Cloud computing. Bezpieczeństwo dzieci i młodzieży w chmurze

Rafał Lew-Starowicz

Wielość danych gromadzonych w komputerach, ogrom miejsca na dysku, który jest niezbędny do ich przechowywania, powoduje, że praktycznie nieograniczone zasoby chmury obliczeniowej są bardzo atrakcyjne.

Każdy komputer ma ograniczoną pojemność dysku twardego, w związku z tym u jego użytkownika pojawia się pytanie, czy jest sens co chwilę kupować bardziej pojemny dysk lub wiele dysków przenośnych, aby zachować np. foldery ze zdjęciami lub ulubione filmy. Same aktualizacje systemów operacyjnych i innego oprogramowania zajmują sporo miejsca. Zatem perspektywa uwolnienia miejsca na dysku jest niezwykle kusząca. Niestety, korzystanie z usług w chmurze wiąże się także z pewnymi zagrożeniami, które postaram się pokrótce omówić.

Powszechnym czynnikiem warunkującym zagrożenia związane z korzystaniem z chmury jest brak skoncentrowania uwagi jej użytkowników na tym, kto jest faktycznym, prawnym dysponentem ich danych, kto ma do nich dostęp, a jedynie na samym procesie ich zamieszczania. Bardzo często uwaga użytkownika koncentruje się na kwestii atrakcyjności formy i łatwości, z jaką można zamieścić dane w chmurze, a nie na tym co może nastąpić po ich eksporcie do sieci. Przypomina to sytuację wysłania cennego ładunku na statku pod obcą banderą na wody chętnie odwiedzane przez piratów.

Istotna z punktu widzenia bezpieczeństwa użytkownika jest sprawa regulacji prawnych obowiązujących w państwie, w którym przechowywane są dane. Serwery, na których są one gromadzone, bywają ulokowane w różnych krajach. Wielość i różnorodność systemów prawnych poszczególnych krajów powoduje, że nie we wszystkich z nich np. naruszenie ochrony danych czy prawo autorskie może być traktowane w ten sam sposób.

Zagrożenie związane z naruszeniem prawa autorskiego

Artykuł 1.1 ustawy o prawie autorskim i prawach pokrewnych stanowi, że *przedmiotem prawa autorskiego jest każdy przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci*[2]. Z materiałów dostępnych w sieci można korzystać tylko do dozwolonego użytku osobistego[3]. W praktyce oznacza to, że można pobierać to, co zostało rozpowszechnione w Internecie, na użytek swój oraz osób najbliższych. Gdy dana treść zostanie wprowadzona do sieci, można ją uznać za rozpowszechnioną. Ale uwaga: nie dotyczy to programów komputerowych. Tych nie można udostępniać zarówno w postaci oprogramowania, jak i gier komputerowych. Zatem zarówno portale takie jak Chomikuj.pl, Wrzuta.pl, jak i ich użytkownicy wymieniający się tam plikami łamią prawo, jeśli na zamieszczanie tam materiałów nie została wyrażona zgoda osoby dysponującej do nich prawami autorskimi. Serwisy te nie powinny być traktowane jako miejsce składowania utworów w rozumieniu

[2] http://isap.sejm.gov.pl/DetailsServlet?id=WDU19940240083
[3] Ibidem.

ww. ustawy, ponieważ dostęp do nich mają osoby postronne. Należy przy tym zaznaczyć, że coraz częściej właściciele praw autorskich upominają się o swoje prawa. Tak było niedawno, gdy portal umożliwiający pobieranie polskich filmów fabularnych udostępnił kancelarii prawnej dane 100 000 użytkowników, która następnie wezwała ich do uiszczenia opłaty w wysokości 500 zł od osoby. Stało się tak, ponieważ przy korzystaniu z serwisu BitTorrent nie ma możliwości pobrania filmu czy muzyki, nie udostępniając jednocześnie chronionych prawem dzieł innym internautom, co jest czynem karalnym[4].

Prawo do prywatności

Prawo użytkownika do prywatności jest kolejnym zagadnieniem, które w świetle korzystania z chmury jest trudne do wyegzekwowania. Wyobraźmy sobie sytuację, w której nasz album z rodzinnymi zdjęciami trzymany w domu umieścimy na ławce w parku. Tak mniej więcej wygląda sytuacja publikowania przez młodzież zdjęć na portalach społecznościowych.

Portale społecznościowe, takie jak Facebook, stały się niezwykle popularne wśród młodych ludzi. Ponad 90% nastolatków w wieku 14-17 lat ma konto na takim portalu[5]. Mało który z ich użytkowników zadaje sobie trud zapoznania się z regulaminem takiego czy innego serwisu. Same portale zachęcają do uzupełniania profili użytkowników o coraz to nowe osobiste informacje. Ma to uatrakcyjnić wizerunek użytkownika w danej wirtualnej społeczności. Sugestie ze strony portalu mogą dotyczyć prośby o zamieszczenie zdjęcia, podanie nazwy szkoły, ostatnio odwiedzanych miejsc, informacji o związku, geolokacji. Z aplikacji wykorzystujących mechanizm pozycjonowania GPS (Google Maps, Sports Tracker czy Endomondo) korzysta ponad 62% uczniów[6].

Użytkownicy często nie zdają sobie sprawy, że prawa do zamieszczanych przez nich materiałów przechodzą na portal. W przypadku młodych ludzi istnieje też większe ryzyko zamieszczania przez nich zdjęć, komentarzy, których w przyszłości mogą się wstydzić. Młodzi ludzie nie myślą często o konsekwencjach podejmowanych przez siebie działań. Czasem pod wpływem impulsu, chcąc zaimponować rówieśnikom, przekraczają granice dobrego smaku, zamieszczając np. wulgarne komentarze, które może przeczytać ich przyszły potencjalny pracodawca.

Seksting

Można zdefiniować to zjawisko jako upublicznianie w Internecie swojego wizerunku o seksualnym charakterze lub wysłanie wiadomości zawierającej takie zdjęcie. Czasem jest to spowodowane namową ze strony innego użytkownika, ale może też wiązać się u nastoletniej osoby z potrzebą dowartościowania, zdobycia popularności czy zwykłą chęcią zwrócenia na siebie uwagi. W skrajnych przypadkach może być świadomym sposobem na uzyskanie korzyści majątkowej.

Młodzi użytkownicy Internetu nie są w stanie przewidzieć wszystkich konsekwencji rozpowszechniania takich materiałów. W momencie przesłania zdjęcia do sieci tracą nad nim kontrolę, może ono zostać powielone nieskończoną ilość razy. W efekcie takie działanie może zaważyć na ich dalszym życiu osobistym i zawodowym.

Ilość tego typu zachowań, powszechnych na portalach społecznościowych, z których korzystają zarówno dzieci, jak i młodzież, wytwarza wśród nich modę i zachęca innych do zamieszczania podobnych treści. Potencjalnych popularnych stron i aplikacji, z którymi wiąże się tego typu ryzyko eksponowania swojego wizerunku, do którego osoba postronna może zdobyć dostęp, jest wiele, między innymi: Facebook, Pinterest, Instagram, iCloud, Dropbox, YouTube. Niektóre z nich co prawda przewidują opcję łatwego zgłaszania naruszenia prawa, lecz wciąż trzeba edukować użytkowników, aby z niej korzystali.

Autorzy raportu „Dzieci Sieci 2.0" przytoczyli przykłady niebezpiecznych zachowań gimnazjalistów na portalach społecznościowych, które mogą przyciągać uwagę osób chcących nawiązać z nimi kontakt w celu ich uwiedzenia. Przynależność użytkowniczek do społeczności o nazwie „dupeczki",

[4] http://tech.wp.pl/kat,1009785,title,550-zl-kary-za-jeden-film-Polacy-otrzymuja-poczta-wezwania-do-zaplaty,wid,16179732,wiadomosc.html?ticaid=1134a9, dostęp 2.07.2015.

[5] Badanie EU NET ABD 2013, www.saferinternet.pl/images/stories/pdf/raport-eu-net-adb-pl-final.pdf

[6] *Postrzeganie zagadnień związanych z ochroną danych i prywatności przez dzieci i młodzież*. Raport z badań GIODO 2012, s. 21.

brak blokowania możliwości oznaczania siebie na zdjęciach zamieszczanych przez innych użytkowników to jedne z przykładów zachowań tego typu[7].

Należy zatem zalecić wszystkim użytkownikom selekcję danych, które zamieszczają w sieci, dotyczy to tak dorosłych, jak i dzieci. Bywa tak, że to rodzice swoim nieodpowiedzialnym działaniem narażają dzieci np. na negatywne skutki zamieszczania ich ośmieszających, w oczach rówieśników, zdjęć w Internecie.

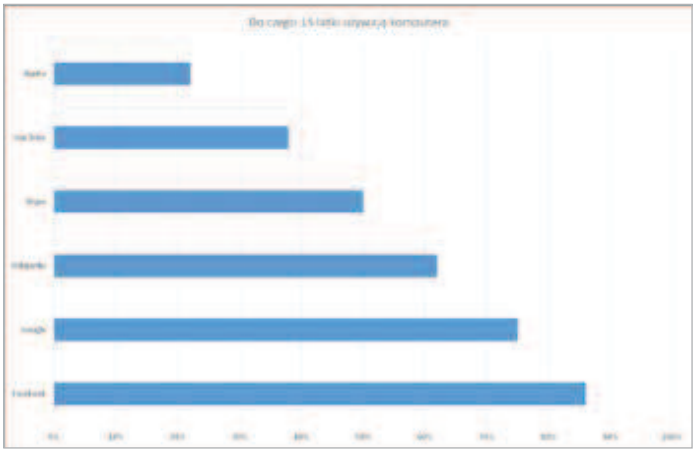
Nadaktywne korzystanie z Internetu

Dziecko, w wyniku braku uwagi ze strony rodziców i nieorganizowania mu przez nich czasu wolnego, może zostać pochłonięte tworzeniem równoległej rzeczywistości, swojego drugiego życia (jak w grze Second Life). W takim wirtualnym świecie można obecnie przebywać nieprzerwanie, korzystając z urządzeń mobilnych. To dla dziecka „dom w chmurze", który można budować całymi latami. Również monitorowanie treści zamieszczanych przez znajomych oraz informowanie ich o wszystkim, w czym się samemu uczestniczy i czego się doświadcza w realnym świecie, może doprowadzić do sytuacji spędzania wielu godzin *online*. Łatwo przewidzieć negatywne skutki zarówno dla organizmu dziecka (problemy ze wzrokiem, zaburzenia systemu nerwowego, brak snu), jak i jego osiągnieć szkolnych i relacji rodzinnych.

Nieuprawniony dostęp

Jednym z podstawowych zagrożeń związanych ze stosowaniem technologii chmury jest ryzyko nieuprawnionego dostępu do danych w niej umieszczonych. Ochrona dostępu do danych domowego komputera pozostaje w gestii jego właściciela, natomiast udowodnienie udzielenia nieuprawnionego dostępu w chmurze jest niezwykle trudne.

W interesie państwa leży, aby dzieci były bezpieczne, lecz by tak się stało, muszą się one nauczyć prawidłowo i odpowiedzialnie użytkować Internet. W przypadku wielu aplikacji w chmurze mamy do czynienia z współdzielonym dostępem do danych. Może to być korzystne, ale w pewnych przypadkach może także powodować pewne problemy. Jeśli dziecko przechowuje dane w chmurze, a rówieśnicy mają dostęp do tych informacji i plików, może to powodować poważne zagrożenie jego bezpieczeństwa. Szczególnie, jeśli będzie to wpływało na relacje dziecka z rówieśnikami w szkole. Może być tak, że osoby, z którymi ma konflikt, będą miały dostęp np. do jego zdjęć, co może stać się pożywką dla aktów cyberprzemocy.



Rysunek 1.
Do czego nastolatki używają komputera? Opracowanie własne na podstawie: Sijko K. [red.] *Kompetencje komputerowe i informacyjne młodzieży w Polsce.* Raport z międzynarodowego badania kompetencji komputerowych i informacyjnych ICILS 2013, IBE 2014

Cyberagresja rówieśnicza jest stałym elementem przestrzeni internetowej. Ofiarami napastowania przez innych w Internecie pada 6% dzieci w wieku 9-16 lat, i jest to odsetek identyczny zarówno w Polsce, jak i pozostałych krajach Unii Europejskiej. Chociaż może się to wydawać mniejszą liczbą w porównaniu z nękaniem występującym na co dzień na terenie szkoły, trzeba pamiętać, iż charakter cyberagresji jest inny, przede wszystkim nie jest incy-

[7] dzieci-sieci.pl/uploads/static/assets/Dzieci_sieci_2.0.pdf

dentalny i nie odchodzi w niepamięć tak szybko, jak incydentalne zdarzenie w szkole czy na podwórku. Skutkiem takiego nękania może być nawet samobójstwo dziecka. Ze wszystkich zagrożeń związanych z korzystaniem z komputera i Internetu przez dzieci, najmniejszą świadomość ich opiekunowie mają właśnie na temat napastowania ich przez rówieśników w sieci – 63% rodziców dzieci, które były nękane w Internecie, uważa, że takie zdarzenie nie miało miejsca[8].

Dane wrażliwe

Coraz więcej platform edukacyjnych, medyczne bazy danych informacji na temat zdrowia pacjenta, bazy wyników uczniów, umiejscowione są w chmurze administrowanej przez zewnętrzne firmy. Zawierają one cały szereg danych wrażliwych, podobnie jak bazy danych z realizowanych w szkole badań przez podmioty zewnętrzne, w tym firmy marketingowe. Są to dane dotyczące miejsca zamieszkania, numery PESEL, inne szczególne dane służące do losowania próby badawczej. Zdarza się, że jedynym zabezpieczeniem takich informacji stanowi hasło dostępu a nie szyfrowane połączenie. Naraża to osoby, których dane są gromadzone na działania marketingowe, oszustwa, upublicznianie informacji poufnych.

Na zagrożenie dotyczące ewentualnego dostępu do danych gromadzonych o uczniach w Systemie Informacji Oświatowej zwracał uwagę między innymi Generalny Inspektor Ochrony Danych Osobowych[9].

Z badania GIODO realizowanego w latach 2011--2012 można wnioskować, że 21% dzieci i młodzieży (11-16 lat) korzysta z aplikacji w Internecie umożliwiających przechowywanie, publikację i edycję swoich dokumentów lub innych plików (np. Picasa, Dropbox), przy czym większe zainteresowanie tego typu usługami wykazują gimnazjaliści – 27% badanych podało innej osobie swoje hasło lub nazwę użytkownika, pozwalające na zalogowanie się do ich poczty elektronicznej, profil na portalu społecznościowym czy też konto innego serwisu lub aplikacji internetowej[10]. Wyniki tego badania świadczą o pilnej potrzebie edukacji młodych ludzi na temat ochrony danych osobowych.

Problematyczny jest też zakres informacji, jaki posiadają rodzice na temat przekazywanych danych przez przedszkola, szkoły czy przychodnie o ich dzieciach, a także o procesie, w jaki się to przekazywanie danych odbywa.

Już w przedszkolach prowadzi się wiele badań naukowych, w których grupę badaną stanowią dzieci. Niektóre uczelnie i poszczególni badacze nie zabezpieczają odpowiednio wyników swoich badań, narzędzi w postaci ankiet, baz danych respondentów (w tym teleadresowych).

Podobnie szkolne biblioteki katalogów użytkowników, kart bibliotecznych. Ważne tutaj jest przestrzeganie zasad archiwizacji dokumentów, dbania o to, by zastrzec w umowie odpowiednie klauzule chroniące dane wrażliwe osób, także po okresie wykonania usługi. Trzeba wziąć pod uwagę czynniki ryzyka związane z ewentualnym zakończeniem działalności, np. dostawcy platformy e-learningowej. Trzeba zadać sobie pytanie, co się stanie z danymi będącymi w jej posiadaniu w sytuacji, gdy dana firma przestanie istnieć? Podobnie – co się z nimi stanie, jeśli przejmie ją inny podmiot gospodarczy?

Do bardzo niekomfortowej dla użytkowników sytuacji doszło w 2009 roku w związku z serwisem z książkami Magnolia, kiedy to w wyniku awarii serwera serwis stracił bezpowrotnie pół terabajta danych swoich klientów[11].

Zawsze może do tego dojść w wyniku awarii lub celowego działania cyberprzestępcy

Działania profilaktyczne

Celem działań profilaktycznych kierowanych do młodzieży powinno być *powstrzymywanie lub ograniczanie zachowań niekorzystnych społecznie, zwiększanie zdolności do podejmowania konstruktywnych decyzji, usuwanie lub ograni-*

[8] Pyżalski J. *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży,* Oficyna Wydawnicza „Impuls", Kraków 2012, s.202-209.

[9] http://prawo.rp.pl/artykul/759828.html

[10] Postrzeganie..., op. cit., s. 21-22.

[11] Lew-Starowicz R. *Zagrożenia dzieci w chmurach i ich przezwyciężanie* [w:] Szpor G. [red.] *Internet Cloud computing. Przetwarzanie w chmurach,* Wydawnictwo Beck S.A., Warszawa 2013, s. 194.

czanie zewnętrznych zagrożeń zwiększających ryzyko powstania zachowań niekorzystnych, a także podnoszenie poziomu zdolności do obrony przed różnego rodzaju zagrożeniami zewnętrznymi[12]. Trudno mówić o kontroli treści zamieszczanych na serwisach typu YouTube, który codziennie odwiedza 2 mld osób, a każdej minuty jest tam zamieszczanych przez użytkowników 60 godzin materiału filmowego. Niemniej odpowiednio prowadzona edukacja medialna w szkole, która zapobiegałaby bezkrytycznemu podejściu do Internetu, jak również uczyła selektywnego doboru danych przy ich zamieszczaniu *online* przyniosłaby pożądany skutek działań profilaktycznych. Dyrektorzy szkół winni mieć świadomość tego, gdzie można zdobyć materiały edukacyjne, propozycje standardów bezpieczeństwa w szkole, przykłady programów profilaktycznych dla szkół, systemy zabezpieczeń danych.

Warta podkreślenia jest także rola rodziców monitorujących treści, jakie ich dzieci zamieszczają w Internecie, spędzających z nimi czas na rozmowie i dbający o to, jak są chronione ich dane w szkołach, bankach, na portalach społecznościowych. Trzeba uczulić dzieci na to, aby krąg odbiorców zamieszczanych przez nich danych był jak najbardziej ograniczony i by w sytuacji, gdy natrafią na informacje o sobie, których nie tworzyły, poinformowały o tym rodziców. Warto edukować młodzież, aby zamieszczając informacje o innych osobach, takie jak ich poglądy, dane osobowe czy inne poufne dane, zawsze prosiły o zgodę osób, których one dotyczą.

Na portalach społecznościowych trzeba pomóc dziecku ustawić ograniczenia dostępu do prywatnych informacji. Nie powinno zdawać się tu na zabezpieczenia wyjściowe oferowane przez administratora portalu, które zwykle ustawione są na podstawowym poziomie.

Przede wszystkim jednak trzeba uczyć dzieci i młodzież zachować równowagę między światem Internetu – tym w chmurach – a tym na ziemi, zapewniając im dostęp do ciekawych zajęć i poświęcając im uwagę.

[12] Szymański A. *Niedostosowanie społeczne dzieci i młodzieży*. Wybrane problemy, Warszawa 2010, s. 218.

Bibliografia

1. Dziecko krzywdzone. Teoria, badania, praktyka, vol. 12 nr 1/(2013).
2. Siuda P., Stunża G.D., Dąbrowska A.J., Klimowicz M., Kulczycki E., Piotrowska R., Rozkosz E., Sieńko M., Stachura K. *Dzieci Sieci 2.0. Kompetencje komunikacyjne młodych,* Instytut Kultury Miejskiej, Gdańsk 2013.
3. Pyżalski J. *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży,* Oficyna Wydawnicza „Impuls", Kraków 2012.
4. Szpor G. [red.] I*nternet Cloud computing. Przetwarzanie w chmurach,* Wydawnictwo Beck S.A., Warszawa 2013.
5. Postrzeganie zagadnień związanych z ochroną danych i prywatności przez dzieci i młodzież. Raport z badań GIODO 2012.
6. Szymański A. *Niedostosowanie społeczne dzieci i młodzieży. Wybrane problemy,* Warszawa 2010.
7. http://tech.wp.pl/kat,1009785,title,550-zl-kary-za-jeden-film-Polacy-otrzymuja-poczta-wezwania-do-zaplaty,wid,16179732,wiadomosc.html?ticaid=1134a9
8. http://www.creditcards.com/credit-card-news/schools-student-personal_data_privacy-cloud-1282.php
9. https://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/Cyber-Bullying procent20and procent20Online procent20Grooming

Rafał Lew-Starowicz jest absolwentem Wydziału Dziennikarstwa i Nauk Politycznych UW oraz studiów doktoranckich w Zakładzie Edukacji Medialnej, Wydziału Nauk Pedagogicznych, Akademii Pedagogiki Specjalnej im. Marii Grzegorzewskiej w Warszawie. Jako pracownik Instytutu Badań Edukacyjnych brał udział w ewaluacji Rządowego Programu „Cyfrowa Szkoła". Członek Rady Ogólnoeuropejskiego Systemu Oznaczeń Gier Komputerowych i Wideo PEGI (Pan European Game Information Council) oraz Komitetu Konsultacyjnego Programu „Safer Internet" w Polsce, ekspert programu „Szkołą z klasą 2.0". Jest autorem kilkunastu publikacji na temat bezpieczeństwa dzieci i młodzieży w Internecie.