



Kompetenčné
a certifikačné
centrum
kybernetickej
bezpečnosti

Už konečne nastal čas pre Business continuity management?

15.03.2022 , eFocus konferencia



Výsledky prvních auditů kybernetické bezpečnosti



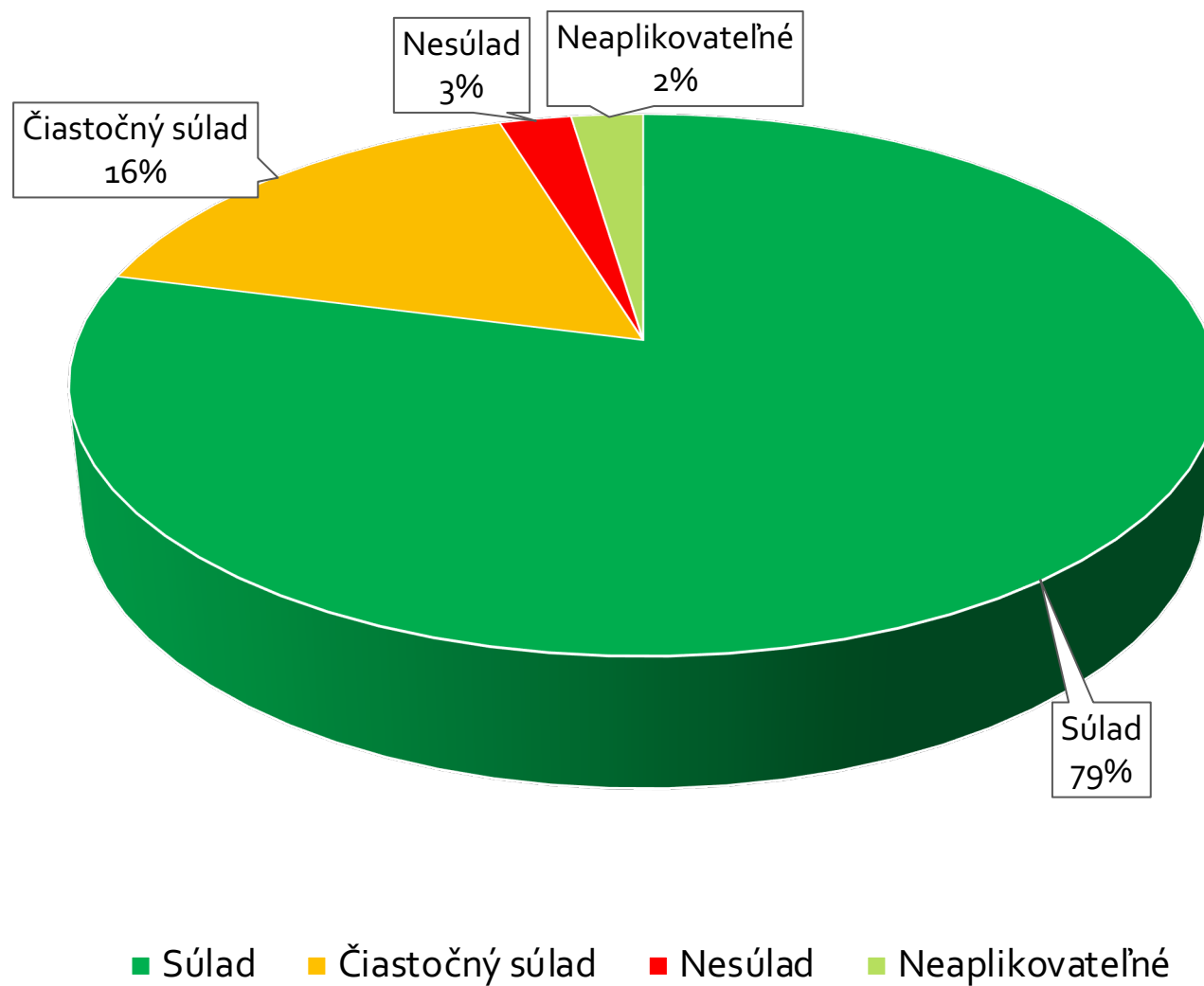
AUDIT KYBERNETICKEJ BEZPEČNOSTI

- **Audit kybernetickej bezpečnosti** je podľa § 29 ods. 1 zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti **overenie plnenia povinností** podľa zákona č. 69/2018 Z.z., **posúdenie zhody prijatých bezpečnostných opatrení** s požiadavkami tohto zákona a osobitných predpisov, ktoré sa vzťahujú na bezpečnosť sietí a informačných systémov prevádzkovateľa základnej služby pre jednotlivé siete a informačné systémy základnej služby a pre prostriedky, ktoré podporujú základné služby
 - **Hlavný cieľ auditu** kybernetickej bezpečnosti je identifikovať nedostatky kybernetickej bezpečnosti u prevádzkovateľa základnej služby
 - **Sekundárny cieľ auditu** je navrhnúť prijatie opatrení na odstránenie zistených nedostatkov, s úmyslom napraviť existujúci stav a predísť kybernetickým bezpečnostným incidentom
- **Oprávnenie vykonať audit** kybernetickej bezpečnosti má výhradne len certifikovaný audítor kybernetickej bezpečnosti



STAV SÚLADU V KOMERČNOM PROSTREDÍ

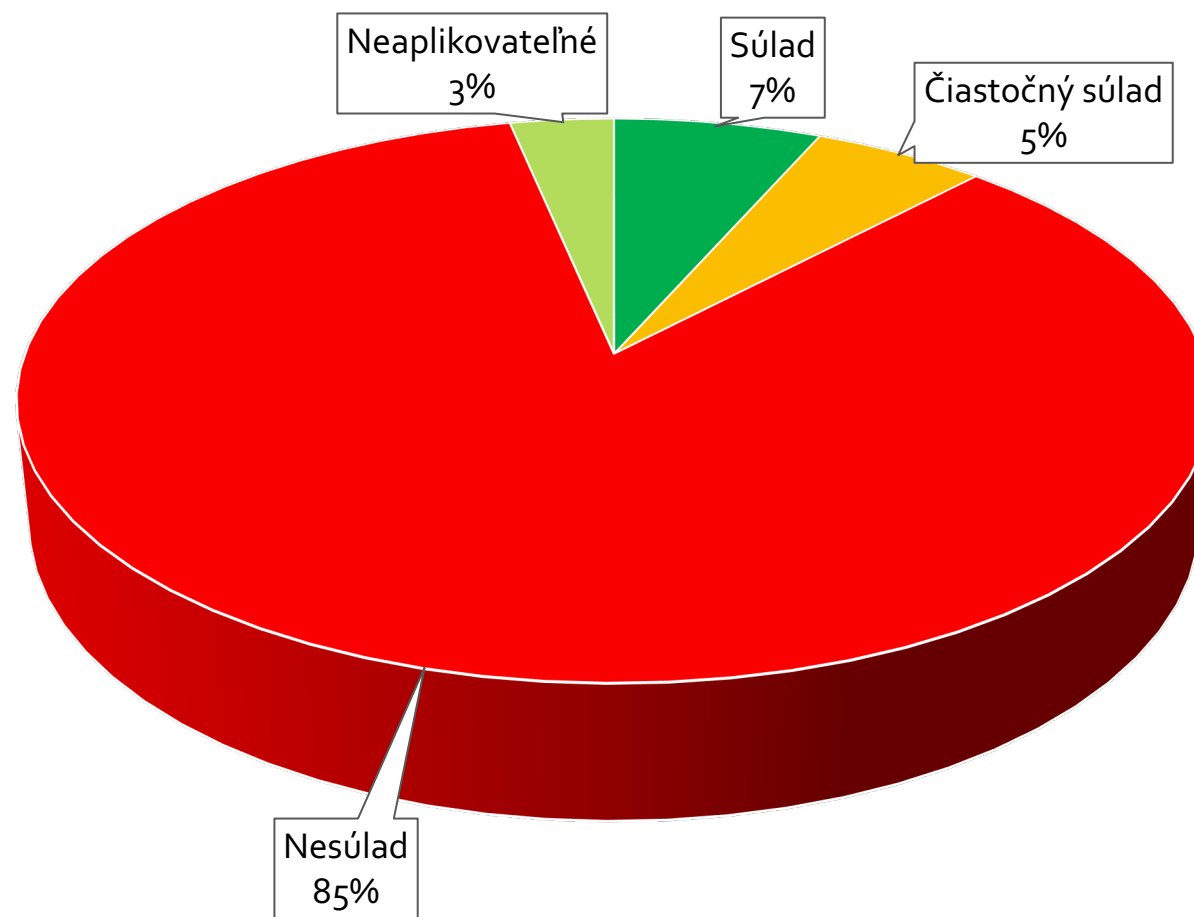
■ Priemerný stav súladu: 50%





STAV SÚLADU VO VEREJNEJ SPRÁVE

- Priemerný stav súladu: 20-30%



■ Súlad ■ Čiastočný súlad ■ Nesúlad ■ Neaplikovateľné



NAJČASTEJŠIE NÁLEZY AUDITU

- Neexistujúca stratégia KB a (ne)podpora najvyššieho vedenia
- Neurčený Manažér KB, prípadne neformálne zaradený
- Neexistencia vzdelávania v oblasti informačnej bezpečnosti
- Nedostatočná, alebo chýbajúca bezpečnostná dokumentácia (aj pri PZS s certifikátmi ISO27001)
- Bezpečnostná dokumentácia často tvorená len dodávateľmi konkrétneho projektu
- Bezpečnosť podriadená IT
- Závislosť na dodávateľoch (vendor lock)
- Neexistujúce riadenie aktív, hrozieb a rizík
- Nízka vyspelosť procesu riadenia rizík
- Chýbajúci vlastníci rizík a ich zodpovednosti
- Neformálne riadenie prevádzky IT
- Chýbajúci monitoring a logovanie
- Nesystematické riešenie incidentov
- Nedostatky v riadení bezpečnosti sietí (typicky - plný outsourcing bez prehľadu o procese)
- Chýbajúca topológia, segmentácia, zoznamy portov
- Nezabezpečenie a nevybavenosť „serverovní“, často plných kvalitného HW
- **Neexistencia procesov riadenia kontinuity činností**
- **Nejasné a neformálne postupy zálohovania, obnova netestovaná**
- **(Ne)šifrovanie komunikácie, prenosov údajov a záloh**
- **Nepripravenosť na krízové situácie**



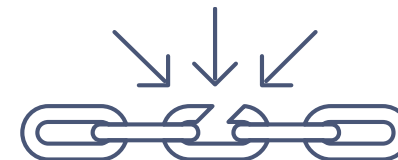
Riadenie kontinuity činností

Business Continuity Management - BCM



RIADENIE KONTINUITY ČINNOSTÍ

- **Business continuity management** (BCM) je schopnosť organizácie pokračovať v dodávke produktov alebo služieb na prijateľných vopred definovaných úrovniach po závažnom incidente [ISO 22301:2012]
- **Kríza** - nepredvídateľná, kritická udalosť alebo situácia s následkami, ktorá:
 - Ohrozuje časť alebo celú spoločnosť
 - Môže spôsobiť nenaplnenie očakávaní zainteresovaných strán
- Finálnym výstupom BCM sú tzv. plány kontinuity činností (z angl. „**Business Continuity Plan**“- BCP), ktoré všeobecne obsahujú najmä podrobnosti na zvládnutie okamžitých následkov prerušenia činností





CIELE RIADENIA KONTINUITY ČINNOSTÍ

- Organizácia sama určí, **čo má byť hlavným cieľom plánov kontinuity:**
 - a) Ochrana prioritných činností
 - b) Stabilizácia a obnova prioritných činností, ich závislostí a podporných zdrojov
 - c) Zmiernenie dopadov a reakcia na negatívne vplyvy vyvolané krízovou situáciou.

- Organizácia sama určí, **čo má byť strategickým imperatívom procesu BCM:**
 - 1. Náležitý ohľad na záujem jednotlivca
 - 2. Predchádzanie ďalším stratám alebo nevykonateľnosti prioritných činností
 - 3. Vplyv na prostredie.





STANOVENIE POŽIADAVIEK NA ZDROJE

- V rámci plánovania kontinuity organizácia stanoví požiadavky na zdroje, ktoré budú potrebné na implementáciu vybraných stratégií kontinuity činností.
- Medzi **zdroje**, ktoré by mali byť v BCP posúdené a vyčlenené, patria najmä:
 - a) Ľudia
 - b) Informácie a dáta
 - c) Budovy, pracovné prostredie a súvisiace inžinierske siete
 - d) Zariadenia, vybavenie a spotrebný materiál
 - e) Systémy informačných a komunikačných technológií (IKT)
 - f) Preprava a logistické činnosti
 - g) Financovanie
 - h) Partneri a dodávatelia.
- V **stratégii BCM** má byť s ohľadom na potrebu riadenia zdrojov zahrnuté aj schválenie prioritných časových rámcov na obnovu činností a hodnotenie spôsobilosti tretích strán zaručiť kontinuitu dodávateľských činností.



PLÁNY KONTINUITY A KRÍZOVÉ SCENÁRE

- Nevyhnutným predpokladom efektívneho plánovania kontinuity je, aby boli vopred definované scenáre rôznych udalostí, ktoré potenciálne môžu mať negatívny vplyv na bežné činnosti organizácie.
- Typickými kategóriami scenárov BCM sú napr.:
 - 1. Náhla nedostupnosť personálu**
 - 2. Náhla nepoužiteľnosť pracoviska/budovy**
 - 3. Náhla nepoužiteľnosť technológií**
 - 4. Náhla nedostupnosť médií.**
- Vedenie podniku by malo formálne rozhodnúť, ktoré scenáre majú byť vzhľadom na obmedzené zdroje predmetom BCM.
- Zvyčajne sú riešené len vyššie uvedené kategórie scenárov, pričom nie sú zahrnuté scenáre ako prírodné katastrofy, vojnové konflikty, občianske nepokoje a podobné, ktoré prekračujú rámec plánovacích možností bežnej organizácie.

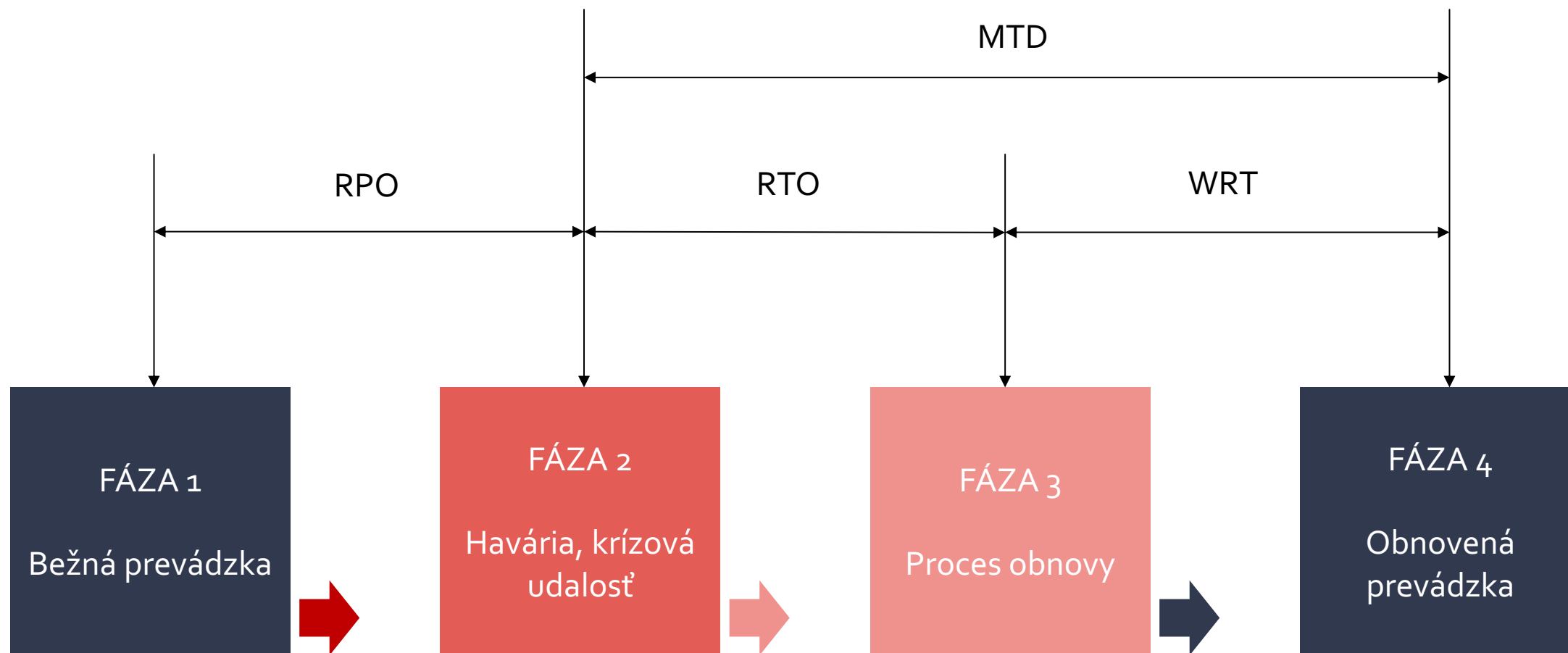


ANALÝZA FUNKČNÉHO DOPADU

- **Analýza funkčných dopadov** (Business Impact Analysis - BIA) identifikuje, kvalifikuje a kvantifikuje potenciálne dopady a straty v prípade prerušenia alebo narušenia prevádzky u všetkých procesov organizácie s cieľom identifikovať tie procesy, ktoré sú pre organizáciu kľúčové / kritické.
- Jedná sa o posúdenie ekonomických, reputačných a regulačných vplyvov, hrozieb a nákladov na obnovenie procesu v prípade výpadku v rôznych časových intervaloch od začiatku výpadku
- Neoddeliteľnou súčasťou BIA sú:
 - **RTO** (Recovery Time Objective) - identifikácia maximálne tolerovanej doby pre obnovenie činnosti na prijateľnej úrovni
 - **RPO** (Recovery Point Objective) - identifikácia maximálne prijateľného množstva straty údajov merané v čase - cieľového bodu obnovenia



CIEĽOVÁ DOBA OBNOVY A CIEĽOVÝ BOD OBNOVY





TESTOVANIE BCP/DRP

Test úplného prerušenia (Failover)

- Najťažší test, pri ktorom sa simuluje úplné zničenie lokality s následnou obnovou funkčnosti v záložných priestoroch.

Paralelné testy

- Presunutie jedného alebo viacerých vybraných kritických procesov organizácie do záložnej lokality a ich obnova v požadovanom čase.
- Technicky zamerané testy s cieľom overenia schopnosti organizácie pokračovať v činnosti v prípade vzniku krízovej udalosti.

Simulačné testy

- Praktický nácvik a preverovanie jednotlivých postupov a tímovej interakcie podľa vopred pripravených scenárov.
- Súčasťou testu je overenie funkčnosti komunikačných liniek, otestovanie komunikácie s dodávateľmi, médiami a záchrannými zložkami.
- Príkladom simulačných testov môže byť napr. nácvik evakuácie budovy alebo fiktívny požiar serverovne.



TESTOVANIE BCP/DRP

Teoretický prechod plánom (Walkthrough)

- Kontrola úplnosti plánov rozšírená o teoretické preverenie konkrétnych postupov obnov, overenie znalosti rolí jednotlivých členov tímu a ich vzájomnej komunikácie.
- Cieľom testov je odhaliť nedostatky v navrhnutých postupoch obnovy jednotlivých procesov, prípadne zaškolenie členov tímu.

Kontrola úplnosti plánov (Table-Top)

- Najjednoduchší typ testov.
- Zahŕňa teoretické preskúmanie kompletnosti informácií obsiahnutých v plánoch, overovanie správnosti, úplnosti a aktuálnosti uvedených údajov (kontaktné informácie na členov tímu, záložné lokality, kontakty na servisné spoločnosti, zoznam technických prostriedkov).



Ochrana vlastnických práv

Všetky autorské práva k tomuto dokumentu sú vyhradené pre Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (ďalej len „KCCKB“). Autorské práva k tomuto dokumentu má a autorské práva k tomuto dokumentu vykonáva KCCKB.

Vlastnícke práva tretích strán

Všetky ochranné známky a iné obdobné právne chránené označenia spomenuté v tomto dokumente sú výhradným vlastníctvom ich vlastníkov, ktorí sú, pokiaľ sa nejedná o KCCKB, v dokumente označení vo forme príslušnej citácie.

Akékoľvek kopírovanie či iné neoprávnené použitie celého dokumentu alebo jeho časti, v elektronickej alebo listinnej podobe, bez predchádzajúceho písomného súhlasu jeho autorov, napr. KCCKB, je zakázané. Porušenie vlastnických a iných súvisiacich práv bude riešené v zmysle právnych predpisov Slovenskej republiky.

Limity informácií

Informácie obsiahnuté v tomto dokumente sú poskytované iba na informačné účely a bez akejkoľvek záruky, výslovnej či implicitnej. Názov KCCKB, logo KCCKB a ďalšie produkty a služby KCCKB sú ochrannými známkami KCCKB. Ostatné názvy spoločností, produktov alebo služieb môžu byť ochrannými známkami, alebo značkami služieb iných organizácií.



www.cybercompetence.sk



www.linkedin.com/company/cybercompetence



@CybercenterSk