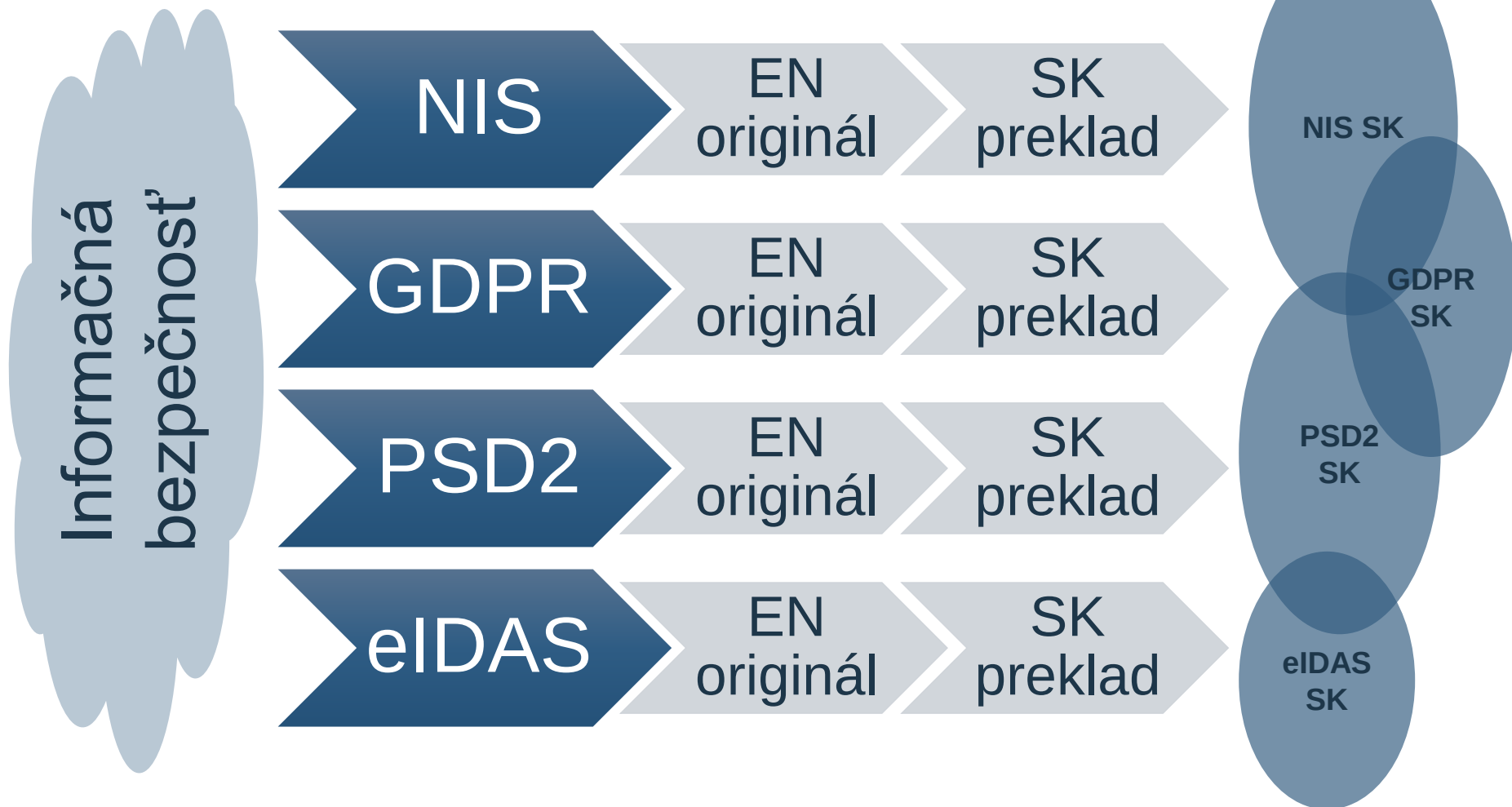
- Všeobecné nariadenie o ochrane údajov (General Data Protection Regulation “**GDPR**”)
- Nariadenie o elektronickej identifikácii a dôveryhodných službách (Regulation on Electronic identification and trust services for electronic transactions „**eIDAS**“)
- Smernica o platobných službách (Payment Services Directive „**PSD2**“)
- Smernica pre sieťovú a informačnú bezpečnosť (Network Information Security Directive “**NIS**“)
- Pripravovaná revízia smernice o súkromí a elektronických komunikáciách (Regulation on Privacy and Electronic Communications „**ePrivacy**“)

Regulácie EÚ sú typicky vysokoúrovňové a všeobecné

- Právna úprava, ktorá má byť platná pre 28 krajín s rôznou vyspelosťou hospodárstva, zrejme nenavrhne konkrétne návody
- Nie je možné stanoviť univerzálne pravidlá, platné naprieč všetkými odvetvami
- Európska regulácia vo svojej väčšine popisuje iba „ČO“ je potrebné vykonať, nedočítate sa však „AKO“ to vykonať
- **Laická interpretácia zákonných požiadaviek je často založená na mylnej predstave, že preštudovaním zákona je možné pochopiť princípy informačnej bezpečnosti**



Nejednoznačné názvoslovie, chyby v preklade...



Nezosúladené definície...



“data breach”

“substantial impact”

„significant impact“

“impact on data protection rights of individuals”

“personal data breach to a data subject”

“rights of the data subject”

„significant disruptive effects”

“users’ rights relating to electronic communications networks and services”

Niektoré nové povinnosti prevádzkovateľov podľa GDPR

- Prevádzkovateľ musí byť schopný doložiť, že spracovanie je vykonávané v súlade s Nariadením
- Povinnosť prevádzkovateľa **zaviesť vhodné technické a organizačné opatrenia**
- **Posudzovanie vplyvu** na ochranu údajov (tzv. Data Protection Impact Assessment)
- **Povinné ohlasovanie** prípadov narušenia bezpečnosti (notifikačná povinnosť)

...a niektoré ďalšie... Tento zoznam súvisí s nasledujúcou krátkou analýzou.



Technické a organizačné opatrenia



Spôľahlivosť informácie je daná iba tromi jej atribútmi...

Confidentiality (Dôvernosť):

- miera obmedzenia prístupu k informáciám len pre osoby, alebo skupiny osôb, ktoré sú oprávnené na prístup k príslušným informáciám.

• Privacy (ochrana súkromia):

- ochrana pred nežiadanou publicitou, verejnou kontrolou, sledovaním alebo neoprávneným zverejnením osobných údajov



Integrity (Celistvosť)

- miera bezchybnosti a informácie
- Charakteristikami integrity sú:
 - Úplnosť informácie
 - Správnosť informácie

Availability (Dostupnosť)

- miera dostupnosti informácie pre používateľa a systém vo chvíli, keď je informácia potrebná a požadovaná

Bezpečnosť spracúvania osobných údajov

- Prevádzkovateľ a sprostredkovateľ **prijmú primerané technické a organizačné opatrenia** s cieľom **zaistiť úroveň bezpečnosti primeranú tomuto riziku**, pričom uvedené opatrenia prípadne zahŕňajú aj:
 - schopnosť zabezpečiť trvalú **dôvernosť, integritu, dostupnosť** a odolnosť systémov spracúvania a služieb
 - schopnosť včas **obnoviť dostupnosť osobných údajov** a prístup k nim v prípade fyzického alebo technického incidentu
 - proces pravidelného **testovania, posudzovania a hodnotenia účinnosti** technických a organizačných opatrení na ~~zaistenie bezpečnosti spracúvania~~
- **Pri posudzovaní primeranej úrovne bezpečnosti sa prihliada predovšetkým na riziká, ktoré predstavuje spracúvanie**



Historicky prvá legislatívna zmienka o všeobecnej povinnosti riadenia rizika!

Čo sú to „vhodné technické a organizačné opatrenia“...?

- Ochranné (bezpečnostné) opatrenia:
 - Sú **praktiky, procedúry a mechanizmy**, ktoré môžu pomôcť chrániť pred nejakou hrozbou, znížiť zraniteľnosť, obmedziť vplyv nechcenej udalosti, odhaliť malígnu udalosť a umožniť zotavenie alebo odškodnenie.
 - Ich prijatím je:
 - **neoprávneným osobám** znemožnený nedovolený prístup k osobným údajom, manipulácia s technickými zariadeniami určenými na spracovanie osobných údajov a manipulácia s nosičmi osobných údajov
 - **oprávneným osobám** zaistený prístup k osobným údajom v rozsahu potrebnom pre plnenie ich povinností

Čo sú to „vhodné technické a organizačné opatrenia“...?

- Generické rozdelenie opatrení:
 - **Technické** – opatrenia na zníženie bezpečnostných rizík pomocou prostriedkov fyzickej a technologickej povahy
 - **Organizačné** - opatrenia na zníženie bezpečnostných rizík pomocou zmien procesov a úpravou dokumentácie

Dosiahnutie efektívnej bezpečnosti zvyčajne vyžaduje kombináciu rôznych opatrení



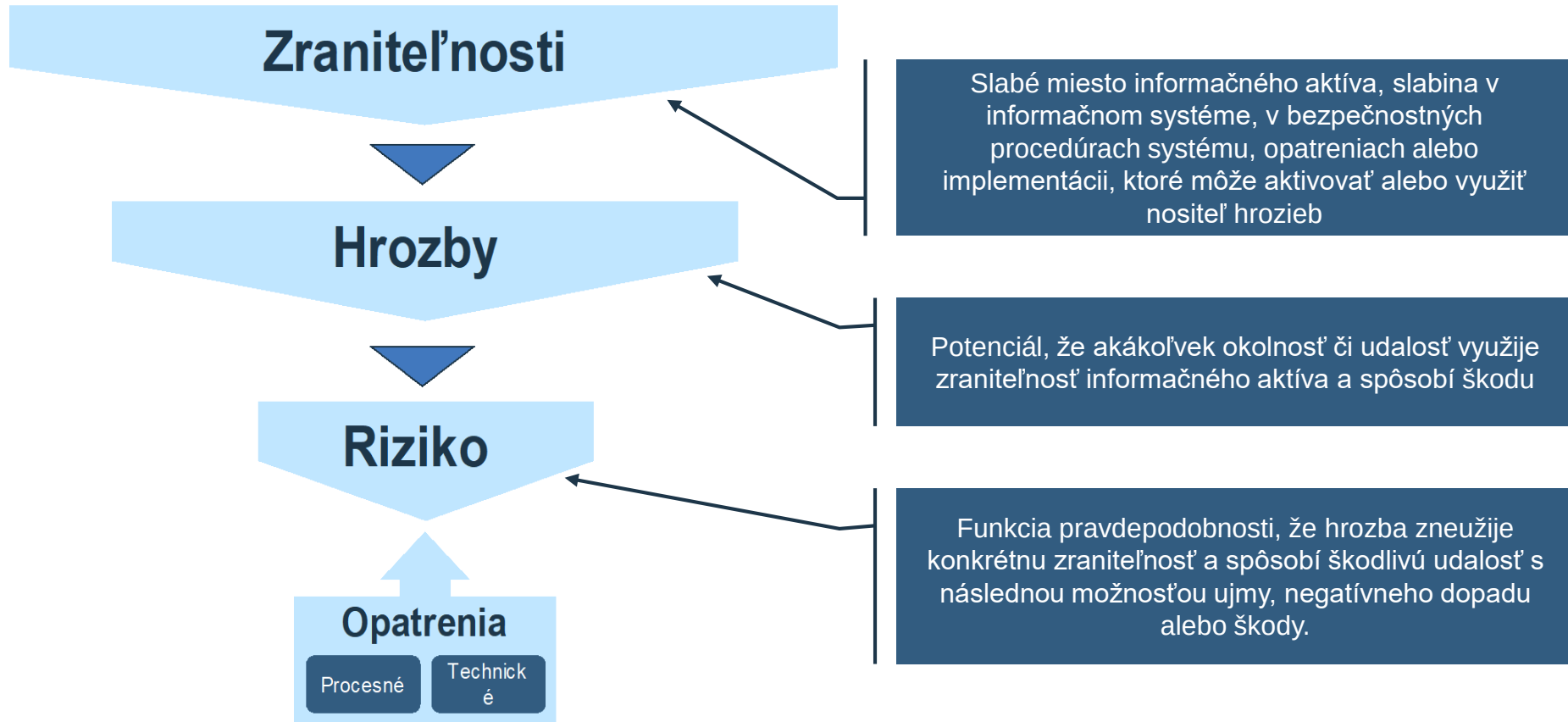


Základy teórie riadenia rizika



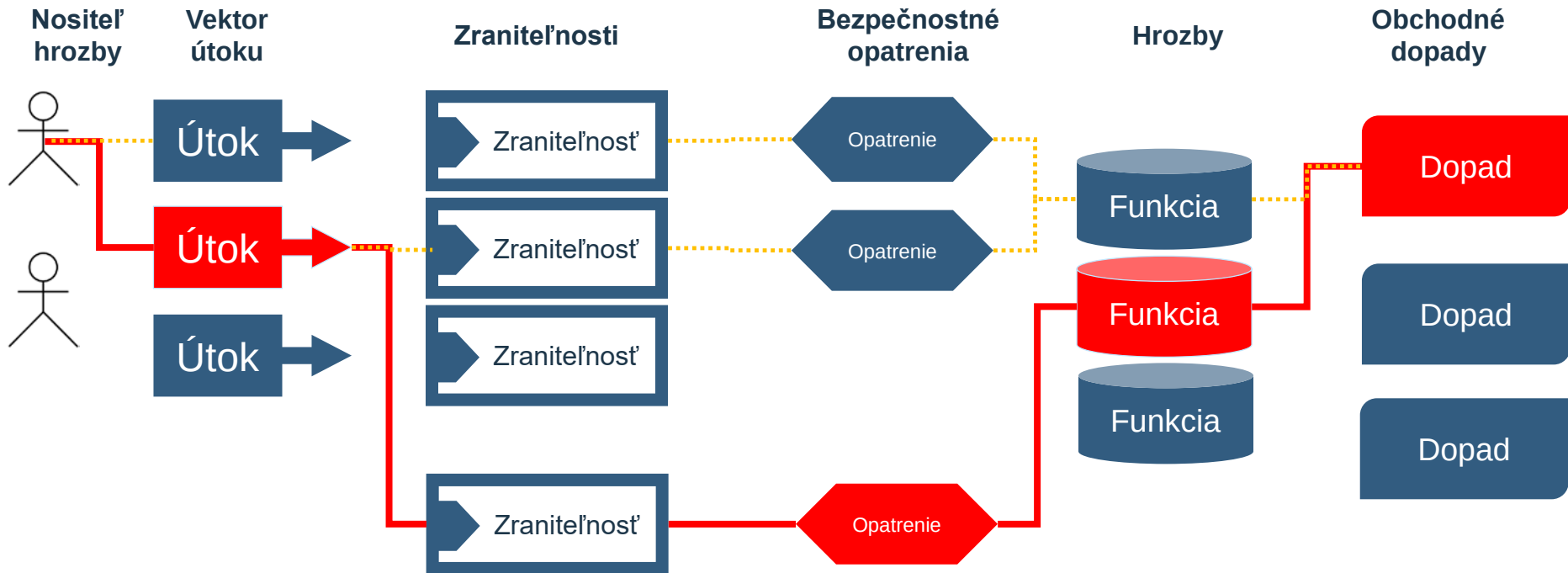


Základné názvoslovie v procese riadenia rizík



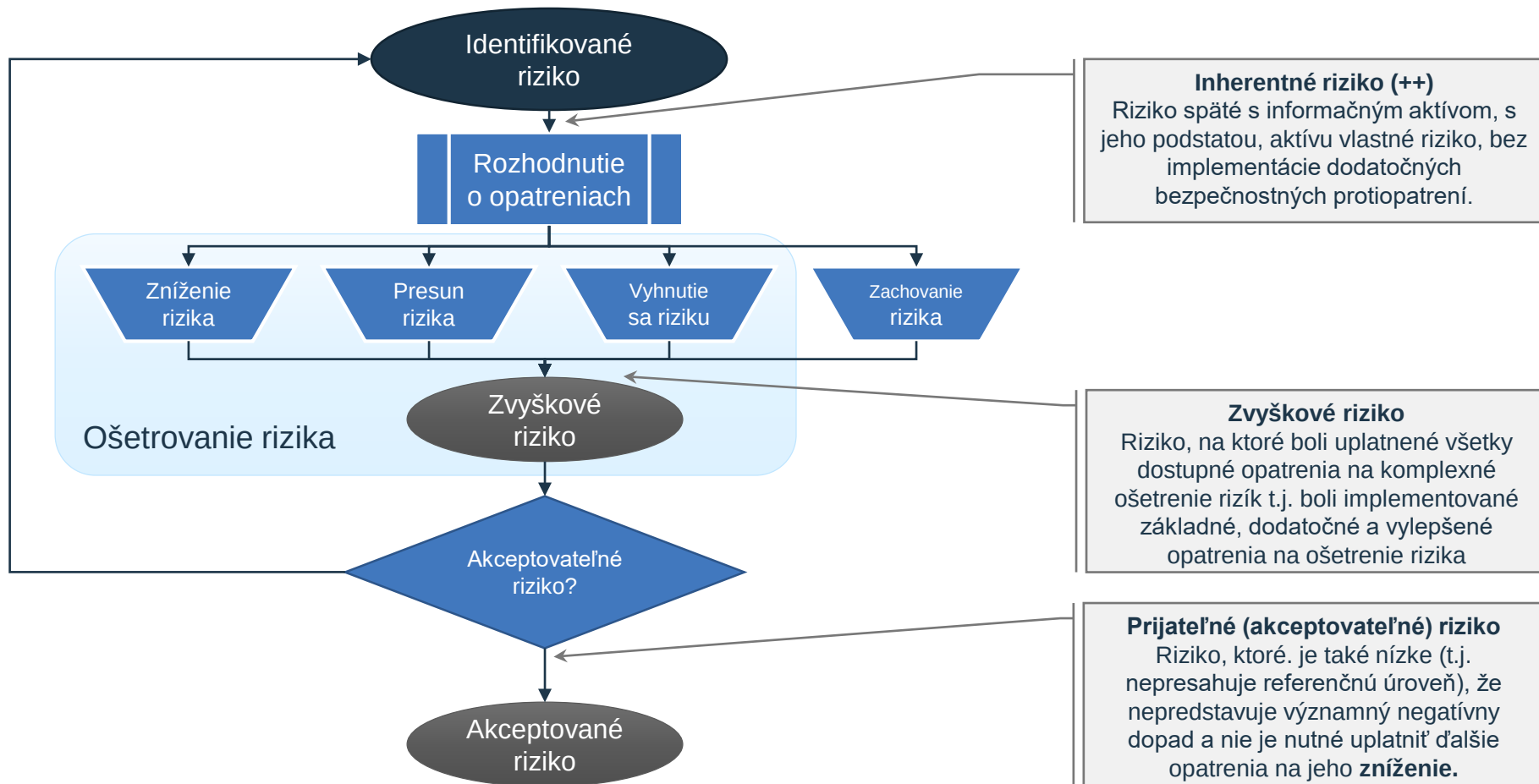
Zraniteľnosť -> Hrozba -> Riziko -> Dopad

- Vektor útoku** - smer interakcie, súhrn všetkých vstupno-výstupných bodov prostredia, prostredníctvom ktorých sa neoprávnený užívateľ môže pokúsiť zadať alebo extrahovať dáta (v prenesenom zmysle každá cesta, spôsob, mechanizmus, ktorý útočník môže zneužiť na neoprávnený prístup k informačným aktívam)



Zdroj: The Open Web Application Security Project (OWASP)

Generický proces ošetrovania rizika



Metódy ošetrovania rizika

- **Zníženie rizika**

- Zníženie rizika je metóda ošetrovania rizika, pri ktorej je uplatnený výber vhodných opatrení tak, aby riziko bolo znížené až na úroveň zostatkového rizika, ktoré môže byť následne prehodnotené ako akceptovateľné.

- **Presun rizika**

- Presun rizika je metóda ošetrovania rizika, pri ktorej bude určitá časť rizika zdieľaná s externými subjektmi (typicky poistenie, alebo výber zmluvného partnera, ktorého úlohou bude monitorovať proces a prijať okamžité opatrenia na zastavenie hrozby skôr, ako vznikne škoda).

- **Vyhnutie sa riziku**

- Keď je identifikované riziko považované za príliš vysoké, alebo náklady na implementáciu ošetrovania rizika presahujú prínosy, rozhodnutím môže byť aj úplné vyhnutie sa riziku, a to odobratím plánovanej alebo existujúcej aktivity alebo súboru aktivít, resp. zmenou podmienok, podľa ktorých bude činnosť prevádzkovaná.

- **Zachovanie rizika**

- Ak úroveň rizika spĺňa kritériá na prijatie rizika, nie je potrebné implementovať opatrenia a riziko môže zostať zachované v pôvodne ohodnotenej úrovni.



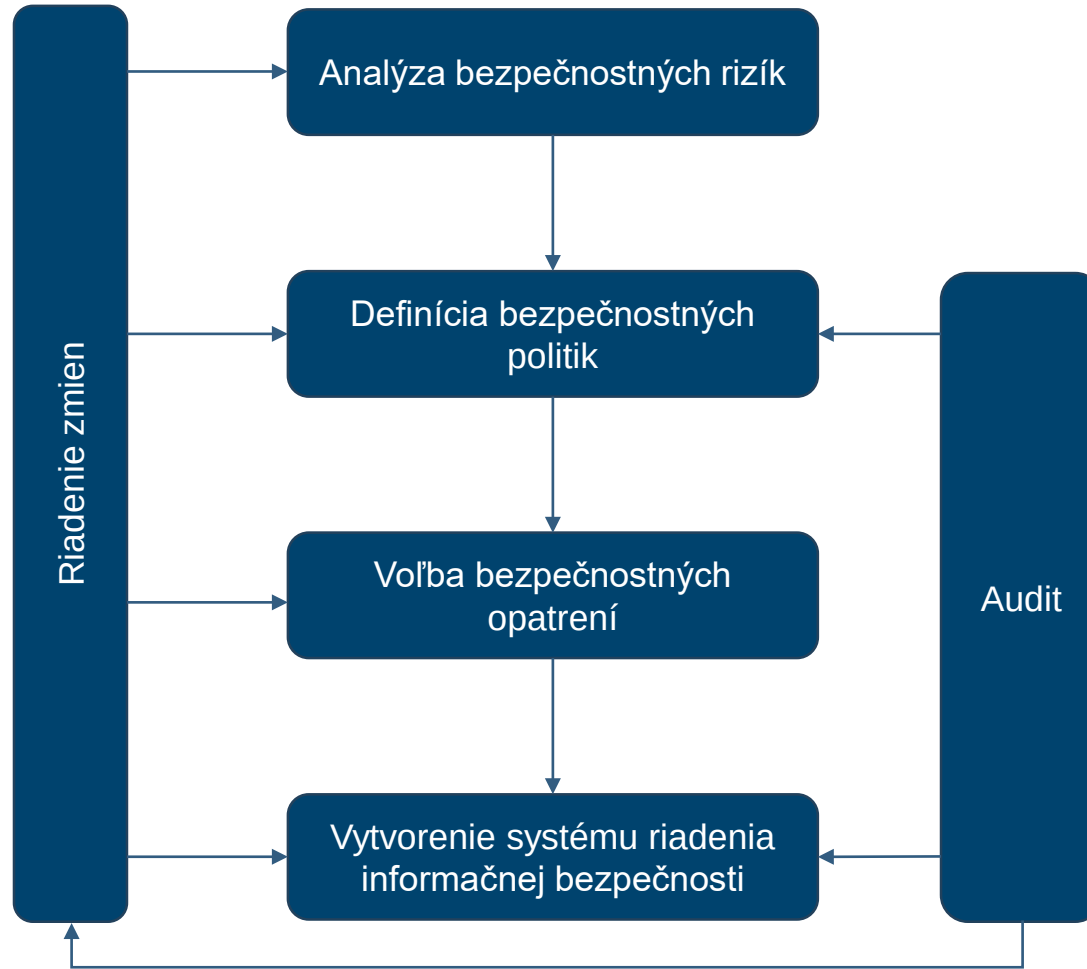
Posudzovanie vplyvu na ochranu údajov



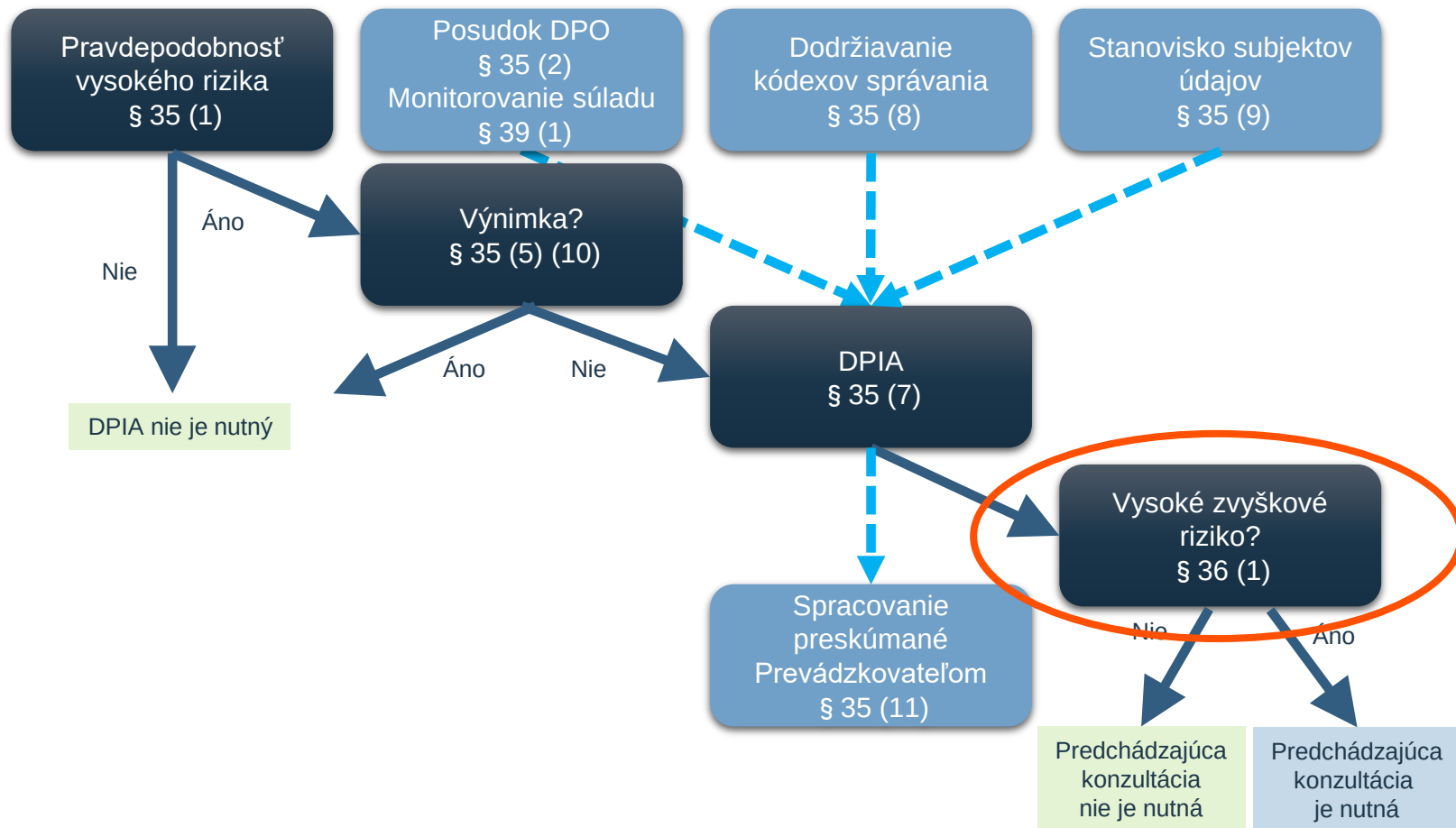
Generický proces DPIA podľa WP29



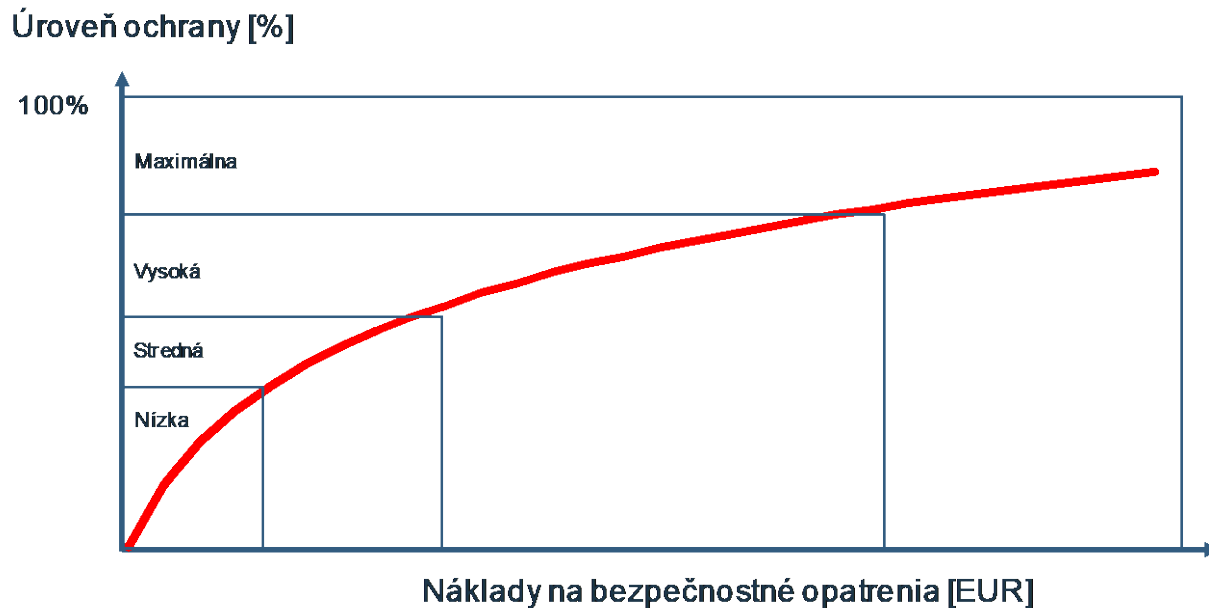
Životný cyklus bezpečnosti informácií podľa ISO 27000



Princípy výkonu DPIA podľa WP29

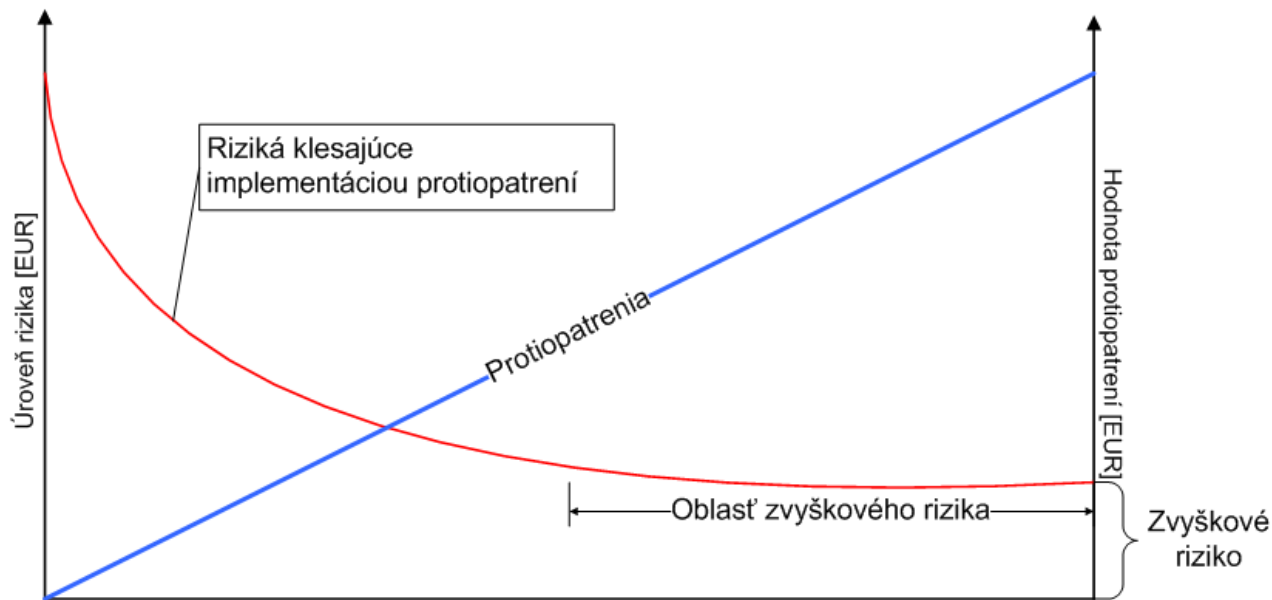


Náklady vs. efektivita bezpečnosti Informací



- Absolútna úroveň ochrany nie je dosiahnuteľná ani pri neobmedzených nákladoch
- Rozhodovať o účinnosti opatrení je úlohou vlastníkov rizík
- Cieľom Nariadenia je dosiahnuť žiaduce správanie zainteresovaných strán

Zvyškové riziko



- Za predpokladu, že hodnota implementovaných opatrení postupne narastá, riziko sa oproti východiskovej hodnote postupne znižuje
- Pokles úrovne rizika sa zásadne spomalí na určitej hodnote, ktorá nebude mať tendenciu ďalšieho zníženia ani po implementácii ďalších patrení. Táto hodnota môže byť označená ako **zvyškové riziko**.
- Nulové riziko nie je možné dosiahnuť ani pri neobmedzených nákladoch

Zvyškové riziko

- **Zvyškové riziko** je také riziko, ktorého hodnota po komplexnom ošetrení rizík implementáciou pôvodných, dodatočných a vylepšených opatrení na ošetrenie rizika je taká nízka (t.j. nepresahuje referenčnú úroveň), že je pre spoločnosť prijateľné a nie je nutné uplatniť ďalšie opatrenia na jeho zníženie.
- Referenčná hodnota by mala byť stanovená na takej úrovni, **aby dopad hrozby bol taký nízky, že ho bude možné zanedbať**



- **Tým je vylúčená možnosť, že vysoké riziko bude označené za zvyškové...**
- Zvyškové riziko musí byť vždy zásadne akceptované vedením organizácie

Dostupné metodiky analýzy hrozieb a rizik

- STN ISO/IEC 27005 Informační technologie – Bezpečnostné metódy - Riadenie rizík informačnej bezpečnosti
- NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems
- SANS Institute: Realistic Risk Management Using the CIS 20 Security Controls
- LINDDUN Privacy by Design framework
- OWASP Risk Rating Methodology
- PIAF Recommendations for a privacy impact assessment framework for the European Union
- WP29: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679



Notifikačné povinnosti



Uplatňujú sa rôzne lehoty pre notifikáciu...



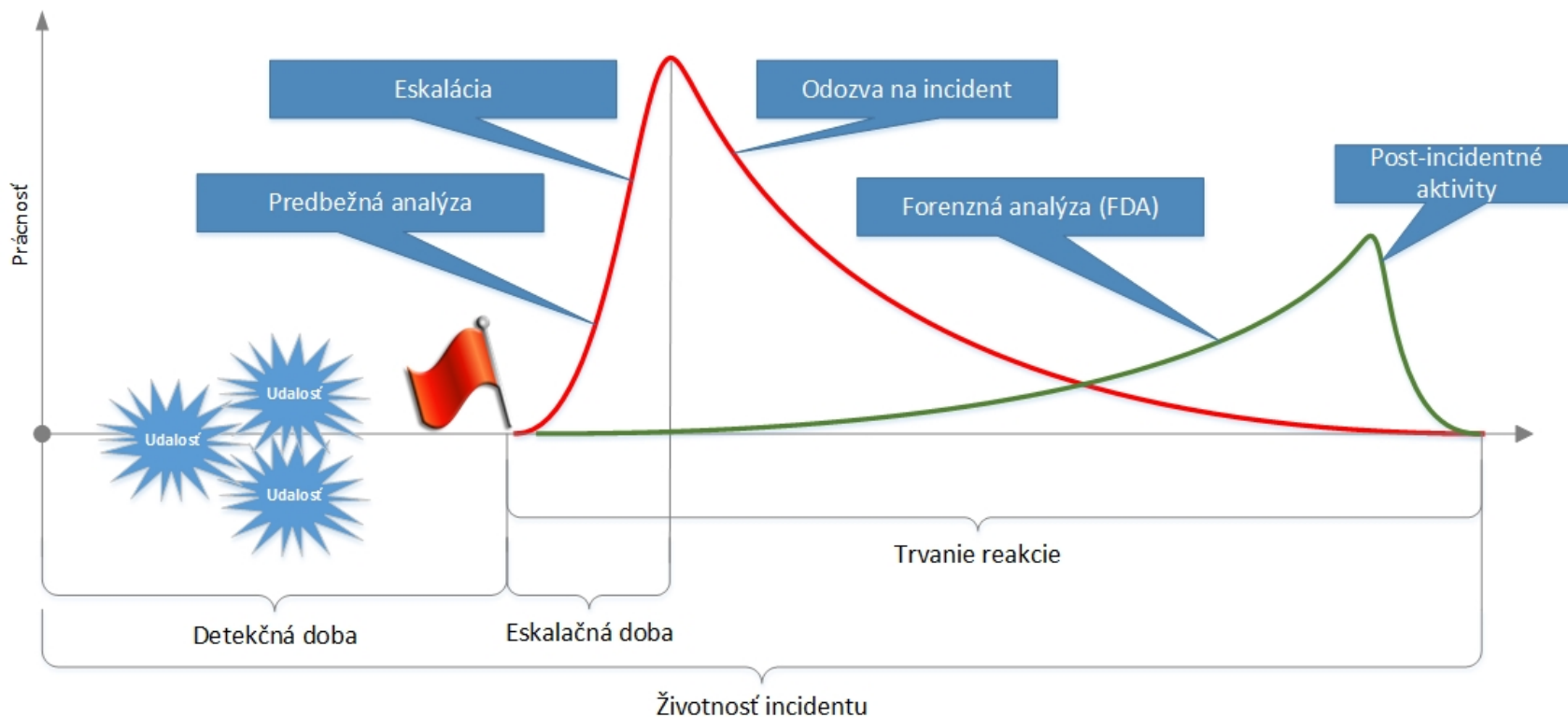
„without undue delay“...

“not later than 24 hours”...

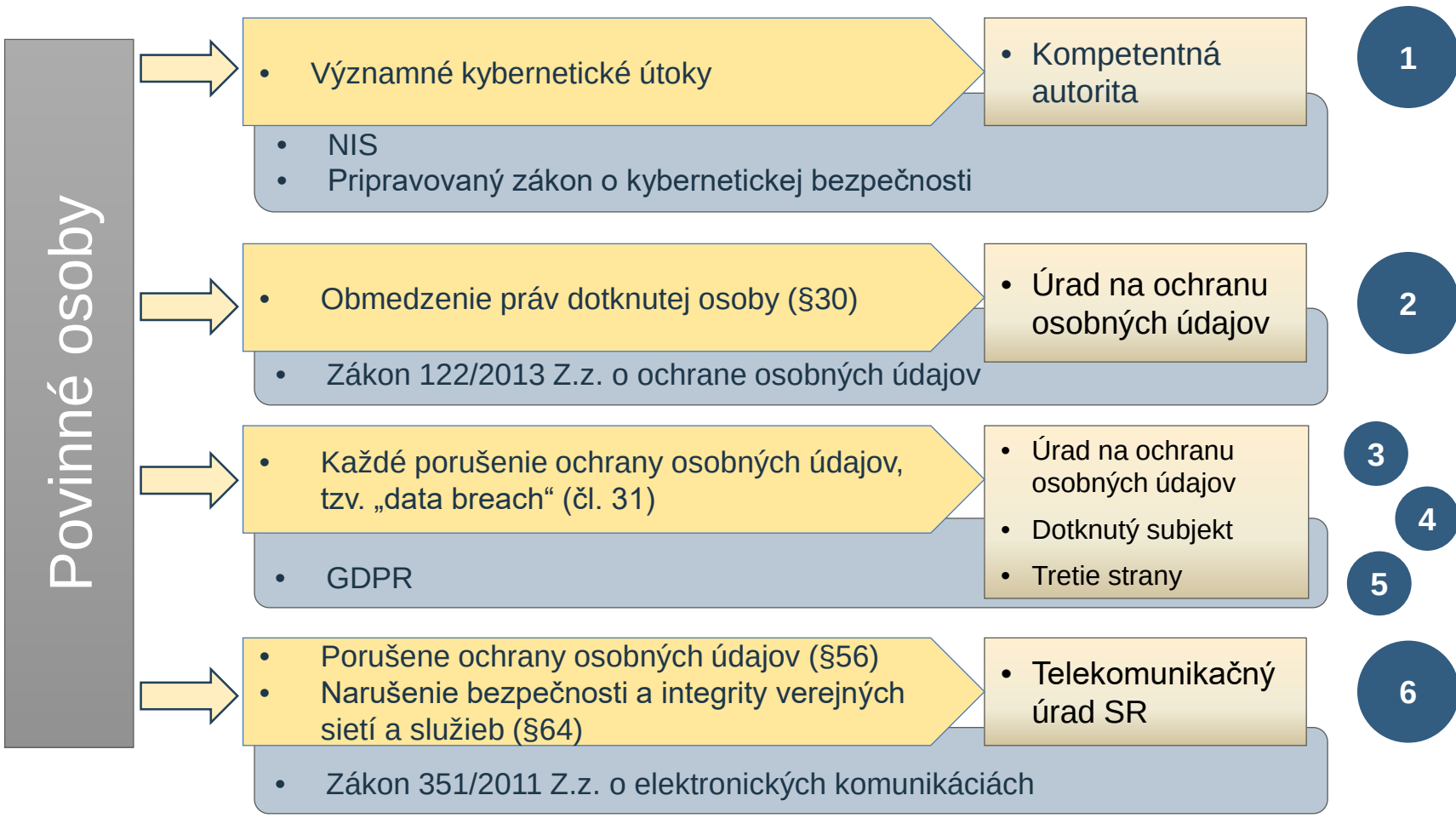
“in 72 hours”...

Časové rozlíšenie incidentu – v ktorej chvíli identifikujete porušenie práv?

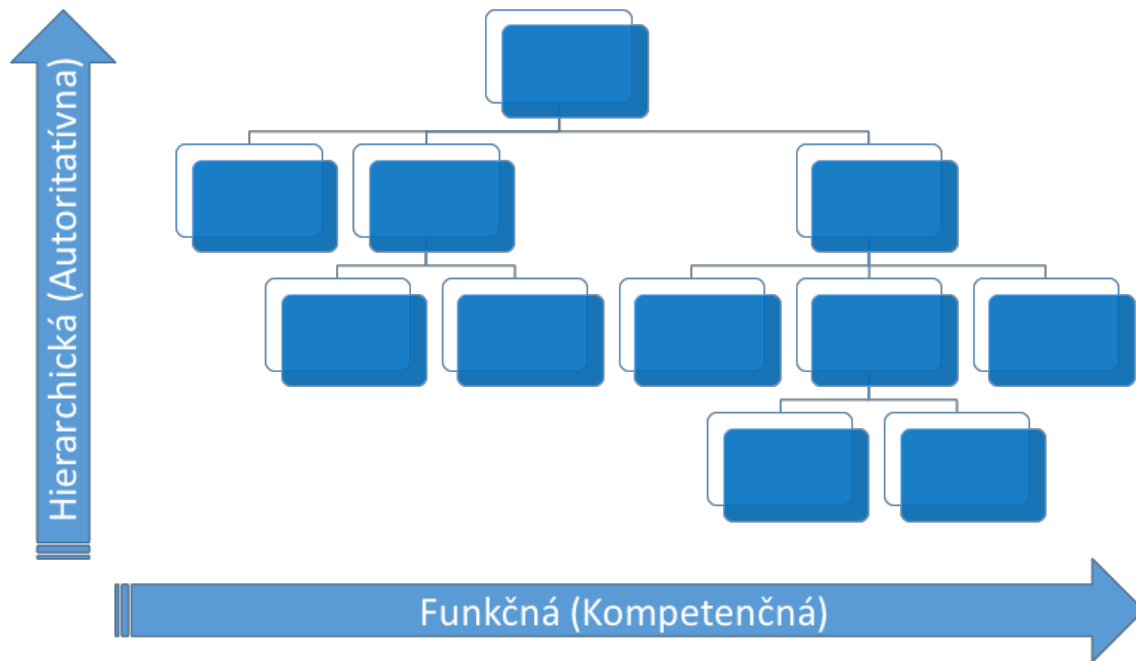
- Incident počas svojej životnosti prechádza niekoľkými fázami, ktoré sa vzájomne prelínajú
- Tieto fázy majú rôznu, v čase sa meniacu prácnosť i zložitosť:



Pôvodný koncept „Single Point of Contact“, vs. realita povinností



Neefektívny tlak na hierarchickú notifikáciu incidentov...



- cieľom je skrátenie celkovej doby eskalácie a čo najskôr začať reálne práce na riešení incidentu
- reakcia na incident nie je v možnostiach jedného človeka - je nutné zabezpečiť eskaláciu iným útvarom
- manažéri a politici ku úspešnému zvládnutiu incidentu nedokážu prispieť viac, než profesionálni informatici
- pre vyššiu efektivitu odozvy na incident je odporúčané dať prednosť horizontálnej eskalácii



Záver





- Neočakávajte od zákonov návrh postupov v riadení rizík ani návrhy bezpečnostných opatrení
- Poskytovanie technických návodov je úlohou technických noriem, nie legislatívy
- Bezpečnostné riziká sú každodennou realitou. Nová legislatíva prináša základnú pozitívnu zmenu: povinnosť subjektov prevziať zodpovednosť za riadenie rizík
- Bezpečnosť založená na riadení rizika môže organizáciám napomôcť:
 - získať prehľad o celkovej rizikovej expozícii podniku
 - stanovovať priority pre testovanie a ošetrovanie zraniteľností, ktoré budú v súlade s obchodnou stratégiou podniku a rizikovým apetítom
 - efektívne pridelovať zdroje, s cieľom zabrániť narušeniam z najvyššou pravdepodobnosťou a najväčším dopadom
 - hodnotiť progres ošetrovania zraniteľností v kontexte bezpečnostných cieľov

ĎAKUJEM ZA POZORNOST

 ibm.com/security
 securityintelligence.com
 xforce.ibmcloud.com
 [@ibmsecurity](https://twitter.com/ibmsecurity)
 ivan.makatura@sk.ibm.com

© Copyright IBM Corporation 2016. 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.