Instytut Europy Środkowej

Komentarze IEŚ

Nr 1011 (259/2023) | 30.11.2023

ISSN 2657-6996

Agata Tatarenko

Jak Czechy radzą sobie z cyberbezpieczeństwem i dezinformacją po rozpoczęciu wojny w Ukrainie

Od kilkunastu lat systemy administracji publicznej, infrastruktury oraz służby zdrowia Republiki Czeskiej są celem regularnych ataków cybernetycznych. Ich liczba wzrosła po wybuchu pełnoskalowej inwazji Rosji na Ukrainę. Tendencję tę pokazują raporty na temat cyberbezpieczeństwa w 2022 r., opublikowane przez czeskie instytucje – Informacyjną Służbę Bezpieczeństwa (BIS) oraz Narodową Agencję ds. Bezpieczeństwa Cybernetycznego i Informatycznego (NÚKIB). W odpowiedzi na zagrożenia cybernetyczne władze Republiki Czeskiej podejmują szereg inicjatyw, które mają przeciwdziałać atakom i minimalizować ich skutki.

Ataki i przestępstwa cybernetyczne w Republice Czeskiej. Pod koniec października 2023 r. strony internetowe czeskiej administracji państwowej (Izby Poselskiej, Senatu, Ministerstwa Spraw Wewnętrznych) oraz operatorów infrastruktury stały się celem ataku hakerskiego. Przedstawiciele firm antywirusowych działających w Republice Czeskiej o atak posądzają jedną z prorosyjskich grup hakerskich. Podejrzenie to potwierdził minister spraw wewnętrznych Vít Rakušan (STAN), który stwierdził, że jest to jedna z wersji śledczych, a także Martin Churavý, rzecznik marszałka Izby Poselskiej.

Od momentu pełnoskalowej agresji Rosji na Ukrainę liczba ataków cybernetycznych w Republice Czeskiej gwałtownie wzrosła. Pokazuje to roczny raport Informacyjnej Służby Bezpieczeństwa (Bezpečnostní informační služba, BIS) za 2022 r., który został opublikowany pod koniec października 2023 r. Według dokumentu celem rosyjskich ataków w 2022 r. były strony internetowe instytucji państwowych, operatorów telefonicznych, operatorów infrastruktury transportowej oraz mediów. Wzrost aktywności rosyjskich hakerów w czeskiej przestrzeni internetowej jest, zdaniem BIS, bezpośrednio związany z rosyjską inwazją na Ukrainę.

Dane opublikowane przez BIS potwierdzają ustalenia zawarte w „Raporcie o stanie cyberbezpieczeństwa Republiki Czeskiej za 2022 r."[1] Narodowej Agencji ds. Bezpieczeństwa Cybernetycznego i Informatycznego (Národní úřad pro kybernetickou a informační bezpečnost, NÚKIB), który czeski rząd zatwierdził w lipcu 2023 r. Z dokumentu wynika, że w 2022 r. w Republice Czeskiej odnotowano niewielki spadek liczby incydentów cybernetycznych zarejestrowanych przez NÚKIB – ze 157 do 146. Jednak równolegle Policja Republiki Czeskiej odnotowała prawie dwukrotny wzrost działalności cyberprzestępczej. Największe zagrożenie dla cyberbezpieczeństwa Republiki Czeskiej niezmiennie stanowią działania podmiotów cybernetycznych sponsorowanych przez państwa trzecie oraz działalność grup cyberprzestępczych. Do najczęstszych typów ataków w 2022 r. należały różne rodzaje phishingu[2], takie jak spear-phishing[3] czy vishing[4], oraz ataki mające na celu zakłócenie dostępu do sieci internetowej, głównie DDoS[5]. W 2022 r. NÚKIB odnotował najwięcej incydentów cybernetycznych w sektorze publicznym, w tym w służbie zdrowia, oraz w sektorze prywatnym. Zarejestrował także znaczny, prawie dwukrotny wzrost liczby incydentów w krytycznej infrastrukturze informatycznej,

[1] NÚKIB, *Zpráva o stavu kybernetické bezpečnosti české republiky za rok 2022*, https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2022.pdf.
[2] Metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji.
[3] Rodzaj phishingu o bardziej ukierunkowanym charakterze; personalizacja wiadomości wywołuje u użytkownika wrażenie, że zna nadawcę – prywatną osobę bądź instytucję.
[4] Wyłudzanie danych przy pomocy rozmowy telefonicznej.
[5] Rodzaj ataku, którego celem jest zablokowanie dostępu do serwera lub usługi poprzez zalewanie go dużą liczbą fałszywych żądań.

z których większość stanowiły ataki ograniczające dostępność usług. W 2022 r. NÚKIB wydał łącznie 16 alertów i 3 ostrzeżenia w kontekście bieżących zagrożeń. Tendencja wzrostowa w zakresie przestępstw cybernetycznych utrzymuje się w 2023 r. Rekordowa aktywność przypadła na marzec, kiedy to czeski NÚKIB zanotował 28 tego typu incydentów.

Warto dodać, że Republika Czeska zmagała się z atakami cybernetycznymi na długo przed wybuchem pełnoskalowej wojny w Ukrainie. Od 2011 r. regularnie ich celem są systemy informatyczne czeskich szpitali oraz innych instytucji zdrowia. W 2018 r. ofiarą ataku hakerskiego była jedna z wiodących czeskich firm antywirusowych. W marcu 2021 r. doszło do zmasowanego cyberataku na systemy administracji publicznej Pragi. Przykładów takich działań można podać o wiele więcej. Władze Republiki Czeskiej podjęły stosowne kroki, aby zminimalizować ich liczbę i skutki. Należą do nich powoływanie instytucji odpowiedzialnych za wzmacnianie cyberbezpieczeństwa, wspieranie sektora prywatnego, edukacja społeczeństwa oraz ustawodawstwo.

Instytucje. Centralnym organem administracji publicznej odpowiedzialnym za cyberbezpieczeństwo jest wspominana wyżej Narodowa Agencja ds. Bezpieczeństwa Cybernetycznego i Informatycznego, powołana 1 sierpnia 2017 r. Do jej zadań należą: ochrona informacji niejawnych w systemach teleinformatycznych, ochrona kryptograficzna, obsługa rządowego CERT[6] oraz współpraca z innymi zespołami CERT w wymiarze krajowym i międzynarodowym, opracowywanie standardów cyberbezpieczeństwa, wsparcie edukacji w zakresie cyberbezpieczeństwa oraz prowadzenie badań i rozwój w tym obszarze. Dyrektor NÚKIB regularnie uczestniczy w posiedzeniach Rady Bezpieczeństwa Państwa (BRS) i jest członkiem Komitetu ds. Bezpieczeństwa Cybernetycznego, który jest stałym organem roboczym BRS, zajmującym się koordynacją i planowaniem działań w zakresie cyberbezpieczeństwa w Republice Czeskiej. NÚKIB zyskał międzynarodowy rozgłos i uznanie w grudniu 2018 r., kiedy ogłosił, że chińskie produkty Huawei i ZTE stanowią zagrożenie dla bezpieczeństwa, zwłaszcza w związku z rozwojem sieci 5G. Z kolei w marcu 2023 r. agencja opublikowała dokument, w którym instalację i używanie aplikacji TikTok uznała za poważne ryzyko dla bezpieczeństwa urządzeń posiadających dostęp do systemów informacyjnych i komunikacyjnych krytycznej infrastruktury informacyjnej, systemów informacyjnych ważnych usług i innych ważnych systemów IT. Komunikat został przedrukowany w wielu światowych mediach.

W czeskich siłach zbrojnych działa specjalna jednostka ds. Internetu – Wydział Cyberbezpieczeństwa i Operacji Informacyjnych (Velitelství informačních a kybernetických sil). Odpowiada on za ochronę informatycznych systemów wojskowych oraz za łączność strategiczną. Współpracuje z wywiadem wojskowym, a także innymi instytucjami zajmującymi się cyberpezpieczeństwem i obronnością Republiki Czeskiej.

Dużą wagę w Republice Czeskiej przykłada się do edukacji społecznej w kwestii cyberbezpieczeństwa. Jest to ważne zadanie realizowane przez NÚKIB. Agencja kształci zarówno urzędników służby cywilnej i pracowników instytucji publicznych (w tym sił bezpieczeństwa), jak i uczniów we wszystkich grupach wiekowych i na wszystkich poziomach edukacji. Prowadzi także wykłady i seminaria dla studentów oraz współpracuje z uczelniami w celu przygotowania ekspertów ds. cyberbezpieczeństwa. W Republice Czeskiej działa również szereg instytucji pozarządowych, których celem jest edukacja społeczna na temat cyberbezpieczeństwa oraz walka z fałszywymi informacjami i dezinformacją, zwłaszcza w Internecie. Najbardziej znaną tego typu organizacją jest czeski Demagog.

Działania i plany władz. Władze Republiki Czeskiej podejmują szereg inicjatyw w zakresie cyberbezpieczeństwa. Przykładem takiego działania była konferencja poświęcona temu problemowi w zakresie sieci 5G, zorganizowana na początku maja 2019 r. przez czeskie Ministerstwo Spraw Zagranicznych. W spotkaniu wzięło udział ponad 200 uczestników z 32 państw. Zaproszenia nie otrzymali przedstawiciele Rosji ani Chin. Efektem konferencji były tzw. propozycje praskie. Z uwagi na konwencję spotkania dokument miał dość ogólny charakter, jednak zawierał także pewne szczegółowe rekomendacje. Punktem wyjścia deklaracji wieńczących konferencję jest konstatacja,

[6] CERT, ang. Computer Emergency Response Team, organizacja, której zadaniem jest całodobowe nadzorowanie ruchu internetowego i podejmowanie natychmiastowych akcji w razie pojawienia się zagrożeń.

że sieć 5G pozwoli na automatyzację wielu czynności, co zasadniczo wpłynie zarówno na funkcjonowanie gospodarek, jak i życie codzienne ludzi. Rozwój cyfrowy będzie wiązał się jednak z rosnącym ryzykiem ataków cybernetycznych. Aby im zapobiegać, poszczególne państwa powinny dążyć do budowania odporności w tym zakresie. W praskich propozycjach rekomendowano jawność finansowania sieci telekomunikacyjnych oraz pogłębianie współpracy międzynarodowej, polegającej na wymianie informacji o atakach. Wzmocnienie europejskich zdolności obronnych i bezpieczeństwa w cyberprzestrzeni było także jednym z priorytetów Republiki Czeskiej w czasie jej prezydencji w Radzie UE w drugim półroczu 2022 r.

W 2022 r. władze Republiki Czeskiej rozpoczęły przygotowanie nowej ustawy o cyberbezpieczeństwie, która odpowiadałaby przepisom zawartym w Dyrektywie w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii Europejskiej (dyrektywa NIS2). Dyrektywa dotyczy m.in. bezpieczeństwa łańcucha dostaw technologii informacyjno-komunikacyjnych do infrastruktury o znaczeniu strategicznym. W Republice Czeskiej wejście w życie nowej ustawy o cyberbezpieczeństwie przewidywane jest w październiku 2024 r., kiedy zakończy się okres przejściowy dla przyjęcia dyrektywy NIS2. Projekt ustawy został przygotowany przez NÚKIB i przesłany do międzyresortowych konsultacji 19 czerwca 2023 r. Dokument poddano także obszernym konsultacjom społecznym.

Równolegle do prac nad projektem NÚKIB tworzył stronę internetową poświęconą nadchodzącej regulacji cyberbezpieczeństwa w Republice Czeskiej oraz UE. Pod adresem nis2.nukib.cz został opublikowany, w dwóch wersjach językowych, projekt ustawy, w formie, w jakiej przekazano go do procedury międzyresortowych konsultacji. Na stronie zamieszczono również podstawowe informacje na temat tego, czym jest nowa dyrektywa NIS2. Ponadto opisano główne zmiany, jakie zostaną wprowadzone do obowiązujących obecnie przepisów, oraz sposób, w jaki dyrektywa będzie wdrażana. Opublikowano także instrukcję mówiącą o tym, co zainteresowane podmioty muszą zrobić, zanim nowe prawo zacznie obowiązywać, oraz jakie są przewidywane koszty finansowe związane ze spełnieniem wymogów bezpieczeństwa wynikających z NIS2.

Podsumowanie. Na przestrzeni ostatnich kilkunastu lat Republika Czeska zyskała reputację lidera UE w zakresie cyberbezpieczeństwa. Stało się tak z kilku powodów. W czeskiej architekturze bezpieczeństwa cyfrowego działa kilka instytucji, wśród których wiodącą rolę pełni NÚKIB. Dodatkowo władze Republiki Czeskiej podejmują działania w obszarze cyberbezpieczeństwa tak w wymiarze krajowym, jak i międzynarodowym. Inicjują spotkania i konferencje, których efekty mają być głosem w dyskusji o cyberbezpieczeństwie nie tylko w Republice Czeskiej, ale także w całej UE. Ponadto stwarzają odpowiednie warunki do rozwoju sektora IT, który nierzadko współpracuje z instytucjami państwowymi. Podejmowane działania pozwalają na szybkie reagowanie na ataki hakerskie.