Kyberbezpečnost CRA v eIntranetu

Příručka pro výrobce: proč a jak začít – krok za krokem

Nařízení (EU) 2024/2847 o kybernetické odolnosti (Cyber Resilience Act) · modul Kyberbezpečnost CRA · verze 1.0, září 2026

Tato příručka provede vaši firmu prvními kroky v modulu **Kyberbezpečnost CRA** – od zapnutí modulu přes registr produktů a gap analýzu až po připravenost hlásit zneužité zranitelnosti do 24 hodin. U každého kroku najdete, proč ho dělat, co přesně udělat a co z toho vznikne.

> **Nejdřív to naléhavé:** povinnost hlásit platí od 11. 9. 2026, i pro výrobky uvedené na trh dříve. Pokud ještě nemáte zástupce na platformě ENISA a postup na 24 hodin, začněte kroky 1, 2, 3 a 6. Registr produktů, gap analýzu a dokumentaci pak doplňujte postupně – celé nařízení platí od 11. 12. 2027.

1. Proč řešit CRA právě teď

Nařízení (EU) 2024/2847 (Cyber Resilience Act, CRA) se týká každého **produktu s digitálními prvky**, který se uvádí na trh EU: strojů s řídicí elektronikou, elektrotechniky, zařízení IoT i softwaru prodávaného jako produkt. Nejde tedy jen o IT firmy – týká se i běžných strojírenských a elektrotechnických výrobců.

- **Hlásit se musí už teď.** Od 11. 9. 2026 musí výrobce hlásit aktivně zneužívané zranitelnosti a závažné incidenty svých produktů na jednotné platformě agentury ENISA (SRP): včasné varování do 24 hodin, oznámení do 72 hodin a závěrečnou zprávu. Platí to i pro produkty uvedené na trh dříve, a i po skončení jejich podpory.
- **Od 11. 12. 2027 platí celé nařízení.** Základní požadavky na kybernetickou bezpečnost (příloha I), řešení zranitelností po celou dobu podpory, technická dokumentace, EU prohlášení o shodě a označení CE. U hardwaru se posuzuje každý kus – i starší model dodaný po tomto datu musí CRA plně splňovat. Týká se to i zakázek, které podepisujete dnes.
- **Sankce jsou vysoké.** Za porušení základních požadavků a povinností podle čl. 13 a 14 hrozí pokuta až 15 mil. EUR nebo 2,5 % celosvětového ročního obratu, podle toho, co je vyšší.
- **Ptají se odběratelé.** Velcí zákazníci, zejména němečtí výrobci, už dnes chtějí SBOM, dobu podpory a doklad o připravenosti na CRA. Kdo odpoví rychle a doloženě, má výhodu.

Klíčová data

Datum	Co začíná platit	Co to znamená pro vás
11. 6. 2026	Pravidla pro oznámené subjekty (kapitola IV)	Oznámené subjekty se připravují na posuzování shody. U produktů, které je potřebují (krok 4), plánujte posouzení s předstihem.
11. 9. 2026	Hlášení podle čl. 14	Zástupci na platformě SRP, rozhodovatel, postup na 24 hodin a evidence případů.
20. 1. 2027	Nařízení o strojních zařízeních (EU) 2023/1230	Požadavky 1.1.9 a 1.2.1 na ochranu řídicího systému proti poškození a neoprávněné manipulaci. EU prohlášení podle CRA pro ně presumpci shody nedává.
11. 12. 2027	Celé nařízení CRA	Základní požadavky, technická dokumentace, EU prohlášení o shodě, kontaktní místo a politika koordinovaného zveřejňování zranitelností.

2. Co vám modul dá

Modul **Kyberbezpečnost CRA** sbírá na jednom místě vše, co po vás nařízení chce doložit, a hlídá lhůty. Každá změna se zapisuje do auditní stopy (kdo, kdy a co změnil) a schválené dokumenty se ukládají jako zmrazené PDF s kontrolním otiskem SHA-256, takže dozoru doložíte i to, v jakém znění platily.

Co po vás CRA chce	Kde to v modulu najdete
Vědět, kterých produktů se CRA týká a jak	**Produkty s digitálními prvky** – režim CRA, kategorie, postup posuzování shody, doba podpory
Zjistit, co firmě chybí, a naplánovat nápravu	**Gap analýza CRA** – 50 otázek, skóre ve třech časových hladinách, akční plán, zpráva PDF
Hlásit zneužité zranitelnosti a incidenty (čl. 14)	**Hlášení čl. 14** – případy, lhůty, anglický formulář pro SRP, upomínky, spis

Co po vás CRA chce	Kde to v modulu najdete
Přijímat hlášení zranitelností (kontaktní místo, CVD)	**Kontaktní místo pro zranitelnosti** – evidence, veřejný formulář, security.txt, politika CVD
Soupis komponent (SBOM) a sledování zranitelností	**Verze a SBOM** v detailu produktu a záložka **Zranitelnosti** – denní porovnání s databázemi OSV a NVD a s katalogem zneužívaných zranitelností (KEV)
Technická dokumentace a EU prohlášení o shodě	**Shoda a technická dokumentace** – požadavky přílohy I, rizika, příloha VII, EU prohlášení, informace pro uživatele

3. Než začnete

Připravte si zodpovědné osoby a podklady – modul pak vyplníte rychle:

- **Odpovědnou osobu za CRA** – vlastníka tématu, který bude mít v modulu nejvyšší oprávnění.
- **Rozhodovatele o zjištění zneužití a jeho zástupce** – někoho, kdo i večer a o víkendu rozhodne, jestli se hlásí.
- **Zástupce pro platformu ENISA (SRP)** – aspoň dvě osoby, kteří si zřídí EU Login s vícefázovým ověřením.
- **Seznam produktů** – typy a varianty, země prodeje, hlavní zákazníky a plánované dodávky po 11. 12. 2027.
- **SBOM** – soupis softwarových komponent ze sestavení nebo od dodavatelů. Pokud ho zatím nemáte, gap analýza ukáže, co chybí.
- **Volitelně konzultanta** – gap analýzu může vést externí konzultant přímo v systému.

4. Krok za krokem

Kroky jsou seřazené tak, jak na sebe navazují. Kroky 1–3 a 6 zajistí připravenost na hlášení, která platí už teď; kroky 4, 5 a 7–11 vás dovedou k plné shodě do prosince 2027.

Krok 1: Aktivujte modul a přidělte práva

Proč: Dokud modul nezapnete, v levém menu se Vám nezobrazí. Práva určují, kdo smí nahlásit podezření, kdo řeší případy a kdo spravuje nastavení.

Jak na to:

1. Otevřete **Nastavení → Povolené moduly** a aktivujte modul **Kyberbezpečnost CRA**. Kdo modul zapne, dostane k němu plná přístupová práva.
2. V levém menu otevřete **Kyberbezpečnost CRA** a přes odkaz **Nastavení** v záhlaví přejděte do nastavení modulu (nebo využijte možnost **Nastavení → Kyberbezpečnost CRA**).
3. V části **Přístupová práva** přidělte uživatelům úroveň podle tabulky. Práva lze přidělit i podle pozic.
4. Konzultanta založte jako externího uživatele s úrovní **Správa** a přístupem k modulu.

Úroveň	Co smí	Typicky kdo
Čtení a nahlášení podezření	Uživatel vidí modul a nahlásí podezření.	Servis, podpora, obchod – každý, kdo se o problému může dozvědět první.
Řešení	Produkty, gap analýza, případy a podání do SRP.	Vývoj, kvalita, bezpečnost produktu.
Správa	Navíc finalizace gap analýzy, oprava času zjištění, zrušení případu a koš.	Vedoucí vývoje nebo kvality, konzultant.
Nastavení	Navíc nastavení modulu, zástupci a práva.	Odpovědná osoba za CRA.

> **Tip:** Nahlášení podezření dejte všem, kdo mluví se zákazníky. Signál, který nikdo nezapíše, nikdo neposoudí – a lhůta přitom může běžet.

Krok 2: Vyplňte nastavení modulu

Proč: Údaje z nastavení se propisují do EU prohlášení o shodě, do informací pro uživatele i do hlášení. Upozornění na signály a termíny musí chodit správným lidem.

Jak na to (Kyberbezpečnost CRA → Nastavení → Obecná nastavení):

1. **Údaje výrobce pro CRA** – obchodní jméno a adresa, které se uvedou v prohlášení a v informacích pro uživatele.

2. **Hlášení podle čl. 14 CRA** – stát hlavní provozovny (určuje koordinující CSIRT; u české firmy NÚKIB), velikost podniku, **kdo rozhoduje o zjištění zneužití** a jeho zástupce, cíl pro prvotní posouzení signálu (výchozí 24 hodin) a příjemci upozornění.

3. **Kontaktní místo pro hlášení zranitelností** – kontaktní e-mail (například security@vase-firma.cz), politika koordinovaného zveřejňování zranitelností podle šablony a soubor security.txt, který modul vytvoří sám.

4. **AI pomocníci** – ve výchozím stavu je vypnuto. Zapněte je, jen pokud firma souhlasí, že podklady včetně informací o neopravených zranitelnostech odcházejí externímu poskytovateli AI.

> **Dobré vědět:** koordinující CSIRT určuje hlavní provozovna, tedy místo, kde se o kybernetické bezpečnosti produktů převážně rozhoduje (čl. 14 odst. 7). Česká dceřiná společnost, o jejíž produktech se rozhoduje v Německu, tak může hlásit německému CSIRT.

Krok 3: Určete zástupce pro platformu ENISA (SRP)

Proč: Hlášení se podává na jednotné platformě pro podávání hlášení (SRP) agentury ENISA. Platforma nemá rozhraní pro automatické podání, takže hlášení musí podat člověk přihlášený přes EU Login. Bez registrovaného zástupce lhůtu 24 hodin nestihnete.

Jak na to:

1. Každý zástupce se zaregistruje na portálu SRP (portal.cra-srp.enisa.europa.eu) přes EU Login s vícefázovým ověřením. Vazbu zástupce na vaši firmu ověřuje koordinující CSIRT.

2. V nastavení modulu v části **Zástupci pro platformu ENISA (SRP)** klikněte na **Přidat zástupce** a vyplňte uživatele, roli (primární nebo sekundární) a datum ověření CSIRT.

3. Každý zástupce si pravidelně vyzkouší přihlášení do SRP a potvrdí to na přehledu modulu tlačítkem **Přihlášení do SRP funguje**. Kontrolní seznam připravenosti chce test mladší než 90 dní.

> **Tip:** SRP dovoluje jednoho primárního a až 20 sekundárních zástupců – určete aspoň dva. Pokud používáte modul Dovolené, upozorní vás modul 14 dní předem na dny, kdy nebude k dispozici žádný zástupce ani rozhodovatel. Koncept hlášení v SRP vidí jen jeho autor, sdílený koncept proto vedete v modulu.

Krok 4: Zapište produkty do registru

Proč: Registr produktů definuje platné údaje o produktech. Z údajů modul odvodí, v jakém režimu CRA produkt je, jaký postup posuzování shody přichází v úvahu a do kterých států se hlásí.

Jak na to (záložka Produkty s digitálními prvky → Přidat produkt):

1. **Identifikace** – oficiální název (použije se v SRP a v prohlášení), typové označení, varianty (objednací kódy pod jednou dokumentací) a druh: hardware s digitálními prvky, nebo samostatný software.

2. **Rozsah** – datové spojení včetně servisních rozhraní (USB, sériová linka, diagnostický port). Produkt bez jakéhokoli datového spojení nebo s vlastní úpravou (zdravotnické prostředky, motorová vozidla, letectví…) označte jako mimo rozsah a vyberte důvod.

3. **Klasifikace** – kategorie (výchozí, důležitý produkt třídy I nebo II, kritický produkt) a položka přílohy III nebo IV s povinným odůvodněním. U vybrané položky modul ukáže doslovný technický popis kategorie z prováděcího nařízení (EU) 2025/2392.

4. **Trh a podpora** – stav produktu, datum prvního uvedení na trh, zda budete nové kusy dodávat i po 10. 12. 2027, očekávaná doba užívání, konec doby podpory s odůvodněním a členské státy, kde se produkt prodává.

5. **Související předpisy** – označte rádiové zařízení (RED) a strojní zařízení; modul pak ukáže, co z nich platí a kdy.

6. V detailu produktu přidejte **zákazníky (instalovanou bázi)** z CRM – hodí se pro informování uživatelů a pro státy v hlášení.

V detailu produktu pak uvidíte **režim CRA** (mimo rozsah, jen hlášení podle čl. 14, nebo plná CRA od 11. 12. 2027), doporučené postupy posuzování shody a upozornění k době podpory.

Kategorie produktu	Postup posuzování shody
Výchozí kategorie (mimo přílohy III a IV)	Stačí vnitřní kontrola (modul A).
Důležitý produkt – třída I	Modul A jen při plném použití harmonizované normy, společné specifikace nebo certifikace citované v Úředním věstníku (k září 2026 žádná citovaná není); jinak moduly B a C nebo modul H.
Důležitý produkt – třída II	Moduly B a C, modul H, nebo evropský certifikační systém.

Kategorie produktu	Postup posuzování shody
Kritický produkt (příloha IV)	Evropský certifikační systém podle čl. 8 odst. 1; dokud ho Komise nestanoví, platí postupy jako pro třídu II.

> **Tip:** rozhoduje hlavní funkce produktu jako celku. Vestavěná komponenta – například síťový modul nebo vestavěný prohlížeč – z produktu důležitý produkt nedělá. A doba podpory má odpovídat očekávané době užívání: pět let je zákonné minimum, ne výchozí hodnota; u strojů a PLC bývá doba užívání mnohem delší.

Krok 5: Proveďte gap analýzu

Proč: Gap analýza porovná současný stav firmy a produktů s požadavky CRA a ukáže, co chybí, v jakém pořadí to řešit a kolik to bude stát. Hodnotí tři časové hladiny: povinnosti platné teď, požadavky strojního nařízení od 20. 1. 2027 a plnou CRA od 11. 12. 2027.

Jak na to (záložka Gap analýza CRA → Nová gap analýza):

1. Zadejte název, hodnotitele (vlastní pracovník, nebo konzultant) a produkty, kterých se analýza týká.
2. Projděte otázky katalogu v sedmi oblastech. U každé otázky je nápověda, odkaz na článek nařízení a očekávané důkazy.
   - rozsah, role a klasifikace; hlášení podle čl. 14; řešení zranitelností;
   - bezpečnostní vlastnosti produktu; dokumentace a informace pro uživatele;
   - dodavatelský řetězec a open source; organizace a řízení.
3. Firma vyplní **sebehodnocení**, konzultant **ověřené hodnocení**. K otázkám připojte podklady (důkazy) a zapište **rozhovory** s lidmi z firmy.
4. U nesplněných bodů sestavte **akční plán**: priorita, odpovědná osoba, termín, pracnost a externí náklady. Z opatření můžete rovnou založit úkol.
5. Stav **Návrh k připomínkám** vytvoří zprávu s vodoznakem NÁVRH. Po připomínkách zvolte **Finalizovat** – zpráva se uloží jako zmrazené PDF a odpovědi se zamknou. Akční plán zůstává upravitelný.

Výstupy: zpráva PDF (manažerské shrnutí, skóre po oblastech a produktech, klasifikační memo, roadmapa do prosince 2027), seznam podkladů pro sběr důkazů (PDF a XLSX) a akční plán s roadmapou (XLSX).

> **Tip:** finální gap analýzu už nejde znovu otevřít. Další kolo založte jako novou gap analýzu s volbou **Navázat na předchozí gap analýzu** – odpovědi se převezmou jako výchozí sebehodnocení a uvidíte vývoj skóre v čase.

Krok 6: Připravte se na hlášení do 24 hodin

Proč: Lhůty podle čl. 14 běží v kalendářních hodinách – i o víkendu a o dovolené. Připravenost je potřeba prověřit dřív, než přijde skutečný případ.

Jak na to (záložka Přehled CRA):

1. Projděte kontrolní seznam **Připravenost na hlášení (čl. 14)**: zástupci ověření CSIRT, vyzkoušené přihlášení do SRP, rozhodovatel a jeho zástupce, příjemci upozornění, produkty na trhu s vyplněnými státy, klasifikací a režimem, cvičení za posledních 12 měsíců a kontaktní místo.
2. Stáhněte **Postup na 24 hodin (PDF)** – jednostránkový postup s kontakty a kroky od signálu po závěrečnou zprávu. Vytiskněte ho a dejte rozhodovateli a zástupcům.
3. Nacvičte postup: **Nahlásit podezření** a zaškrtněte **Cvičení**. Cvičný případ projde celým postupem, nic se nepodává, nese vodoznak CVIČENÍ a nepočítá se do statistik.

> **Tip:** cvičení jednou za rok odhalí chybějící přístupy, kontakty a podklady dřív, než je budete opravdu potřebovat.

Krok 7: Když přijde podezření – případ podle čl. 14

Proč: Modul hlídá lhůty, připraví anglické texty pro SRP a vede spis, kterým doložíte, že jste postupovali včas.

Jak na to:

1. Kdokoli s právem čtení klikne na **Nahlásit podezření** (v záhlaví modulu nebo v detailu produktu) a popíše, co se stalo. Rozhodovatel dostane e-mail.
2. Rozhodovatel signál **posoudí** bez zbytečného odkladu. Výsledek je **zjištěno**, **sledujeme** (s datem dalšího posouzení), nebo **nehlásíme** s důvodem – například „Zranitelnost v našem produktu nelze zneužít“.
3. Po potvrzení zjištění běží lhůty podle tabulky. Modul ukazuje odpočet a posílá upomínky e-mailem – ve výchozím nastavení 12, 4 a 1 hodinu před termínem.

4. Pro každou fázi vyplňte formulář hlášení. Pole odpovídají glosáři platformy SRP a jsou anglicky; údaje o produktu a případu se předvyplní z evidence. Tlačítka **Kopírovat** a **Kopírovat vše** usnadní přenos do SRP. Máte-li zapnuté AI pomocníky, navrhne anglické texty z českého popisu tlačítko **Navrhnout anglické texty**.

5. Po podání v SRP klikněte na **Zaznamenat podání**, zapište čas podání a číslo hlášení ze SRP a přiložte potvrzení. Podané hlášení se zamkne; další změny jdou jen jako aktualizace na žádost CSIRT.

6. Jakmile je k dispozici náprava nebo zmírňující opatření (aktualizace, obejití, návod), zapište **Náprava nebo zmírnění** – u zranitelnosti od toho běží lhůta závěrečné zprávy.

7. **Zaznamenat informování** dotčených uživatelů (čl. 14 odst. 8): rozsah, kanál a text ze šablony v češtině, angličtině nebo němčině. Příjemci se nabídnou z instalované báze produktu.

8. Případ uzavřete. **Spis (PDF)** shrne časovou osu, podané fáze proti lhůtám, souběžná hlášení a historii.

Lhůty hlášení

Fáze hlášení	Lhůta	Počítá se od
Včasné varování	24 hodin	zjištění
Oznámení	72 hodin	zjištění
Závěrečná zpráva – zranitelnost	14 dní	dostupnosti nápravného nebo zmírňujícího opatření
Závěrečná zpráva – závažný incident	1 měsíc	podání oznámení

> **Co je „zjištění“:** rozumná jistota, že je zneužíván **váš** produkt. Shoda CVE v SBOM, výsledek skenu ani záznam v katalogu zneužívaných zranitelností samy o sobě zjištěním nejsou – jsou podnětem k okamžitému posouzení. V případu si odškrtejte i **souběžná hlášení**: porušení zabezpečení osobních údajů (ÚOOÚ do 72 hodin), incident vlastních systémů (NÚKIB) nebo smluvní oznámení odběratelům.

Krok 8: Zřiďte kontaktní místo pro hlášení zranitelností

Proč: Od 11. 12. 2027 musí mít výrobce kontaktní místo a zveřejněnou politiku koordinovaného zveřejňování zranitelností (čl. 13 odst. 17 a příloha I část II). Už dnes je to hlavní zdroj signálů pro hlášení podle čl. 14 – zákazníci a výzkumníci musí vědět, kam zranitelnost nahlásit.

Jak na to:

1. Na záložce **Kontaktní místo pro zranitelnosti** zapisujte přijatá hlášení tlačítkem **Zapsat přijaté hlášení** (e-mail, zákazník, CSIRT, výzkumník). Každé dostane číslo VR-RRRR-NNN a vlastní stav od přijetí po vyřešení.

2. Pokud z hlášení vyplyne podezření na zneužití, použijte **Založit případ podle čl. 14** – vznikne signál s odkazem na hlášení.

3. V nastavení modulu upravte **politiku koordinovaného zveřejňování zranitelností** podle šablony a zveřejněte ji na webu. Vygenerovaný **security.txt** uložte na web jako /.well-known/security.txt a jednou ročně ho obnovte.

4. Volitelně zapněte **Veřejný formulář pro hlášení zranitelností** – stránku bez přihlášení na adrese https://<vaše doména>/Security s captchou a limitem hlášení z jedné IP adresy. Oznamovatel dostane potvrzení s číslem hlášení, vy upozornění.

Krok 9: Evidujte verze produktů a SBOM

Proč: CRA vyžaduje soupis softwarových komponent (SBOM) aspoň pro závislosti nejvyšší úrovně a odběratelé často chtějí SBOM podle BSI TR-03183-2. Ze SBOM modul každý den hledá zranitelnosti.

Jak na to (detail produktu → Verze a SBOM → Přidat verzi, pak detail verze):

1. **Importovat SBOM** – nahrajte soubor ze sestavení (CycloneDX 1.4–1.6 nebo SPDX 2.2, 2.3 či 3.0.1 ve formátu JSON).

2. Zkontrolujte **náhled**: počet komponent, rozdíl proti předchozí verzi a kontrolu kvality podle minima CRA a BSI TR-03183-2. Komponenty se zapíšou až po **Potvrdit import**.

3. Co nástroj pro SBOM nevidí (RTOS, bootloader, staticky přilinkované knihovny), doplňte tlačítkem **Přidat komponentu**. Nový import ruční komponenty nezmění.

4. Pro zákazníky vytvoříte SBOM tlačítkem **Exportovat CycloneDX 1.6**.

> **Tip:** pro vyhodnocení komponenty je třeba identifikátor purl s verzí nebo CPE. Detail verze ukáže, kolik komponent vyhodnotit nejde a proč.

Krok 10: Posuzujte zjištěné zranitelnosti

Proč: Modul jednou denně porovná komponenty verzí s veřejnými databázemi OSV a NVD a s katalogem aktivně zneužívaných zranitelností (KEV). O problému se tak dozvíte dřív, než vám ho nahlásí zákazník.

Jak na to (záložka Zranitelnosti):

1. Každé zjištění má termín posouzení podle závažnosti, aktivně zneužívané (KEV) do jednoho dne. O novém zjištění z katalogu KEV přijde e-mail hned.

2. **Posoudit zjištění** – stav **Posuzuje se**, **Zasaženo**, **Nezasaženo** (s odůvodněním) nebo **Opraveno**. Stejné posouzení lze použít pro více zjištění najednou (**Posoudit vybrané**) a u stejné komponenty v další verzi produktu se převezme.

3. Jakmile máte rozumnou jistotu, že je zneužíván váš produkt, klikněte na **Založit případ čl. 14**. Případ se nikdy nezakládá sám.

> **Tip: f**iltr **Jen aktivně zneužívané** ukáže to nejnaléhavější.

Krok 11: Shoda a technická dokumentace (do 11. 12. 2027)

Proč: Před uvedením na trh podle plné CRA musí mít každý produkt technickou dokumentaci (příloha VII), posouzení kybernetických rizik a EU prohlášení o shodě. Dokumentaci je třeba uchovávat 10 let od uvedení na trh, nebo po dobu podpory, je-li delší.

Jak na to (detail produktu → Shoda a technická dokumentace → Otevřít):

1. **Základní požadavky (příloha I)** – u každého požadavku stav, způsob splnění a důkazy (přílohy a směrnice z modulu Dokumenty). Volbu „neuplatňuje se“ lze použít jen u bezpečnostních vlastností (část I bod 2) a vždy s odůvodněním.

2. **Posouzení kybernetických rizik** – aktivum, hrozba, pravděpodobnost a dopad (matice 5 × 5), opatření s vazbou na požadavky a zbytkové riziko.

3. **Technická dokumentace (příloha VII)** – oddíly 1–8. Co modul zná (produkt, SBOM, rizika, doba podpory), doplní sám; ostatní dopíšete.

4. **EU prohlášení o shodě** (příloha V) v češtině, angličtině a němčině. Podléhá-li produkt i dalším předpisům Unie, které vyžadují EU prohlášení (například RED, EMC nebo strojní nařízení), zaškrtněte je – vydá se jedno prohlášení za všechny s odkazy na Úřední věstník (čl. 28 odst. 3). K dispozici je i zjednodušené prohlášení (příloha VI).

5. **Informace pro uživatele (příloha II)** v češtině, angličtině a němčině, včetně konce doby podpory.

6. **Schválení** – každá schválená verze dokumentu se uloží jako zmrazené PDF s otiskem SHA-256, časem a jménem schvalovatele. Produkt s vydaným prohlášením nejde smazat.

Krok 12: Běžný provoz

- **Odznak u položky menu** ukazuje, co čeká: nové signály, blížící se nebo prošlé termíny hlášení, nová hlášení zranitelností a zjištění po termínu posouzení.
- **Karta na nástěnce** shrne otevřené případy s nejbližším termínem, připravenost a skóre poslední gap analýzy.
- **Jednou ročně** udělejte cvičení, vyzkoušejte přihlášení do SRP, obnovte security.txt a projděte **Končící podporu** na přehledu – uživatelé se o konci podpory mají dozvědět předem.
- **Auditní stopa** – každá změna je zapsaná (kdo, kdy, co). Smazané záznamy najdete pod tlačítkem **Smazané** v záhlaví modulu; obnovit je může správce.

5. Co modul nedělá

- **Nepodává hlášení do SRP za vás.** Platforma ENISA nemá rozhraní pro automatické podání; modul připraví texty a vede záznam o podání.
- **Nenahrazuje právní posouzení.** Klasifikace, zprávy a prohlášení jsou podklad – odpovědnost za ně nese výrobce. Příručka popisuje předpisy k září 2026; závazné je jejich znění v Úředním věstníku EU.
- **Nevytváří SBOM z binárních souborů a nedělá penetrační testy.** SBOM přichází ze sestavení nebo od dodavatelů.

> **Potřebujete pomoc?** Se zavedením modulu i s gap analýzou vám rádi pomůžeme – kontakty najdete v zápatí.