KAMIENIAMI W CYBERPRZESTRZEŃ

Cyberprzestrzeń nie jest obszarem do którego ochrony, poza szczególnymI przypadkami, można używać kamieni.

autor: **Marek Gładysz**

Publikacja w ramach projektu NEPTUNE fundacji Stratpoints. 2021r.

Kamieniami w cyberprzestrzeń

Siedem lat temu tygodnik „Wprost" opublikował rozmowy polityków w restauracji Sowa i Przyjaciele, którzy byli nielegalnie podsłuchiwani przez obsługę restauracji. Wybuchła tzw. „afera taśmowa", która była początkiem końca rządów Platformy Obywatelskiej, a zarazem otworzyła drzwi do przyjęcia władzy przez partię Prawo i Sprawiedliwość. To wówczas politycy PiS, którzy obecnie sprawują najważniejsze funkcje w strukturze administracji państwowej na zachowaniu polityków PO i urzędników związanych z ówczesną władzą nie pozostawili suchej nitki. Zarzucali im nonszalancję, małostkowość, a w postępowaniu z informacją brak przestrzegania elementarnych zasad bezpieczeństwa. Wydawałoby się, że politycy wywodzący się z każdej strony sceny politycznej, a w szczególności politycy PiS powinni wyciągnąć wnioski płynące z afery taśmowej. To przecież ci ostatni, przyjmując władzę w 2015 roku na sztandarach nieśli hasła związane m.in. z poprawą bezpieczeństwa państwa i nową jej jakością. Tymczasem 9 czerwca 2021 roku stało się inaczej. Szef Kancelarii Prezesa Rady Ministrów minister Michał Dworczyk poinformował, że stał się obiektem ataku hakerskiego i w jego wyniku, wykradziono mu zawartość prywatnej skrzynki poczty elektronicznej. Jednocześnie oświadczył, że nie posiadał w wykradzionej korespondencji żadnych materiałów niejawnych, doskonale przy tym manipulując słowem lub nie tłumacząc się wcale, co jest zwyczajnym skandalem. Owszem, wszystko na to wskazuje, iż nie było tam dokumentów z naniesioną klauzulą tajności, natomiast treść dokumentów pozostawia co do tego szereg wątpliwości. Dwa dni później rząd, media, naród w kawiarniach rozprawiał o ataku cybernetycznym na Najjaśniejszą Rzeczpospolitą i rozprawia nadal. Jedni krzyczą, że to wraży naród, knując przeciwko Rzeczpospolitej stoi za tym aktem agresji i jest to niewątpliwie preludium do dalszych działań. Z każdego możliwego medium, w zależności od zabarwienia politycznego wyłaniają się specjaliści opisujący zdarzenie. W związku z powyższym Wicepremier, a następnie Premier Rzeczpospolitej Polskiej ogłosili, że obrona cyberprzestrzeni jest objęta najwyższym priorytetem, a w związku z faktem, że atak pochodzi ze wschodu, sprawa musi znaleźć się na forum Sojuszu Północnoatlantyckiego i Unii Europejskiej. Dzisiejsza opozycja parlamentarna podnosi zaś fakt niezwykłej nonszalancji osób sprawujących główne stanowiska w państwie oraz brak reakcji służb wobec tych osób.

Spójrzmy jednak na to co się stało z innej perspektywy, zadajmy kilka prostych pytań aby dokładnie zdefiniować problem bez zajadłości politycznej, a z niewątpliwą intencją chłodnej analizy wydarzeń i ich konsekwencji. Zacznijmy od definicji ataku cybernetycznego.

Za Centrum Zasobów Bezpieczeństwa Komputerowego rządu Stanów Zjednoczonych, za cyber atak uważamy działanie za pośrednictwem sieci informatycznej, której celem jest wykorzystanie cyberprzestrzeni przez państwo, organizację lub pojedynczą osobę w celu zakłócenia, wyłączenia, niszczenia lub złośliwego kontrolowania środowiska/infrastruktury komputerowej albo niszczenia integralności danych lub kradzież kontrolowanych informacji[1]. Biorąc powyższe pod uwagę zadajmy kilka pytań, a następnie spróbujmy znaleźć na nie odpowiedź. Pytanie pierwsze jest następujące: Czy wyciek danych z prywatnej poczty elektronicznej ministra, jest klasycznym atakiem cybernetycznym, a jeśli tak, jaki jest jego cel, co atakujący aktem tym chciał osiągnąć? Jakie korzyści zostały osiągnięte i przez kogo? Odpowiedź wcale nie jest prosta. Bo czy zwrócenie uwagi na nonszalancję Szefa KPRM i jego otoczenia w sposobie prowadzenia korespondencji służbowej przez jawne media może być tym celem? Z pewnością nie. Jeśli ktoś jest podsłuchiwany w większości przypadków o tym nie wie, a podsłuchujący nie odkrywa swoich zamiarów, chyba że przez przypadek zostanie to ujawnione. Zdecydowanie jest lepiej posiadać informację i nie ujawniając, że ją się posiada. W tym przypadku stało się inaczej. Zasoby prywatnej skrzynki pocztowej ministra Michała Dworczyka zostały ujawnione. Czy wobec tego była to kradzież prywatnej zawartości jego skrzynki e-mail, czy też atak na Państwo? Kwestia ta jest szalenie ciekawa, a co więcej, problem ten jest zaledwie czubkiem góry lodowej ujawniającej ogrom nieprawidłowości, lekceważącego podejścia do problemu przez większość osób zajmujących istotne dla państwa stanowiska.

Kwestie te znajdują swoje miejsce w ustawodawstwie. Dwie ustawy porządkują ten obszar. Są to: Ustawa z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa oraz Ustawa o ochronie informacji niejawnych z dnia 5 sierpnia 2010. Pierwsza z nich opisuje strukturę organizacyjną oraz odpowiedzialność instytucji odpowiedzialnych z ochronę cybernetyczną Państwa Polskiego. Ustawa o ochronie informacji niejawnych traktuje o sposobie ochrony informacji niejawnych i definiuje również kryteria nadawania odpowiedniej klauzuli niejawności.

W tym świetle nie jest trudno zauważyć, że to co się stało z wyciekiem informacji z prywatnego konta Ministra Michała Dworczyka, winno być analizowane zgodnie z literą tychże ustaw. [2]Sprawą najważniejszą powinno stać się ustalenie przez odpowiednie organa, czy informacje które zostały wykradzione, a następnie opublikowane, stanowią informację

[1] www.csrc.nist.gov
[2] Warto zwrócić uwagę w jaki sposób FBI potraktowało sprawę Hilary Clinton

niejawną czy też nie, a także jaka jest odpowiedzialność osób które to były autorami tejże informacji w ujawnionej korespondencji. Należy zauważyć, że wymiana korespondencji pomiędzy osobami ujawnionymi w wycieku, dotyczyła osób będących w jurysdykcji różnych służb. Kto wobec tego jest odpowiedzialny aby ocenić całokształt problemu? Służba Kontrwywiadu Wojskowego czy też Agencja Bezpieczeństwa Wewnętrznego? Niestety, z pewnością nie doczekamy się rzetelnego i obiektywnego śledztwa w tej sprawie. Prawdopodobieństwo wyciągnięcia konsekwencji służbowych czy tych wynikających z przepisów ustawy o ochronie informacji niejawnych wobec osób, którzy dopuścili się nieprawidłowości podczas przetwarzania informacji służbowych i niejawnych także jest niewielkie. Sprawa jest polityczna i politycznie rozgrywana. Głosy polityków, a nawet niejawne posiedzenie parlamentu jest tylko i wyłącznie fasadą odwracającą uwagę od prawdziwego problemu. Problemem nie jest brak możliwości przesłania informacji w sposób dający większą pewność jej ochrony. Istnieją narzędzia i programy które umożliwiają szyfrowanie przesyłanych informacji. Warto wspomnieć o systemie CATEL dający możliwość prowadzenia rozmowy na poziomie zastrzeżonym. System ten jest świetnym przykładem niechęci do korzystania z tego typu urządzeń przez kluczowe osoby w państwie – mówiąc wprost z czystego lenistwa. Dlatego jest pewnym, że urządzenia te w znakomitej większości przypadków leżą w szufladach biurek lub sejfów i odnajdywane są kiedy to trzeba, z jakiś powodów rozliczyć się ze sprzętu.

Od zawsze wiadomo, że z punktu widzenia ochrony informacji niejawnych czy wrażliwych, najsłabszym ogniwem pozostaje człowiek. Tak też się stało i w tym przypadku. Niezależnie od tego, kto stoi za włamaniem do prywatnej poczty ministra Michała Dworczyka, to gdyby przestrzegane były wszystkie zasady przez osoby uwikłane w sprawę – problemu by nie było. Należy również zauważyć pewną tendencję w tego typu przypadkach. Poczynając od podsłuchów, z którymi mieliśmy do czynienia w poprzedniej konstelacji politycznej do kwestii ostatnich, to sprawy te dotyczą osób cywilnych, polityków którym wydaje się, że stoją ponad systemem jeśli nie prawem. Tego rodzaju przypadków niewiele pojawia się w środowiskach mundurowych. Wiąże się to z prostą zależnością, a mianowicie liczbą szkoleń tej grupy zawodowej, możliwych konsekwencji, ale i przede wszystkim personalnej odpowiedzialności żołnierzy czy funkcjonariuszy.

Cyberprzestrzeń stała się przestrzenią, w której funkcjonują coraz to większe grupy ludzi. Jak ona jest kształtowana, pokazała chociażby pandemia COVID 19, kiedy znakomita większość poszczególnych grup społecznych wykonywała swoje obowiązki zdalnie. Ciekawą

kwestią jest fakt, że obszar cyberprzestrzeni stał się niezauważalny na co dzień, dopóki coś się nie wydarzy. Oznacza to, że traktujemy cyberprzestrzeń jak powietrze, jest niezauważalne do momentu, kiedy go zabraknie, lub też stanie się nieprzyswajalne przez organizm. Cyberprzestrzeń w zasadzie nie ma granic. To cyberprzestrzeń i rozwój transportu wygenerowały pojęcie globalnej wnioski.

Z tego też powodu, Sojusz Północnoatlantycki uznał cyberprzestrzeń za kolejną obok lądowej, powietrznej i morskiej, domenę operacyjną. Oznacza to, że powinna istnieć polityka oraz organizacja dająca gwarancję bezpieczeństwa tego środowiska. Rząd USA traktuję atak w obszarze cyberprzestrzeni na równi z atakiem kinetycznym przeciwko państwu i daje sobie prawo do każdego rodzaju odpowiedzi, z kinetyczną włącznie. Większość państw w swojej legislacji posługuje się określeniem cyber obrona, ale istnieją również państwa, które w zgodzie z własnym prawodawstwem rozwijają również zdolności ofensywne w tym zakresie. Problem jest złożony. Zdecydowanie lepiej z wiadomych względów, radzą sobie w tym zakresie państwa autokratyczne od demokratycznych. Jest jednak faktem, że obszar ten będący niezwykle wrażliwym dla państwa, powinien być właściwie chroniony. Czy więc Państwo Polskie posiada wystarczającą organizację i zdolności aby wyzwaniom tym podołać? Wydaje się że tak nie jest. Ustawa o krajowym systemie cyberbezpieczeństwa powinna ten obszar regulować w sposób skuteczny. Tylko czy ją reguluję? Czy została stworzona odpowiednia struktura organizacyjna podmiotów odpowiedzialnych za cyberprzestrzeń która jest w swej istocie skuteczna, która nie pozostawia możliwości odziaływania destrukcyjnego na ten obszar? Jakie są wytworzone mechanizmy skoordynowanego działania przez te podmioty w przypadku zagrożenia? Jak w końcu powinno się traktować atak cybernetyczny na infrastrukturę krytyczną państwa i czy wojenny system dowodzenia armią czy kierowania państwem traktuje o tych sprawach? Istnieją uzasadnione przypuszczenia, że sytuacja daleka jest od skuteczności. Przykładem jest pomysł utworzenia wojsk obrony cyberprzestrzeni. Czy odpowiedzialność tejże formacji obejmować będzie tylko Siły Zbrojne RP czy też pozostałe struktury państwa? Są to pytania na które warto odpowiedzieć pragmatycznie, a nie politycznie.

Problematyka ochrony cyberprzestrzeni jest szeroka. Każdy z aspektów wymienionych w artykule zasługuje na odrębną analizę i nie sposób jej wyczerpać w kilku zdaniach. Niemniej jednak, na kanwie ostatnich wydarzeń można stwierdzić:

- Ujawniona korespondencja z prywatnej skrzynki e-mail ministra Michała Dworczyka i innych osób, pokazuje z jakim lekceważeniem zdrowego rozsądku oraz zasad

bezpieczeństwa wykazują się osoby które powinny być wzorem w tej sprawie. Zwłaszcza, że w dyspozycji tychże osób pozostają narzędzia ochrony informacji, z których można korzystać. Koniecznym jest stworzenie obligatoryjnego systemu szkolenia dla kluczowych osób w administracji państwowej i samorządowej;

- Rozwój cyberprzestrzeni jest niezwykle dynamiczny, wdrożenie telefonii komórkowej 5G a następnie implementacja sztucznej inteligencji na szeroką skalę postawi przed państwem zupełnie inne wymagania do których nie jesteśmy przygotowani;
- Pragmatyka bezpiecznej wymiany informacji jest dziurawa, niekompatybilna wewnątrz państwa. Brak jednolitej platformy informatycznej wymiany informacji dla administracji państwa skutkuje możliwością utraty informacji wrażliwych, a tym samym pozwala obcym służbom na odziaływanie oraz kształtowanie sceny politycznej, a w krytycznych sytuacjach osłabienia suwerenności państwa. Budowa wielodomenowego, bezpiecznego, funkcjonującego również w stanach zagrożenia państwa, opartego na zasadach federacji systemu teleinformatycznego jest krytycznie niezbędna;
- Ustawa o ochronie informacji niejawnych oraz Ustawa o krajowym systemie cyberbezpieczeństwa winny być poddane analizie i koniecznej nowelizacji dostosowując ich brzmienie do obecnych wyzwań. W aktualnym stanie, zwłaszcza ustawa o KSC nie tworzy jednolitego systemu, mamy tylko ministerialne wyspy;
- Tworzone struktury oddziaływania w cyberprzestrzeni należy tworzyć w sposób wewnętrznie kompatybilnym oraz posiadającym zdolności do reakcji w przypadku zagrożenia. Adaptacja istniejącej struktury organizacyjnej powinna skutkować utworzeniem jednolitej i czytelnej organizacji zdolnej do sprostania wyzwaniom, które niesie rozwój cyberprzestrzeni;
- Należy jasno określić politykę państwa w zakresie posiadania zdolności zarówno do obrony i ochrony własnych systemów informatycznych, ale i do posiadania ofensywnych zdolności w tym zakresie.

Podsumowując, ostatnią kwestią, która zasługuje na uwagę, to standardy demokratycznego państwa w zakresie zarządzania cyberprzestrzenią jako częścią dobra wspólnego, a także jego obszaru rozwoju i funkcjonowania. Nie ma bowiem wątpliwości, że strefa ta będzie przenikać funkcjonowanie społeczeństwa albo inaczej, to społeczeństwa coraz głębiej będą wnikać w cyfrową przestrzeń. Państwa autokratyczne są z reguły sprawniejsze w tworzeniu zasad funkcjonowania społeczeństwa, a tym samym sprawowania kontroli nad

nim. Państwo demokratyczne wytwarza te mechanizmy w sposób demokratyczny. Mechanizmy te nie powinny naruszać praw człowieka i wolności obywateli. Wszelkie ograniczenia w tym zakresie powinny być akceptowane i respektowane przez ogół obywateli. Wypracowane zasady nie powinny być przedmiotem gier politycznych czy wykorzystywania ich personalnie. Kluczową kwestią wobec tego pozostaje sposób w jaki system jest nadzorowany. Na zakończenie postawię pytanie na które co do zasady nie znajdziemy odpowiedzi. Skoro jak zaznaczyłem poprzednio nie znamy celu ani okoliczności wycieku korespondencji z prywatnego konta ministra Michała Dworczyka, to pytanie jest następujące: **Jakie wnioski wyciągają z tej sytuacji służby niekoniecznie nam przychylne oraz nasi sojusznicy?** Cyberprzestrzeń nie jest obszarem do którego ochrony, poza szczególnymi przypadkami, można używać kamieni.

| PUBLIKACJE

www.stratpoints.eu