Cyberdefence 24

30.07.2021

NOWE WERSJE OPROGRAMOWANIA RANSOMWARE ZAGROŻENIEM DLA PRZEMYSŁU

Postępująca cyfryzacja sprawia, że cyberprzestępcy obierają sobie coraz większe cele. Pandemia sprzyja wzrostowi liczby ataków skierowanych na koncerny zajmujące się kluczowymi obszarami gospodarki, m.in. produkcją, transportem i mobilnością. Problem ten będzie narastał - podkreślają eksperci.

Przemysł, stanowiący niegdyś odosobnioną gałąź gospodarki, przekształca się stopniowo w system połączony ze światem zewnętrznym. A to za sprawą takich narzędzi, jak technologia 5G czy Internet Rzeczy, które napędzają rewolucję przemysłową.

Jednak automatyzacja procesów i połączenia między przedsiębiorstwami, poza zwiększeniem możliwości produkcyjnych, niosą ze sobą większe ryzyko ataków hakerskich.

Cyberataki na przemysł

Od początku pandemii coraz więcej incydentów związanych z atakami hakerskimi ma miejsce w przemyśle.

Doświadczyły tego takie koncerny, jak Trigano oraz Honda - producenci samochodów, którzy padli ofiarą złośliwego oprogramowania ransomware. Na skutek cyberataków została wstrzymana produkcja w kilku państwach - w przypadku Hondy utrudnienia dotknęły aż jedenaście fabryk na całym świecie, m.in. w USA, Brazylii, Turcji i Indiach. Podobne incydenty mają miejsce również w Polsce.

„Powyższe przykłady jasno wskazują, że nikt nie może czuć się w pełni bezpieczny, a postępująca cyfrowa transformacja gospodarki nie może odbywać się bez uwzględnienia kwestii cyberbezpieczeństwa. Wdrożenie 5G i Internetu Rzeczy, bez solidnych podstaw w zakresie optymalizacji bezpieczeństwa cyfrowego, wiąże się z większą możliwością znalezienia przez przestępców luk. Wykorzystując je mogą oni infekować system i paraliżować pracę przedsiębiorstwa” - mówi Piotr Zielaskiewicz, product manager w firmie Stormshield - dystrybutora rozwiązań do ochrony sieci.

Ransomware zagrożeniem

Trudność w wykrywaniu oprogramowania ransomware polega na ciągłym udoskonalaniu tego narzędzia przez cyberprzestępców i dostosowywaniu go do konkretnych gałęzi przemysłu. W tym celu powstał również nowy wirus wyspecjalizowany w tym obszarze.

„Jednym z nich jest malware EKANS, relatywnie prosty w porównaniu do innych znanych w branży przemysłowej – choćby liczącego blisko 10 lat robaka Stuxnet czy mającego na koncie ataki na

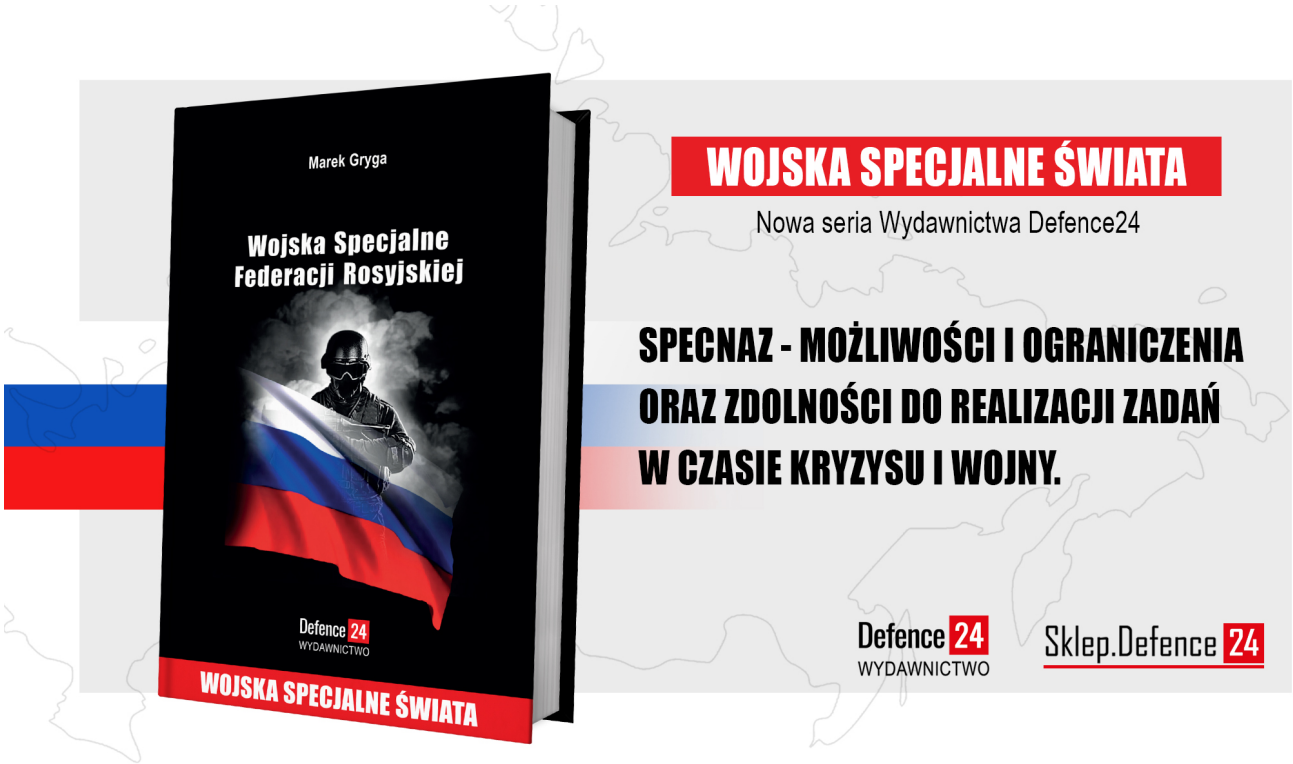
systemy sterowania ukraińskimi sieciami elektroenergetycznymi BlackEnergy. Jednakże nowością jest tu fakt, że **szyfruje on pliki systemów służących do kontroli pracy maszyn i instalacji technologicznych,** w efekcie powodując wyłączenia oraz straty producentów" - dodaje Piotr Zielaskiewicz.

Specjaliści uważają, że szczególną uwagę należy skupić na połączeniach pomiędzy fabrykami, które dysponują dużymi zasobami przemysłowymi, a także na zwiększenie kompetencji pracowników w zakresie cyberzarządzania.

Monitoring sieci, jej segmentacja oraz wprowadzenie odpowiednich zabezpieczeń to tylko kilka przykładów działań, które mogą pomóc zminimalizować ryzyko cyberataków w przemyśle.

Na podst. informacji prasowej.

Chcemy być także bliżej Państwa – czytelników. Dlatego, jeśli są sprawy, które Was nurtują; pytania, na które nie znacie odpowiedzi; tematy, o których trzeba napisać – zapraszamy do kontaktu. Piszcie do nas na: redakcja@cyberdefence24.pl. Przyszłość przynosi zmiany. Wprowadzamy je pod hasłem #CyberIsFuture.



Fot. Reklama