aut. Szymon Palczewski 11.07.2019

AMERYKAŃSKA STRAŻ PRZYBRZEŻNA ALARMUJE: SŁABE ZABEZPIECZENIA STATKÓW PODNOSZĄ RYZYKO KATASTROFY

Straż przybrzeżna USA wydała oficjalne ostrzeżenie dla właścicieli statków, w którym wskazuje na konieczność aktualizacji systemów znajdujących się na okrętach oraz mniejszych łodziach. Służby podkreślają, że cyberbezpieczeństwo jest również kluczowym elementem żeglugi morskiej.

W raporcie Marine Safety Alert stwierdzono, że przeprowadzenie kompleksowej oceny cyberbezpieczeństwa powinno być podstawowym elementem kontroli okrętów morskich. Ostrzeżenie wydane przez służby jest związane z cyberatakiem wymierzonym w jeden ze statków płynących do portu w Nowym Jorku. Zdarzenie miało miejsce w lutym br.

Według analizy incydentu z początku roku, w wyniku działalności hakerów jeden z systemów komputerowych okrętu został zakłócony. Społeczeństwa nie są świadome, że również statki oraz mniejsze łodzie mogą stać się celem cyberprzestępców. Taka sytuacja podnosi ryzyko wystąpienia incydentu.

Okręty posiadają wiele systemów, które mogą być narażone na cyberataki. W tym miejscu można wskazać na mapy elektroniczne i nawigację, zarządzanie danymi pokładowymi, a także komunikację z pobliskimi portami oraz przybrzeżnymi stacjami kontrolnymi. Każdy z nich może zostać naruszony przez hakerów.

Większość zaleceń skierowanych do osób odpowiedzialnych za okręty morskie, zawarte w Marine Safety Alert dotyczy podstawowych rzeczy. Wśród nich można wskazać na m.in.:

- konieczność podziału głównych systemów na podsystemy, aby w ten sposób utrudnić hakerom dostęp do podstawowych sieci i urządzeń;
- utworzenie odrębnych profili z indywidualnym hasłem dla każdego pracownika. Równocześnie od personelu należy wymagać regularnego zmieniania haseł;
- konta przeznaczone wyłącznie dla administratora należy używać tylko w razie potrzeby;
- niezbędne jest zainstalowanie i regularne aktualizowanie oprogramowania antywirusowego;
- konieczność cyklicznego przeglądu zabezpieczeń w celu wykrycia luk, a następnie ich skuteczne usunięcie.

W raporcie podkreślono również istotną rolę czynników zewnętrznych, które mogą mieć wpływ na zwiększenie ryzyka. Jednym z nich jest korzystanie z nośników pamięci USB. Podłączenie urządzenia ze złośliwym oprogramowaniem bez wcześniejszego skanowania może zainfekować kluczowe systemy.

Źródło: Forbes