TABULKA Č. 1: PŘEHLED KYBERNETICKÝCH INCIDENTŮ V SEKTORU VODNÍHO HOSPODÁŘSTVÍ

Cíl útoku	Stát	Typ útočníka	Typ subjektu	Rok	Prostředí	Průběh a následky
Maroochy Water Services	Austrálie	Insider	Čistírna odpadních vod	2000	OT	Bývalý zaměstnanec využil toho, že v čistírně nebyla nastavena žádná kyberbezpečnostní politika, a pomocí vzdáleného přístupu získal kontrolu nad SCADA systémem. Během tří měsíců útočník vypustil z různých stanic zhruba milion litrů surové odpadní vody do řeky, místních parků a obytných oblastí ve vzdálenosti 500 metrů od otevřeného odtoku. Zaměstnanec se údajně chtěl pomstít svému bývalému zaměstnavateli.
Tehama-Colusa Canal	USA	Insider	Správa vodních kanálů	2007	OT	Zaměstnanec správy kanálů nainstaloval do SCADA systému neautorizovaný software, což vedlo k jeho poškození. Kanály, které sloužily k odvádění vody pro místní farmy, však bylo možné operovat i manuálně. Hlavním dopadem tak byly finanční škody.
Key Largo Wastewater Treatment District	USA	Insider	Čistírna odpadních vod	2012	IT	Vedoucí finančního úseku čistírny odpadních vod, kterému nebyla prodloužena smlouva, využil přihlašovacích údajů ostatních zaměstnanců k získání přístupu k e-mailům a jiným osobním dokumentům. Útok byl nicméně omezen pouze na IT infrastrukturu a neměl závažnější dopady.
Bowman Avenue Dam	USA	Státem sponzorovaná skupina	Vodní nádrž (přehrada)	2013	OT	V roce 2013 získala skupina hackerů vzdálený přístup ke SCADA systému, který ovládal stavidlovou bránu. Kontrolní systém byl totiž přístupný z internetu a nebyl chráněn firewallem či autentizačními přístupovými kontrolami. Brána byla nicméně v dané době manuálně odpojena z důvodu údržby. Podle otevřených zdrojů za útokem údajně stáli Íránem sponzorovaní hackeři.[i]
Americké vodárenské společnosti	USA	Insider	Vodárenská společnost	2013	IT a OT	Během jara 2014 začalo 5 vodárenských společností ze 3 různých států USA hlásit problémy s jejich smart vodoměry. Společnosti se potýkaly s nepřesnými účty za vodu či rušením signálu vodoměrů. Za těmito problémy stál vyhozený zaměstnanec společnosti, která smart vodoměry vyráběla. Bývalý zaměstnanec využil svého stále platného

						přístupu do sítě a prováděl zde různé škodlivé aktivity jako změny root hesel, přepisování počítačových skriptů apod.
Kemuri Water Company (pseudonym)	N/A	Státem sponzorovaná skupina	Vodárenská společnost	2016	IT a OT	Společnost Verizon Security Solutions při hodnocení kybernetické bezpečnosti vodárenské společnosti nalezla řadu vysoce rizikových zranitelností včetně užívání zastaralých a nepodporovaných IT i OT systémů. Pozdější vyšetřování zahrnující analýzu internetového provozu odhalilo přítomnost IP adres státem sponzorovaných útočníků, kteří se snažili získat finanční záznamy a manipulovali s procesy pro čištění pitné vody. Podle výpovědí někteří zaměstnanci o neautorizovaném přístupu do systémů a neobvyklých vzorech manipulace s ventily věděli již dříve.
Evropská společnost (název nezveřejněn)	Velká Británie	Insider	Vodárenská společnost	2017	IT	Regionální dodavatel vody ve Velké Británii byl upozorněn svými klienty na to, že v jejich online účtech došlo ke změně údajů. Posléze vyšlo najevo, že byly změněny jejich bankovní účty, na které byly podvodně převedeny žádosti o vrácení peněz v hodnotě půl milionu liber. Útočník využil metod sociálního inženýrství k tomu, aby banky, které tyto účty spravovaly, převedly dané peníze na jiné bankovní účty, a následně za ukradené peníze nakoupil kryptoměny. Za tímto útokem stál zaměstnanec nikoliv samotné vodárenské společnosti, ale zaměstnanec třetí strany, která byla zodpovědná za správu online účtů a zpracovávání telefonních plateb.
Evropská společnost (název nezveřejněn)	N/A	Kyberkriminální skupina	Vodárenská společnost	2018	OT	V roce 2018 zaznamenala nespecifikovaná evropská vodárenská společnost podezřelý síťový provoz ve SCADA síti. Vyšetřování nalezlo přítomnost softwaru na těžbu kryptoměn v OT síti. Podle analýzy až 40 % provozu souviselo s těžbou kryptoměn. Žádné pokusy o manipulaci řídicích systémů nebyly zaznamenány. Útok pravděpodobně usnadnil neaktualizovaný antivirový software.
Onslow Water and Sewer Authority	USA	Kyberkriminální skupina	Vodárenská společnost	2018	IT	Americká vodárenská společnost se stala cílem ransomwarového útoku, který vedl k zašifrování databází nacházejících se v IT síti. Útočníkům se podařilo dostat do systémů společnosti a nainstalovat zde malware EMOTET, pomocí kterého následně nasadili

						ransomware RYUK. Podle autorit se jednalo o cílený útok, protože si útočníci vybrali cíl, který byl nedávno ovlivněn přírodní katastrofou. Útok se odehrál necelý měsíc po ničivém hurikánu Florence. K narušení dodávek pitné vody i přesto nedošlo; společnost byla schopna přejít na manuální provoz, nicméně na několik následujících týdnů klesla její funkčnost a efektivita.
Post Rock Water District	USA	Insider	Úpravna vody	2019	OT	Bývalý zaměstnanec se necelé dva měsíce po svém propuštění vzdáleně připojil k systému úpravny a zastavil procesy čištění a dezinfekce. Dovršení útoku se podařilo zabránit, nicméně bližší informace o případu nejsou známy.
Povodí Vltavy s. p.	Česká republika	Neznámý	Správa vodních toků	2020	IT	V dubnu 2020 došlo v ČR k napadení informačních systémů pro administrativní činnosti podniku Povodí Vltavy. Prvky kritické infrastruktury nebyly útokem dotčeny, protože byly fyzicky odděleny od prostředí informačních systémů podniku. Útoky nicméně znemožnily fungování spisové služby, e-mailů a dalších interních systémů.
Izraelská společnost (název nezveřejněn)	Izrael	Státem podporovaný aktér	Úpravna vody	2020	OT	Izraelská úpravna vody se stala cílem kybernetického útoku, který vedl ke kompromitaci HMI (Human Machine Interface), jež bylo připojeno k internetu bez nutnosti jakékoliv autentizace či jiného typu ochrany. Cílem byla pravděpodobně nádrž na regenerovanou vodu (odpadní voda upravená pro další použití). Izraelské autority útok včas zastavily. Podle informací Washington Post za útokem údajně stál Íránem podporovaný aktér.[ii]
Zemědělské subjekty v Izraeli (název nezveřejněn)	Izrael	Neznámý	Zemědělská čerpadla	2020	OT	Izrael byl v roce 2020 zasažen dvojicí kybernetických útoků na zemědělská čerpadla v Horní Galileji a v provincii Mateh Yehuda. Útočníci se zaměřovali na průmyslové řídicí systémy a pokoušeli se o manipulaci s ventily a průtoky. Útoky nezpůsobily žádné škody, ani omezení provozu. Podle šéfa Národního kybernetického ředitelství Yigala Unny však mohly mít útoky zásadní dopady, kdyby útočníky včas neobjevili.
Americká společnost	USA	Neznámý	Úpravna vody	2021	OT	Na začátku roku 2021 došlo ke kybernetickému útoku na úpravnu vody v San Franciscu. Útočník získal přihlašovací údaje k účtu bývalého zaměstnance do softwaru pro

(název nezveřejněn)						vzdálenou plochu TeamViewer, pomocí kterého byly spravovány procesy úpravy vody, a vymazal programy, které úpravna užívala pro procesy čištění vody. Zaměstnanci se o útoku dozvěděli až následující den a okamžitě podnikli kroky k nápravě. K žádné poruše či újmě na zdraví nedošlo.
Bruce T. Haddock Water Treatment Plant	USA	Neznámý	Úpravna vody	2021	OT	Neidentifikovaný útočník získal přístup ke SCADA systému úpravny vody na Floridě, pomocí kterého zvýšil hodnoty hydroxidu sodného, užívaného při úpravě pitné vody, na nebezpečnou úroveň. Útočník tak učinil skrze přístup do softwaru pro vzdálenou plochu TeamViewer, pomocí kterého byly spravovány procesy úpravy vody. Manipulace si okamžitě všiml operátor, který byl v dané době u monitorovacího systému přítomen.
Americká společnost (název neznámý)	USA	Neznámý	Vodárenská společnost	2021	OT	V červnu 2021 využili útočníci vzdáleného přístupu k zavedení ransomwaru ZuCaNo do SCADA systému používaného pro čištění odpadních vod. Útok se obešel bez závažnějších dopadů, nicméně proces čištění musel být po určitou dobu provozován manuálně.
Americká společnost (název nezveřejněn)	USA	Neznámý	Vodárenská společnost	2021	OT	V srpnu 2021 zaútočili neznámí aktéři na nejmenovanou vodárenskou společnost v Kalifornii. Útočníci v rámci útoku využili variantu ransomwaru Ghost. Zhruba měsíc poté, co útočníci získali přístup do dané sítě došlo na SCADA serverech ke spuštění ransomwaru. Bližší informace o útoku nejsou známy.
Americká společnost (název nezveřejněn)	USA	Neznámý	Vodárenská společnost	2021	N/A	Pensylvánská Water Action Response Network sdružující řadu vodohospodářských společností sdělila svým členům, že došlo ke kompromitaci dvou systémů nejmenovaného subjektu či subjektů. Útočníci se pokusili skrze webshell získat vzdálený přístup do systému, nicméně jejich akce byly včas detekovány a zastaveny.

[i] Thompson, M. 2016. Iranian Cyber Attack on New York Dam Shows Future of War. https://time.com/4270728/iran-cyber-attack-dam-fbi/

[ii] Warrick, J. Nakashima, E. 2020. Foreign intelligence officials say attempted cyberattack on Israeli water utilities linked to Iran. https://www.washingtonpost.com/national-security/intelligence-officials-say-attempted-cyberattack-on-israeli-water-utilities-linked-to-iran/2020/05/08/f9ab0d78-9157-11ea-9e23-6914ee410a5f_story.html