GEN. MOLENDA: UŻYTKOWNICY ZAUWAŻYLI, ŻE BEZ NAS, JAKO BEZ CYFROWEGO SERCA ARMII NIE MOGŁABY REALIZOWAĆ SWOICH ZADAŃ

Gen. Karol Molenda, dyrektor Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni: użytkownicy z resortu, o których bezpieczeństwo w sieci dbamy w trybie 24/7/365, a których jest ponad sto tysięcy zauważyli, że bez nas, jako cyfrowego serca armii nie mogliby realizować swoich zadań. Każdy komputer, każdy telefon, a nawet każda wgrana na nim aplikacja, jest efektem pracy NCBC.

„W ostatnim czasie zwróciliśmy uwagę na globalnie odnotowywany fakt, że przestępcy intensywnie wykorzystują aspekt związany z poczuciem zagrożenia wśród użytkowników bazując na strachu m.in. w związku z COVID-19" – przyznał gen. bryg. Karol Molenda. W trakcie wywiadu wskazał również na konieczność przygotowania się na być może kolejną falę pandemii, kiedy pracownicy wojska ponownie będą zmuszeni do przejścia w tryb pracy zdalnej.

„Pandemia koronawirusa pozwoliła zwrócić uwagę wielu naszym użytkownikom na aspekty związane z infekcją i koniecznością działań profilaktycznych"

Generał metaforycznie wskazuje, że jako obywatele wiedzieliśmy, że wirusy istnieją i że należy myć ręce, jednak nie każdy robił to z należytą starannością - tym samym, pandemię koronawirusa można również przełożyć na sytuację, z którą musimy zmagać się każdego dnia w sieci, a która również wymaga od nas „cyber higieny" oraz wzmożonej czujności.

Więcej było kampanii phishingowych, w którym motywem przewodnim był COVID-19

„Zwróciliśmy uwagę na fakt, że przestępcy intensywnie wykorzystywali aspekt związany z poczuciem zagrożenia pośród użytkowników" – przyznał generał w trakcie wywiadu. Wskazał, że CSIRT MON odnotował więcej ataków phishngowych, spamu, działań socjotechnicznych wykorzystujących motyw koronawirusa. „Więcej było kampanii phishingowych, w którym motywem przewodnim był COVID-19" - podkreślił.

Wskazał jednak, że był to zaledwie ruch statystyczny „nasze urządzenia wykrywały go szybko i odcinały cały ruch. Faktem jest, że odnotowaliśmy więcej tego typu prób natomiast nie przełożyło się to na obniżenie bezpieczeństwa naszych użytkowników, gdyż nasze systemy, procedury i ludzie zadziałały prawidłowo" - podkreślił.

„Sytuacja związana z COVID -19 pozwoliła na uświadomienie sobie ważności higieny, chociażby higieny cyberbezpieczeństwa"

„Część użytkowników zauważyła, że bez nas, jako bez cyfrowego serca armii nie mogłaby realizować swoich zadań” – podkreślił gen. Molenda. Jak wskazał, praktycznie z dnia na dzień, użytkownicy zostali niejako zmuszeni do korzystania z systemów teleinformatycznych w sposób zdalny.

Pandemia koronawirusa stanowiła duże wyzwanie także dla CSIRT MON. „Dla nas jednym z większych wyzwań był fakt, że armia nie jest strukturą, która na co dzień pracuje zdalnie z domu” – wskazał Molenda. NCBC musiało w dość krótkim czasie przygotować odpowiednie (bezpieczne) narzędzia i systemy do pracy zdalnej dla potrzebujących tego pracowników wojska, którzy byli kierowani na tego typu pracę.

„Zespoły cyberbezpieczeństwa, szczególną uwagę musiały zwracać na pracę zdalną oraz na fakt, że część naszych systemów jest poza strefami administracyjnymi resortu obrony narodowej” – wskazał Molenda w trakcie wywiadu. „Pewnym wyzwaniem w dalszym ciągu zostaje fakt, że gro kluczowych systemów teleinformatycznych to systemy przetwarzające informacje niejawne” – podkreślił. W opinii generała praca zdalna wymaga dalej pewnych analiz, a nawet kroków prawnych, tak aby przygotować się na potencjalne zdarzenie w przyszłości, które wymagało będzie dostępu chociażby do części takich systemów, jak do systemów obsługujących dane z nadaną klauzulą „zastrzeżone”, aby zapewnić możliwość pracy zdalnej w ramach tych systemów w sposób zdalny.

Tekst powstał we współpracy z Narodowym Centrum Bezpieczeństwa Cyberprzestrzeni.