UCHWAŁA nr 7

RADY do SPRAW CYFRYZACJI

z dnia 14 kwietnia 2020 roku

w sprawie działań mających na celu zapobieganie kradzieży tożsamości.

Na podstawie art. 17 ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz .U. z 2019 poz. 700, ze zm.) oraz § 5 Regulaminu Rady do Spraw Cyfryzacji stanowiącego załącznik do Zarządzenia nr 1 Ministra Administracji i Cyfryzacji z dnia 5 stycznia 2015 r. w sprawie ustanowienia regulaminu prac Rady do Spraw Cyfryzacji (Dz. Urz. z 2015 r. poz. 1, ze zm.), uchwala się, co następuje:

Pandemia COVID–19 powoduje istotne zmiany w realizacji obowiązku szkolnego, świadczeniu pracy, świadczeniu usług oraz realizacji zadań publicznych. Zgodnie z art. 3 ustawy z dnia 2 marca 2020 o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz. U. poz. 374) pracodawca może polecić pracownikowi wykonywanie pracy poza miejscem jej stałego wykonywania (praca zdalna), zgodnie zaś z § 3a rozporządzenie Ministra Edukacji Narodowej z dnia 11 marca 2020 r. w sprawie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 (Dz. U. poz. 410 z późn. zm.) zadania wskazanych jednostek systemu oświaty są realizowane z wykorzystaniem metod i technik kształcenia na odległość.

Pandemia COVID–19 jest również wykorzystywana przez różne podmioty – w tym przestępców - do działań, które prowadzą do podsycania niepokoju, manipulowania opinią publiczną, rozprzestrzeniania dezinformacji. Dla cyberprzestępców pandemia jest okazją do zwiększenia skuteczności ataków opartych na socjotechnice przy popełnianiu oszustw (fałszywe sklepy internetowe ze środkami ochrony osobistej, czy elektroniką), kradzieży z włamaniem środków z rachunków klientów wielu banków przy wykorzystaniu stron internetowych podszywających się pod agentów rozliczeniowych i banki oraz nieuprawnionego uzyskiwania danych w postali loginów i haseł do logowania do portali społecznościowych.

W ostatnich tygodniach można było zaobserwować w szczególności:

1. Ataki, w których pokrzywdzeni otrzymywali linki do stron podszywających się pod agentów rozliczeniowych i banki. Celem ataku jest uzyskanie przez sprawców w nieuprawniony sposób danych do logowania do bankowości elektronicznej i dokonanie kradzieży z włamaniem środków zgromadzonych na rachunku. Pokrzywdzeni otrzymywali:

- wiadomości SMS o treści: *"Zgodnie z specustawa dt kornawirusa wszyscy obywatele RP beda szczepieni. Z refundacja koszt wynosi 70 PLN. Oplac, aby uniknac kolejek"*. Link z wiadomości SMS prowadził do fałszywej strony płatności: https://dpdo-plata[.]org/1;
- wiadomości SMS o treści: *„Informujemy iż zgodnie z spec ustawą dotyczącą koronawirusa Państwa środki na rachunku zostają przekazane do rezerw krajowych NBP. Zaloguj się aby zatrzymać 1000 PLN"*. Link z wiadomości SMS prowadził do fałszywej strony płatności: https://dpdoplata[.]org/0;
- wiadomości SMS o treści*: „Ministerstwo Zdrowia: Dla kazdego obywatela przysluguje wsparcie zywieniowe w zwiazku z epidemia Koronawirusa. Zapisz sie na https://mzgov[.]net."* Link z wiadomości SMS prowadził do fałszywej strony https://mzgov.net;
- wiadomości SMS o treści: *"Wspieramy polska zdrowia w czasie walki z epidemia COVID-19! Wesprzyj szpitale w Polsce przekazujac datek! https://pomoc.sie-pomaga.net/koronawirus?SS52".* Link z wiadomości SMS prowadził do fałszywej strony *https://pomoc.sie-pomaga[.]net/koronawirus?SS52.*

Tylko stron paneli płatności podszywających się pod agentów rozliczeniowych i banki powstaje nawet 100 miesięcznie (do 15 dziennie). Dotychczas wśród wykorzystywanych scenariuszy dominowały opłacenie przesyłki kurierskiej, dopłata do zamówienia, dopłata do przesyłki, anulowanie subskrypcji. W tym scenariuszu ataku dochodzi do wyłudzenia na fałszywej stronie danych do logowania do bankowości elektronicznej, a następnie do wyłudzenia kodu służącego do autoryzacji transakcji, który sprawcy wykorzystają do zdefiniowania nowego odbiorcy zaufanego. Następnie po zdefiniowaniu odbiorcy zaufanego z rachunku bankowego pokrzywdzonego zlecane są przelewy. Środki zazwyczaj trafiają na rachunki tzw. „słupów", czyli osób, które za drobną opłatą sprzedają dostęp do własnych rachunków bankowych lub osób, których tożsamość została wykorzystana.

2. Ataki polegające na stworzeniu strony internetowej podszywającej się pod portal informacyjny. Celem ataku jest uzyskanie przez sprawców w nieuprawniony sposób danych do logowania do portali społecznościowych, a następnie wykorzystanie przejętych kont przy przejmowaniu kont innych osób oraz dokonywanie oszustw. Przykłady stron internetowych wyłudzających dane:

- hxxp://fakt24warszawka[.]com[.]pl/, hxxps://warszawa-info24[.]pl z informacją o porwaniu dziecka ze szpitala zakaźnego;
- ikoronawirusnews[.]pl z nagłówkiem wiadomości „Nowe fakty na temat koronawiurusa [wideo]";
- domeny używane do takich oszustw to również m.in. koronawirusnews[.]com.pl, e-koronawirusnews[.]pl.

Osoby, które chciały zapoznać się z nagraniami, przekierowywane były do strony podszywającej się pod portal Facebook i nakłaniane do zalogowania się w celu potwierdzenia pełnoletniości. Następnie z przejętych kont wysyłane są do znajomych osoby, której dane

przejęto, prośby np. o pożyczenie niewielkiej kwoty pieniędzy i przekazanie wygenerowanego przez pokrzywdzonego kodu BLIK, który umożliwia sprawcy wypłacanie środków w dowolnym bankomacie.

Sprawcy wskazanych powyżej oraz podobnych ataków pozostają najczęściej nieuchwytni z uwagi na stosowanie przez nich różnych metod ukrycia własnej tożsamości. Najczęściej sprawcy bezprawnie posługują się fikcyjną lub przejętą tożsamością przy rejestracji domen, kart SIM (podając dane osobowe innych osób jako abonentów usług przedpłaconych), korzystaniu z usług świadczonych drogą elektroniczną, zakładaniu kont poczty elektronicznej, profili na portalach społecznościowych, kont na giełdach kryptowalut czy w kantorach internetowych.

W związku z szerokim wykorzystywaniem pracy zdalnej, kształcenia na odległość oraz realizacji zadań publicznych online przy jednoczesnym wzroście intensywności ataków ze strony cyberprzestępców wykorzystujących pandemię do zwiększenia skuteczności ataków opartych na socjotechnice, niezbędne jest podjęcie prac legislacyjnych mających na celu przeciwdziałanie kradzieży tożsamości oraz wprowadzenie zmian w zakresie odpowiedzialności karnej za kradzież tożsamości oraz nieuprawniony dostęp do informacji.

Z uwagi na to, że w części z omówionych powyżej ataków wykorzystano nazwy domenowe z domeny *.pl lub domeny gdzie rejestratorami (pośrednikami) są podmioty mające siedzibę na terytorium Polski należy pilnie dokonać zmian w procesie pośrednictwa w rejestracji domen i nałożyć na rejestratorów obowiązki związane z weryfikacją tożsamości podmiotów rejestrujących domeny (abonentów). Aktualnie rejestratorzy opierają się o dane deklarowane przez rejestrujących, co prowadzi do sytuacji, w której cyberprzestępcy na potrzeby rejestracji domeny podają dane innych podmiotów (zarówno osób fizycznych jak i podmiotów prowadzących działalność gospodarczą) lub kreują nową tożsamość. Postuluje się w procesie weryfikacji danych abonenta wprowadzenie mechanizmów weryfikacji tożsamości z wykorzystaniem już istniejących narzędzi takich jak wykorzystanie podpisów elektronicznych i pieczęci elektronicznych w rozumieniu e-IDAS (w tym w szczególności podpisu kwalifikowanego), podpisu osobistego (o którym mowa w ustawie z dnia 6 sierpnia 2010 r. o dowodach osobistych, t.j. Dz. U. z 2020 r. poz. 332), podpisu zaufanego (o którym mowa w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, t.j. Dz. U. z 2020 r. poz. 346 z późn. zm.) lub innych mechanizmów takich jak np. wideoweryfikacja. Jawny rejestr domeny .pl powinien również zawierać dane kontaktowe do abonenta domeny (co najmniej adres e-mail). Aktualnie w bazie WHOIS nie są publikowane dane abonentów będących osobami fizycznymi. Dla porównania należy wskazać, że dla domeny *.eu baza WHOIS zawiera dane w postaci adresu mailowego abonenta. Bezpieczeństwo obrotu gospodarczego i zwiększenie bezpieczeństwa wydania certyfikatu kwalifikowanego wymagają tego, aby istniała możliwość weryfikacji danych w rejestrze krajowym tj. w rejestrze PESEL lub rejestrze RDO. Mając pełną świadomość, że dawanie dostępu do tych rejestrów osobom trzecim może powodować

ryzyka dla ochrony danych osobowych, proponujemy, aby wesprzeć te procesy mechanizmem, który już istnieje i jest dostępny, ale jego dostępność jest tylko i wyłącznie realizowana w oparciu o profil zaufany osoby, która ma dostęp do swoich danych tylko i wyłącznie na portalu obywatel.gov.pl bez możliwości przedstawienia tych danych w e-usłudze wymagającej wiarygodnej identyfikacji. Można zmienić to, dopuszczając dodatkowy schemat działania. Polegałby on na tym, że osoba wnioskująca o rejestrację w usłudze kwalifikowanej może wykorzystać dane zapisane w warstwie elektronicznej dowodu osobistego, profil zaufany lub podpis kwalifikowany do zwrócenia się do rejestru RDO lub PESEL o swoje dane, niezbędne do potwierdzenia tożsamości w procesie wydawania certyfikatu kwalifikowanego, a te dane mogą zostać następnie udostępnione (za zgodą wnioskującego) kwalifikowanej usłudze zaufania celem wydania kwalifikowanego certyfikatu w oparciu o te dane. Aby to osiągnąć ze strony technicznej funkcjonalność dostępna na obywatel.gov.pl powinna być dostępna w interfejsie API dla dostawców usług zaufania. Wniosek o udostępnienie własnych danych, w zakresie wymaganym polityką certyfikacji usługi zaufania, powinien móc być podpisany zarówno podpisem osobistym z dowodu osobistego, podpisem zaufanym (w oparciu o profil zaufany) jak i podpisem kwalifikowanym. Praktycznie taki mechanizm rozwiązałby w znacznym stopniu obecny problem zdalnej identyfikacji.

Biorąc pod uwagę sytuację, w której zarówno obywatele jak i przedsiębiorcy będą korzystali z dostępu do usług publicznych w celu nie tylko załatwiania spraw bieżących, ale także w celu składania wniosków o pomoc wynikającą z regulacji przyjętych w celu zmniejszenia skutków pandemii, należy pilnie umożliwić w systemach dostępowych do tych usług posługiwanie się nie tylko zaufanym profilem, jak obecnie w większości usług publicznych, ale także wykorzystanie w procesie dostępu do usługi publicznej danych zapisanych w warstwie elektronicznej dowodu osobistego i certyfikatu kwalifikowanego. Pomijanie w usługach publicznych kwalifikowanego certyfikatu jest naruszeniem rozporządzenia e-IDAS. Przykładem takiego prawidłowego i przez to bezpiecznego rozwiązania jest dostęp do platformy PUE w ZUS. Należy też zwrócić uwagę na fakt, iż wykorzystanie wyłącznie zaufanego profilu, którego funkcjonowanie zależy od prawidłowego funkcjonowania jednego systemu informatycznego oraz brak innych metod dostępu do usługi publicznej jest z punktu widzenia bezpieczeństwa tych usług, czyli ich dostępności dla obywateli i przedsiębiorców, nieakceptowalnym ryzykiem.

Biorąc powyższe pod uwagę, należy w trybie pilnym uruchomić dla wszystkich usług publicznych, szczególnie tych udostępnianych przez portal obywatel.gov.pl, przez portale ministerstwa finansów i wszystkie inne obsługujące wnioski obywateli i przedsiębiorców, stosowanie w procedurze dostępowej zarówno zaufanego profilu jak to ma miejsce obecnie, jak i certyfikatu kwalifikowanego i mechanizmów zawartych w warstwie elektronicznej dowodu osobistego.

Postulujemy także znacznie szersze dopuszczenie wideoweryfikacji jako metody, przy pomocy której może być potwierdzana tożsamość zwłaszcza przy wykorzystaniu obrazu twarzy zapisanego w warstwie elektronicznej dowodu osobistego, paszporcie, innych środkach oraz wsparciu przez rejestry państwowe. Należy zauważyć, że wideoweryfikacja może być stosowana, pod pewnymi warunkami, nawet w tak wrażliwych usługach jak wydawanie kwalifikowanych certyfikatów. Zgodnie z art. 24 pkt.1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) NR 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (tzw. eIDAS) potwierdzanie tożsamości może odbywać się: ”przy użyciu innych metod identyfikacji uznanych na szczeblu krajowym, które zapewniają pewność równoważną, pod względem wiarygodności, fizycznej obecności. Równoważna pewność musi być potwierdzona przez jednostkę oceniającą zgodność”. Ponadto w ramach tzw. *Questions@Answers on Trust Services under eIDAS*[1] zostało opisane podejście Komisji Europejskiej do kwestii wideoweryfikacji, w którym wprost wskazano na możliwość stosowania wideoweryfikacji o ile dopuszcza je prawo krajowe. Niestety w Polsce takich przepisów nie ma w związku z czym postulujemy by je wprowadzić zarówno w odniesieniu do usług zaufania jak i do tych przepisów, które dotyczą zawierania umów na odległość, np. w Prawie telekomunikacyjnym. Wideoweryfikacja została uznana za bezpieczną metodę przez Urząd Komisji Nadzoru Finansowego, co wskazuje, że nawet tak wyczulony na bezpieczeństwo sektor, jak bankowy, docenia jej zalety.

Pozytywne stanowisko MC w zakresie stosowania wideoweryfikacji, o co zabiegają od wielu miesięcy organizacje branżowe, i zmiana przepisów, mogłyby przyczynić się do znacznego rozwoju usług zaufania w Polsce oraz zlikwidować kilka poważnych barier w rozwoju gospodarki elektronicznej. Jej wprowadzenie najszybciej jak to możliwe jest w związku z utrudnieniami w zakresie przepływu korespondencji i ludzi w czasie stanu zagrożenia epidemicznego szczególnie istotne z uwagi na pilną potrzebę utrzymania ciągłości biznesowej przez firmy. Na szerokie wykorzystanie oczekują także metody oparte o dane i środki zawarte w warstwie elektronicznej dowodu osobistego, a zwłaszcza podpis osobisty.

Za pozytywny krok w kierunku ochrony użytkowników internetu przed wyłudzeniami uznać należy porozumienie z 23.3.2020 r. o utworzeniu listy ostrzeżeń odnoszącej się do domen internetowych, które służą do wyłudzeń danych i środków finansowych, którego sygnatariuszami są MC, NASK - PIB, Orange Polska S.A., Polkomtel Sp. z o.o., P4 Sp. z o.o. oraz T-Mobile Polska S.A. W dniu 31.3.2020 na liście tej znajdowało się już 101 nazw domenowych, w tym 22 to nazwy z domeny .pl. Z uwagi na to, że lista ostrzeżeń jest rozwiązaniem prowadzonym zgodnie z § 1 pkt 1 porozumienia jedynie w okresach stanów nad-

[1] https://ec.europa.eu/digital-single-market/en/news/questions-answers-trust-services-under-eidas

zwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego należy rozważyć kontynuację prowadzenie listy ostrzeżeń również po zakończeniu pandemii oraz wprowadzić zmiany dotyczące weryfikacji tożsamości abonentów domeny .pl lub podmiotów korzystających z pośrednictwa rejestratorów mających siedzibę na terenie Polski. Co więcej, należy również dokonywać lepszej weryfikacji podmiotów świadczących usługi pośrednictwa przy rejestracji nazw w domenie .pl (rejestratorów) w celu podniesienia poziomu cyberbezpieczeństwa i zapewnienia szybkiego reagowania pośredników na incydenty bezpieczeństwa związane z zarejestrowaną przez nich nazwą w domenie .pl.

Dla podniesienia poziomu bezpieczeństwa i przeciwdziałania zjawisku kradzieży tożsamości celowe jest również wprowadzenie obowiązków dotyczących lepszej weryfikacji tożsamości podmiotów korzystających z usług podmiotów świadczących usługi drogą elektroniczną. Aktualnie niemożliwe jest ustalenie danych osoby, która korzysta z konta poczty elektronicznej (np. podanego podczas rejestracji), a podmioty świadczące usługi drogą elektroniczną nie mają obowiązków związanych z gromadzeniem i przechowywaniem logów dostępowych użytkowników. W efekcie to regulamin danego podmiotu, a nie przepis prawa powszechnie obowiązującego decyduje o tym czy i z jakiego okresu można uzyskać dane dotyczące adresów IP, z których logowano się do konta poczty elektronicznej (okres ten w Polsce zgodnie z regulaminami różnych podmiotów jest różny i wynosi od kilku do kilkunastu miesięcy). Powoduje to nie tylko brak możliwości ustalenia, kto korzysta z konta poczty elektronicznej, ale znacząco utrudnia lub wręcz uniemożliwia przeprowadzenie postępowania dotyczącego uzyskania nieuprawnionego dostępu (włamania) do takiego konta. Istotnym problemem jest również zakres danych gromadzonych i udostępnianych jako „logi". Znaczna część podmiotów świadczących usługi drogą elektroniczną czy banków nie gromadzi bowiem informacji o portach. Z uwagi na to, że operatorzy bardzo szeroko wykorzystują NAT i jeden publiczny adres IP przydzielony może być nawet kilkudziesięciu tysiącom użytkowników uniemożliwia to ustalenie abonenta usługi.

W związku z rejestracją kart SIM na dane osób, których dane osobowe zostały nielegalnie pozyskane, postulujemy nałożenie na operatorów telekomunikacyjnych obowiązków monitorowania anomalii (np. faktu rejestracji na jedną osobę fizyczną kilkuset lub kilku tysięcy kart przedpłaconych) i podejmowania bezzwłocznych działań mających na celu dezaktywację usług przedpłaconych w sytuacji ustalenia, że do aktywacji karty SIM posłużono się danymi osobowymi innej osoby. Przestępcy korzystają również z usług podmiotów świadczących działalność gospodarczą i rejestrujących na dane działalności karty SIM, które następnie stają się przedmiotem obrotu. Celowe jest wprowadzenie w sytuacji nabycia karty przedpłaconej od innego podmiotu obowiązku ponownej rejestracji takiej karty pod rygorem dezaktywacji usługi. Aktualna regulacja w zestawieniu z praktyką pokazuje, że cel wprowadzenia rejestracji abonentów usług przedpłaconych ustawą o działaniach antyterrorystycznych nie został osiągnięty, a zarejestrowane na dane innych osób karty SIM można kupić na powszechnie dostępnych portalach ogłoszeniowych oraz na forach w sieci TOR.

Ponadto należy odejść od weryfikacji tożsamości osób fizycznych opartej na znajomości numeru PESEL. Numer PESEL niewątpliwie służy do identyfikacji danej osoby. Z uwagi na to, że numery PESEL nie są daną znaną jedynie uprawnionym podmiotom, ale są szeroko dostępne są w Internecie – w dostępnych online rejestrach publicznych (księgi wieczyste, KRS), czy we wszystkich dokumentach podpisanych przez daną osobę przy pomocy podpisu osobistego, kwalifikowanego podpisu elektronicznego lub podpisu zaufanego, podanie numeru PESEL nie powinno prowadzić do weryfikacji tożsamości (w tym nie powinno być możliwe zawarcie umowy pożyczki z podaniem podstawowych danych osobowych takich jak imię i nazwisko oraz numer PESEL).

Dla przeciwdziałania kradzieży tożsamości bardziej celowe jest oparcie weryfikacji tożsamości o inne mechanizmy, a nie o podanie jednoznacznie identyfikującego osobę, co do zasady niezmiennego (z wyjątkami wskazanymi w ustawie), łatwego w ustaleniu numeru PESEL. Innym mechanizmem mogło by być okazanie dokumentu tożsamości lub przeprowadzenie wideoweryfikacji z dokumentem tożsamości, w szczególności z wykorzystaniem obrazu twarzy zapisanego w warstwie elektronicznej dowodu osobistego i paszporcie, przy zagwarantowaniu szerokiemu kręgowi podmiotów możliwości weryfikacji ważności tych dokumentów w rejestrach publicznych. Obowiązują już przepisy zgodnie z którymi w sytuacji, w której doszło do nieuprawnionego wykorzystania danych osobowych czy utraty dowodu posiadacz może zgłosić osobiście ten fakt organowi dowolnej gminy w celu unieważnienia posiadanego dowodu osobistego (art. 48a ustawy o dowodach osobistych). Zgodnie z art. 53 ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych minister właściwy do spraw informatyzacji prowadzi w systemie teleinformatycznym wykaz zawieszonych i unieważnionych dowodów osobistych zawierający serie i numery zawieszonych i unieważnionych dokumentów oraz serie i numery błędnie spersonalizowanych lub utraconych blankietów dowodów osobistych. Udostępnienie tych informacji wzmocniłoby system ochrony tożsamości. Powszechnie dostępna informacja o zawieszonych czy unieważnionych dokumentach tożsamości nie powinna obejmować danych osobowych dysponenta dokumentu (w tym w szczególności jej numeru PESEL czy imienia i nazwiska). Publikowanie informacji o unieważnieniu dokumentu o określonych danych na liście dokumentów unieważnionych, przeciwdziałałoby wykorzystaniu tych danych np. do rejestracji kart SIM czy zaciągania zobowiązań finansowych. Jednocześnie na podmioty takie jak np. rejestratorzy domen, operatorzy telekomunikacyjni, kredytodawcy, pożyczkodawcy należy nałożyć obowiązek weryfikacji autentyczności i ważności dokumentów potwierdzających tożsamość.

W związku z powszechnym wykorzystywaniem tożsamości innych osób przez cyberprzestępców można zauważyć, że odpowiedzialność karna za przestępstwo kradzieży tożsamości nie jest adekwatna i nie daje skutecznej ochrony pokrzywdzonym, z uwagi na wąsko określony w art. 190a § 2 KK cel działania sprawcy tj. wyrządzenie szkody majątkowej lub osobistej osobie, której tożsamość wykorzystano i pod którą się podszyto. Poza zakresem penalizacji pozostaje sytuacja, w której sprawca działa w celu ukrycia własnej tożsamości

lub wyrządzenia szkody innej osobie niż ta, której danymi się posłużył. Dla skutecznej walki ze zjawiskiem kradzieży tożsamości należy dokonać zmian w art. 190a § 2 KK polegających co najmniej na użyciu zamiast wyrażenia "w celu" sformułowania "w zamiarze", a nadto odstąpienia od zasady tożsamości podmiotu, pod który sprawcy się podszywają i któremu chcą wyrządzić szkodę. Celowe byłoby również podniesienie górnej granicy zagrożenia karą do co najmniej 5 lat.

Mając na względzie skalę oraz skutki ataków polegających na uzyskiwaniu nieuprawnionego dostępu do informacji poprzez przełamanie lub ominięcie zabezpieczeń niezbędne jest również podniesienie górnej granicy odpowiedzialności karnej za czyn z art. 267 § 1 kk. Aktualnie czyn polegający na bezprawnym uzyskaniu dostępu do informacji m.in. poprzez przełamanie lub ominięcie zabezpieczeń zagrożony jest karą do 2 lat pozbawienia wolności. Dla porównania za dokonanie kradzieży w włamaniem (gdzie dla bytu przestępstwa nie ma znaczenia wartość przedmiotu zaboru), górna granica odpowiedzialności karnej wynosi 10 lat. Mając na względzie znaczenie danych w społeczeństwie informacyjnym, elektronicznej administracji i gospodarce, oraz skutki uzyskania dostępu przez cyberprzestępców do zbiorów danych osobowych, loginów i haseł czy do danych stanowiących informacje podlegające ochronie, zagrożenie karane na poziomie 2 lat pozbawienia wolności nie realizuje celów prewencji ogólnej. Postulujemy zatem podniesienie górnej granicy odpowiedzialności karnej za przestępstwo z art. 267 § 1 kk.

Protokół z głosowania

Decyzją Przewodniczącego Rady głosowanie zostało przeprowadzone w trybie obiegowym. Projekt uchwały nr 7 został przesłany członkom Rady 7 kwietnia 2020 r. Do dnia 14 kwietnia 2020 r. wszyscy członkowie Rady oddali swój głos. W głosowaniu wzięło udział 15 członków Rady, z czego oddano:

- 13 głosów „za" przyjęciem uchwały,
- 0 głosów „przeciw" oraz
- 2 głosy „wstrzymuję się".

Uchwała nr 7 Rady do Spraw Cyfryzacji została przyjęta 14 kwietnia 2020 roku w głosowaniu jawnym w trybie obiegowym zwykłą większością głosów.

Szczegóły dotyczące głosowania przedstawia poniższa tabela.

Lp.	Imię	Nazwisko	Głos
1.	Izabela	Albrycht	za
2.	Katarzyna	Chałubińska-Jentkiewicz	za
3.	Jan	Czajkowski	za
4.	Jacek	Czarnecki	wstrzymuję się
5.	Krzysztof	Dyki	wstrzymuję się
6.	Paweł	Gora	za
7.	Agnieszka	Gryszczyńska	za
8.	Michał	Kanownik	za
9.	Anna Beata	Kwiatkowska	za
10.	Tomasz	Łukawski	za
11.	Dariusz	Milka	za
12.	Józef	Orzeł	za
13.	Rafał	Rodziewicz	za
14.	Włodzimierz	Schmidt	za
15.	Sebastian	Szymański	za

Przewodniczący Rady
Józef Orzeł
/-podpisano elektronicznie/