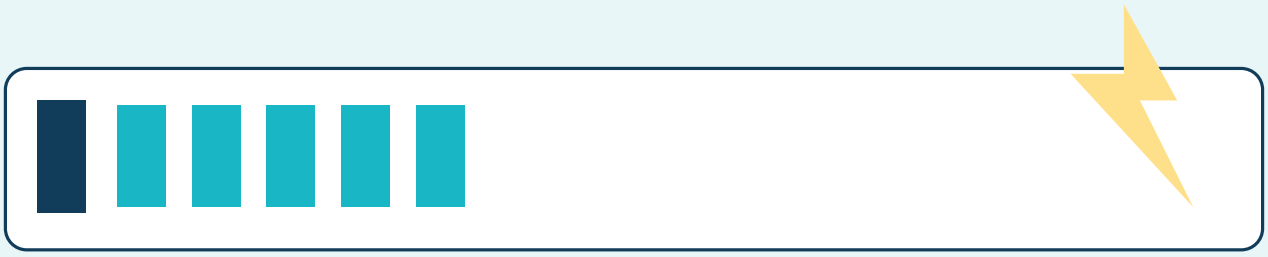
BESS Cyber Readiness Checklist

Je vaše bateriové úložiště připravené na NIS2, nový zákon o kybernetické bezpečnosti a bezpečný provoz v prostředí flexibility a SVR?



BESS | EMS | SCADA | SVR

Praktický checklist pro provozovatele BESS, FVE, EMS, SCADA, flexibility a SVR.
Vyhodnocení za 5-10 minut. Výstupem je rychlé skóre rizika a doporučené další kroky.

Proč se o kybernetickou bezpečnost BESS zajímat

Moderní bateriové úložiště už není pouze baterie. V praxi jde o digitálně řízené energetické zařízení, které komunikuje s EMS, SCADA, dispečinkem, cloudem výrobce, agregátorem flexibility a někdy i s dalšími systémy provozovatele.

Technologie

BESS, EMS, SCADA, měření, datové přenosy a vzdálený dohled.

Provoz

Dostupnost technologie, zálohy, obnova po incidentu a odpovědnosti.

Regulace

NIS2, nZKB, režim povinností a řízení dodavatelů.

Kdy téma typicky začne být důležité

- ☐ BESS má výkon nad 100 kW a je připojena do distribuční nebo přenosové soustavy.
- ☐ Technologie je řízena vzdáleně nebo přes cloud dodavatele.
- ☐ Projekt je připravován pro flexibilitu, agregaci nebo SVR.
- ☐ Výroba nebo provoz zákazníka je citlivý na výpadky, mikrovýpadky nebo ztrátu řízení.

Hlavní myšlenka: Kyberbezpečnost BESS není jen IT problém. Je to projektové, provozní, smluvní a obchodní riziko.

Rychlý screening: týká se vás to?

Zaškrtněte všechna tvrzení, která platí pro váš projekt nebo provoz.

- ☐ Provozujete nebo připravujete bateriové úložiště.
- ☐ Výkon BESS přesahuje 100 kW.
- ☐ Úložiště je připojeno k distribuční nebo přenosové soustavě.
- ☐ Využíváte EMS nebo SCADA.
- ☐ Dodavatel má vzdálený přístup k technologii.
- ☐ Součástí řešení jsou cloudové služby.
- ☐ Plánujete zapojení do flexibility nebo SVR.
- ☐ BESS komunikuje s agregátorem, dispečinkem nebo obchodním systémem.
- ☐ Používáte sdílené nebo technické účty.
- ☐ Není jasně oddělena IT a OT síť.

Orientační výsledek:
4 a více odpovědí ANO znamená, že doporučujeme provést detailnější posouzení architektury, přístupů, dodavatelů a provozních procesů.

10 nejčastějších rizik u BESS projektů

1. **Trvalý vzdálený přístup dodavatele**
2. **Sdílené účty a nejasná odpovědnost**
3. **Chybějící MFA nebo bezpečný ekvivalent**
4. **Společná IT a OT síť**
5. **Nedostatečné logování a monitoring**
6. **Chybějící zálohy konfigurací**
7. **Nejasné role a odpovědnosti**
8. **Neřízené aktualizace a zranitelnosti**
9. **Chybějící incident management**
10. **Slabě ošetřené smlouvy s dodavateli**

Self-audit: 12 kontrolních otázek

Oblast	Kontrolní otázka	ANO	NE
Řízení	Má organizace určenou odpovědnou osobu za kybernetickou bezpečnost?	☐	☐
Řízení	Existuje přehled BESS/EMS/SCADA systémů a návazných aktiv?	☐	☐
Řízení	Jsou pravidelně vyhodnocována rizika?	☐	☐
Přístupy	Má každý uživatel vlastní účet?	☐	☐
Přístupy	Jsou oddělené běžné a administrátorské účty?	☐	☐
Přístupy	Je používáno MFA, certifikát nebo jiný silný způsob ověření?	☐	☐
Technologie	Je OT síť oddělena od kancelářské IT sítě?	☐	☐
Technologie	Jsou vzdálené přístupy omezené a evidované?	☐	☐
Technologie	Jsou evidovány změny konfigurace?	☐	☐
Incidenty	Existuje postup pro řešení incidentů?	☐	☐
Incidenty	Jsou vytvářeny a testovány zálohy konfigurací?	☐	☐
Incidenty	Jsou uchovávány provozní a bezpečnostní logy?	☐	☐

Vyhodnocení skóre

0-4 ANO

Vysoké riziko. Doporučujeme provést detailnější posouzení a rychle řešit přístupy, segmentaci, zálohy a incident management.

5-8 ANO

Střední riziko. Základní prvky existují, ale pravděpodobně chybí propojení do uceleného systému řízení bezpečnosti.

9-12 ANO

Nižší riziko. Projekt má základní předpoklady pro bezpečný provoz, ale doporučuje se ověřit realitu vůči dokumentaci.

Doporučené kroky podle priority

0-3 měsíce

Identifikovat kritická aktiva, zkontrolovat vzdálené přístupy, ověřit účty dodavatelů a zálohy.

3-12 měsíců

Zavést nebo doplnit MFA, segmentaci IT/OT, monitoring a základní incident proces.

12+ měsíců

Rozvíjet řízení rizik, testovat obnovu provozu, aktualizovat dokumentaci a smluvní požadavky.

BESS Cyber Readiness Audit

Audit pomáhá investorům, provozovatelům a průmyslovým podnikům identifikovat technická, provozní a regulatorní rizika související s provozem BESS, EMS, SCADA a vzdáleným řízením.

Co posuzujeme

Regulační dopad, architekturu BESS, EMS a SCADA, vzdálené přístupy, oddělení IT/OT, účty, logování, zálohy, incident management a dodavatele.

Co získáte

Stručné regulační posouzení, GAP analýzu, seznam rizik, priorizaci kroků a přehledný report pro vedení firmy nebo investora.

Chcete zjistit skutečný stav vašeho projektu?
Navštivte SVRporadce.cz a vyžádejte si BESS Cyber Readiness Audit.

Poznámka k použití dokumentu

Tento checklist slouží jako orientační technicko-obchodní materiál. Nenahrazuje právní stanovisko, závazné posouzení NÚKIB, certifikovaný audit kybernetické bezpečnosti ani implementaci bezpečnostních opatření podle konkrétních právních předpisů.

Doporučené použití

- ☐ První interní screening projektu BESS nebo FVE+BESS.
- ☐ Podklad pro diskusi mezi investorem, provozovatelem, IT/OT týmem a dodavatelem technologie.
- ☐ Vstupní materiál před detailní analýzou architektury, přístupů a provozních procesů.

SVRporadce.cz
Odborný portál pro BESS, UPS, mikrovýpadky, flexibilitu a SVR.

Web: www.svrporadce.cz
Služba: BESS Cyber Readiness Audit