MEZINÁRODNÍ BEZPEČNOSTNÍ INSTITUT

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

Kybernetická bezpečnost na železnici

Aktuální studie ENISA se týká úrovně provádění opatření kybernetické bezpečnosti v železniční dopravě v rámci prosazování směrnice o bezpečnosti sítí a informací v každém evropském členském státě. Konstatuje význam objemu železniční doprav v osobním i nákladním sektoru. V tomto kontextu hodnotí stav ve vybraných členských státech EU. Představuje současně kompletní seznam základních železničních služeb, doplněný o detailní přehled o železničních systémech, které je podporují. Na závěr je představen evropský systém řízení železničního provozu, spolu s některými klíčovými aspekty a doporučeními v oblasti kybernetické bezpečnosti. Samotný textový materiál je doplněn četnými grafickými a tabulkovými přílohami.

Zdroj: https://www.enisa.europa.eu/publications/railway-cybersecurity

Struktura materiálu.

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

5.2 úvahy
5.3 DALŠÍ KROKY.

Globálně.

- analýza politického a regulačního kontextu železnic, zejména kybernetické bezpečnosti na železnici,
- identifikace stavu, týkajícího se provedení směrnice o bezpečnosti sítí a informací do členských států EU, zejména do železničního sektoru,
- identifikace základních služeb a kritických informačních systémů pro odvětví železnice na základě odpovědí z průzkumu a rozhovorů,
- posouzení vyspělosti sektoru, týkající se provádění směrnice o bezpečnosti sítí a informací na základě odpovědí z průzkumu a rozhovorů,
- zaměření na evropský systém řízení železničního provozu, nejdůležitější informační systém pro železniční sektor v Evropě.

Trendy.

Podle průzkumů a rozhovorů provedených v rámci této studie byly celkové trendy pro EU při provádění směrnice o bezpečnosti sítí a informací pro provozovatele základních služeb v železničním sektoru následující:

- Obecná implementace bezpečnostních opatření týkajících se správy a řízení ekosystém je heterogenní a nízká ve srovnání s jinými typy opatření. Většina vyspělých OES (Operator of Essential Services) již tato opatření uplatňuje již dlouhou dobu. Mezitím u méně vyspělých OES se právě začalo s prováděním těchto opatření.
- Ochranná bezpečnostní opatření se jeví jako nejlépe implementovaná. Zatímco základy kybernetické bezpečnosti se zdají být již implementovány, bezpečnostní opatření, vyžadující pokročilé technické znalosti ukazují nižší úroveň implementace. Ve zvláštním kontextu operační technologie je často nemožné implementovat základní bezpečnostní prvky bez použití kompenzačních protiopatření,
- Nejjednodušší bezpečnostní opatření (např. komunikace s příslušnými orgány a reakce na bezpečnostní incidenty) se zdají být dobře implementovány. Jiné jsou však implementovány jen zřídka, protože vyžadují značné znalosti a vyspělost v oblasti kybernetické bezpečnosti (např. korelace protokolu a analýza),
- U opatření ve smyslu odolnosti se úroveň provádění jeví jako dobrá. Krizový management je součástí každodenní činnosti železničního sektoru. Toto však musí být kvalifikované: stále ještě existují příležitosti ke zlepšení plné integrace nových

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

kybernetických hrozeb do stávajících procesů pro řešení krizí a zajišťování odolnosti.

Výzvy.

Studie současně identifikuje hlavní výzvy, kterým toto odvětví při prosazování směrnice o bezpečnosti sítí a informací odpovídá:

- Zúčastněné strany v oblasti železnice musí dosáhnout rovnováhy mezi provozními požadavky, konkurenceschopností podnikání a kybernetickou bezpečností, zatímco odvětví prochází cestou digitální transformace, která zvyšuje potřebu kybernetické bezpečnosti.
- Železniční subjekty jsou závislé na dodavatelích s různorodými technickými normami a schopnostmi kybernetické bezpečnosti, zejména pro operační technologie. Systémy OT (Operational Technology) pro železnice byly založeny na systémech, které byly v určitém okamžiku bezpečné podle nejnovějšího stavu techniky, ale vzhledem k dlouhé životnosti systémů jsou nakonec zastaralé nebo zastarávají. Díky tomu je obtížné udržovat je permanentně aktuální se současnými požadavky na kybernetickou bezpečnost. Kromě toho jsou tyto systémy obvykle rozšířené po síti (stanice, trať atd.), což ztěžuje její komplexní schopnost kontrolovat kybernetickou bezpečnost.
- Provozovatelé železnic hlásí problémy s nízkým povědomím o kybernetické bezpečnosti a rozdíly v úrovních, zejména mezi bezpečnostním a provozním personálem.
- Stávající nařízení, týkající se železniční dopravy nezahrnuje ustanovení o kybernetické bezpečnosti. OES často musí splňovat neharmonizované požadavky kybernetické bezpečnosti, vyplývající z různých předpisů.

Rozsah.

Železniční síť v rámci EU představuje 472 miliard „osobokilometrů“, 216 000 km aktivních železnic a 430 miliard „tunokilometrů“. V nákladní dopravě hraje železniční odvětví důležitou a rychle se rozvíjející roli. Železniční infrastruktura a její systémy jsou klíčovými aktivy, které jsou zásadní pro rozvoj a ochranu EU. Železniční sektor prochází zásadní transformací svých provozů, systémů a infrastruktury kvůli digitalizaci OT a IT systémů a infrastruktury, automatizaci železničních procesů, otázkám hromadné dopravy a zvyšujícímu se počtu propojení s externími a multimodálními systémy. Tento sektor se také vyvíjí tak, jak se postupně otevírá soutěž. To vede k přerozdělení odpovědností a oddělení železničních systémů
a infrastruktura, které také ovlivňují systémy IT. V této souvislosti je pro železniční sektor stále důležitější řešit kybernetické hrozby.

MEZINÁRODNÍ BEZPEČNOSTNÍ INSTITUT

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

Klíčové závěry.

Pro železniční sektor je zavedení IP sítí v zabezpečovacích a energetických systémech klíčovým problémem, který bude třeba posoudit a dále pochopit. Provádění směrnice o bezpečnosti sítí a informací v EU v železničním sektoru se mezi členskými státy a OES liší. Pokud jde o provedení NIS Směrnice, každý členský stát přijal svůj vlastní způsob definování základních služeb a identifikace provozovatelů základních služeb (OES), přidělení vnitrostátních nebo odvětvových příslušných orgánů a definování přijatelných prostředků pro dosažení souladu se směrnicí. Kromě toho má každá OES svůj vlastní způsob implementace bezpečnostních opatření, individuální zralost kybernetické bezpečnosti, digitální dovednost, velikost, dodavatele a zdroje přidělené ke kybernetické bezpečnosti.

Celkový trend ukazuje, že bezpečnostní opatření, určená skupinou pro spolupráci pro EU Směrnice o bezpečnosti sítí a informací jsou relevantní pro železniční zúčastněné strany, které na studii odpověděly a zdá se také, že většina bezpečnostních opatření byla zavedena.

Bezpečnostní opatření.

Bezpečnostní opatření, která OES nejčastěji implementuje, jsou následující:

- základy kybernetické bezpečnosti (např. administrativní účty, bezpečnostní politika, protokolování, provoz a filtrování),
- opatření nad rámec požadavků kybernetické bezpečnosti (zejména pro železniční provoz a kontinuitu podnikání),
- právní požadavky, jako je bezpečnost a fyzické zabezpečení (např. fyzická a enviromentální bezpečnost, krizový management, hlášení nehod).

Úvahy.

Implementace bezpečnostních opatření, vyžadující speciální znalosti kybernetické bezpečnosti a přísné řízení kybernetické bezpečnosti je složitější (např. kryptografie, průmyslové řídicí systémy, korelace protokolů a analýza). To musí být přizpůsobeno podle typu systému (IT nebo OT). Je to často nemožné plně prosadit i ta nejjednodušší bezpečnostní opatření v systémech OT. Aby železniční sektor prosazoval směrnici o bezpečnosti sítí a informací, musí se vypořádat s následujícími výzvami:

- celkově nízké povědomí o digitální a kybernetické bezpečnosti v železničním sektoru v železniční dopravě, spojené s konflikty mezi bezpečností a jistotou,
- charakteristika železniční infrastruktury a OT prostředí (závislost na dodavatelském řetězci, geografickém rozšíření železniční infrastruktury, stáří systémů),
- rostoucí úsilí v odvětví dopravy dosáhnout rovnováhy mezi kybernetickou bezpečností, konkurenceschopností a provozní účinností, v kombinaci s probíhající digitální transformací železnice,

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

- složitost a nedostatečná harmonizace předpisů v oblasti kybernetické bezpečnosti, které musí být plně pochopeny, aby byly uvedeny do praxe.

Politika.

Pokud jde o politiku, směrnice o bezpečnosti sítí a informací a národní implementace procházejí nepřetržitým procesem. Evropská komise a členské státy, s pomocí agentury ENISA, pracují na řešení výše uvedených výzev, zejména těch, které se týkají EU v politickém a regulačním kontextu. Zároveň implementaci minimálního zabezpečení ze strany OES monitorují členské státy s cílem identifikovat potenciál vylepšení a oblasti, kde OES vyžadují další podporu. Tato zpráva tuto aktivitu podporuje a zdůrazňuje odvětvové výzvy, specifické pro železnici. Postupy kybernetické bezpečnosti v železničním sektoru se vyvíjejí. Kybernetická bezpečnost se pomalu integruje do návrhu IT a OT pro dopravní systémy. Kybernetická bezpečnost se tak stává zásadním požadavkem pro sektor železniční dopravy.