GEN. MOLENDA: "MOIM GŁÓWNYM CELEM JEST INWESTYCJA W LUDZI"

„Jesteśmy tak silni, jak najsłabszy specjalista, który u nas służy lub pracuje” – stwierdził gen. bryg. Karol Molenda, dyrektor Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni. Jednocześnie podkreślił, że jego głównym celem jest inwestycja w ludzi. CSIRT MON odpowiedzialny za bezpieczeństwo wszystkich systemów resortowych jest kluczowym elementem cyberbezpieczeństwa, zwłaszcza, że - jak podkreślił generał - ataki z którymi musimy się obecnie mierzyć są coraz bardziej zaawansowane.

Zacznijmy od początku! Czym jest CSIRT MON?

Jak podkreślił gen. Molenda CSIRT MON jest jednym z trzech filarów cyberbezpieczeństwa Polski, czyli zespołów reagowania na incydenty bezpieczeństwa komputerowego w kraju (po CSIRT NASK i CSIRT GOV). Zadania dla tej struktury zostały określone w ustawie o krajowym systemie cyberbezpieczeństwa z 2018 r., która określiła jego główne zadanie - czyli ochronę systemów teleinformatycznych. CSIRT jest zespołem funkcjonującym w ramach Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni – jednostki eksperckiej MON.

Monitorujemy incydenty, które materializują się w tych systemach, analizujemy i reagujemy na nie oraz staramy się działać, aby utrzymać bezpieczeństwo na najwyższym poziomie - powiedział gen. bryg. Karol Molenda, zapytany o zakres odpowiedzialności, jaki spoczywa na CSIRT MON.

„Współpraca z pozostałymi CSIRTami jest kluczowa i pozwala nam na wymienianie się informacjami o zagrożeniach” – stwierdził Dyrektor NCBC. Jak podkreślił w wywiadzie, jest ona z każdym dniem coraz efektywniejsza.

Dzięki wzajemnej wymianie informacji zespół posiada pełniejszy obraz sytuacji i jest w stanie szybko reagować na incydenty, a także im skuteczniej przeciwdziałać. Jak podkreślił informacje o zagrożeniach, które próbują się materializować w systemie monowskim są przekazywane w ustalonym zakresie do pozostałych CSIRTów. Jednocześnie zespół jest na bieżąco informowany o aktorach, w tym narodowych, które próbują się materializować w systemach resortowych.

CSIRT MON nie pracuje w próżni – współpraca z ramach UE i NATO

W UE i NATO funkcjonują zespoły reagowania na incydenty komputerowe: CERT-UE Computer Emergency Response Team for the European Union for the EU institutions oraz NATO Computer Incident Response Capability (NCIRC). „Współpracujemy z jednym i drugim. Zespół zorganizowany w ramach struktur NATO i UE jest w dużej mierze zespołem, który jest podobny do naszej struktury” – podkreślił gen. Molenda. „Oczywiście ta współpraca ma różne wymiary i dotyczy kluczowych obszarów

działania w ramach naszego partnerstwa" – dodał. Generał przypomniał, że w lipcu zeszłego roku zostało podpisane porozumienie między Polską a NATO i w jego ramach zadeklarowano wzajemną wymianę informacji o zagrożeniach oraz potwierdzono utworzenie i utrzymywanie punktów kontaktowych pracujących w trybie 24/h, które odpowiedzialne są za zbieranie informacji i przetwarzanie ich pomiędzy zespołami.

„CSIRT MON – co nas wyróżnia"

„Osoby, które chcą się rozwijać, które nie boją się wyzwań, które chcą odpowiadać za bezpieczeństwo najbardziej wrażliwych systemów w kraju są oczywiście u nas mile widziane" – podkreślił gen. Molenda. Jak wspomniał – „Przestrzeń do pracy oraz rozwoju swoich pasji w ramach NCBC jest duża". CSIRT MON szuka specjalistów z odpowiednim doświadczeniem i wiedzą, ale również nie zamyka się na osoby, które dopiero rozpoczynają swoją karierę i budowanie swojej wiedzy w zakresie cyberbezpieczeństwa, dla których jest zaprojektowana satysfakcjonująca ścieżka rozwoju.

Zespół odpowiedzialny jest nie tylko za system jawny, ale jak wskazał generał odpowiada również za bezpieczeństwo niejawnych systemów resortu obrony narodowej. „Nie ma co ukrywać, najbardziej wrażliwymi systemami są te, które przetwarzają informacje niejawne stąd musimy dbać w sposób szczególny o ich bezpieczeństwo" – kontynuował.

„Jestem przekonany, że aktorzy, przeciwnicy, którzy próbują operować w naszych sieciach cechują się o odpowiednio wysokim poziomem wiedzy i doświadczenia. Stąd ich próby ataków, są bardzo zaawansowane, ale po naszej stronie mają najlepszych w naszym kraju ekspertów, których zatrudniamy w CSIRT MON" – odpowiedział gen. Molenda zapytany o zagrożenia, za zwalczanie których odpowiedzialna jest podległa mu struktura.

CSIRT MON stanowi strukturę, która otwarta jest na osoby, które posiadają już spory bagaż doświadczeń zawodowych, ale również na te które dopiero rozpoczynają swoją karierę w zakresie cyberbezpieczeństwa. Są jednak kluczowe wymagania, którym należy sprostać – umiejętność pracy pod presją czasu i chęć do nieustannego rozwoju, gdyż obszar, którego broni CSIRT podlega dynamicznym zmianom. „Osoby, które chcą dołączyć do naszego zespołu muszą charakteryzować się tym, że chcą (i potrafią) rozwijać się w sposób ciągły" – podkreślił Molenda. „Taka osoba musi umieć pracować / służyć pod presją czasu, ale jednocześnie zapewniamy takim osobom możliwość budowania swojej wiedzy, by skuteczniej przeciwdziałać tego typu atakom" – dodał.

„Moim głównym celem jest inwestycja w ludzi"

„Jesteśmy tak silni jak najsłabszy u nas specjalista" – podkreślił gen. Molenda w trakcie wywiadu. Określając plany na przyszłość wspomniał, że w pierwszej kolejności będzie to budowanie kompetencji i rozwijanie ich właśnie pośród kadry. Generał postawił na inwestycje w szkolenia i zgrywanie zespołu, które w jego opinii są tak samo ważnym elementem, jak budowanie indywidualnych umiejętności poszczególnego specjalisty.

Jaki jest plan na przyszłość? „Inwestycja w ludzi, pozyskiwanie nowych kadr. Napływ „świeżej krwi" jest kluczowy by tak duży organizm jakim jest resort obrony narodowej mógł być chroniony na najwyższym poziomie i funkcjonować w sposób sprawny" – stwierdził w odpowiedzi na to pytanie – „Moim planem jest także doskonalenie umiejętności kadry, która już jest zatrudniona w naszych strukturach. To jest nasz plan na przyszłość".

Tekst powstał we współpracy z Narodowym Centrum Bezpieczeństwa Cyberprzestrzeni.