



PRAKTICKÉ ŘEŠENÍ PROCESŮ KYBERNETICKÉ BEZPEČNOSTI

Dotace, procesy a nástroje pro kybernetickou bezpečnost

Radim Trávníček | BeSecured

CO - VEŘEJNÉ



RADIM TRÁVNÍČEK

15 let v oboru informační a kybernetické bezpečnosti
Advisor | Školitel | Auditor | Manažer KB | CISO

radim@besecured.online | +420 731 209 891



URČETE SPRÁVNĚ ROZSAH ISMS

Co je regulovaná služba, co potřebujeme chránit?

Na tento rozsah se zaměřte při zahájení projektu.
Rozšiřovat můžete časem.

Aktiva hodnotte jednoduše.





2

NETRAPTE SE (PŘÍLIŠ) S ANALÝZOU RIZIK

Zkuste použít metodiku z VoKB. A pokud nevyhovuje, tak se vrhněte na jinou.

Ten, kdo zná své (IT) prostředí, tak nepotřebuje metodiku.

Metodika je nástroj pro získání pozornosti vedení.

3

ZÍSKEJTE PODPORU VEDENÍ

Bez podpory nejvyššího vedení a kolegů kolem vás (vedoucích pracovníků) nic nezmůžete.





4

POZOR NA NEDOSTATEČNÉ VZDĚLÁVÁNÍ

E-learning 1x ročně nestačí.

Podpořte to mail kampaní, plakáty, brožurami...

5

ŘÍZENÍ PŘIVILEGOVANÝCH OPRÁVNĚNÍ

Minimalizujte počet privilegovaných oprávnění.

Monitorujte jejich používání. Odeberte je, pokud nejsou potřeba.

```
mirror_mod = modifier_ob.  
set mirror object to mirror  
mirror_mod.mirror_object  
operation == "MIRROR_X":  
mirror_mod.use_x = True  
mirror_mod.use_y = False  
mirror_mod.use_z = False  
operation == "MIRROR_Y":  
mirror_mod.use_x = False  
mirror_mod.use_y = True  
mirror_mod.use_z = False  
operation == "MIRROR_Z":  
mirror_mod.use_x = False  
mirror_mod.use_y = False  
mirror_mod.use_z = True  
selection at the end -add  
mirror_ob.select= 1  
modifier_ob.select=1  
context.scene.objects.active  
("Selected" + str(modifier  
mirror_ob.select = 0  
= bpy.context.selected_obj  
data.objects[one.name].sel  
print("please select exactly  
-- OPERATOR CLASSES ----  
types.Operator):  
X mirror to the selected  
object.mirror_mirror_x"  
mirror X"  
context):  
context.active_object is not
```



6

ZAJIŠTĚNÍ DOSTUPNOSTI ČINNOSTÍ/SLUŽEB

Identifikujte, co je důležité (“regulovaná služba”) a proved'tě BIA.
Zpracujte odpovídající BCP a DRP.

7

ŘÍZENÍ BEZPEČNOSTNÍCH INCIDENTŮ

Jsou jen 2 typy společností. Ty, které už bezpečnostní incident zažily.
A ty, které o tom ještě neví.

Incident Response Plan je klíč! A komunikace.





8

NEZAPOMÍNEJTE NA MONITOROVÁNÍ A TESTOVÁNÍ

Systémové audity, testy technických zranitelností, penetrační testy, simulované phishing kampaně, testy funkčnosti fyzických opatření, testy BCP a DRP, přezkoumání přístupů...

Logování a vyhodnocování událostí – SIEM, EDR, antiviry+, chování uživatelů...



PROSTOR PRO VAŠE DOTAZY