Úvod

Tento dokument se zabývá návrhem doplnění metodického dokumentu – Metodický návod ke zpracování posouzení rizik systémů zásobování pitnou vodou podle zákona o ochraně veřejného zdraví (Metodika posouzení rizik).

Hlavní myšlenkou za navrhovanými změnami je implementování základů problematiky kybernetické a částečně i fyzické bezpečnosti. Je důležité zdůraznit skutečnost, že návrhy změn jsou připravovány během „nejisté" doby implementace Směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (NIS2) do českého legislativního rámce. Prozatím nejsou přesně jistá kritéria pro subjekty, kterých se začnou nová pravidla týkat, ale je naprosto jisté, že dojde k drastickému nárůstu subjektů povinných dodržovat nová opatření.

Implementace NIS2 bude řešit oblast kybernetické bezpečnosti velice zevrubně, a tudíž nemá velký smysl, aby se navrhované změny snažily „konkurovat" těmto novým pravidlům. Pokud subjekt bude implementovat opatření plynoucí z NIS2, navrhované změny by pro něj neměly znamenat dodatečnou práci. Tyto změny jsou primárně zaměřeny na malé subjekty. Autoři návrhu změn si uvědomují skutečnost a priority praxe, a tudíž je snaha nastavit pouze úplný základ a donutit osoby zodpovědné za vypracování rizik zamyslet se nad problematikou kybernetické a fyzické bezpečnosti ve svém provozu.

Kolektiv autorů:	Ing. Ondřej Dolejš (MBI z.ú.) Ing. Helena Sochorová, Ph.D. (ÚHAV v.v.i.)	Datum zpracování: 1.11.2023
Koordinátor projektu:	Ing. Petr Dolejš, Ph.D. (VŠCHT Praha) Email: dolejsp@vscht.cz	

Vytvořeno v rámci projektu: kód, finanční podpora	VB01000006; Tento projekt TWIN SKIN – Digitální dvojče úpravny vody pro efektivní řízení rizik kritické vodárenské infrastruktury byl podpořen Ministerstvem vnitra ČR z Programu bezpečnostního výzkumu ČR 2021-2026: vývoj, testování a evaluace nových bezpečnostních technologií (SECTECH).

Doplnění 1. Legislativní požadavky – NIS2

Smyslem tohoto doplnění je informovat o existenci NIS2 a subjekty, které se jí musí řídit ujistit, že mohou použít již zpracované materiály. Pro subjekty, které nespadají pod tato pravidla, je tato část pouze informativní, například pokud by se jejich podnik blížil podmínkám velikosti podniku.

Směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (NIS2) byla do českého legislativního rámce implementována zejména pomocí:

- Vyhláška o regulovaných službách
- Nový zákon o kybernetické bezpečnosti
- Vyhláška o bezpečnostních opatřeních pro vyšší režim
- Vyhláška o bezpečnostních opatřeních pro nižší režim

Aby subjektu vznikla povinnost se těmito opatřeními řídit, musí spadat do regulovaného odvětví. Pro odvětví vodohospodářství se jedná zejména o oblast:

- Pitná voda – Dodavatelé a distributoři vody určené k lidské spotřebě, kromě těch, pro které je to vedlejší činnost k jejich hlavní činnosti zabývající se distribucí jiných komodit a zboží.
- Odpadní voda – Subjekty shromažďující, vypouštějící nebo upravující městské nebo průmyslové odpadní vody nebo splašky, kromě těch, pro které se jedná pouze o vedlejší činnost k jejich hlavní činnosti.

Zároveň musí subjekt naplnit podmínky na velikost podniku:

- Subjekt je středním nebo velkým podnikem, tedy zaměstnává 50 a více zaměstnanců, nebo dosahuje ročního obratu nebo bilanční sumy roční rozvahy alespoň 10 milionů EUR (zhruba 250 milionů CZK).

NÚKIB spolupracuje s odvětvovými regulátory a informace o poskytovatelích regulované služby bude sám vyhledávat a tyto organizace bude upozorňovat na potřebu registrace. Tato činnost však nenahrazuje povinnost organizace se sama registrovat, pokud identifikační kritéria naplní.

Doplnění 2. Zdůraznění zapojení osob odpovědných za fyzickou a kybernetickou bezpečnost

V případě složitějších, a hlavně větších systémů zásobování vodou by měl posouzení rizik zpracovat tým, který by měl optimálně disponovat multidisciplinárními znalostmi zahrnujícími problematiku znečištění prostředí v ochranných pásmech vodních zdrojů nebo (lépe) v celém povodí těchto zdrojů, dále problematiku čerpání surové vody, úpravy vody a její distribuce – nejen co do možných rizik, ale i příslušných nápravných opatření, problematiku vyhodnocování kvality pitné vody apod. Pokud nejsou všechny výše uvedené oblasti v kompetenci provozovatele, je vhodné do týmu přizvat i osoby z organizací odpovědných za danou oblast (např. pracovník příslušného podniku Povodí, jedná-li se o povrchový zdroj vody, ale i pracovník zodpovědný za informační systémy, popřípadě fyzickou bezpečnost). Klíčová je však přítomnost osob dokonale znajících posuzovaný systém zásobování. V případě rozsáhlých a provozně komplikovaných vodovodů nebo vodárenských soustav může být ustaveno více týmů, které budou mít za úkol zpracování posouzení rizik jen pro jednotlivé části systému (zdroje a čerpání surové vody, úprava vody, distribuce), nicméně v takovém případě je nutné, aby svou činnost vzájemně koordinovaly a na sebe logicky navazovaly.

Doplnění 3. Přidání shromáždění dokumentace ke SCADA

K tomuto úkolu je vhodné si shromáždit následující podklady:

- provozní řád (především provozní řád podle zákona o vodovodech a kanalizacích, pokud ho provozovatel musí zpracovat), včetně mapových podkladů;
- hydrogeologické posudky u zdrojů podzemní vody + informace o ochranných pásmech;
- plány objektů;
- provozní deník(y);
- pokud úpravna využívá SCADA, také dokumentaci a manuály k tomuto systému.

Doplnění 4. Doplnění organizačních a technických opatření fyzické a kybernetické bezpečnosti a vytvoření dokumentace ke SCADA

Aktuální popis systému zásobování by měl obsahovat:

- přehlednou mapu poskytující dobrý přehled o geografickém umístění celého systému zásobování vodou a o jeho okolí (možný příklad viz obr. 1);
- schéma zařízení (hydraulický diagram) s vyznačením všech objektů (možný příklad viz obr. 2) a směru proudění vody v distribuční síti (vhodná je elektronická verze, systém GIS) – není nutné u malých a velmi jednoduchých systémů;
- soupis základních informací o systému zásobování, včetně stručné charakteristiky odběratelů (způsobů užití vody): domácnosti, průmysl, citliví odběratelé (např. nemocnice, potravinářské provozy…) apod. – příklad možného formuláře k zápisu v příloze A;
- popis využívaného zdroje či zdrojů vody, jejich vydatnost a jímání (popř. popis náhradního zdroje vody pro případ havárie), včetně kvality vody a jejích změn; popis využití povodí v případě odběru surové povrchové vody;
- popis (plány) ochranných pásem (OP) vodního zdroje, využití jejich pozemků a pravidel pro činnosti v ochranných pásmech;
- seznam a popis všech vodárenských zařízení (objektů) a délky a druhů materiálů potrubí;
- popis technologie úpravy vody včetně dezinfekce a výčet všech chemických látek používaných k úpravě vody;
- způsob vedení provozních záznamů (dokumentace činnosti);
- pokud úpravna používá SCADA, je nutné shromáždit dokumenty/manuály od vývojáře, a v případě absence je potřeba vytvořit dokument obsahující základní informace o systému a ověřené kontaktní informace na podporu v případě poruchy;
- popis režimových, personálních a technických opatření kybernetické a fyzické bezpečnosti včetně fyzické ostrahy.[1]

[1] Doplňující informace k základům kybernetické a fyzické bezpečnosti

Doplnění 5. Doplnění fyzických a bezpečnostních incidentů

Pro následující krok je pak důležité a již v tomto kroku vhodné zpracovat:

- přehled havárií za posledních nejméně 5 let;
- přehled jakosti dodávané pitné vody za posledních nejméně 5 let vycházející z povinných kontrolních i provozních rozborů, zaměřený na ukazatele překračující limitní hodnoty nebo pohybující se na hranici limitní hodnoty; pokud by došlo k situaci, že provozovatel převezme provozování nějakého vodovodu nově a od předešlého provozovatele nedostane tyto informace, lze se obrátit na příslušnou krajskou hygienickou stanici nebo Státní zdravotní ústav, která historická data kontrolních rozborů mohou vytáhnout z informačního systému a novému provozovateli za účelem posouzení rizik poskytnout;
- přehled bezpečnostních incidentů fyzické (např. vandalismu) a kybernetické bezpečnosti (např. phishing).

Doplnění 6. Zdůraznění dopadů fyzických a kybernetických hrozeb na distribuci a kvalitu vody

Pro účely zpracování rizik je vhodné definovat terminologii, se kterou se v průběhu zpracování a vyhodnocování rizik dále pracuje. Nebezpečím se obvykle rozumí neoddělitelná vlastnost určité látky (nebo situace) vyvolat nepříznivý účinek – poškození či újmu. Pro účely této metodiky rozumíme ve shodě se Světovou zdravotnickou organizací a vyhláškou č. 252/2004 Sb. pod pojmem nebezpečí jakýkoli biologický, chemický, fyzikální nebo radiologický činitel ve vodě nebo stav vody, který může ohrozit zdraví odběratelů nebo spotřebitelů vody nebo způsobit organoleptické závady vody; nebezpečím se dále rozumí i omezení nebo úplné přerušení dodávky vody odběratelům. Nebezpečnou událostí či příčinou nebezpečí pak rozumíme událost, která buď způsobuje vnos nebezpečí do systému zásobování, nebo selhání bariéry určené k odstranění existujícího nebezpečí. Příkladem první události je např. silný déšť nebo povodeň, která zdroj vody mikrobiologicky znečistí. Příkladem druhé události může být selhání technologie úpravy na odstranění dusičnanů, které způsobí, že vysoká koncentrace dusičnanů v surové vodě bude i v distribuované vodě pitné. Na distribuci a kvalitu vody mohou mít dopady také např. porucha na SCADA systému, kybernetický útok na informační systémy objektu nebo vandalismus na systém distribuce nebo u zdroje vody.

Doplnění 7. Přidání generického rizika spojené s kybernetickou bezpečností

Většina nebezpečí je místně specifická, to znamená, že se nevyskytuje ve všech systémech zásobování, ale jen v některých z nich podle místní situace. Nicméně několik nebezpečí souvisejících s distribuční sítí a vodojemy bude společných všem provozovatelům vodovodů. Tato rizika lze označit jako tzv. generická a měla by být uvažována při každém posouzení rizik:

- Vniknutí neznámé (neautorizované) osoby do vodojemu.
- Nevhodný materiál distribuční sítě podléhající korozi nebo uvolňující nežádoucí chemické látky nebo podporující růst bakterií.
- Nevhodný způsob odkalování sítě.
- Náhlý pokles tlaku v síti v důsledku havárie na řadu.
- Hygienicky nedokonalý způsob opravy řadů a jejich znovuuvedení do provozu po haváriích a rekonstrukcích.
- Absence nebo nefunkčnost zařízení zabraňujícího zpětnému toku v objektech napojených na vodovod, ve kterých existuje riziko propojení s rozvodem nepitné vody nebo domovní studnou. Takové propojení se sice zakázané, ale na základě zkušeností z praxe víme, že je nelze vyloučit.
- Různé formy kybernetických útoků na informačním sytému, popřípadě přímo SCADA úpravny.

Doplnění 8. Zdůraznění fyzické a kybernetické bezpečnosti

Posledním úkolem tohoto kroku je inventura již existujících kontrolních opatření (bariér). Pod pojmem kontrolní opatření rozumíme jakoukoli činnost, která se může použít pro předcházení nebezpečí, která nelze žádným opatřením zcela vyloučit nebo která s ním související riziko snižuje na přijatelnou úroveň. Kontrolní opatření mohou mít povahu infrastrukturní (např. oplocení zdroje), technickou (např. úprava vody, dezinfekce, prvky elektronické zabezpečovací signalizace) či organizační (např. omezení používání pesticidů v ochranném pásmu, řízení vstupu do objektu). Zároveň je potřeba posoudit jejich účinnost a spolehlivost, což je potřebné pro následující krok hodnocení rizik. K tomuto kroku je ideální využít zdroje, které byly shromážděny v kroku 2.

Doplnění 9. Doplnění přílohu tabulek hrozeb o kybernetickou a fyzickou bezpečnost

B. Jímání, úprava, akumulace a distribuce vody

Kód	Zdroje nebezpečí	Možné nebezpečí
6…	**Jímání a úprava vody (podzemní a povrchové)**	
7…	**Vodojemy**	
8…	**Vodovodní síť a přípojky**	
9.	**SCADA a informační systémy**	
9.1	Porucha nebo poškození softwaru/hardwaru	Přerušení/omezení vzdáleného řízení úpravny
9.2	Přerušení podpory a aktualizací SCADA systému	Omezení řízení vzdáleného řízení úpravny a komplikace při údržbě či doplnění technologie úpravny.
9.3	Kybernetický útok na informační systémy	Ztráta dat a přerušení/omezení vzdáleného řízení úpravny
9.4	Kybernetický útok na SCADA	Špatné dávkování chemických látek nebo přerušení zásobování pitnou vodou

Doplňující informace k základům kybernetické a fyzické bezpečnosti

Jednotlivá opatření v rámci fyzické a kybernetické bezpečnosti můžeme pro zjednodušení rozdělit na čtyři hlavní části – technická, režimová a personální bezpečnostní opatření a zajištění služby fyzické ostrahy nebo zásahu. Už podle názvu je možné odhadnout, co tyto skupiny zahrnují.

- V případě **technických opatření** jde zejména o různé typy technických prostředků, které zajišťují vyšší stupeň ochrany, a tedy i bezpečnosti a to buďto formou mechanických bezpečnostních zábran (např. bezpečnostní ploty, zábrany, zámky, trezory, dveře, brány, apod.) nebo formou SW opatření a zábran (např. antiviry, firewall, šifrování apod.) a nebo formou detekčních technických prostředků, které dokáží identifikovat různé typy útoků (např. kamerové systémy, poplachový zabezpečovací a tísňový systém, elektrická požární signalizace, perimetrický systém, apod.) …)
- V případě **režimových opatření** jde zejména o různé typy bezpečnostních pravidel pro předcházení bezpečnostním incidentům nebo o různé typy postupů, které se vztahují na detekci a následné řešení bezpečnostních incidentů, přičemž jejich dodržování přímo závisí na jednotlivých pracovnících a managementu organizace (řízení vstupu, aktualizace softwaru, nepřipojování neautorizovaných zařízení k počítačové síti organizace, pravidla používání služebních počítačů a telefonů, oznamování bezpečnostních incidentů, apod.)
- V případě **personálních opatření** jde zejména o aplikace právního řádu do smluvních nebo pracovních vztahů, aplikace možností legálního prověřování důvěryhodnosti osob pracujících na kritických pracovních pozicích, pravidelné školení a vzdělávání pracovníků v oblasti bezpečnosti a potenciálních hrozeb a rizik včetně možností jejich včasné detekce a řešení k minimalizaci škod a ztrát.
- V případě **služby fyzické ostrahy nebo zásahu** se jedná zejména o možnosti zajištění kvalifikovaného místního nebo vzdáleného monitoringu (dohledová poplachové přijímací centrum) bezpečnostních technologií, systémů nebo služeb za účelem zajištění včasné a adekvátní reakce na zjištění bezpečnostní hrozby nebo incidenty. Tuto službu lze zajistit pomocí vlastních zaměstnanců, soukromých bezpečnostních služeb, případně pomocí IZS.

Je důležité zdůraznit, že jednotlivá opatření zpravidla nefungují samostatně a jsou často provázaná mezi sebou vzájemně tak, že teprve jako celek, tvoří smysluplný systém zajištění ochrany a bezpečnosti organizace. Například pokud je objekt zabezpečen zamčenými dveřmi v rámci technických opatření, musí zároveň v rámci režimových opatření být stanoveno kdo má od těchto dveří klíče a kdo a za jakých podmínek může do objektu vstupovat. Tudíž je potřeba nevnímat jednotlivá opatření jako samostatnou jednotku a během popisu opatření je provazovat.

Závěr

V rámci závěru je potřeba zdůraznit 3 nejdůležitější body, které by měly mít dopad na praxi. Jedná se zejména o ***Doplnění 3. Přidání shromáždění dokumentace ke SCADA*** *a* ***Doplnění 4. Doplnění organizačních a technických opatření fyzické a kybernetické bezpečnosti a vytvoření dokumentace ke SCADA,*** *jejichž cílem je přimět odpovědné osoby zpracovávající posouzení rizik své úpravny, shromáždit relevantní dokumenty ke kybernetické a fyzické bezpečnosti.*

Dalším důležitým bodem je ***Doplnění 9. Doplnění přílohu tabulek hrozeb o kybernetickou a fyzickou bezpečnost****, která přidává do tabulky přílohy kybernetickou bezpečnost (fyzická je již zmíněna v předchozích částech). Podle zkušeností z praxe je tato příloha stěžejní při zpracování posouzení.*

Doplnění předpokládají, že osoby zodpovědné za zpracování pomocí metodiky nebudou z pochopitelných důvodů nutně znalé v oblasti kybernetické bezpečnosti a z těchto důvodů byl vytvořen doplňující stručný dokument ***Doplňující informace k základům kybernetické a fyzické bezpečnosti****, který by měl představit základní pojmy v této oblasti.*