



CO VŠECHNO (NE)DĚLÁME PRO AUDITOVÁNÍ BEZPEČNOSTI

SECURITY TALK OSTRAVA | 31.5.2024

Radim Trávníček

BeSecured





CO JE TO AUDIT?

Cílená a **plánovaná** aktivita, s jasným zadáním, jasným postupem, jasnými kritérii a jasnými výsledky.

Dva typy auditů

- Hledáme shodu
- Hledáme neshodu

1

KOMPETENCE

Ověřujte kvalifikaci auditorů a jejich praxi.

Vzdělávejte vlastní auditory.

Teoretik vám skutečné problémy v IT zabezpečení neodhalí.





2

POSTUP AUDITOVÁNÍ A KRITÉRIA

Nastavte si konkrétní postup, konkrétní kritéria.

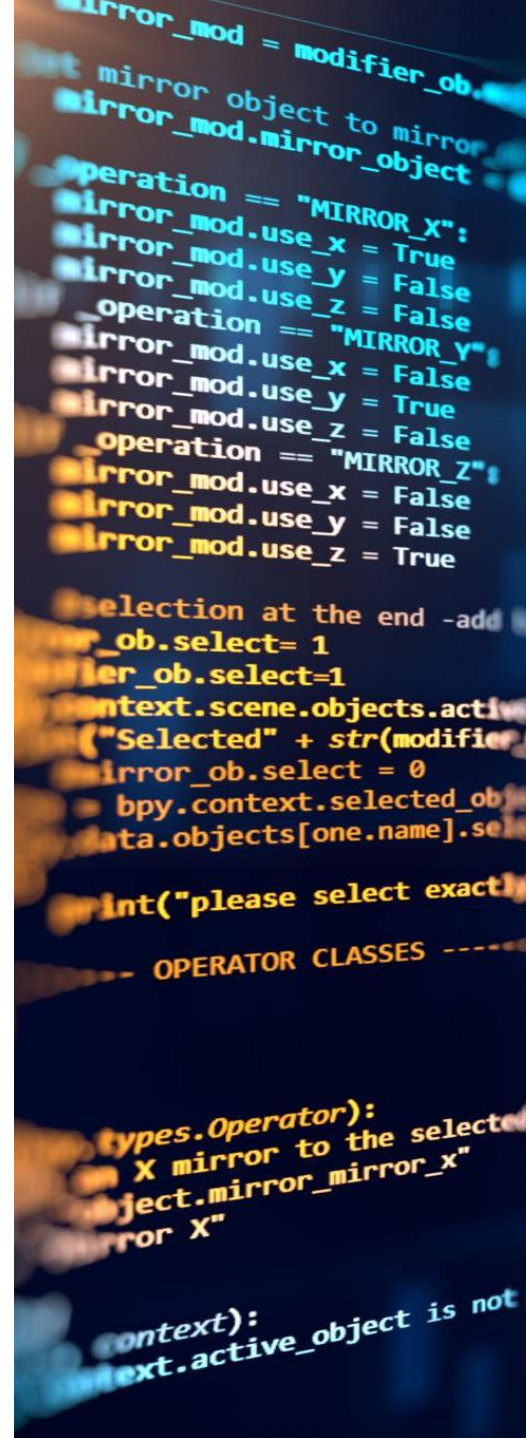
Pokud využíváte externího dodavatele, nechte si zaslat metodiku předem. Projděte si ji. Upravte ji tak, aby vyhovovala vám.

3

KRITÉRIA A PODMÍNKY PROVEDENÍ AUDITU

Trvejte na hodnocení, které vám bude dávat smysl.

Audit nesmí ohrozit fungování společnosti/služeb/výroby produktů apod.





4

KYBER OBSAHUJE I FYZICKOU BEZPEČNOST

Správně řešení kybernetická bezpečnost začíná u dobře zvládnuté fyzické bezpečnosti.

- Kontrola klíčů,
- Nastavení přístupových čipů a kartiček,
- Soulad s legislativou v rámci CCTV,
- Reakce ostražky,
- Funkčnost EZS

5

TESTOVÁNÍ PLÁNU REAKCE NA INCIDENTY

Simulace bezpečnostního incident vám ukáže, kde máte v slabiny.





6

OVĚŘOVÁNÍ ZNALOSTÍ KOLEGŮ

Phishingové kampaně

Podvržené USB flash disk

Reakce na podezřelou situaci – hlásí nám pracovníci?

7

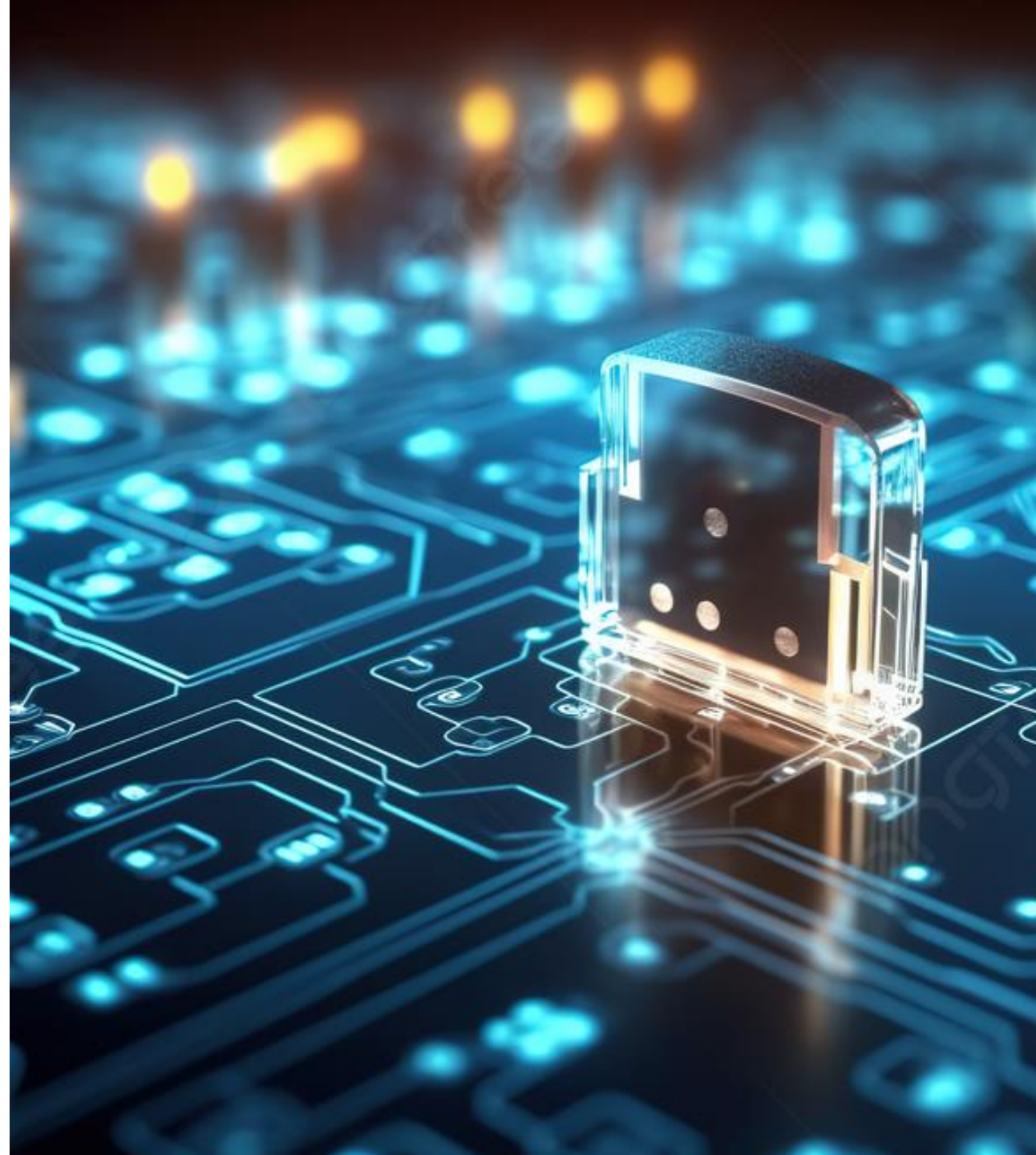
PŘEZKOUMÁNÍ PŘÍSTUPŮ

Nejsmutnější oblast vůbec.

Ověřujeme aktivní účty – spolupráce s HR

Jak jsou na tom přístupy v aplikacích, které nemáme ve správě?

A co webové aplikace – shadow IT?





8

PENETRAČNÍ TESTY A TESTY ZRANITELNOSTÍ

Retestujeme výsledky?

Udržíme pravidelnost?

Máme nástroje?

9

AI – ÚMĚLÁ INTELIGENCE

Nekontrolujeme výsledky AI

Jaká data nám pracovníci posílají do AI?

Zranitelný kód





10

TESTOVÁNÍ PLÁNŮ

Plány kontinuity - BCP

Plány obnovy technologií - DRP

Obnova ze zálohy



SHRNUTÍ NA ZÁVĚR

- KOMPETENCE
- METODIKA, KRITÉRIA HODNOCENÍ
- ČETNOST AUDITŮ
- INTERNÍ VS. EXTERNÍ AUDITY

- JEDEN AUDIT KB ROČNĚ NESTAČÍ



PROSTOR PRO VAŠE DOTAZY