Instrukce – Asset Register

Účel

Risk Register slouží k evidenci a řízení bezpečnostních rizik vztahujících se k IT / OT / IoT aktivům.
Umožňuje:

- identifikovat rizika navázaná na konkrétní aktiva
- vyhodnotit jejich dopad a pravděpodobnost
- stanovit prioritu řešení
- sledovat stav a odpovědnost za riziko

Je navržen jako jednoduchý a praktický nástroj vhodný pro malé a střední organizace.

Zásady vyplňování

- Každý řádek = jedno riziko
- Rizika se zapisují **pouze pro relevantní aktiva** (ne všechna aktiva musí mít riziko)
- Asset ID se vybírá z rozevíracího seznamu napojeného na Asset Register
- Hodnoty Dopad a Pravděpodobnost se vybírají z číselníků
- Úroveň rizika a Priorita se dopočítávají automaticky – tyto buňky se ručně neupravují
- Stav rizika se aktualizuje průběžně podle postupu řešení

Popis sloupců

Risk ID

Jednoznačný identifikátor rizika
(př. R-001, R-OT-05)

Asset ID

Odkaz na aktivum z Asset Registeru, ke kterému se riziko vztahuje.
Vyplňuje se výběrem z rozevíracího seznamu.

Název aktiva

Automaticky doplněný název aktiva dle zvoleného Asset ID.
Slouží pro přehlednost – neupravuje se ručně.

Název rizika

Krátký výstižný název rizika.
(př. „Neautorizovaný vzdálený přístup k PLC“)

Vlastník rizika (Risk Owner)

Role odpovědná za řízení daného rizika.
(př. IT Manager, Vedoucí provozu, Security Officer)
Nepoužívejte osobní jména – pouze role.

Popis rizika

Stručný popis scénáře rizika:

- co se může stát
- čeho se to týká
- proč je to problém

Dopad
Hodnocení závažnosti následků při realizaci rizika.
Hodnoty: Nízký / Střední / Vysoký

Pravděpodobnost
Odhad pravděpodobnosti výskytu rizika.
Hodnoty: Nízká / Střední / Vysoká

Úroveň rizika
Automaticky vypočtená kombinace Dopadu a Pravděpodobnosti dle Risk Matrix.
Slouží jako objektivní velikost rizika.
Hodnoty: Nízká / Střední / Vysoká

Priorita
Určuje pořadí řešení rizik z pohledu organizace.
Může zohlednit kapacity, rozpočet nebo strategický význam.
Počítá se automaticky z úrovně rizika.

Poznámka:
Úroveň rizika = velikost hrozby
Priorita = pořadí řešení

Stávající opatření

Popis již existujících kontrol nebo opatření, která riziko snižují.
(př. firewall, fyzické uzamčení, řízení přístupů)

Doporučené opatření
Návrh dalších kroků ke snížení rizika.
(př. zavést VPN, segmentaci sítě, aktualizaci firmware)

Stav
Aktuální fáze řízení rizika:
- Otevřené
- Řeší se
- Akceptované
- Uzavřené

Datum revize
Datum poslední kontroly nebo aktualizace záznamu rizika.
Slouží jako auditní stopa.

Číselníky
Hodnoty pro Dopad, Pravděpodobnost, Stav a další rozevírací seznamy jsou definovány v listu Číselníky.
Běžní uživatelé je neupravují.

Rozsah CORE verze
Tato CORE verze:

- používá jednoduchou 3×3 Risk Matrix
- neobsahuje finanční kvantifikaci rizik
- neřeší residual risk po opatřeních
- neobsahuje vazbu na konkrétní bezpečnostní kontroly ISO Annex A

Tyto oblasti patří do rozšířených verzí.

Doporučení

- Risk Register revidujte pravidelně (minimálně 1× ročně)
- Zaměřte se nejdříve na klíčová aktiva
- Rizika, která vedení vědomě přijímá, označte jako **Akceptované**
- Uzavřená rizika nemažte – slouží jako historický záznam

Dokonalost není cílem.
Řízený přehled rizik je cílem.

Volitelné vizuální zvýraznění

Úroveň rizika:
Nízká → #D4EDDA
Střední → #FFE5B4
Vysoká → #F8D7DA

Stav rizika:
Řeší se → #FFF3CD
Akceptované → #E8F0FE
Uzavřené → #E9ECEF

Použití barev je nepovinné a nemá vliv na význam dat.