**aut. Szymon Palczewski** 23.10.2019

# IOT I PRZESTARZAŁE SYSTEMY OPERACYJNE GŁÓWNYM ŹRÓDŁEM NARUSZEŃ BEZPIECZEŃSTWA

60 proc. systemów w biznesie obsługiwanych jest przez przestarzałe produkty Microsoft, takie jak Windows 2000 i XP, które nie otrzymują już żadnych aktualizacji bezpieczeństwa. Urządzenia zaliczane do Internetu rzeczy (IoT) oraz przemysłowe systemy kontroli (ICS) stanowią główne źródło naruszeń bezpieczeństwa w firmach - wynika z raportu opracowanego przez CYBERX.

Najnowsza edycja raportu „2020 Global IoT/ICS Risk Report" analizuje dane zebrane z 1821 sieci z całego świata. Informacje pochodzą z wielu branż, które bazują na technologii IoT lub ICS. Mowa tutaj m.in. o podmiotach z sektora chemicznego i farmaceutycznego, petrochemicznego, produkcji energii, transportu czy robotyki i automatyzacji. Dokument opiera się przede wszystkim na danych zebranych podczas 12-miesięcznego okresu badawczego – od października 2018 roku.

Eksperci podkreślają, że raport różni się od innych podobnych dokumentów tym, że zawiera analizę przeprowadzoną na bazie danych uzyskanych bezpośrednio z systemów oraz sieci badanych podmiotów. Zgodnie z przedstawionymi liczbami specjaliści uzyskali dostęp do ponad 3000 sieci na całym świecie.

Systemy oraz sieci IoT i ICS nadal pozostają „miękkimi celami dla złośliwych aktorów" – stwierdzili specjaliści CYBERX w raporcie. Mowa tutaj zarówno o podmiotach państwowych, których celem jest m.in. zniszczenie infrastruktury krytycznej danego kraju, jak i cyberprzestępcach przeprowadzających zaawansowane cyberataki dla celów zarobkowych lub pobudek ideologicznych. Co więcej, dokument wskazuje również na główne grupy incydentów, do których zalicza działania ukierunkowane na kradzież własności intelektualnej lub tajemnicy handlowej oraz operacje skupiające się na wyrządzeniu znacznych szkód, bądź zakłócenia funkcjonowania konkretnych podmiotów.

W dokumencie przedstawione zostały także dane liczbowe, według których ponad 60% systemów obsługiwanych jest przez przestarzałe produkty Microsoft, takie jak Windows 2000 i XP, które nie otrzymują już żadnych aktualizacji bezpieczeństwa. Warto zaznaczyć, że szacowana liczba znacznie wzrośnie w przyszłości – nawet do 71% – ze względu na fakt, że w 2020 roku również Windows 7 nie będzie otrzymywał bezpłatnych poprawek.

Co więcej, prawie dwie trzecie systemów (64%) nie jest zabezpieczonych hasłem, a ponad połowa zbadanych przedsiębiorstw (54%) korzysta z urządzeń, które są zdalnie dostępne za pośrednictwem standardowych protokołów zdalnego zarządzania, takich jak RDP, SSH i VNC. Taki stan rzeczy sprawia, że hakerzy mogą w bardzo łatwy sposób uzyskać dostęp do krytycznych danych lub zainfekować sieć złośliwym oprogramowaniem. Przykładem może być cyberatak TRITON na systemy bezpieczeństwa w zakładzie petrochemicznym obsługiwanym przez Saudi Aramco i Sumitomo Chemical. Wówczas hakerzy wykorzystali RDP w celu zainfekowania systemów złośliwym oprogramowaniem – wskazują

eksperci CYBERX.

Równie istotny jest fakt, że tylko w 1 na 5 systemów specjaliści napotkali na wskaźniki zagrożeń, które alarmowałyby o pojawieniu się podejrzanego zachowania w ramach konkretnej sieci, np. nadmiernej liczby połączeń między danymi urządzeniami.

**Co można poprawić?**

Niniejszy raport wskazuje na realizację 7-etapowego procesu podnoszenia cyberbezpieczeństwa, wzorowanego na zaleceniach opracowanych przez Idaho National Labs (INL). Zgodnie z rekomendacją ekspertów należy kłaść nacisk na „bezwzględne ustalanie priorytetów" ochrony najbardziej krytycznych systemów i eliminację wszystkich niepotrzebnych „cyfrowych ścieżek", które mogą zostać wykorzystane przez złośliwych aktorów.

Dodatkowo, zaleca się wdrożenie odpowiednich mechanizmów, takich jak całodobowe monitorowanie bezpieczeństwa sieci, aby za ich pomocą natychmiast wykryć incydent i załagodzić jego skutki na samym początku złośliwej kampanii.

Raport wskazuje również na konieczność nieustannego monitorowania bezpieczeństwa sieci z wykrywaniem anomalii behawioralnych (BAD) jako kluczowym elementem bezpieczeństwa w podtrzymywaniu operacji biznesowych. Taki stan rzeczy może poprawić niezawodność ICS, a także zapewnić określone korzyści płynące z cyberbezpieczeństwa.

„Nie wiedząc o własnych słabościach, nie możemy podjąć kroków w celu ograniczenia ryzyka" – mówi treść „2020 Global IoT/ICS Risk Report". Jak wskazują specjaliści, dokument ma na celu zwrócenie uwagi liderów wielu branż oraz specjalistów ds. bezpieczeństwa na problem związany z zagrożeniami dotyczącymi sektora IoT oraz ICS.

**Czytaj też:** Cyberatak na litewskie MSZ. Hakerzy wykorzystali motyw amerykańskiej obecności w regionie