Szef australijskich służb wywiadowczych ostrzega, że chińscy hakerzy przygotowują się do sabotażu

- Szef australijskich służb wywiadowczych ostrzega, że chińscy hakerzy państwowi przygotowują się do sabotażu.
- Celem ataków są infrastruktury krytyczne związane z zaopatrzeniem w wodę, energię i telekomunikacją.
- Grupy hakerskie przygotowują się do zakłócenia działania sieci.
- Ich zamiary ewoluowały od szpiegostwa do potencjalnego zniszczenia i chaosu.
- Sektor prywatny znajduje się na pierwszej linii frontu tego zagrożenia dla bezpieczeństwa narodowego.

Żyjemy w świecie, w którym światło, woda i komunikacja, które łączą nasze społeczeństwo, są obecnie celem cichej wojny cyfrowej. Szef australijskiego wywiadu wydał poważne ostrzeżenie, że chińscy hakerzy wspierani przez państwo aktywnie badają najbardziej krytyczne systemy kraju, a ich zamiary zdecydowanie zmieniły się ze szpiegostwa na przygotowania do aktów niszczycielskiego sabotażu. W uroczystym przemówieniu skierowanym do liderów biznesu Mike Burgess, dyrektor generalny Australijskiej Organizacji Wywiadu Bezpieczeństwa (ASIO), ujawnił kampanię cyberagresji, która

zagraża fundamentalnym filarom współczesnego życia.

Podmioty stanowiące zagrożenie, zidentyfikowane jako grupy hakerskie Salt Typhoon i Volt Typhoon, nie są zbuntowanymi przestępcami, ale „hakerami pracującymi dla chińskich służb wywiadowczych i wojska" – stwierdził Burgess. Ich działania są częścią skoordynowanych wysiłków „jednego państwa – nietrudno zgadnąć, którego – [które] wielokrotnie próbowało skanować i penetrować infrastrukturę krytyczną w Australii i innych krajach należących do sojuszu Five Eyes". Celami są podstawowe usługi: sieci wodociągowe, transportowe, energetyczne i telekomunikacyjne.

Burgess ujawnił niepokojącą złożoność tych ataków. „Kiedy penetrują sieci, agresywnie mapują systemy" – wyjaśnił, opisując strategię utrzymywania długotrwałego, ukrytego dostępu. Nie chodzi tu tylko o kradzież tajemnic, ale o „przygotowanie się do chaosu". Celem jest uzyskanie możliwości zakłócenia i zniszczenia infrastruktury krytycznej w wybranym przez nich momencie, zamieniając naszą zależność technologiczną w głęboką słabość.

Zmiana intencji ze szpiegostwa na sabotaż oznacza niebezpieczną eskalację. Burgess ostrzegł, że reżimy autorytarne są obecnie bardziej skłonne do „zakłócania i niszczenia" w celu osiągnięcia swoich celów strategicznych. Nakreślił przerażające scenariusze, w których obce państwo mogłoby sparaliżować konkurencyjną australijską firmę, wywołać panikę podczas wyborów lub powstrzymać Australię przed wsparciem sojusznika w konflikcie. „Po uzyskaniu dostępu to, co dzieje się dalej, jest kwestią intencji, a nie możliwości" – ostrzegł.

Stawka ekonomiczna jest ogromna. Burgess poinformował, że szpiegostwo i ingerencja zagraniczna kosztowały australijską gospodarkę ogromną kwotę 12,5 mld dolarów w latach 2023–24. Jednak potencjalny koszt pojedynczego aktu sabotażu cybernetycznego jest jeszcze bardziej szokujący – ostrożne

szacunki wskazują, że wynosi on 1,1 mld dolarów na jeden incydent. Tygodniowe zakłócenie mogłoby spowodować szkody w wysokości 6 mld dolarów, co Burgess określił jako „bardzo ostrożne szacunki”. ”

Sektor prywatny musi być w stanie gotowości

W obliczu tego zagrożenia Burgess przekazał sektorowi prywatnemu mocne przesłanie, oświadczając: „Wasza działalność może nie dotyczy bezpieczeństwa narodowego, ale bezpieczeństwo narodowe dotyczy waszej działalności”. Wezwał liderów korporacyjnych do uznania swojej pierwszoplanowej roli w obronie kraju, wykraczając poza samozadowolenie i pustą retorykę. „Nie da się uniknąć tego ryzyka za pomocą prezentacji PowerPoint” – stwierdził, wzywając ich do podjęcia wszelkich rozsądnych kroków w celu zabezpieczenia swojej infrastruktury cyfrowej.

Ostrzeżenia te opierają się na rzeczywistych wydarzeniach. Burgess zauważył, że Volt Typhoon już naruszył krytyczną infrastrukturę Stanów Zjednoczonych, w tym systemy związane z wojskiem na Guam, dając Chinom możliwość „wyłączenia telekomunikacji i innej krytycznej infrastruktury”. Potwierdził, że podobne próby wykryto w Australii. „Zapewniam was: to nie są hipotetyczne scenariusze – zagraniczne rządy mają elitarne zespoły, które właśnie teraz badają te możliwości” – powiedział.

Pekin, jak można było przewidzieć, odrzucił te zarzuty jako „fałszywe narracje”. Burgess ujawnił jednak, że Komunistyczna Partia Chin aktywnie naciska na ASIO, aby złagodziła swoje publiczne oświadczenia. Jego odpowiedź była zdecydowana: „Gdyby byli mądrzy, zrozumieliby, jak działa zachodnia liberalna demokracja. Narzekanie na ASIO, że wykonuje swoją pracę, nie powstrzyma mojej determinacji”.

To zagrożenie cybernetyczne istnieje równolegle z rosnącymi napięciami militarnymi. W ostatnich miesiącach chiński myśliwiec wystrzelił flary w pobliżu australijskiego samolotu patrolowego na Morzu Południowochińskim, co było prowokacyjnym aktem podkreślającym szerszy wzorzec stosowania przymusu i testowania determinacji przez autorytarny reżim w Pekinie.

Cyfrowe linie frontu nie ograniczają się już do serwerów rządowych; przebiegają one przez systemy kontroli naszych elektrowni i sieci dostarczające wodę. Ostrzeżenie szefa australijskiego wywiadu przypomina, że wolność wymaga ciągłej, proaktywnej obrony. W epoce, w której chaos można wywołać jednym naciśnięciem klawisza, czujność jest ceną za zachowanie wolnego i funkcjonującego społeczeństwa.