Cyberdefence 24

aut. Andrzej Kozłowski 18.05.2020

GENERAŁ MOLENDA: „SYSTEMY WOJSKOWE ŁAKOMYM KĄSKIEM DLA HAKERÓW. CODZIENNIE SĄ CELEM ATAKU” [WIDEO]

„Obserwujemy szereg grup hakerskich, za którymi prawdopodobnie stoją służby specjalne niekoniecznie przyjaznych nam krajów, które testują nasze możliwości obronne, po to, aby włamać się do systemów wojskowych” powiedział generał brygady Karol Molenda. W wywiadzie dyrektor Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni mówił o problemach z wdrażaniem wojskowych systemów teleinformatycznych oraz planach MON w obszarze kryptologii.

W naszych systemach bezpieczeństwo wygrywa nad funkcjonalnością

„Systemy teleinformatyczne w wojsku przetwarzają informacje niejawne, dlatego cechują się odpowiednimi wymaganiami cyberbezpieczeństwa, które muszą być spełnione, tak aby zapewnić poufność, dostępność i integralność danych” – powiedział w wywiadzie dla CyberDefence24.pl gen. bryg. Molenda. Systemy te podlegają stałej akredytacji i testom penetracyjnym. Jak podkreślił, jest to ogromne wyzwanie, aby system zaprojektować, zbudować a następnie wdrożyć i utrzymać. „Odpowiadamy za jego cały cykl życia, od jego uruchomienia po wycofanie z eksploatacji” – dodał generał. „W naszych systemach bezpieczeństwo wygrywa nad funkcjonalnością, odwrotnie niż jest to na rynkach prywatnych, gdzie funkcjonalność jest kluczowa” – tłumaczył w trakcie rozmowy.. Wspomniał również, że wojsko nie może pozwolić sobie na luki bezpieczeństwa, gdyż zostaną one wykorzystane przez adwersarzy. Podkreślił rolę NCBC, które jest odpowiedzialne za wszystkie systemy stacjonarne w polskich siłach zbrojnych. „Praktycznie każdy komputer, urządzenie mobilne wykorzystywane w resorcie obrony narodowej i wojsku jest zakupione i skonfigurowane przez NCBC lub jednostki bezpośrednio podległe” – potwierdził Molenda.

„Na podstawie zdolności, które muszą posiadać siły zbrojne definiujemy rozwiązania niezbędne do zapewnienia odpowiedniej poufności danych”

Na uwagę zasługuje fakt, że modernizacja sił zbrojnych wymaga nie tylko sprzętu i nowoczesnego uzbrojenia, ale również rozwiązań teleinformatycznych, które zapewniają dowódcy możliwość podjęcia decyzji i dostęp do danych. Te rozwiązania teleinformatyczne muszą być odpowiednio zabezpieczone kryptograficznie, żeby funkcjonowały poprawnie”– wyjaśniał w trakcie rozmowy generał. „Na podstawie zdolności, które muszą posiadać siły zbrojne, definiujemy rozwiązania niezbędne do zapewnienia odpowiedniej poufności danych, czyli opracowania odpowiednich narzędzie kryptograficznych” - powiedział.

W odniesieniu do sprawy szwajcarskiej firmy kryptograficznej AG, która miała być prowadzona przez niemiecki i amerykański wywiad, Dyrektor NCBC stwierdził, że w tym przypadku zabrakło odpowiedniego nadzoru kontrwywiadowczego. W Polsce to SKW i ABW zapewniają tego typu ochronę firmom, które realizują badania, wdrażają sprzęt lub rozwiązania kryptograficzne do resortu obrony

narodowej lub instytucji rządowych.

„Współpraca z polskim przemysłem jest dla nas kluczowa”

„Polski przemysł jest informowany o kierunkach i priorytetach, jeżeli chodzi o kryptografię. Dostrzegamy potrzebę, by wykorzystywać polski przemysł do uruchamiania, wdrażania narzędzi kryptograficznych, ale również do pracy nad standardami” – kontynuował Molenda. Przypomniał również, że rozwiązania kryptograficzne muszą funkcjonować w sposób bezpieczny, ale również tak, by zapewniły interoperacyjność z rozwiązaniami sojuszniczymi, czyli by potrafiły w pewnych standardach ze sobą „rozmawiać” i wymieniać informacje. „Dlatego kładziemy nacisk na informowanie polskiego przemysłu by wspólnie z nami, w ramach badań naukowych i rozwojowych szereg tych zadań mógł być realizowany przez polskie firmy. Współpraca z nimi jest dla nas kluczowa” – podkreślił generał Molenda.

„Nasze systemy są łakomym kąskiem. Próby ataków, przełamania naszych zabezpieczeń i szukania najsłabszych punktów odbywają się codziennie”

Odpowiadając na pytanie o różnice w atakach na systemy wojskowe i cywilne, generał stwierdził, że jest to kwestia różnego typu adwersarzy, którzy stoją za działaniami wymierzonymi w instytucje wojskowe.

Zdaniem Dyrektora NCBC w sektorze cywilnym znaczną część atakujących stanowią cyberprzestępcy, którzy podążają za pieniędzmi. Włamują się po to, aby uzyskać pewne informacje, by móc je sprzedać i uzyskać profity. Taki typ atakującego, zdaniem generała, będzie sięgał po najłatwiejsze cele. Jęsli jednak bezpieczeństwo jednej firmy będzie stało na wyższym poziomie niż innej, to atakujący może uznać, że nie warto się starać i zrezygnuje z ataku.

„W wojsku mamy do czynienia z zupełnie innym typem aktorów, którzy ciągle nas testują lub próbują włamać się nam do systemów. Mówimy tutaj o aktorach, za którymi stoją służby specjalne” – podkreślił generał. „Takie grupy hakerskie są ustrukturyzowane i hierarchiczne. Jeżeli oni (hakerzy – red.) już atakują, to znaczy to, że dostali takie polecenie i nie wycofują się, jeżeli napotkają trudności” – tłumaczył generał. „Szukają podatności i ścieżek dostępu, aby się dostać do systemu. Jeśli nie udało się dzisiaj, to spróbują jutro. Ten proces jest ciągły” – podkreślał Molenda w trakcie rozmowy.

Obserwujemy szereg grup hakerskich, za którymi prawdopodobnie stoją służby specjalne z niekoniecznie przyjaznych nam krajów, które testują nasze możliwości obronne, po to, aby włamać się do systemów wojskowych, gdzie jest bardzo dużo wrażliwych informacji – mówił generał. Więc w każdym z tych przypadków, nasze systemy są łakomym kąskiem - próby ataków, przełamania naszych zabezpieczeń i szukania najsłabszych punktów odbywają się codziennie - dodał.

Generał Molenda mówiąc o tym na jakim etapie znajduje się rozwój Wojsk Obrony Cyberprzestrzeni wyjaśnił, że zakończono obecnie fazę uregulowania systemu cyberbezpieczeństwa w resorcie obrony narodowej. Jak podkreślił, zostało jednoznacznie wskazane, gdzie umiejscowiony jest CSIRT MON oraz jakie są jego procedury, mechanizmy funkcjonowania i reagowania. Wspomniał również, że obecnie głównym celem jest zrekrutowanie odpowiedniej ilości osób do Wojsk Obrony Cyberprzestrzeni. Dlatego też trwają prace nad właściwymi mechanizmami, które mogłyby przyspieszyć rekrutację. Dodał również, że sytuacja epidemiologiczna w oczywisty sposób wpływa na możliwość spotykania się twarz w twarz.. Natomiast, jak wspomniał, zostało uruchomionych wiele rozwiązań w trybie online jak np. komunikatory internetowe, rozmowy kadrowe czy czynna w dni robocze infolinia rekrutacyjna. „Staramy się rekrutować pomimo trudnej sytuacji. W najbliższym czasie uruchomimy nawet możliwość oceniania kandydatów online, więc będziemy mogli cały proces zakończyć zdalnie” – zakończył generał.

Szef SKW jako nowy pełnomocnik MON ds. bezpieczeństwa cyberprzestrzeni

Generał Molenda skomentował również wybór szefa SKW – Ministra Macieja Materki na pełnomocnika ministra obrony narodowej ds. bezpieczeństwa cyberprzestrzeni. Przyznał, że miał możliwość służyć pod jego komendą i w jego opinii jest to wybór bardzo trafny.

Pod komendą Ministra Materki, w SKW kładziono bardzo duży nacisk, żeby rozwijać kompetencje w zakresie cyberbezpieczeństwa. „Służba realizuje swoje zdolności w ramach cyberkontrwywiadu czy w zakresie certyfikacji rozwiązań teleinformatycznych, więc nacisk był zauważalny i widać było, że temat ten był priorytet jego działań" – dodał Molenda.

Pełna treść rozmowy z dyrektorem NCBC – gen. bryg. Karolem Molendą dostępna jest w ramach programu Skaner CyberDefence24.pl.

Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni jest jednostką ekspercką, która realizuje zadania w trzech domenach: informatyki, kryptologii i cyberbezpieczeństwa. Jest jednostką podległą Ministrowi Obrony Narodowej.