

Implementace BEZPEČNOSTNÍ POLITIKY v organizaci



RNDr. Luboš Číž, CISA, CISM

ciz@dcit.cz

DCIT, a.s., <http://www.dcit.cz>



Bezpečnostní politika – ví každý co to je?

Typy bezpečnostních politik

Postup implementace

Zásady úspěšné implementace

Nejlepší praktiky

CO ZÍSKÁME?



- Organizační pohled
- Personální pohled
- Technický pohled



- *Promiskuitní bezpečnostní politika*
(vše dovoleno – bezpečnost se řeší mimo IT)
- *Liberální bezpečnostní politika*
(každý může dělat vše, až na věci explicitně zakázané)
- *Opatrná /racionální/ bezpečnostní politika*
(zakazuje dělat vše, co není explicitně povoleno)
- *Paranoidní bezpečnostní politika*
(zakazující dělat vše i potenciálně nebezpečné)



- Předběžná studie
- Zadání,
- analýza rizik,
- bezpečnostní politika organizace,
- realizace BP,
- realizace a tvorba bezpečnostní dokumentace nižší úrovně,
- průběžná realizace osvěty – udržování bezpečnostního povědomí zaměstnanců.



- Přezkoumání vedením
- Zlepšování

**JED
NEJ**

- Hodnocení nebezpečí
 - bezpečnostních rizik
 - Právní a jiné požadavky
 - Cíle a cílové hodnoty
- Projekty na realizaci cílů

**PLÁ
NUJ**

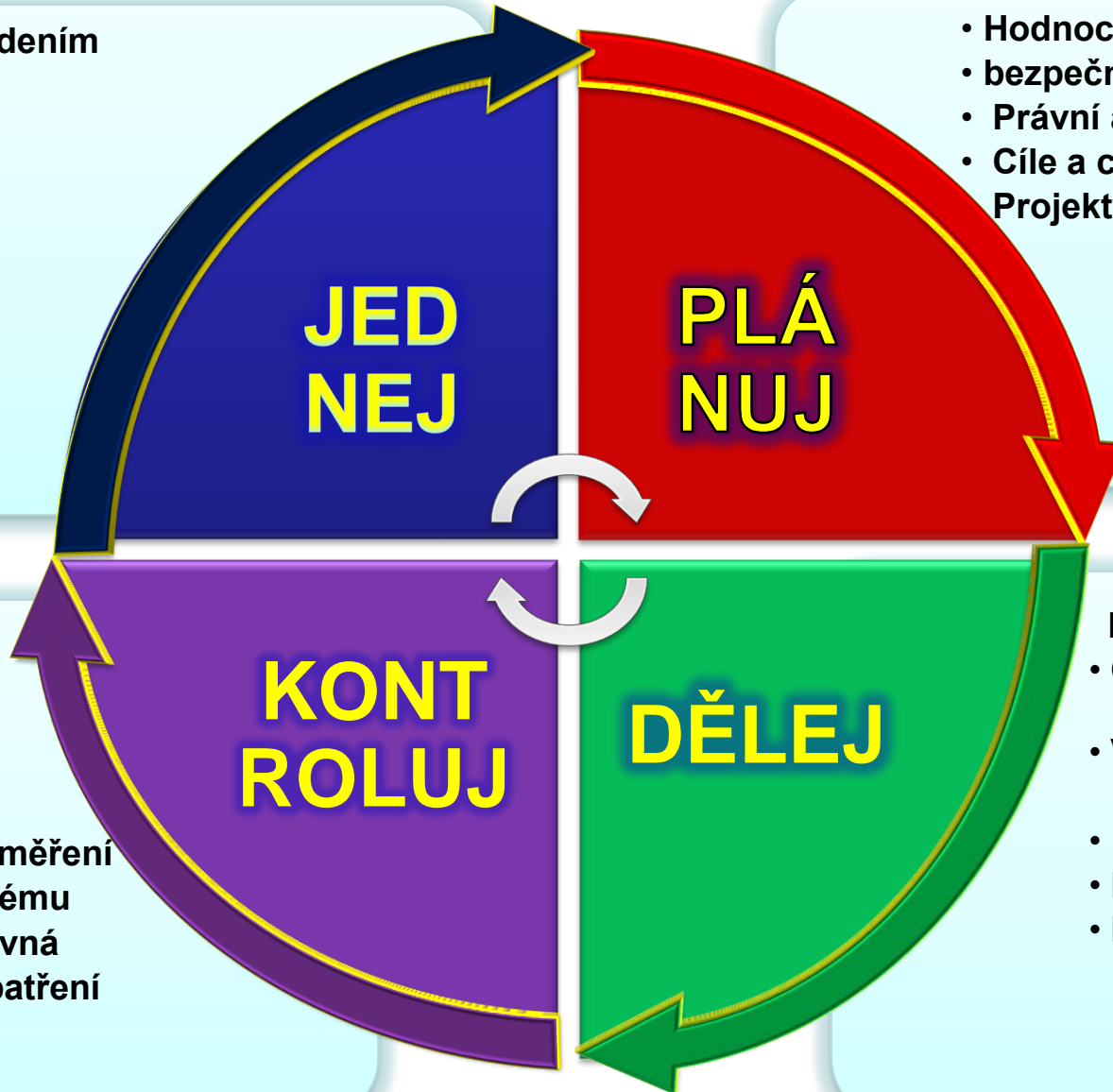
- Monitorování a měření
- Hodnocení systému
- Neshody, nápravná a preventivní opatření
- Záznamy
- Audity

**KONT
ROLUJ**

IMPLEMENTACE

- Odpovědnosti a kompetence
- Výcvik, povědomí komunikace
- Dokumentace
- Řízení operací
- Připravenost na bezpečnostní situace/schopnost reakce

DĚLEJ



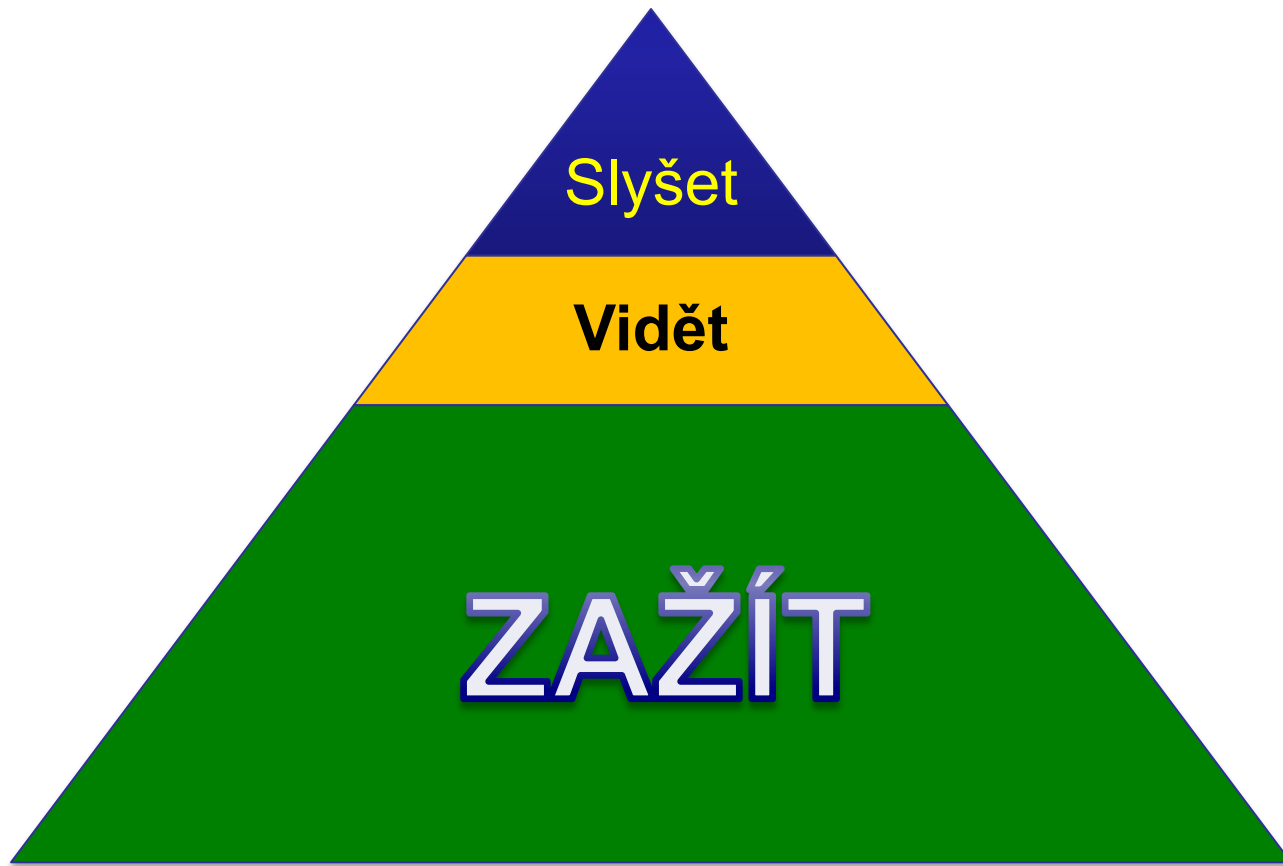
- Vždy přináší problémy! PROČ?
 - Omezení jsou vidět ihned
 - Přínosy nejsou zřejmé

- Co pomáhá?
 - Ustavit odpovědnosti a kompetence
 - Výcvik, povědomí
 - » komunikace !
 - » komunikace !!
 - » komunikace ?
 - Dokumentace
 - Řízení provozu (i z hlediska bezpečnosti ICT)
 - Připravenost na bezpečnostní situace/schopnost reakce



	CEO	CFO	BE	CIO	BPO	HO	CA	HD	HA	PM	CA
Aktivita											
Definovat a udržovat plán zabezpečení IT.	I	C	C	A	C	C	C	C	I	I	R
Definovat, ustavit a provozovat proces řízení identit			I	A	C	R	R	I			C
Sledovat potenciální a skutečné bezpečnostní incidenty.				A	I	R	C	C			R
Pravidelně revidovat uživatelská přístupová práva a oprávnění				A	I	C					R
Vytvořit a udržovat postupy pro udržení a zachování kryptografických klíčů.				A		R			I		C
Zavést a udržovat technickou a procedurální ochranu informační toků v sítích				A	C	C	R	R			C
Provádět pravidelné hodnocení zranitelností.		I		A	I	C	C	C			R





- Bezpečnostní politika
- Dokumentovaný rozsah ISMS
- Zpráva o analýze rizik
- Prohlášení o aplikování protiopatření
- Plán zvládnání rizik
- Zpráva o řízení rizik
- Systémová bezpečnostní politika
- Smlouva o výměně informací
- Zpráva o analýze stavu
- Program zvyšování úrovně bezpečnosti



- zpracování a zacházení s informacemi;
- zálohování dat
- časové návaznosti zpracování, včetně vzájemných souvislostí s jinými systémy, čas začátku první a dokončení poslední úlohy;
- popis činnosti při výskytu chyb nebo jiných mimořádných stavů, které by mohly vzniknout při běhu úlohy, včetně omezení na používání systémových nástrojů
- spojení na kontaktní osoby v případě neočekávaných systémových nebo technických potíží;
- instrukce pro zacházení se speciálními výstupy, jako například se speciálním spotřebním materiálem, správa důvěrných výstupů, včetně instrukcí pro nakládání s chybnými výstupy z aplikací v případě jejich selhání
- postupy při restartu systému a obnovovací postupy v případě selhání systému
- zpracování záznamů z auditu a systémových záznamů



- zpětná vazba na hlášení incidentu
- formuláře podporující proces hlášení bezpečnostních událostí formuláře podporující proces hlášení bezpečnostních událostí
- nastavení správného chování v případě bezpečnostní události
- odkaz na zavedená formalizovaná pravidla pro disciplinární proces s těmi co způsobili narušení bezpečnosti.



- Keep simply (jak je to jen možné)
- Technika je spolehlivější než člověk
(co lze vynutit technicky, vynuťte technicky)
- Opakování je matka moudrosti
- Důslednost, důslednost, důslednost!



PŘIMĚŘENOU BEZPEČNOSTNÍ KULTURU

CHOVÁNÍ A JEDNÁNÍ UŽIVATELŮ V SOULADU
S BESPEČNOSTNÍMI CÍLY ORGANIZACE



- Kontakt
info@dcit.cz

ciz@dcit.cz

