Centrum Wymiany i Analiz Informacji
podsektora transportu kolejowego
„ISAC - Kolej”

Warszawa, 26 kwietnia 2021 r.

Dyrektor Robert Kośla
Departament Cyberbezpieczeństwa
Kancelaria Prezesa Rady Ministrów
Al. Ujazdowskie 1/3, 00-583 Warszawa

Pismo: ISAC-Kolej 2021-04-01
dot. Uwag do Dyrektywy NIS 2

Szanowny Panie Dyrektorze,

Centrum Wymiany i Analizy Informacji podsektora transportu kolejowego „ISAC – Kolej” zgłasza niniejszym następujące uwagi do opublikowanego projektu „Dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, uchylającej Dyrektywę 2016/1148” (Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148) czyli do tak zwanej Dyrektywy NIS-2:

- uwaga do art. 18 - wnioskujemy o doprecyzowanie pojęcia bezpieczeństwa łańcucha dostaw m.in. w zakresie ograniczeń wyboru dostawcy w zakresie kompatybilności z zapisami wymogów unijnego i krajowego prawa zamówień publicznych.
- uwaga do art. 20 - artykuł wymaga doprecyzowania. Obowiązujący obecnie tekst Dyrektywy NIS wskazuje precyzyjne parametry zagrożeń, które należy raportować.
- uwaga do art. 22 - artykuł na obecnym poziomie jest niewystarczający. Wymagane jest powstanie standardów oraz wsparcie przejścia do essential entities oraz important entities w postaci prowadzenia działań komplementarnych na poziomie CENELEC oraz Komisji Europejskiej. Dyrektywa powinna zobowiązywać Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji oraz sektorowe Agencje (w przypadku transportu kolejowego - Agencję Kolejową Unii Europejskiej) do opracowania co najmniej dobrych praktyk lub przygotowania mandatów dla Europejskich Organizacji Normalizacyjnych. Naszym zdaniem niezbędne jest powstanie kliku dokumentów pomiędzy poziomem Dyrektywy a normami, które odpowiadałyby na pytanie w jakim obszarze powinny być podejmowane działania na poziomie zarządców infrastruktury i przewoźników kolejowych. Kolejnym rozwiązaniem jest doprecyzowanie Rozporządzeń Komisji Europejskiej dotyczących Technicznych Specyfikacji Interoperacyjności lub zobowiązanie Agencji Kolejowej Unii Europejskiej do opracowania konkretnych standardów na wzór pakietu 6 wspólnych metod bezpieczeństwa (CSM) opracowanych na podstawie Dyrektywy ds. bezpieczeństwa kolei i przyjętych jako Rozporządzenia Wykonawcze Komisji Europejskiej.
- Doprecyzowania wymagają także obszary, które powinny zostać zabezpieczone przed cyberatakami. Usługi Kluczowe powinny zostać dopracowane z podziałem na grupy na przykład na usługi, które muszą zostać zabezpieczone oraz usługi o zabezpieczeniu których decydować będzie podmiot. Jasne powinno być także, kto podejmuje decyzje w jaki sposób powinny zostać zabezpieczone poszczególne usługi. Wyeliminuje to obecnie funkcjonujące bardzo zróżnicowane podejście poszczególnych podmiotów, które jako niewłaściwa praktyka zostało wskazane w

Raporcie Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji dot. sektora transportu kolejowego wydanym w listopadzie 2020 r.

- Raz jeszcze zwracamy także uwagę na niewystarczającą naszym zdaniem spójność pomiędzy dyrektywą w sprawie bezpieczeństwa kolei (Dyrektywa (UE) 2016/798 – Railway Safety Directive – dyrektywa RID) oraz dyrektywą w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów (Dyrektywa (UE) 2016/1148 – dyrektywa NIS). Kwestia ta była już podnoszona w uwagach formalnie zgłoszonych w imieniu Polskiego Komitetu Normalizacyjnego PKN do specyfikacji technicznej TS 50701 opracowanej przez CENELEC a dedykowanej cyberbezpieczeństwu w transporcie kolejowym.
  Prawo kolejowe przewiduje, że systemy zarządzania bezpieczeństwem i odpowiednie formalne dopuszczenia do prowadzenia działalności muszą posiadać zarządcy kolejowi, przewoźnicy kolejowi i podmioty odpowiedzialne za utrzymanie (entity in charge of maintenance - ECM). Dyrektywa RID uznaje, że ECM to podmioty odpowiedzialne za utrzymanie taboru. Jest to szczególnie istotne w kontekście funkcjonowania właścicieli taboru, nie będących przewoźnikami i tym samym nie zobowiązanych do wdrożenia systemu zarządzania bezpieczeństwem (zgodnie z dyrektywą RID), gdyż za bezpieczne utrzymanie takiego taboru odpowiadają podmioty formalnie zaakceptowane jako ECM-y, ale z zakresu ich odpowiedzialności wyłączono cyberzagrożenia, gdyż nie uwzględniono ich w dyrektywie NIS. Jednocześnie wskazać należy, że norma CENELEC EN 50126-1 opracowana w związku z mandatem KE dla CENELEC nakłada obowiązki w zakresie współdziałania z przemysłem w kwestii akceptacji rozwiązań technicznych na zarządców infrastruktury, przewoźników kolejowych i podmioty odpowiedzialne za utrzymanie uwzględniając zarówno utrzymanie taboru jak i utrzymanie infrastruktury. Norma ta wprowadza w tym celu pojęcie „podmiotu odpowiedzialnego za kolej" (ang. „railway duty holder").

> **3.48**
> **podmiot odpowiedzialny za kolej**
> podmiot na którym spoczywa pełna odpowiedzialność za eksploatację systemu kolejowego w ramach przepisów prawa
>
> Uwaga 1 do hasła: Odpowiedzialność podmiotu odpowiedzialnego za cały system kolejowy lub jego części oraz działanie w cyklu życia jest niekiedy dzielona pomiędzy kilka podmiotów lub jednostek. Na przykład pomiędzy:
>
> — właściciela (właścicieli) zasobów lub pewnej części zasobów i ich przedstawicieli handlowych;
>
> — operatora systemu;
>
> — podmiot (podmioty) utrzymujący(-e) część lub pewne części systemu.
>
> Uwaga 2 do hasła: Na ogół podmiotami odpowiedzialnymi za kolej są przedsiębiorstwa kolejowe oraz zarządcy infrastruktury. Takie podziały opierają się albo na instrumentach statutowych, albo na uzgodnieniach kontraktowych. Taka odpowiedzialność jest definiowana na najwcześniejszych etapach cyklu życia systemu.

Obowiązki podmiotu określanego mianem „podmiotu odpowiedzialnego za utrzymanie" szeroko uwzględniają zarówno normy EN 50126-1:2017 oraz EN 50126-2:2017 dotyczące bezpieczeństwa całego systemu kolejowego jak i norma EN 50129:2018 dedykowana systemom eksploatacyjnym (OT) odpowiedzialnym za sterowanie ruchem kolejowym.
Naszym zdaniem, takie podejście (uwzględniające podmioty odpowiedzialne za kolej włącznie z odpowiedzialnymi za utrzymania taboru i odpowiedzialnymi za utrzymania infrastruktury) powinno mieć zastosowanie także w przypadku cyberzagrożeń.

z wyrazami szacunku
koordynator ISAC-Kolej

ZASTĘPCA DYREKTORA
DS. INTEROPERACYJNOŚCI KOLEI
dr hab. inż.
Marek Pawlik, prof. IK

Elektronicznie podpisany przez Marek Pawlik
Data: 2021.04.26 13:00:02 +02'00'