PRAKTICKÉ ŘEŠENÍ PROCESŮ KYBERNETICKÉ BEZPEČNOSTI

Dotace, procesy a nástroje pro kybernetickou bezpečnost

Radim Trávníček | BeSecured

C0 - 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 hodnoťte 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.

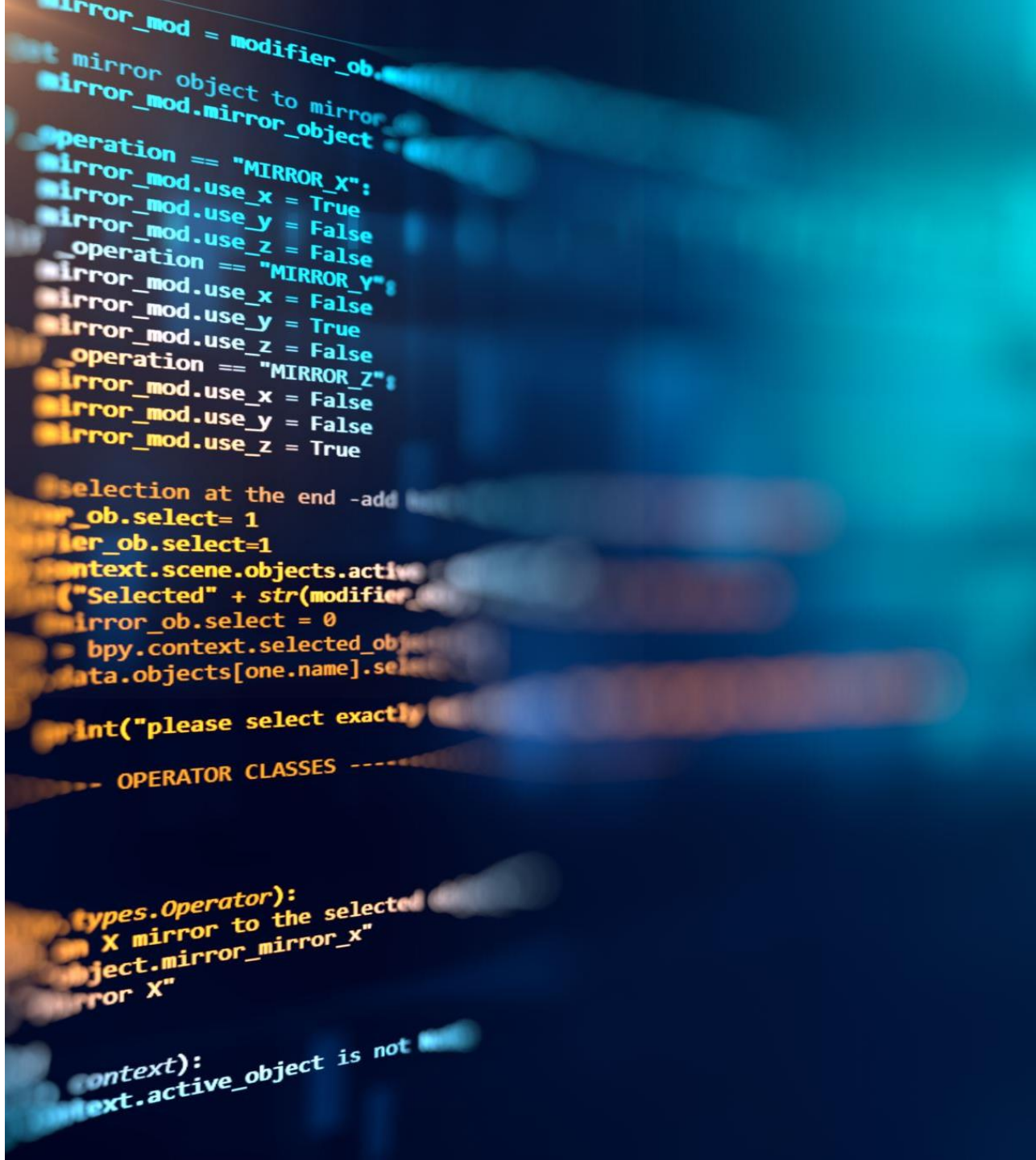
Podpořte to mail kampaní, plakáty, brožurami…

5

ŘÍZENÍ PŘIVILEGOVANÝCH OPRÁVNĚNÍ

Minimalizujte počet privilegovaných oprávnění.

Monitorujte jejich používání. Odeberte je, pokud nejsou potřeba.



6

ZAJIŠTĚNÍ DOSTUPNOSTI ČINNOSTÍ/SLUŽEB

Identifikujte, co je důležité (“regulovaná služba”) a proveďtě BIA.

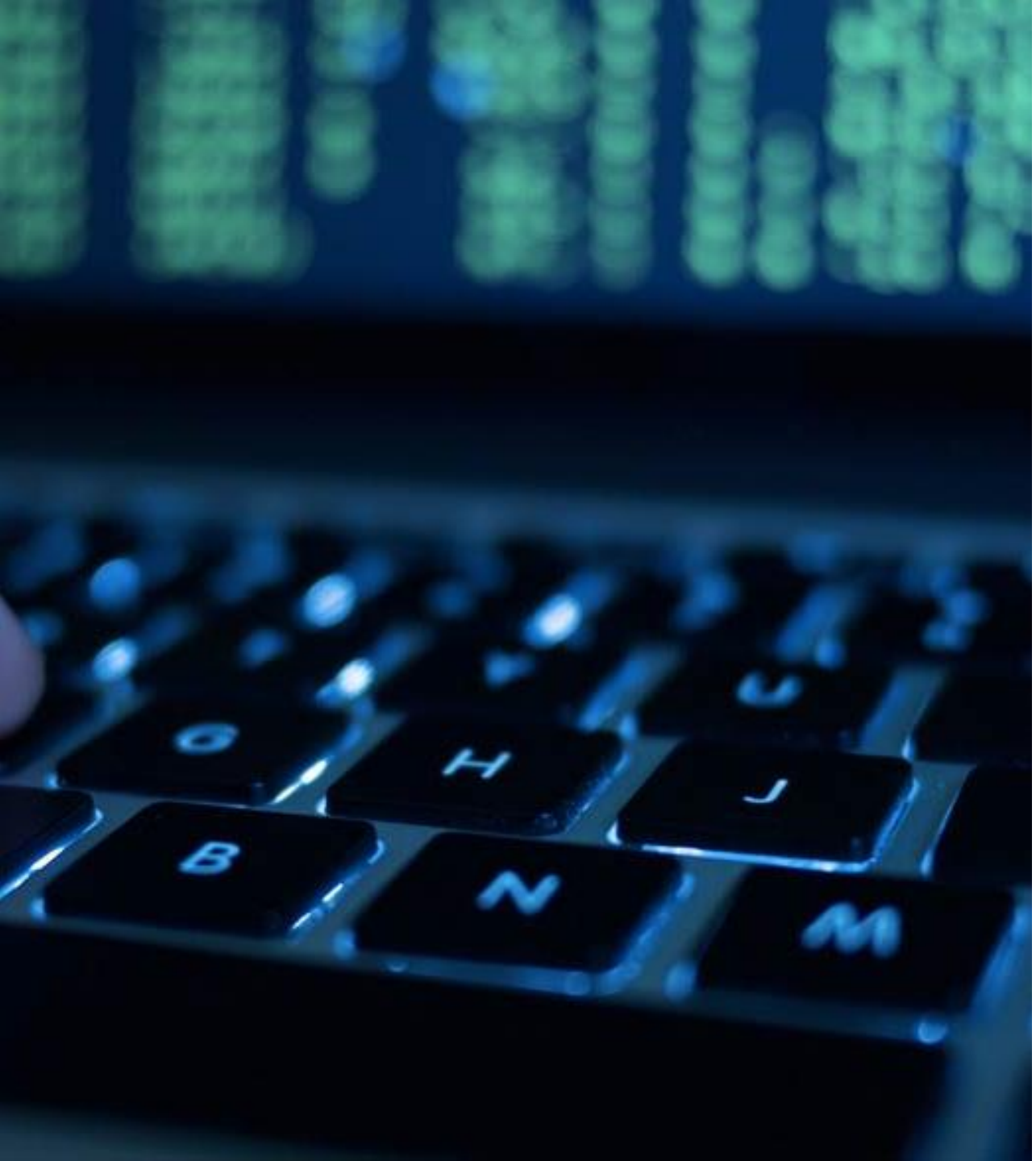
Zpracujte odpovídající BCP a DRP.

7

ŘÍZENÍ BEZPEČNOSTNÍCH INCIDENTŮ

Jsou jen 2 typy společností. Ty, které už bezpečnostní incident zažily. A ty, které o tom jestě 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 fuknčnosti fyzických opatření, testy BCP a DRP, přezkoumání přístupů…

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

PROSTOR PRO VAŠE DOTAZY