

Kybernetická bezpečnosť - návrhy
de lege ferenda alebo čo možno
očakávať od novej právnej úpravy

*e*FOCUS

Kybernetická bezpečnosť

Návrhy de lege ferenda alebo čo možno očakávať od novej právnej úpravy



BUKOVINSKÝ & CHLÍPALA

ADVOKÁTSKA KANCELÁRIA • LAW FIRM • RECHTSANWÄLTE

Bratislava, september 2017

Obsah

- **Smernica EP A RADY (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (NIS)**
- **Európska komisia – smerom k náležitej transpozícii NIS**
- **Transpozícia NIS v SR**

NIS

- Prevádzkovateľ základných služieb (PZS), poskytovateľ digitálnych služieb (PDS) a ich identifikácia
- Národná stratégia v oblasti NIS, VPO, JKM, CSIRT, sieť CSIRT, Skupina pre spoluprácu
- Bezpečnostné požiadavky, Oznamovacie požiadavky
- Posúdenie, následné opatrenia dohľadu
- Sankcie

...k náležitej transpozícii NIS

- Národná stratégia v oblasti NIS
- VPO, JKM, CSIRT
- Povinné osoby (PZS, PDS), bezpečnostné a oznamovacie požiadavky
- Vzťah NIS k osobitným právnym úpravám
- Zoznam „best practices“ odporúčaných ENIS-ou

VPO

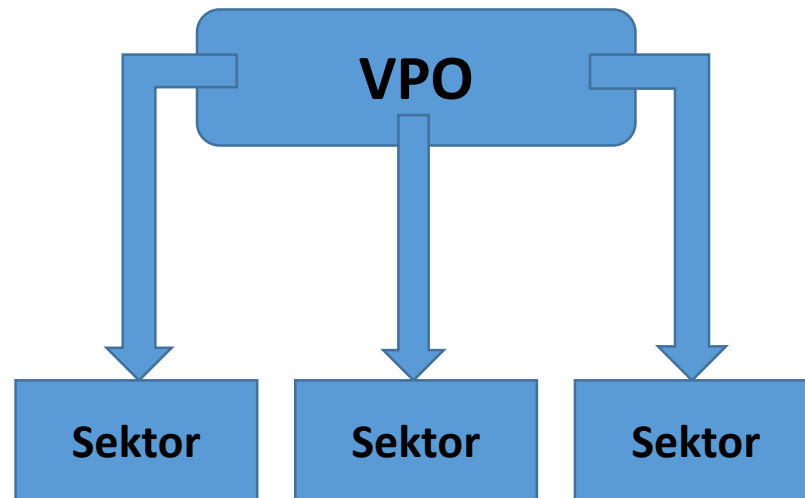
- Vzhľadom na rozdiely v jednotlivých vnútroštátnych úpravách, s cieľom zachovať existujúce štruktúry a zabrániť tvorbe duplicít sú členské štáty oprávnené ustanoviť:

jeden alebo viac VPO zodpovedných za plnenie úloh NIS

Odporúčanie EK na využitie existujúcich prístupov, napr. aplikovaných pri ochrane národných kritických infraštruktúr

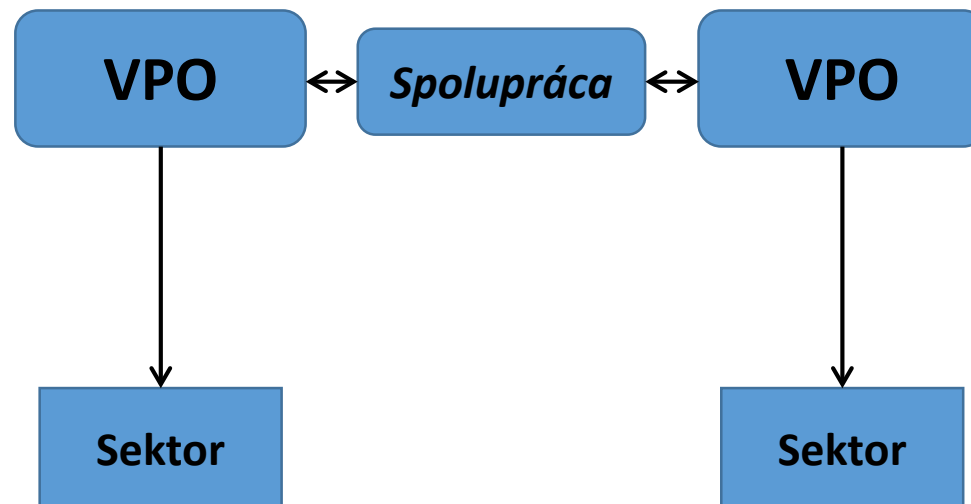
VPO

- Centralizovaný prístup



VPO

- Decentralizovaný prístup



CSIRT

- Vzhľadom na postavenie CSIRT v rámci mechanizmu nahlasovania bezpečnostných incidentov:

priame nahlasovanie príslušnému CSIRT

úlohou CSIRT je najmä monitorovanie, odhaľovanie, reakcia a zmierňovanie alebo odstraňovanie dopadu bezpečnostných incidentov

priame nahlasovanie VPO s oprávnením prístupu CSIRT

- **verejný alebo súkromný subjekt, ktorého typ sa uvádza v prílohe II, spĺňajúci nasledovné kritériá (čl. 5 ods. 2 NIS):**

- a) subjekt poskytuje službu, ktorá má zásadný význam z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností;
- b) poskytovanie tejto služby je závislé od sietí a informačných systémov; a
- c) incident by mal závažný rušivý vplyv na poskytovanie uvedenej služby.

Sektory ZS

Energetika

Doprava

Bankovníctvo

**Infraštruktúra
finančných
trhov**

Zdravotníctvo

Pitná voda

**Digitálna
infraštruktúra**

Identifikácia PZS

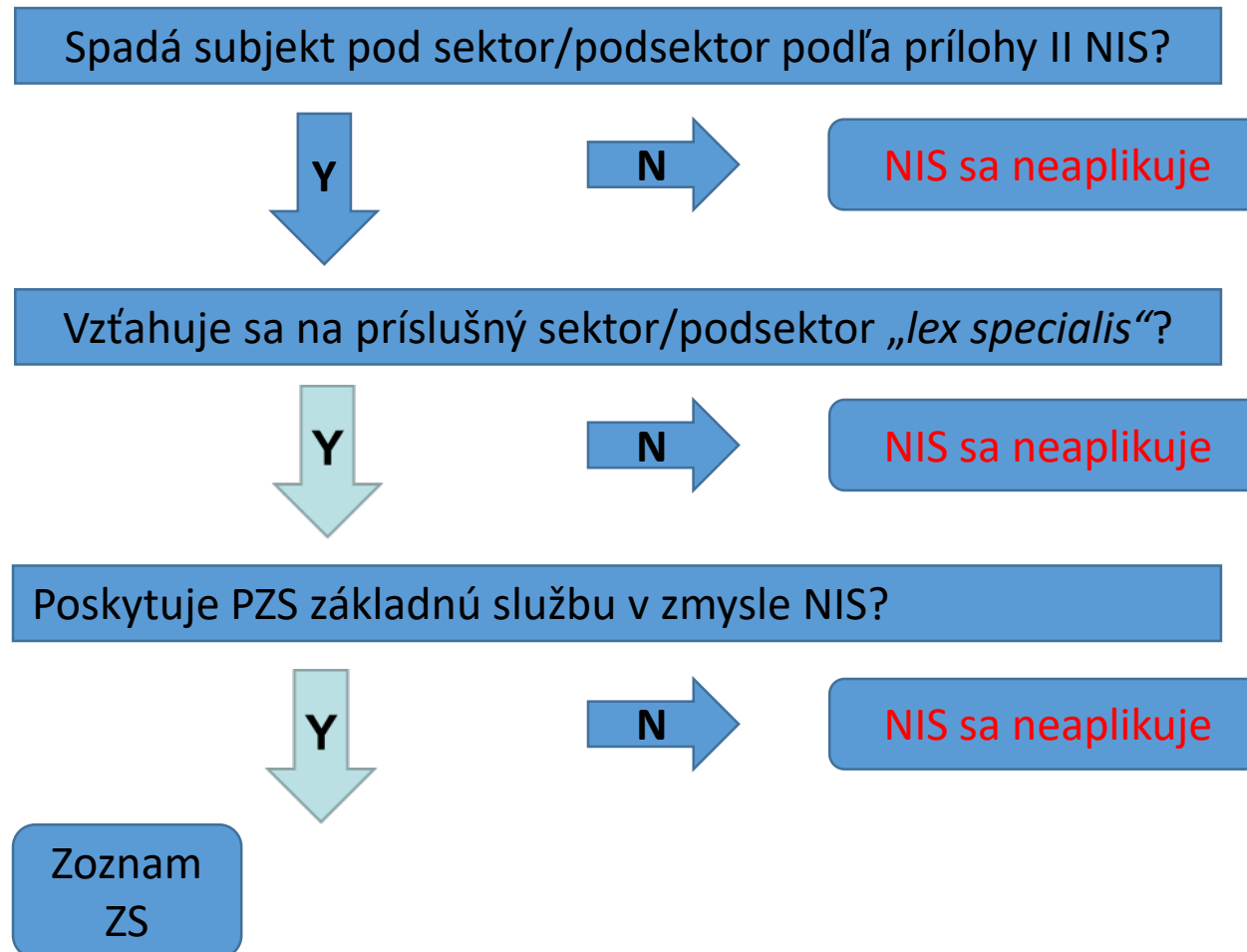
- ČS sú povinné do 9. novembra 2018 identifikovať všetkých PZS pre každý sektor a podsektor prílohy II NIS

všetky subjekty, ktoré spĺňajú kritériá stanovené v článku 5 ods. 2 NIS, sa označujú ako PZS a vzťahujú sa na ne bezpečnostné a oznamovacie povinnosti.

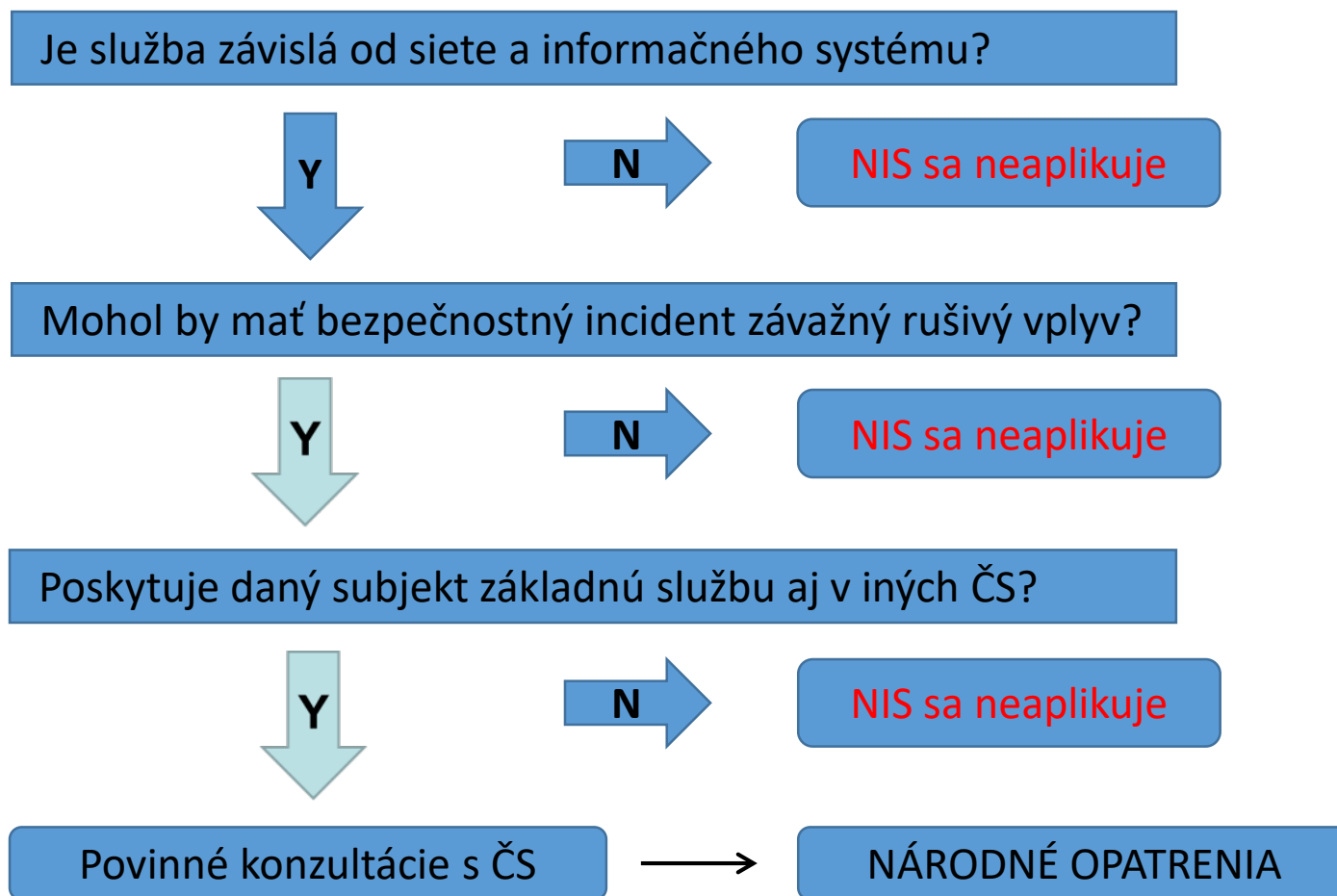
6 kľúčových otázok, ktoré by VPO mal pri identifikácii PZS preskúmať

1. Spadá subjekt pod sektor/podsektor podľa prílohy II NIS?
2. Vzťahuje sa na príslušný sektor/podsektor „*lex specialis*“?
3. Poskytuje PZS základnú službu v zmysle NIS?
4. Je služba závislá od siete a informačného systému?
5. Mohol by mať bezpečnostný incident závažný rušivý vplyv?
6. Poskytuje daný subjekt základnú službu aj v iných ČS?

Identifikácia PZS



Identifikácia PZS



Bezpečnostné požiadavky PZS

PZS majú prijať **vhodné a primerané technické a organizačné opatrenia** na riadenie rizík súvisiacich s bezpečnosťou sietí a informačných systémov, ktoré využívajú vo svojej prevádzke. **S ohľadom na najnovší technický vývoj** tieto opatrenia zabezpečujú takú úroveň bezpečnosti sietí a informačných systémov, ktorá zodpovedá miere daného rizika.

Skupina pre spoluprácu vydá:

- nezáväzná usmernenia týkajúce sa bezpečnostných opatrení v 4.Q 2017

Výzva EK na dôsledné využitie vydaných usmernení s cieľom zosúladenia požiadaviek v rámci celej EÚ.

bezpečnostných

Oznamovacie požiadavky PZS

Nahlasovanie „všetkých“ incidentov so **závažným vplyvom** na kontinuitu ZS (dôvernosť, dostupnosť, integritu, autenticitu)

Skupina pre spoluprácu vydá:

- nezáväzná usmernenia týkajúce sa oznamovacích požiadaviek v 4.Q 2017

Výzva EK na dôsledné využitie vydaných usmernení s cieľom zosúladenia oznamovacích požiadaviek v rámci celej EÚ.

- každá právnická osoba, ktorá poskytuje digitálnu službu

Digitálna služba:

V zmysle článku 1 ods. 1 písm. b) smernice (EÚ) 2015/1535 je ZS definovaná ako *"každá služba poskytovaná informačnou spoločnosťou, to jest každá služba, ktorá sa bežne poskytuje za odmenu, na diaľku, elektronickým spôsobom a na základe individuálnej žiadosti príjemcu služieb"*, pričom ich rozsah zužuje na druhy služieb uvedené v prílohe III NIS:

- a) Online trhovisko,
- b) Internetový vyhľadávač,
- c) Služby cloud computingu.

NIS nevyžaduje identifikáciu všetkých PDS (ako v prípade PZS), bezpečnostné a oznamovacie požiadavky sa vzťahujú na **všetkých PDS**.

Bezpečnostné požiadavky PDS

PDS identifikujú riziká a prijmu **vhodné a primerané technické a organizačné opatrenia** na ich riadenie a s ohľadom na **najnovší technický vývoj**, zohľadňujúc:

- a) bezpečnosť systémov a zariadení,
- b) riešenie incidentov,
- c) riadenie kontinuity činnosti,
- d) monitorovanie, audit a skúšanie,
- e) súlad s medzinárodnými normami.

Bezpečnostné požiadavky PDS

Opatrenia prijme PDS na **zabránenie a minimalizovanie** vplyvu incidentov ovplyvňujúcich bezpečnosť ich sietí a informačných systémov na služby uvedené v prílohe III, s cieľom zabezpečiť **kontinuitu** týchto služieb.

EK prijme vykonávací akt bližšie špecifikujúci požiadavky na bezpečnosť sietí a informačných systémov PDS, a to v 3. Q 2017.

Oznamovacie požiadavky PDS

Nahlasovanie „všetkých“ incidentov so **závažným vplyvom** na poskytovanie služby uvedenej v prílohe III

EK prijme vykonávací akt bližšie špecifikujúci požiadavky na oznamovacie požiadavky PDS ako súčasť vykonávacieho aktu špecifikujúceho požiadavky na bezpečnosť sietí a informačných systémov PDS (3. Q 2017).

...podniky, ktoré zamestnávajú menej ako 250 osôb a ktorých ročný obrat nepresahuje 50 miliónov EUR a / alebo celková ročná súvaha nepresahuje 43 miliónov EUR, nie sú bezpečnostnými a oznamovacími požiadavkami viazané.

„Best practices“

Incident response

- Strategies for incident response and cyber crisis cooperation

Incident handling

- Incident handling automation project
- Good Practice Guide for Incident Management

Incident classification and taxonomy

- Overview of existing taxonomies
- Good practice guide of using taxonomies in incident prevention and detection

CSIRT maturity

- Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity
- Study on CSIRT Maturity – Evaluation Process
- Guidelines for national and governmental CSIRTs on how to assess maturity

CSIRT capacity building and training

- Good Practice Guide on Training Methodologies

lex generalis vs. lex specialis

- Nariadenie o mimoburzových derivátoch, centrálnych protistranách a archívoch obchodných údajov
- Smernica o trhoch s finančnými nástrojmi v spojení s delegovaným nariadením EK, ktorým sa dopĺňa smernica
- PSD2

Transpozícia v SR – Návrh zákona

Rozsah úpravy

- Organizácia a pôsobnosť orgánov verejnej moci v oblasti KB
- Národná stratégia KB
- Jednotný informačný systém KB
- Postavenie a povinnosti povinných osôb
- Organizácia, pôsobnosť a akreditácia jednotiek CSIRT
- Systém zabezpečenia kybernetickej bezpečnosti
- Kontrolný a sankčný mechanizmus

Transpozícia v SR – Návrh zákona

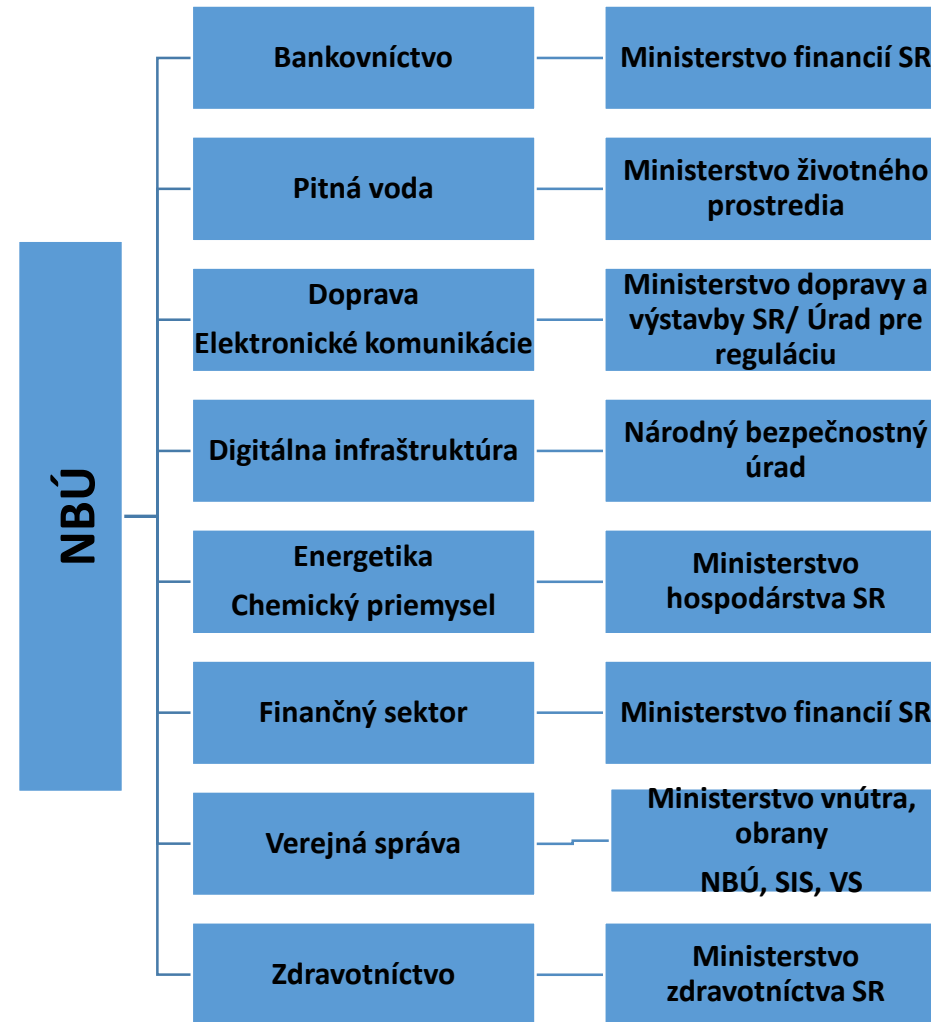
VPO

Hybridný prístup (decentralizovaný prístup v podobe vecne príslušných autorít s jediným ÚOŠS, ktorý riadi a kontroluje výkon ŠS v oblasti KB)

Vecne príslušné authority

- úrad,
- Ministerstvo dopravy a výstavby Slovenskej republiky,
- Ministerstvo financií Slovenskej republiky,
- Ministerstvo hospodárstva Slovenskej republiky,
- Ministerstvo obrany Slovenskej republiky,
- Ministerstvo vnútra Slovenskej republiky,
- Ministerstvo zdravotníctva Slovenskej republiky,
- Ministerstvo životného prostredia Slovenskej republiky,
- Slovenská informačná služba.

Zodpovedné subjekty



Transpozícia v SR – Návrh zákona

Povinné osoby:

- **Prevádzkovatelia základných služieb**

- Splnenie požadovaných kritérií (sektor/parametre (všeobecné alebo špecifické sektorové)
 - Notifikačné povinnosti
 - a) identifikačné údaje, základné služby ktoré prevádzkuje
 - b) % podiel služby na trhu
 - c) cezhraničný presah služby
 - d) geografické rozšírenie služby
 - e) alternatívna možnosť zachovania prevádzkovania služby
- + vlastná identifikácia, nahlásenie VPA, alebo úradom

- **Poskytovatelia digitálnych služieb**

- PO, FO – podnikateľ, ktorý poskytuje digitálnu službu (má 50 a viac zamestnancov a ročný obrat viac ako 10 miliónov eur)
- Notifikačné povinnosti (identifikačné údaje, služba)

Transpozícia v SR – Návrh zákona

- a) **podrobnosti o technickom, technologickom a personálnom vybavení CSIRT,**
- b) **prahové hodnoty pre identifikáciu základnej služby,**
- c) **obsah bezpečnostných opatrení, obsah a štruktúru bezpečnostnej dokumentácie, rozsah bezpečnostných opatrení,**
- d) **kategórie a prahové hodnoty kybernetických bezpečnostných incidentov hlásených PZS a PDS,**
- e) **podrobnosti o požiadavkách na audit, opakovaný audit a rozsahu auditu,**
- f) **bezpečnostné štandardy a znalostné štandardy v oblasti kybernetickej bezpečnosti,**
- g) **klasifikácia informácií a kategorizácia sietí a informačných systémov ...**

.

Ďakujem za pozornosť



spilar@bch.sk

+421.2.3301.4760

+421.948.553.160