Cyberdefence 24

aut. Szymon Palczewski 13.08.2019

REPUTACJA PONAD CYBERBEZPIECZEŃSTWO. PRZEMYSŁ MORSKI BAGATELIZUJE PROBLEM CYBERATAKÓW

Osoby odpowiedzialne za żeglugę morską muszą być świadome zagrożeń występujących w cyberprzestrzeni. We współczesnym świecie hakerzy ukierunkowują swoje działania w różne cele. Wśród nich znajdują się statki oraz inne okręty. W związku z tym cyberbezpieczeństwo musi stać się integralną częścią zarządzania bezpieczeństwem w branży morskiej – alarmuje dziennik Lloyd's List.

Cyberataki dotykają zarówno duże, jak i małe firmy przemysłu morskiego. Częstotliwość incydentów stale rośnie, jednak świadomość oraz gotowość do reakcji na działalność hakerów stale utrzymuje się na niezadawalającym poziomie – informuje dziennik.

Podmioty odpowiedzialne za żeglugę morską są zobligowane do zgłaszania incydentów, które naruszają dane osobowe klientów władzom lokalnym i krajowym, a także wskazanym organom regulacyjnym. Zgodnie z prawem poinformowane muszą zostać również osoby poszkodowane.

Z kolei jeśli chodzi o inne rodzaje cyberataków, jak np. phishing czy ransomware, regulacje nie nakładają na firmy obowiązku zgłaszania incydentów innym organom. Brak takiego wymogu sprawia, że przedsiębiorstwa bardzo często ukrywają całą sytuację z obawy przed utratą reputacji. Według Lloyd's List całość składa się na budowę fałszywego poczucia bezpieczeństwa w branży morskiej.

W celu rozwiązania problemu brytyjska firma CSO Alliance opracowała anonimowy system raportowania o incydentach, aby stworzyć firmom morskim odpowiednią platformę, która zagwarantuje im pełną anonimowość i poufność.

Informowanie o cyberatakach jest pierwszym kluczowym krokiem w stronę cyberbezpieczeństwa całego sektora, ponieważ przyczyni się do zwiększenia świadomości oraz gotowości na działania hakerów – wskazuje dziennik. Mechanizm jest bardzo prosty – im więcej firm zidentyfikuje cyberataki w swoich systemach i poinformuje o tym środowisko, nawet w sposób anonimowy, tym bardziej inne podmioty branży będą świadome zagrożeń oraz skali całego problemu. Wówczas podejmą odpowiednie działania w celu lepszego zabezpieczenia swoich sieci i systemów, zmniejszając ryzyko strat.