Cyberdefence 24

aut. Andrzej Kozłowski 02.10.2019

„BEZ RODZIMYCH ROZWIĄZAŃ IT NIE BĘDZIE BEZPIECZEŃSTWA INFRASTRUKTURY KRYTYCZNEJ” [SCF2019]

Drugi panel Strategic Cyber Forum dotyczył bezpieczeństwa infrastruktury krytycznej w kontekście nadchodzącej rewolucji sieci 5G i Przemysł 4.0. Według Dyrektora Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji Roberta Kośli najważniejsze dla bezpieczeństwa infrastruktury krytycznej są następujace obszary reagowania na zagrożenia bezpieczeństwa infrastruktury krytycznej: standaryzacja minimalnych środków bezpieczeństwa, model przetwarzania, analityka, reagowanie na poziomie krajowym i regionalnym oparte na partnerstwie.

W panelu zatytułowany: „Cyberbezpieczeństwo infrastruktury krytycznej w erze czwartej rewolucji przemysłowej” wzięli udział:

- **Robert Kośla** – Dyrektor Departamentu Cyberbezpieczeństwa, Ministerstwo Cyfryzacji;
- **Nikodem Bończa Tomaszewski** – Prezes Zarządu Exatel;
- **Czesław Warsewicz** – Prezes Zarządu PKP CARGO S.A.;
- **Ph.D. Aneta Dobruk-Serkowska** – Senior Consultant, Bezpieczeństwo OT/IoT, EY Polska;
- **płk Przemysław Przybylak** – Komendant Centrum Operacji Cybernetycznych;
- **płk dr hab. inż. Piotr Dela** – Akademia Sztuki Wojennej, Zakład Cyberbezpieczeństwa

Infrastruktura krytyczna jest najbardziej newralgicznym z punktu widzenia państwa obiektem ataków hakerów. W przeszłości mieliśmy już przypadki poważnych cyberataków na sektor energetyczny czy transportowy - rozpoczął dyskusję moderator.

Przed skutkami potencjalnego konfliktu w sieci i związanymi z tym zagrożeniami dla infrastruktury krytycznej ostrzegał płk dr hab. inż. Piotr Dela. W jego opinii skutki konfliktu w sieci mogłoby nas cofnąć nawet do czasów, które znamy z XIX wieku. "Gdy dojdzie do eskalacji konfliktu na szeroką skalę, można stwierdzić, że infrastruktura może przestać funkcjonować - w szczególności, że do obecnych zagrożeń dojdą nowe, związane z postępem technologicznym" - dodał.

Postęp jest nieunikniony i jednym z jego przejawów jest technologia 5G, która wpłynie na infrastrukturę krytyczną i przemysł. Prezes Zarządu Exatel Nikodem Bończa Tomaszewski powiedział, że „wdrożenie sieci 5G pozwoli nam dokonanie bardzo dużego skoku. Przejdziemy z mroków średniowiecza do technologii komórkowej 5 generacji".

Aneta Dobruk-Serkowska z EY Polska wyjaśniła natomiast jaki nowy rodzaj zagrożeń wiąże się z „Przemysłem 4.0”. "Oznacza to, że do procesów produkcyjnych dopuszczeni zostaną dostawcy i klienci np. poprzez chmurę. To sprawia, że staniemy twarzą w twarz z nowymi zagrożeniami" - stwierdziła. Dodała również, że tylko część przemysłu w Polsce jest przygotowana do wdrożenia technologii. Niestety wiele przedsiębiorstw ma jeszcze problemy z erą 3.0.

Branża transportowa wciąż zmaga się z pewnymi brakami cyberbezpieczeństwa. Prezes Zarządu PKP CARGO S.A. Czesław Warsewicz stwierdził, że zderzamy się z problemem braku świadomości odnośnie zagrożeń cyberbezpieczeństwa. "Istnieje też problem ludzki i technologiczny, które to w naszym dziale powinniśmy uzupełnić" - stwierdził. Dodał też, że branża transportowa nie odnotowała żadnych poważniejszych incydentów. Przypomniał także, że PKP Cargo jest operatorem usługi kluczowej. "W związku z tym przeanalizowano wszystkie systemy pod względem ich podatności na ataki, firma przygotowała się do szybkiego reagowania 24/7" - podsumował.

Robert Kośla z Ministerstwa Cyfryzacji podkreślił znaczenie Ustawy o Krajowym Systemie Cyberbezpieczeństwa, która weszła w życie rok temu. "Ustawa o krajowym systemie cyberbezpieczeństwa określa najistotniejsze dla funkcjonowania Państwa sektory gospodarki: energetyczny, transportowy, bankowy i infrastruktury rynków finansowych, ochrony zdrowia, zaopatrzenia w wodę pitną (wraz z dystrybucją) i infrastruktury cyfrowej" – podkreślił. Dyrektor Departamentu Cyberbezpieczeństwa zwrócił także uwagę, że podstawowym zadaniem operatorów usług kluczowych jest szacowanie ryzyka. Dlatego konieczne jest określenie wspólnej metodologii. "Ministerstwo Cyfryzacji wspiera operatorów usług kluczowych oferując im narzędzia budowania kompetencji czy dokonywania analizy ryzyka" - powiedział podczas panelu. Przeprowadzane są również szkolenia, które mają lepiej przygotować operatorów usług kluczowych na zagrożenia. Rolę Ustawy o KSC docenił również Prezes Zarządu PKP CARGO S.A.

W dyskusji na temat bezpieczeństwa infrastruktury krytycznej nie mogło zabraknąć elementu wojskowego. Pułkownik Przybylak przypomniał, że Siły Zbrojne zostały powołane, aby bronić bezpieczeństwa Kraju. "Cyberzagrożenia zmieniają tą perspektywę. Incydent bądź szereg incydentów może stanowić przesłankę, aby wojsko mogło podjąć działania" - stwierdził wojskowy. "Dlatego w ramach naszych ćwiczeń, nacisk położony jest na ustalenie procedur – jest to ważna rzecz. Kluczowy w reagowaniu jest czas – dobre procedury oraz zgrane zespoły dają gwarancję lepszego reagowania na incydenty" - dodał płk Pułkownik Przybylak.

Konieczne jest prowadzenie wspólnych ćwiczeń w ramach infrastruktury krytycznej i współpraca w celu wypracowania skutecznych procedur.

Podsumowując debatę, uczestnicy wskazywali na elementy, które powinien posiadać skuteczny system cyberbezpieczeństwa infrastruktury krytycznej. Według Anety Dobruk-Serkowskiej z EY Polska musi zacząć od skutecznej analizy i priorytetyzacji. Dzięki temu uda się, w jej opinii, znaleźć wszelkie podatności. Piotr Dela dodał, że niezwykle istotna jest również identyfikacja ryzyka, która powinna zostać oparta na aparacie prognozowania. Powinno zwracać się uwagę na zagrożenia, które są mało prawdopodobne. Do tego wszystkie potrzebne jest jednak systemowe podejście i powstanie nowej strategii bezpieczeństwa narodowego. Dla prezesa Warsewicza najważniejsze jest procesowe myślenie oraz elastyczność. "Czynnik zaufania jest też niezwykle istotny" - podkreślił płk Przybylak. Prezes Zarządu Exatela stwierdził, że niemożliwe jest tworzenie systemu cyberbezpieczeństwa bez rodzimych rozwiązać IT.

Panel zakończył dyrektor departamentu cyberbezpieczeństwa w Ministerstwie Cyfryzacji Robert Kośla, który powiedział, że "Musimy zdefiniować środki ochrony na poziomie proceduralnym i technicznym. Techniczne, czyli te które nadążają za najnowszymi zagrożeniami. Chciałbym podziękować za całą roczną współpracę w ramach realizacji strategii".

PARTNERZY GŁÓWNI

PGZ · DELL · EY · Microsoft

PATRONAT HONOROWY

Ministerstwo Cyfryzacji · BBN · UKE · RCB

PARTNERZY

EXATEL · NASK · ORACLE · GRUPA WB · PKPCARGO · PIIT

Defence 24 · Energetyka 24 · CyberDefence 24 · Space 24 · InfoSecurity 24