Annales Canonici 16 (2020) 1 • s. 25–37
DOI: http://dx.doi.org/10.15633/acan.3702
Jakub Kwaśnik
ORCID:0000-0003-1226-6765
Krakowska Akademia im. Andrzeja Frycza Modrzewskiego

Dane osobowe jako kluczowy obiekt zainteresowania cyberprzestępców

Różnorodność funkcji, jakie pełni cyberprzestrzeń, oraz wynikająca z jej specyfiki powszechność i wygoda w używaniu sprawiły, że życie społeczne w znacznej mierze przeniosło się do Internetu. Znaczenie sieci internetowej jest widoczne nie tylko w sektorze prywatnym czy w działalności jednostek publicznych, lecz także wszędzie tam, gdzie wykorzystuje się rozwój i nowe technologie. Jako że ogół ruchu sieciowego tworzą jego użytkownicy, a większość z nich funkcjonuje zazwyczaj w wielu środowiskach społecznych (praca, nauka, hobby, działalność publiczna, życie towarzyskie), poszczególne obszary sieci przenikają się, ale mechanizmy działania pozostają podobne. Stąd też, opisując zachowanie internautów, analizujemy procesy, które dotyczą również podmiotów i osób składających się na codzienność funkcjonowania Kościoła (jako miejsca pracy, miejsca spotkań, środka ewangelizacji czy po prostu podmiotu przetwarzającego duże ilości danych). Z tego tytułu warto przyjrzeć się specyfice działania sieci jako istotnej również dla tego środowiska. Szczególnie widoczną zmianą względem czasów preinternetowych jest wzrost znaczenia sieci w aspekcie komunikacyjno-informacyjnym oraz jej udział w sektorze handlowo-usługowym i rozrywce[1]. Immanentną cechą funkcjonowania sieci internetowej jest nieustanna wymiana informacji, tak między samymi użytkownikami w cyberprzestrzeni, jak i między elementami oraz urządzeniami, które tę sieć tworzą. Przenoszone informacje dzielą się na dwa podstawowe rodzaje: pierwszym są informacje merytoryczne, które tworzą treść Internetu, drugim zaś metadane, które pozwalają określić mechanizmy i reguły systematyzujące określony wycinek cyberprzestrzeni. Wysyłane pakiety kreują sieciową rzeczywistość i nakreślają

1 Por. T. Berners-Lee, *Internet Live Stats*, https://www.internetlivestats.com/ (25.03.2020).

zakres, możliwości oraz ramy działania tych, którzy ją współtworzą. Uwierzytelnione dane pozwalają na szerszy dostęp konkretnego użytkownika do określonych obszarów i działań. Nadawanie i odbieranie uprawnień jest więc kluczowe dla stabilności działania każdego podmiotu w sieci, bowiem cyberprzestrzeń pozwala na podjęcie bogatego spektrum akcji, z których wiele ma istotne znaczenie dla funkcjonowania jednostki w społeczeństwie. Dane identyfikacyjne i uprawnienia są przydzielane dla każdego środowiska sieciowego w sposób indywidualny, dlatego też każda jednostka i każdy użytkownik charakteryzuje się określoną tożsamością w sieci, na którą mogą składać się: identyfikator internetowy, login, hasło, numer IP[2], adres MAC[3] urządzenia, avatar czy dane biometryczne. Pełnią one rolę analogiczną do danych osobowych i dokumentów tożsamości w świecie rzeczywistym i tak też zostały określone w ogólnym rozporządzeniu o ochronie danych[4]. Definicje przyjęte przez unijnego prawodawcę zostały powtórzone w regulacjach szczegółowych dla danych grup podmiotów, stąd też analogia w słowniczku pojęciowym dla jednostek i instytucji kościelnych objętych prawem kanonicznym[5].

Dyspozycje wydane przez określonego użytkownika w sieci mogą mieć zasadnicze konsekwencje dla jego funkcjonowania w świecie rzeczywistym: wystarczy wskazać w tym miejscu choćby na statystykę popularności bankowości elektronicznej oraz procent codziennego czasu, jaki społeczeństwo spędza w Internecie (tak w pracy, jak i realizując swoje życie towarzyskie). Przy tak wielu podejmowanych aktywnościach w cyberprzestrzeni kluczowe dla bezpieczeństwa użytkownika jest więc jego zachowanie, na które składa się świadomość zagrożeń sieciowych oraz wypracowany stopień ostrożności. Niestety, bardzo często jedynym uwierzytelnieniem danego użytkownika w sieci jest wpisywany przez niego na określonym portalu login oraz hasło. Bywa, że są to również dodatkowe akcje, jak potwierdzenie

2 Internet Protocol address (ang.) – numer nadawany urządzeniu przy połączeniu do sieci internetowej w celu jego poprawnej identyfikacji.

3 Media Access Control address (ang.) – sprzętowy adres karty sieciowej pozwalający zidentyfikować konkretne urządzenie fizyczne.

4 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016R0679&from=HU (25.03.2020).

5 Dekret ogólny w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim wydany przez Konferencję Episkopatu Polski w dniu 13 marca 2018 r., https://episkopat.pl/wp-content/uploads/2018/06/DekretOgolnyKEPWSprawieOchronyOsobFizycznychWZwiazkuZPrzetwarzaniemDanychOsobowychWKoscieleKatolickim.pdf (25.03.2020).

swojej tożsamości za pomocą dwustopniowego uwierzytelniania (np. SMS z kodem bądź zatwierdzenie w aplikacji mobilnej). Wzmożone środki bezpieczeństwa przeważnie stosowane są w tych obszarach, które bywają szczególnie newralgiczne dla jednostki. Jednak i one bywają zawodne, bowiem nawet najlepsze zabezpieczenia nie mogą uchronić przed negatywnymi skutkami, jeśli kluczowe operacje uzależnione są od samego użytkownika, a więc obarczone ryzykiem błędu ludzkiego. Zawodność urządzeń, luki w zabezpieczeniach i wypadki losowe istotnie wpływają na stopień bezpieczeństwa. Jednakże zdaniem ekspertów to właśnie słabość czynnika ludzkiego w znacznej mierze determinuje sukces ataku cyberprzestępczego. Zachowanie społeczeństwa w sieci podlega niebezpiecznym trendom. Użytkownicy przedkładają wygodę korzystania z sieci nad własne bezpieczeństwo. Niska świadomość zagrożenia skutkuje równie niskim stopniem ostrożności. Mnogość informacji, jakie umieszczamy w Internecie, oraz powielanie utartych, prostych schematów myślowych przy konfiguracji haseł powoduje, że złamanie kodu staje się proste nie tylko dla cyberprzestępcy posiadającego rozwiniętą wiedzę informatyczną, lecz także dla sprawnego socjotechnika. Badania przeprowadzone przez Marka Burnetta[6] wskazały, że ok. 9,7% użytkowników używa puli pięciuset najpopularniejszych haseł. Na szczycie listy znajdują się takie pozycje, jak: 123456, 1111, qwerty czy też *password*, co świadczy o popularności niezwykle prostych mechanizmów, charakteryzujących się nikłą skutecznością. Najbardziej wyrazistym przykładem jest analiza choćby trzonu zabezpieczeń bankowości elektronicznej, jakim są numery PIN do karty: zabezpieczenia ograniczają się w tym przypadku do puli dziesięciu tysięcy kombinacji. W zestawieniu z faktem, że istnieje wyraźna tendencja do korzystania przez użytkowników z najprostszych technik ustanawiania hasła (najbardziej popularnym rozwiązaniem jest ustawienie daty związanej z istotnym życiowo wydarzeniem lub związanej w określony sposób z preferencjami danego użytkownika), ten sposób zabezpieczeń pomimo jego powszechności jawi się jako słaby i przewidywalny. Według datagenetics.com[7] na przebadanych 3,4 miliona haseł opartych na czterocyfrowej kombinacji, aż 10,17% wyników stanowił ciąg „1234", a kolejne 6,01% – kombinacja „1111". Z kolei grupa numerów PIN oparta na dacie z zakresu 1900–1999 należy do 20% najbardziej popularnych kombinacji. Widać więc wyraźną tendencję użytkowników do szukania prostych, osobistych

6 M. Burnett, *10 000 Passwords*, https://xato.net/10-000-top-passwords-6d6380716fe0 (25.03.2020).

7 N. Berry, *PIN analysis*, https://www.datagenetics.com/blog/september32012/ (25.03.2020).

skojarzeń myślowych, związanych na przykład z wydarzeniem z własnego życia, co ma ułatwić zapamiętanie kluczowego zabezpieczenia[8].

Najpopularniejsze hasła przeważnie składają się z danych osobowych lub prostych informacji o samym internaucie bądź jego preferencjach (głównie imiona bliskich, pseudonimy, data urodzenia, hobby). Wiele z tych informacji zostaje podanych do publicznej wiadomości na portalach społecznościowych lub jest składnikiem innych adresów mailowych i loginów używanych na różnych urządzeniach i w różnych środowiskach (praca, szkoła, stowarzyszenie)[9]. Techniki białego wywiadu[10] pozwalają na łatwe pozyskanie takich informacji przez sprawców, którzy sprawnie filtrują sieć w poszukiwaniu strzępków konkretnych i istotnych danych o potencjalnej ofierze. Ślady, które pozostają po aktywności danej osoby w Internecie, oraz system połączonych kont i urządzeń przez nią używanych, prowadzą cyberprzestępców do kolejnych etapów przejmowania tożsamości ofiary, a tym samym zbliżają sprawcę do celu ataku[11]. Zachowanie w sieci pozwala niejednokrotnie stworzyć zaawansowany portret psychologiczny. Dzięki zdjęciom, relacjom na portalach społecznościowych i zapisom z używanych aplikacji cyberprzestępca może łatwo określić stopień zaawansowania obsługi komputera, preferencje i ulubione aktywności. Sprzyja temu nieustanny rozwój nowych technologii, który umożliwia implementowanie łączności internetowej i modułu zbierania danych przez coraz szerszą gamę urządzeń wykorzystywanych na co dzień w gospodarstwie domowym (Internet of things)[12]. W zależności od celu sprawcy wszystkie takie informacje są mniej lub bardziej pomocne w kolejnych stadiach ataku cyberprzestępczego. Według analityka Michała Kosińskiego już informacja na temat 240 polubień na Facebooku pozwala stworzyć komputerowi obraz osobowości ofiary tak dokładny, jaki ma bliska jej

8 Por. E. Twaróg, *Podaj datę urodzenia, a powiem, jaki masz PIN do karty,* http://www.pb.pl/podaj-date-urodzenia-a-powiem-jaki-masz-pin-do-karty-658891 (25.03.2020).

9 Por. J. Kwaśnik, *Wpływ ataków socjotechnicznych na konstrukcję i kształt polityki bezpieczeństwa*, w: M. Górka, *Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa*, Warszawa 2017, s. 35–48.

10 Open-Source Intelligence (ang.) – forma wywiadu gospodarczego polegająca na rozpoznaniu głównie poprzez informacje pochodzące z ogólnie dostępnych źródeł

11 Por. A. Rashdan, *The Social Media OSINT Challenge to US Intelligence: Culture Not Gigabytes*, w: *New Media Politics Rethinking Activism and National Security in Cyberspace*, Cambridge 2015, s. 155–172.

12 Por. M. Goodman, *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*, New York [2016], s. 276–281.

osoba[13]. Opracowanie profilu psychologicznego nie nastręcza większych trudności cyberprzestępcom, a przecież najczęściej nie muszą oni w ogóle sięgać po tak wyrafinowane metody. Sprawnym analitykom wystarczy pobieżne poznanie systematyki dróg komunikacji i przepływu informacji w konkretnym środowisku, by poprzez umiejętne postawienie pytań bądź sformułowanie wiarygodnej prośby uzyskać interesujące dane lub zmusić ofiarę do określonej akcji[14].

Słowem, które stało się kluczem w analizie obecnego kształtu cyberprzestępczości, jest socjotechnika. Zależnie od przyjętego zakresu definicji ataku opartego na socjotechnice, badania wykazują różny udział procentowy popularności tego typu ataków względem ogółu działań cyberprzestępczych. Wąska definicja ataku socjotechnicznego zakłada bezpośredni i indywidualny kontakt sprawcy z celem ataku, natomiast szeroka definicja zalicza do tej grupy wszelkie próby oparte na masowym rozsyłaniu wiadomości zawierających szkodliwe załączniki. W takim przypadku do grupy ataków opartych na socjotechnice można zaliczyć aż 98% wszelkiej cyberprzestępczej aktywności (badania purplesec.us[15]). Funkcjonariusze z Wydziału do walki z Cyberprzestępczością Komendy Wojewódzkiej Policji w Krakowie wyróżnili kilkadziesiąt scenariuszy związanych z inżynierią społeczną, które miały na celu pozyskanie określonych informacji bądź wywołanie pożądanego zachowania ofiary. Do szczególnie popularnych technik należą różne odmiany kradzieży tożsamości oraz oszustw w formie podszywania się pod określone instytucje lub osoby[16]. Metody opracowane przez cyberprzestępców charakteryzuje różnorodność i wyrafinowanie wynikające z dokładnego poznania mechanizmów społecznych oraz tendencji do określonych zachowań jednostki tak w świecie rzeczywistym, jak i w cyberprzestrzeni. Dominującym scenariuszem jest wymyślenie historii i przybranie roli legendy, która ma uwiarygodnić nietypową prośbę w postaci przesłania określonych informacji lub pieniędzy. W skład tej grupy przestępstw wchodzą wszelkie oszustwa „na wnuczka" i bazujące na tym samym schemacie: „na urząd", „na kuriera", „na współpracę biznesową", „na bank" czy też „na szefa", gdzie sprawcy odgrywają przyjętą wcześniej rolę, by zwiększyć

13 Za M. Kuchta-Nykiel, *Jesteś tym, co lubisz, czyli ile mówią o Tobie lajki na Facebooku?*, https://socialpress.pl/2017/01/jestes-tym-co-lubisz-czyli-ile-mowia-o-tobie-lajki-na-facebooku (25.03.2020).

14 Por. R. Cialdini, *Wywieranie wpływu na ludzi. Teoria i praktyka*, tłum. B. Wojciszke, Gdańsk 1999, s. 11–23.

15 Zob. https://purplesec.us/resources/cyber-security-statistics/ (25.03.2020).

16 Por. K. Mitnick, W. L. Simon, *The Art of Deception: Controlling the Human Element of Security*, Wiley 2003, s. 368–373.

prawdopodobieństwo odpowiedniej reakcji ofiary. Typowy atak socjotechniczny w zależności od pola zastosowania złożony jest z kilku faz, może również przybierać różne formy. Cyberprzestępcy najczęściej rozpoczynają aktywność od gromadzenia informacji, następnie przechodzą do „wywoływania", a więc wyboru celu i namierzenia korzystnych warunków do przeprowadzenia ataku. Potem następuje przybranie odpowiedniej roli, zastosowanie odpowiednich psychologicznych sztuczek w celu zwiększenia wiarygodności i w końcu – wywarcie wpływu, czyli zmuszenie ofiary za pomocą perswazji bądź manipulacji do określonego zachowania[17]. Sama koncepcja może być mniej lub bardziej skomplikowana. Niektóre ze scenariuszy bazują na prostym mechanizmie związanym z określonymi emocjami. Przykładowo, sprawca poprzez przybranie początkowej postawy osoby pomocnej i uczynnej może próbować wywołać u ofiary poczucie zobowiązania, istnienia długu wdzięczności bądź potrzeby wzajemności. Zdobycie zaufania poprzez zdanie się na pomoc ofiary i poparcie prośby przez racjonalne i logiczne uzasadnienie często skutkuje osiągnięciem przez cyberprzestępcę zamierzonego efektu. Silnie działa również powołanie się na autorytet oraz znajomość mechanizmów przepływu informacji w danej instytucji. Załóżmy, że socjotechnik pozyskał informacje o planowanym urlopie dyrektora jednostki. Za pomocą narzędzia, które fałszuje tożsamość nadawcy wiadomości mailowej może spreparować polecenie służbowe i poinformować wybranego pracownika, że w niedługim czasie będzie z nim kontaktował się prawnik, który poprosi o określone dokumenty. Następnie dochodzi do kontaktu sprawcy z innego adresu mailowego, w którym nawiązuje on do e-maila od dyrekcji i przedstawia się ofierze jako przywołany prawnik. Prosi o przesłanie szczególnie ważnych dokumentów bądź podjęcie określonej akcji. Inny przykład to sytuacja, w której do firmy zgłasza się nowy podmiot pod przykrywką chęci zawarcia współpracy biznesowej. Podsyła dane do strony internetowej, na której można zweryfikować podmiot, a w kolejnych e-mailach przesyła załączniki mające rzekomo zawierać ofertę bądź cennik. Pobranie załącznika może skutkować zainfekowaniem złośliwym oprogramowaniem i przejęciem komputera ofiary. Przykłady można mnożyć. Sprawcy cyberprzestępstw testują skuteczność określonych scenariuszy i wybierają te, które są najbardziej efektywne. Jak pokazuje praktyka, do najbardziej popularnych metod należą fałszywe informacje z banku dotyczące prośby o przesłanie lub weryfikację danych z powodu tymczasowej blokady konta, e-maile od firm

17 Por. Ch. Hadnagy, *Socjotechnika. Sztuka zdobywania władzy nad umysłami*, tłum. M. Witkowska, Gliwice 2017, s. 41–129.

kurierskich, poczty czy też dostawców usług, które mają zawierać elektroniczną fakturę oraz e-maile konkursowe i promocyjne informujące potencjalną ofiarę, że została beneficjentem określonej nagrody, jednakże musi dokonać rejestracji na danej stronie internetowej. Cyberprzestępcy sięgają w swych technikach także po legendy, które wykorzystują bieżące wydarzenia. Wyrazistym przykładem są rozsyłane masowo w czasie epidemii koronawirusa wiadomości o rzekomej blokadzie środków w banku w związku z pandemią czy też informacje o potrzebie rejestracji w narodowym programie szczepionek bądź konieczności uiszczenia specjalnej opłaty za dezynfekcję przesyłki. Wszystkie wiadomości zawierają oczywiście łącza prowadzące do stron przechwytujących dane osobowe i loginy wykorzystywane na stronach związanych z bankowością elektroniczną.

Po omówieniu charakterystyki pozyskiwania informacji przez kryminalistów w sieci dochodzimy do kluczowego dla niniejszego artykułu pytania: skąd tak duże zainteresowanie cyberprzestępców akurat danymi osobowymi? Odpowiedzią jest wartość pośrednia takich danych w podejmowanej działalności kryminalnej. Dane osobowe pozwalają najczęściej na uzyskanie dostępu do określonego obszaru w sposób najmniej odbiegający od typowego, właściwego dla danej akcji czy danego środowiska. Jeśli przestępca zaloguje się na konto za pomocą prawidłowych danych, w systemie zostanie odnotowany jedynie fakt i okoliczności uzyskania dostępu, co nie jest wystarczające do stwierdzenia naruszenia. W przypadku włamania cyberprzestępca musiałby znaleźć lukę, umieć ją właściwie wykorzystać oraz zatrzeć ślady po swojej aktywności. Stąd też łatwiej szukać rozwiązań, które będą efektywne, a przy tym mało skomplikowane i trudne do namierzenia. Pozyskane wcześniej dane osobowe mogą posłużyć do przeprowadzenia szeregu akcji cyberprzestępczych. Znaczną część kryminalnej działalności związanej z wyłudzeniami danych stanowi phishing[18], gdzie dane wykorzystywane są w celu osiągnięcia określonych korzyści majątkowych. Jest to ogół ataków z wykorzystaniem opisanych wcześniej mechanizmów opartych na podszywaniu się pod określone instytucje, osoby, przejmowaniu kont i profili oraz tworzeniu fałszywych stron internetowych np. banku czy też innej jednostki zaufania społecznego. Poza phishingiem dane osobowe mogą być wykorzystane do przeprowadzenia precyzyjnego ataku na konkretną jednostkę, w którym istotną rolę odgrywa użytkownik i przypisane mu poziomy dostępu do baz danych bądź określonych informacji. Również

18 Metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji.

wykorzystanie danych w dziedzinie cyberprzemocy i stalkingu jest znaczące. Zebrane szczegółowe informacje o prywatnym życiu ofiary są bezlitośnie wykorzystywane przez sprawców do prześladowania i wyrządzania krzywdy innym jednostkom. Spory wycinek cyberprzestrzeni należy do sieci ukrytej, tzw. Darknetu[19], gdzie rozkwita działalność przestępcza i handel nielegalnym towarem. Czarny rynek wykorzystujący mechanizmy pozwalające na uzyskanie względnej anonimowości (jak oprogramowanie sieci TOR[20]) przepełniony jest ofertami nielegalnej sprzedaży danych w celach komercyjnych (sprzedaż danych firmom, które używają ich do rozsyłania swoich reklam, w tym agresywnego spamu)[21]. Przejęcie kont i komputerów wielu użytkowników pozwala również cyberprzestępcom tworzyć tzw. botnety, czyli sieci zainfekowanych złośliwym oprogramowaniem urządzeń, które są wykorzystywanie w atakach typu DDoS bez wiedzy i zgody właścicieli. Na podstawie danych osobowych łatwo także wykreować nowy profil użytkownika i następnie sprzedać lub wykorzystać do spreparowania fałszywej dokumentacji lub dowodów tożsamości, na które jest duży popyt w Darknecie. Cała fałszywa dokumentacja ma z kolei zastosowanie przy handlu ludźmi oraz przy przemycie i innych podejmowanych pod przykryciem aktywnościach przestępczych. Dane osobowe są w końcu również dobrem samym w sobie i stanowią towar, który jest interesujący dla wszelkich legalnie działających agencji reklamowych oraz podmiotów zajmujących się marketingiem. Poznanie preferencji użytkowników pozwala na opracowanie odpowiedniej strategii, by przekonać ich do zakupu określonych dóbr. Stąd też firmy zajmujące się reklamą prześcigają się w tworzeniu atrakcyjnych fanpage'y. Wykorzystując chwilową popularność danego sloganu czy też memów, tworzone są bazy (tzw. farmy) użytkowników wyrażających zainteresowanie konkretnym profilem lub grupą, które następnie zostają sprzedane zainteresowanym koncernom. Handel danymi osobowymi z roku na rok stanowi coraz bardziej istotny element statystyk kryminalnych na świecie. W zależności od charakteru danych mogą one również posłużyć do podjęcia określonych zobowiązań, takich jak wzięcie kredytu czy dokonanie zakupu. Dzięki podszyciu pod strony bankowe

19 Ukryta część Internetu, która nie jest pozycjonowana w wynikach wyszukiwarek, a w której funkcjonują serwisy czarnorynkowe oraz komunikują się społeczności cyberprzestępców.

20 Wirtualna sieć komputerowa implementująca zaawansowane sposoby maskowania ruchu sieciowego (obejmujące na przykład multiplikowane przekierowanie adresów IP pochodzących od nadawcy), co w konsekwencji może zapewnić użytkownikom prawie anonimowy dostęp do zasobów Internetu.

21 Niechciane lub niepotrzebne wiadomości elektroniczne często o charakterze reklamowym, przez które cyberprzestępcy mogą także próbować wyłudzić informacje o użytkownikach.

czy też portale świadczące usługi turystyczne cyberprzestępcy mogą przejąć dane dotyczące kont bankowych i kart płatniczych, a więc mogą uzyskać łatwy dostęp do środków pieniężnych ofiar.

W obliczu przedstawionego wyżej stanu faktycznego wydaje się, że w codziennej pracy wielu inspektorów ochrony danych osobowych (IOD) największym wyzwaniem staje się zabezpieczenie co najmniej dwóch najbardziej newralgicznych (krytycznych) obszarów funkcjonowania danej jednostki lub instytucji. Pierwszy z nich stanowią stanowiska (urządzenia plus użytkownicy), które pozwalają na uzyskanie dostępu do istotnych mechanizmów oraz baz danych. Drugim zaś jest ogół tych zachowań użytkowników, które mają wpływ na bezpieczeństwo danych. Rolą IOD powinno być podnoszenie świadomości dotyczącej zagrożeń u współpracowników oraz wypracowanie z nimi odpowiedniego dla danego stanowiska oraz charakterystyki podmiotu stopnia ostrożności w codziennej pracy. Przede wszystkim należy pamiętać, że implementacja zaawansowanych zabezpieczeń technicznych ma sens jedynie wtedy, gdy zyskamy przekonanie, że wszyscy użytkownicy będą je stosować i korzystać z pełni ich możliwości. Zdaniem autora stara maksyma traktująca o tym, że łańcuch jest tak mocny, jak jego najsłabsze ogniwo, wydaje się niezwykle trafna przy projektowaniu systemów bezpieczeństwa.

Od czego zatem zacząć właściwą konfigurację zabezpieczeń? To, co jest spójne dla przebiegu przywołanych powyżej ataków cyberprzestępczych, to fakt bazowania na socjotechnice oraz wykorzystanie przez sprawców zbyt prostej polityki hasłowej i błędów wynikających z rutyny oraz niedbalstwa użytkowników[22]. Wydaje się więc, że pierwsze działania IOD powinny skupić się na takim zaprojektowaniu zabezpieczeń, by już od początku móc wprowadzić wysoki standard (próg) ochrony indywidualnej. Użytkownicy, zwłaszcza nowi, powinni szybko zdać sobie sprawę, że istnieje nieustanna potrzeba aktualizacji odpowiednich działań zabezpieczających oraz że konieczna jest odpowiednia postawa, która nie pozwoli na rutynę i rezygnację z wypracowanych dobrych nawyków[23]. Wypracowanie wstępnego poczucia, że istniejące zagrożenia w sieci są realne i poważne oraz przyzwyczajenie pracowników do regularnej pracy nad obszarem bezpieczeństwa nie stało się niestety standardem. Wejście w życie RODO w wielu podmiotach tak sektora

22 Por. J. Menn, *The vast majority of successful hacking attacks can be attributed to the errors of computer users* http://www.businessinsider.com/r-user-mistakes-aid-most-cyber-attacks-verizon-and-symantec-studies-show-2015-4?IR=T (25.03.2020).

23 Por. A. Kaczmarek, *Wytyczne w zakresie opracowania i wdrożenia polityki bezpieczeństwa*, http://www.giodo.gov.pl/163/id_art/1063/j/pl/ (25.03.2020).

publicznego, jak i prywatnego zostało odebrane jako jednorazowa konieczność spełnienia wymogów związanych z organizacją dokumentacji ochrony informacji lub ewentualnie z inwestycją w zabezpieczenia techniczne i sprzętowe. Tymczasem to właśnie regularne zwracanie uwagi użytkownikom na kwestie bezpieczeństwa może pozwolić rozwijać zarówno stopień świadomości, jak i ostrożności w firmie. Warto zacząć od zmiany typowych przyzwyczajeń pracowników wynikających z chęci pracy w stylu wygodnym. Przede wszystkim istotna jest nauka odpowiedniej polityki hasłowej oraz zachowanie zdrowego rozsądku przy komunikacji wewnętrznej oraz zewnętrznej w danym podmiocie. Dobrym nawykiem jest weryfikacja poleceń i próśb, które użytkownik otrzymuje z zewnątrz. Takie dwustopniowe uwierzytelnienie stało się standardem również w sieci, gdzie instytucje związane z obsługą obszarów szczególnie ważnych dla użytkownika, np. w bankowości elektronicznej, proszą o potwierdzenie operacji za pomocą innej metody komunikacji. Także implementacja nowoczesnych rozwiązań wydaje się odpowiedzią na niektóre zarzuty użytkowników wobec trudności związanych ze stosowaniem zaawansowanej polityki hasłowej. By uniknąć niedogodności, można wprowadzić urządzenia, które będą weryfikować tożsamość użytkownika, np. za pomocą indywidualnych cech biometrycznych, jak choćby czytniki linii papilarnych. Rozwiązania, które niegdyś wiązały się z dużą inwestycją, teraz są niedrogie i powszechnie dostępne.

Sektor prywatny stosunkowo szybko zdał sobie sprawę z faktu, że od bezpieczeństwa danych, które powierzają użytkownicy, zależy prestiż i wiarygodność firmy. Pojedyncza wpadka może oznaczać utratę zaufania klientów, co szybko znajduje odzwierciedlenie w finansach danego podmiotu[24]. Niestety brakuje analogicznej postawy w przypadku podmiotów sektora publicznego i użyteczności społecznej. Bardzo często ograniczenia budżetowe powodują opóźnienie podmiotów publicznych w adaptacji wymogów stawianych przez rozwój technologiczny. Brakuje choćby odpowiednio przygotowanego programu szkoleniowego, zawierającego kampanie edukacyjne dla obywateli, którzy często nie wiedzą, jakie zagrożenia czyhają w sieci podczas codziennego użytkowania Internetu i jak można im przeciwdziałać czy też zabezpieczyć się przed nimi. Jest to duży błąd, bo aktualnie już od najmłodszych lat dzieciom towarzyszy obcowanie z cyberprzestrzenią. W szkołach podstawowych pojawiają się pierwsze doświadczenia z mechanizmami hejtu i cyberprzemocy, a niedługo później jednostki padają ofiarami kradzieży tożsamości i phishingu. Tak

24 Por. T. Kowalczyk, *Ile kosztuje utrata danych*, https://www.computerworld.pl/news/Ile-kosztuje-utrata-danych,417779.html (25.03.2020).

w miejscach nauki i pracy, jak i w środowisku domowym oraz towarzyskim – wszędzie mogą przydarzyć się próby socjotechnicznego wyłudzenia danych, a następnie ich przestępczego wykorzystania, często ze szkodą dla danej jednostki. Pozostaje mieć nadzieję, że wyposażenie jednostek i instytucji w inspektorów ochrony danych pozwoli stopniowo zwiększać świadomość i bezpieczeństwo użytkowników, a oni będą przenosić swoją wiedzę do innych środowisk.

SUMMARY

Personal data as a key interest of cybercriminals

The development of new technologies has caused the situation that the significant part of the daily operation of an individual has moved to cyberspace. The Internet with its easy and common access has become an effective tool both at work and education process for the whole society. What is more people use the Internet to pursue a hobby and for their social life. Unfortunately, the society still has low awareness of the online threats and there can be observed a lack of proper caution, which is efficiently exploited by cybercriminals. Basing on social engineering and the tendency of users to place a lot of information about themselves on the web, the cybercriminals are able to easily break a simple security and gain access to the information they are interested in. Therefore cybercriminals activity is one of the biggest challenges for data protection officers. The article aims to describe cyber criminal mechanisms and methods of their operation and at the same time trying to answer the question how to successfully fight this phenomenon.

Keywords: personal data protection, cybercrime, data protection officer, Internet, social engineering

Dane osobowe jako kluczowy obiekt zainteresowania cyberprzestępców

Rozwój nowych technologii spowodował, że znaczna część codziennego funkcjonowania jednostki przeniosła się do cyberprzestrzeni. Powszechność i łatwy dostęp do Internetu sprawiły, że społeczeństwo sprawnie używa Internetu zarówno w pracy i nauce, jak i realizując swoje hobby oraz życie towarzyskie. Niestety, w społeczeństwie nadal występuje niska świadomość zagrożeń w sieci i brak odpowiedniej ostrożności, co bezwzględnie wykorzystują cyberprzestępcy. Bazując na socjotechnice i tendencji użytkowników do umieszczania wielu informacji o sobie w sieci, w łatwy sposób przełamują oni proste zabezpieczenia

i uzyskują dostęp do interesujących ich obszarów. Działalność cyberprzestępców to obecnie jedno z największych wyzwań, przed jakimi stają w swojej pracy inspektorzy ochrony danych. Artykuł ma na celu opisanie cyberprzestępczych mechanizmów i metod działania. Stanowi również próbę odpowiedzi na pytanie, jak skutecznie walczyć z tym zjawiskiem.

Słowa kluczowe: ochrona danych osobowych, cyberprzestępczość, inspektor ochrony danych, Internet, socjotechnika

Bibliografia

1. Dekret ogólny w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim wydany przez Konferencję Episkopatu Polski w dniu 13 marca 2018 r. podczas 378. Zebrania Plenarnego w Warszawie, na podstawie kan. 455 Kodeksu Prawa Kanonicznego, w związku z art. 18 Statutu KEP, po uzyskaniu specjalnego zezwolenia Stolicy Apostolskiej z dnia 3 czerwca 2017 r., „Akta Konferencji Episkopatu Polski" 30 (2018), s. 31–54.

2. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L. z 2016 r. Nr 119 z późn. zm.).

3. Cialdini R. B., *Wywieranie wpływu na ludzi. Teoria i praktyka*, tłum. B. Wojciszke, Gdańsk 1999.

4. Goodman M., *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*, Anchor 2016.

5. Hadnagy Ch., *Socjotechnika. Sztuka zdobywania władzy nad umysłami*, Gliwice 2017.

6. Kaczmarek A., *Wytyczne w zakresie opracowania i wdrożenia polityki bezpieczeństwa*, Generalny Inspektor Ochrony Danych Osobowych, http://www.giodo.gov.pl/163/id_art/1063/j/pl/ (25.03.2020).

7. Kwaśnik J., *Wpływ ataków socjotechnicznych na konstrukcję i kształt polityki bezpieczeństwa*, w: M. Górka, *Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa*, Warszawa 2017, s. 35–48.

8. Menn J., *The vast majority of successful hacking attacks can be attributed to the errors of computer users*, http://www.businessinsider.

com/r-user-mistakes-aid-most-cyber-attacks-verizon-and-symantec-studies-show-2015-4?IR=T (25.03.2020).

9. Mitnick K., Simon W. L., *The Art of Deception: Controlling the Human Element of Security*, Wiley 2003.

10. Rashdan A., *The Social Media OSINT Challenge to US Intelligence: Culture Not Gigabytes*, w: *New Media Politics Rethinking Activism and National Security in Cyberspace*, Cambridge 2015, s. 155–172.

11. Twaróg E., *Podaj datę urodzenia, a powiem, jaki masz PIN do karty*, http://www.pb.pl/podaj-date-urodzenia-a-powiem-jaki-masz-pin-do-karty-658891 (25.03.2020).