aut. Bartosz Józefiak 19.07.2016

WOJSKO USA CHCE WIĘKSZEGO ZAANGAŻOWANIA SZEFÓW DZIAŁÓW IT

Szefowie działów IT są coraz ważniejszą częścią armii, a wielu wojskowych podkreśla, że powinni mieć podobne uprawnienia, jak ich odpowiednicy w firmach komercyjnych. W biznesie nierzadko CIO są członkami zarządu i decydują o długofalowej strategii przedsiębiorstwa. Również w amerykańskiej armii są głosy, że powinno się przyznać im więcej uprawnień.

Armia mogłaby podnosić swoje kompetencje operacyjne, i tym samym poprawiać cyberbezpieczeństwo poprzez poszerzenie kompetencji stanowiska CIO, czyli szefów działów informatycznych (Chief Information Officer).

Według Generała Williama Bendera, który pełni funkcję CIO w siłach powietrznych USA, osoby na tych stanowiskach powinny być nie tylko menedżerami działów IT, ale przede wszystkim członkami kadry zarządzającej całą organizacją, także militarną. Powinni mieć również możliwości operacyjne. W ten sposób mieliby wpływ na długofalową strategię związaną z cyberbezpieczeństwem danej jednostki. Bender podzielił się swoim pomysłem podczas śniadania prasowego w Waszyngtonie.

W praktyce chodzi o to, aby zwiększyć uprawnienia CIO, wyposażając ich w narzędzia pozwalające na realizowanie celów i strategii cyberbezpieczeństwa. W ten sposób szefowie działów informatycznych mieliby wpływ na to, jak działają systemy pozwalające na prowadzenie misji oraz obrony w cyberprzestrzeni.

Zdanie Bendera podkreśla rosnące znaczenie CIO, także w armii. Obecne trendy zmierzają do tego, by to właśnie na tej osobie spoczywała odpowiedzialność za bezpieczeństwo całej sieci. W świecie biznesu coraz powszechniejsze jest zwiększanie ich odpowiedzialności za powodzenie całego przedsiębiorstwa. Stają się oni liderami w znaczeniu biznesowym, nie tylko technicznym. Odpowiadają coraz częściej tylko przed dyrektorami generalnymi (CEO), są współodpowiedzialni za sukces biznesowy firmy.

Portal C4ISR.NET informując o wypowiedzi Bendera przypomniał również, że podobne słowa wypowiedział Dyrektor Służby obrony cyfrowej (Defence Digital Service) Chris Lynch. Podczas konferencji w czerwcu mówił, że Departament Obrony jest jedną z najsprawniej działających organizacji prowadzących codzienne operacje militarne, muszą być one jednak wspierane przez odpowiednią technologię. Dlatego właśnie rola CIO jest tak ważna.

W tej koncepcji rolą szefów działów IT byłaby więc kontrola nie tylko ich działu, ale przede wszystkim dbałość o zachowanie bezpieczeństwa przez wszystkich członków firmy/instytucji. Chodzi o tzw. cyber higienę – przestrzeganie podstawowych standardów i procedur gwarantujących lepszą ochronę sieci. Tym zasadom muszą się jednak podporządkować wszyscy pracownicy, nie tylko ci związani z IT. Bo też i każdy musi być świadom cyberzagrożeń. Gen. Bender stwierdził, że niewłaściwa cyber higiena odpowiada za 80 procent incydentów związanych z bezpieczeństwem we wszelkich instytucjach.

Siły powietrzne USA chcą rozwijać serwis zajmujący się cyber higieną, edukacją i rozwojem systemu cyberochrony w codziennych czynnościach kadry. Dowództwo uznało bowiem, że zagrożenie jest realne. Chodzi też o ochronę codziennych operacji wojskowych. W rozmowie z dziennikarzami Bender podkreślił, że nie ma takiego rodzaju aktywności sił powietrznych, w których nie musieliby oni polegać na dziale IT. Nie chodzi tylko o wykonywanie operacji. Mowa też o takich działaniach, jak przypisywanie kadry do samolotów, sterowanie i kontrolowanie lotów czy tankowanie pojazdów w powietrzu. Wszystkie te zadania są uzależnione od systemów podatnych na cyberataki. Zdaniem Bendera to wystarczający powód, by rozwijać uprawnienia szefów działów IT.

Czytaj też: Cyberdowództwo wojsk USA z nowymi uprawnieniami