**Czy Doom to wytrych do firmowych systemów IT?**

* **Niewinna demonstracja w postaci instalacji gry Doom na komputerze nowoczesnego traktora, ujawniła poważny problem związany z cyberbezpieczeństwem maszyn. Stało się to podczas DEF CON Hacking Conference.**
* **Według prognoz G Data CyberDefense, liczba ataków na infrastrukturę krytyczną może wzrosnąć w 2023 roku. Szczególnie firmy powinny zadbać o swoje bezpieczeństwo.**
* **Sposoby na minimalizację ryzyka cyberataku na firmową infrastrukturę IT to m.in. Web Application Firewall i testy penetracyjne.**

Głośno było niedawno o sytuacji znanej z konferencji DEF CON w Las Vegas. Haker Sick Codes uruchomił w czasie swojej prezentacji kultową grę Doom na komputerze nowoczesnego ciągnika rolniczego marki John Deere. Gra została w tym celu przygotowana w specjalnej, „rolniczej” wersji, a panelista w humorystyczny sposób obnażył niski poziom cyberbezpieczeństwa traktora i zwrócił uwagę na fakt, że problem może być znacznie szerszy.

*– Użytkownicy wielu urządzeń czasem nie zdają sobie sprawy, że interfejs maszyny może zostać zaatakowany przez hakera. Albo nawet jeśli o tym wiedzą, to uważają, że ryzyko ataku i jego potencjalne skutki są zbyt niskie, by stwarzało jakiekolwiek zagrożenie. Jak się okazuje – to błąd, ponieważ hakerzy potrafią wykorzystać brak zabezpieczeń urządzeń IoT, żeby wejść głębiej do systemu firmowego i wykraść dane lub przynajmniej doprowadzić do paraliżu infrastruktury, co powoduje realne strat finansowe. W przypadku maszyny rolniczej może to oznaczać zatrzymanie jej pracy, a nawet uszkodzenie, co może narazić rolnika na ogromne koszty –* mówi Patrycja Tatara, ekspertka ds. cyberbezpieczeństwa w Sprint S.A.

**Cyberataki na maszyny to poważne niebezpieczeństwo**

Australijski haker Sick Codes słynie z cyberataków na urządzenia IT w maszynach rolniczych. W ten sposób próbuje inspirować do podniesienia poziomu ich cyberbezpieczeństwa. Hakerzy potrafią też zablokować linię produkcyjną, a to może prowadzić do ogromnych strat finansowych i wizerunkowych. Znane przypadki z ostatnich lat, to m.in. atak ransomware na szwedzką sieć sklepów spożywczych Coop, czy amerykańską firmę Colonial Pipeline (operator największego rurociągu w USA). Według prognoz G Data CyberDefense, liczba ataków na infrastrukturę krytyczną może wzrosnąć w 2023 roku, podobnie jak ataki killware. Te drugie mogą bezpośrednio wpływać nawet na bezpieczeństwo fizyczne, stwarzając zagrożenie życia. Stąd taka nazwa – za pomocą programów ransomware hakerzy blokują systemy, mające kluczowe znaczenie w funkcjonowaniu elektrowni czy placówek medycznych. Wystarczy przypomnieć cyberatak na szpital w Düsseldorfie. Na jego skutek doszło do paraliżu systemu, co uniemożliwiło przyjmowanie kolejnych pacjentów. Karetki trzeba było kierować od innych miast, w tym ambulans z pacjentką w stanie krytycznym, który skierowano do oddalonego o 32 km Wuppertalu. Kobieta zmarła w drodze. Potwierdza się więc zasada, że nie należy zadawać sobie pytania, czy dojdzie do cyberataku, ale – kiedy on nastąpi.

**Jak zabezpieczyć sieć firmową przed złośliwym ruchem?**

Humorystyczny wyścig na metody uruchomienia Dooma rozpoczął się po decyzji twórców kultowej gry z 1993 roku, którzy po latach opublikowali jej kod źródłowy dla programistów w celach edukacyjnych. Niekończąca się zabawa związana z pomysłami na włączenie gry na rozmaitych urządzeniach stała się elementem internetowej popkultury. Jednocześnie obnaża to ciemną stronę cyberbezpieczeństwa firm. A co jeśli hakerzy wpadną na pomysł zagrania w tę grę na sprzęcie konkretnej firmy i tym sposobem poznają luki w jej zabezpieczeniach IT? Mogą to wykorzystać do przeprowadzenia cyberataku albo jeszcze gorzej – zablokują infrastrukturę i uzyskają dostęp do firmowych danych?

*– Na szczęście istnieją narzędzia, które umożliwiają wykrycie i filtrację złośliwego ruchu, który może prowadzić do poważniejszych zagrożeń. Mam na myśli nie tylko paraliż infrastruktury IT, ale także wyciek danych lub blokadę dostępu i wymuszenie okupu w celu ponownego odblokowania. Warto więc zainstalować Web Application Firewall (WAF), który na bieżąco będzie wykrywał złośliwy ruch w aplikacjach firmowych i skutecznie je blokował. Dodatkowy sposób na wzmocnienie zabezpieczeń to cykliczne testy penetracyjne, które wykażą luki w systemie i pomogą je trwale usunąć –* dodaje Patrycja Tatara ze Sprint S.A.

Testy penetracyjne to przeprowadzane przez specjalistów, symulowane ataki hakerskie. W ten sposób istnieje możliwość skutecznego wykrycia luk w zabezpieczeniu firmowej infrastruktury IT i ich usunięcia. Po przeprowadzeniu testu specjaliści przedstawiają raport wraz z sugestiami uszczelnienia zabezpieczeń.

**Gdzie można uruchomić Dooma?**

Lista przykładów urządzeń i przedmiotów, na których udało się uruchomić kultową grę, jest naprawdę imponująca. Chyba prościej jest zadać sobie pytanie, gdzie jeszcze nie udało się tego zrobić. Dotychczas Doom zadziałał m.in. na:

* touchbarze komputera,
* wyświetlaczu drukarki sieciowej,
* skanerze kodów kreskowych,
* bankomacie,
* kalkulatorze,
* kiosku do zamawiania posiłków w restauracji McDonald’s.

Pod koniec 2022 roku udało się włączyć grę w… notatniku i to z prędkością 60 FPS! Jednak najbardziej dziwacznym, choć trochę naciąganym przykładem, wydaje się kopiec ziemniaków. Oczywiście Doom nie został na nich uruchomiony bezpośrednio. Warzywa posłużyły tylko jako generator energii elektrycznej. Ziemniaki zawierają bowiem kwas fosforowy, który po stworzeniu obwodu z cynku i miedzi jest w stanie wytwarzać prąd. W ten sposób 45 kg gnijących już kartofli zapewniło energię dla kalkulatora graficznego TI-84, na którym uruchomiono grę. Autorem tego przedsięwzięcia był youtuber Equalo. Udało mu się tego dokonać w 2020 roku, po kilku miesiącach obliczeń i eksperymentów.

Źródło: Sprint S.A.