BEZPIECZEŃSTWO TEORIA I PRAKTYKA SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2023
Nr 4 (LIII)

DOI: 10.48269/2451-0718-btip-2023-4-008
Data wpłynięcia: 13.06.2023
Data akceptacji: 6.10.2023

Mariusz Grzyb

mgr inż., Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
https://orcid.org/0000-0001-8439-9650

Marta Woźniak-Zapór

dr inż., Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
https://orcid.org/0000-0002-7773-2408

Bezpieczeństwo danych w małej firmie – wybór rozwiązań chmurowych

Wprowadzenie

W ostatnich latach widoczny jest efekt znacznej cyfryzacji procesów biznesowych. Dodatkowym mechanizmem powodującym przyspieszenie tego procesu była bezsprzecznie pandemia COVID-19 oraz wojna na Ukrainie. Cyfryzacja procesów biznesowych jest więc dziś jednym z aspektów zarządzania współczesną organizacją[1]. W związku z aktualnymi przepisami dotyczącymi ochrony danych, ważnym elementem zarządzania w organizacji staje się zarządzanie ochroną danych. Dlatego sposób przetwarzania danych w firmie się zmienia. Coraz częściej firmy wybierają rozwiązania chmurowe. Przy zarządzaniu ochroną danych w przedsiębiorstwie[2]

[1] A.E. Sawicka, *Cyberbezpieczeństwo jako współczesne wyzwanie w zarządzaniu małym i średnim przedsiębiorstwem*, „Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie" 2022, nr 47, s. 43–59, https://znz.pcz.pl/fcp/uGBUKOQtTKlQhbx08SlkTUQJEUWRuHQwFDBoIVURNWHlBG1gnBVcoFW8SBDRKTxMWRxcBFyUJT1hLd1kIU0FYMA/_users/code_BEFIYKhdNJlY7HgMxDRFLAVVDMzgvF0MSBQ/znz/zeszyty/47/47_4.pdf [dostęp: 18.05.2023].

[2] W naukach o zarządzaniu pojęcia „firma" i „przedsiębiorstwo" są traktowane jak synonimy i stosowane zamiennie.

należy zwrócić uwagę na wybór odpowiedniego rozwiązania, które umożliwi bezpieczne funkcjonowanie i prowadzenie działalności.

Zarządzanie bezpieczeństwem. Pojęcie cyberbezpieczeństwa

Jedna z definicji bezpieczeństwa mówi, że jest ono „pewnym stanem obiektywnym, polegającym na braku zagrożenia, odczuwanym subiektywnie przez jednostki i grupy. Oznacza to, że bezpieczeństwo składa się z dwóch elementów, obiektywnego i subiektywnego. Pierwszy z nich, mający charakter obiektywny, jest zewnętrzny w stosunku do jednostki, grupy społecznej, zbiorowości. Z kolei drugi ma charakter subiektywny i jest poczuciem bezpieczeństwa"[3]. Przeciwieństwem bezpieczeństwa jest stan, w którym występuje poczucie zagrożenia. Bezpieczeństwo ma dynamiczny charakter, zmienny w zależności od wieloczynnikowych zjawisk o charakterze obiektywnym i subiektywnym[4]. Inna definicja, bardziej ogólna, mówi, że bezpieczeństwo „obejmuje zaspokojenie takich potrzeb jak: istnienie, przetrwanie, całość, tożsamość (identyczność), niezależność, spokój, posiadanie i pewność rozwoju. Brak bezpieczeństwa powoduje niepokój i poczucie zagrożenia. Biorąc pod uwagę poczucie tego zagrożenia, w nauce wyróżnia się bezpieczeństwo wewnętrzne i bezpieczeństwo zewnętrzne. Bezpieczeństwo wewnętrzne oznacza stabilność i harmonijność danego organizmu lub podmiotu, natomiast bezpieczeństwo zewnętrzne – brak zagrożenia ze strony innych podmiotów lub czynników zewnętrznych"[5]. Bezpieczeństwo – zgodnie z innym podejściem – „jest to sytuacja odznaczająca się brakiem ryzyka, np. w inwestowaniu, planach strategicznych produktu itp., albo zasobach materialnych i ludzkich"[6].

W literaturze spotkać można także liczne definicje bezpieczeństwa informacji. Może ono być definiowane jako „obrona [...], która polega na uniemożliwieniu i utrudnieniu zdobywania danych o fizycznej naturze aktualnego oraz planowanego stanu rzeczy i zjawisk we własnej przestrzeni funkcjonowania, a także utrudnianiu wnoszenia entropii informacyjnej do komunikatów i destrukcji fizycznej do nośników danych"[7]. Bezpieczeństwo definiowane jest też jako obrona informacyjna, w skład której wchodzą liczne przedsięwzięcia, w tym zapobieganie, odstraszanie,

---

3 H. Korzeniowska, *Edukacja dla bezpieczeństwa w systemie oświatowym Europy na przykładzie Polski i Słowacji*, European Association for Security, Kraków 2004, s. 10.

4 J. Szmyd, *Bezpieczeństwo jako wartość. Refleksja aksjologiczna i etyczna*, [w:] *Zarządzanie bezpieczeństwem*, red. P. Tyrała, Wydawnictwo Profesjonalnej Szkoły Biznesu, Kraków 2000, s. 166; K. Chałubińska-Jentkiewicz, *Cyberbezpieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law" 2019, nr 2 (2), s. 7–23.

5 K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wydawnictwo Adam Marszałek, Toruń 2006, s. 9.

6 W. Šmid, *Metamarketing*, Wydawnictwo Profesjonalnej Szkoły Biznesu, Kraków 2000, s. 50.

7 L. Ciborowski, *Walka informacyjna*, Europejskie Centrum Edukacyjne, Wydawnictwo Adam Marszałek, Toruń 1999, s. 186.

wskazywanie i ostrzeganie, wykrywanie, przygotowanie się na sytuację awaryjną i reakcję na ewentualny atak[8]. Bezpieczeństwo informacji to także działanie zmierzające do zabezpieczenia zgromadzonych informacji poddawanych jakiemukolwiek przetwarzaniu, przechowywaniu czy udostępnianiu z wykorzystaniem komputerów w sieciach teleinformatycznych[9].

„Krajowe systemy teleinformatyczne wraz z przetwarzanymi w nich zasobami informacyjnymi, połączone rozległymi sieciami komputerowymi stanowią cyberprzestrzeń. W cyberprzestrzeni realizowane są usługi cyfrowe obywateli – jako społeczeństwa informacyjnego, podmiotów gospodarczych i różnych organizacji, usługi wspomagające działalność administracji i podmiotów realizujących zadania publiczne. Równolegle do realizowanych działań o charakterze rozwojowym, w cyberprzestrzeni realizowane są szkodliwe działania i działalność przestępcza, wywołująca ogromne szkody procesowe, finansowe, społeczne, w tym ograniczenie wzajemnego zaufania"[10]. Cyberbezpieczeństwo rozumiane może być jako „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy"[11]. Cyberbezpieczeństwo jest także „ogółem technik, procesów oraz praktyk, które stosuje się w celu ochrony sieci informatycznych, urządzeń, programów i danych przed atakami lub dostępem nieautoryzowanym. [...] Cyberbezpieczeństwo to także zespół zagadnień związanych z zapewnianiem ochrony w obszarze cyberprzestrzeni"[12].

Zarządzanie bezpieczeństwem organizacji jest procesem złożonym, który powinien obejmować wszystkie sfery i kierunki działania i rozwoju organizacji[13]. „System bezpieczeństwa organizacji jest to celowo zaprojektowany i zorganizowany układ materialny, zespołów ludzkich i informacyjny (ideowy) eksploatowany przez człowieka, służący zachowaniu założonego poziomu oddziaływania zróżnicowanych zagrożeń (ryzyka) w celu zachowania bytu organizacji w postaci zapewnienia niezbędnych zasileń i samodzielnego kształtowania możliwości jej rozwoju w danych warunkach

---

8 M. Jabłoński, M. Mielus, *Zagrożenia bezpieczeństwa informacji w organizacji gospodarczej*, [w:] *Bezpieczeństwo informacji i biznesu. Zagadnienia wybrane*, red. M. Kwieciński, Krakowskie Towarzystwo Edukacyjne sp. z o.o. – Oficyna Wydawnicza AFM, Kraków 2010, s. 25.

9 P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006, s. 71.

10 G. Mąkosa, *Zarządzanie bezpieczeństwem krajowych systemów teleinformatycznych*, „Studia Bezpieczeństwa Narodowego" 2020, R.10, nr 17, s. 123, https://doi.org/10.37055/SBN/144283.

11 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. z 2018 r., poz. 1560 ze zm., art. 2, pkt 4.

12 K. Wojciechowska, *Cyberbezpieczeństwo – definicja*, ISPortal, 3.01.2023, https://isportal.pl/cyberbezpieczenstwo-definicja [dostęp 12.05.2023].

13 M. Huczek, *Problematyka zarządzania bezpieczeństwem w organizacjach samorządu terytorialnego i szkołach wyższych*, „Zeszyty Naukowe Wyższej Szkoły Humanitas. Zarządzanie" 2010, nr 2, s. 96–102.

otoczenia"[14]. Zarządzanie bezpieczeństwem powinno pozwalać na utrzymanie poczucia bezpieczeństwa wśród interesariuszy procesów (również tych związanych z cyberbezpieczeństwem) w organizacji na wysokim poziomie.

Uwarunkowania prawne w zakresie cyberbezpieczeństwa

W strategii zarządzania cyberbezpieczeństwem należy uwzględnić wytyczne zawarte w obowiązujących ustawach, dyrektywach, rozporządzaniach oraz zasady i rekomendacje opracowywane przez organizacje zajmujące się cyberbezpieczeństwem[15]. Są to:

- Rozporządzenie o ochronie danych osobowych (RODO)[16],
- Ustawa o krajowym systemie cyberbezpieczeństwa[17],
- Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[18].

Dla firm prowadzących swoją działalność z uwzględnieniem powyższych wytycznych ważną informacją jest ogłoszenie nowej dyrektywy UE, skrótowo nazywanej NIS2[19]. Pierwsza dyrektywa NIS (Network and Information Systems Directive)[20] zawierała definicję założeń cyberbezpieczeństwa dla państw będących członkami Unii Europejskiej. Na jej podstawie 28 sierpnia 2018 r. wdrożona została zmiana Ustawy o krajowym systemie cyberbezpieczeństwa. Projekt dyrektywy NIS2 został

[14] M. Kwieciński, *Zarządzanie bezpieczeństwem działalności przedsiębiorstwa – zarys problematyki*, „Prace Naukowo-Dydaktyczne Państwowej Wyższej Szkoły Zawodowej im. Stanisława Pigonia w Krośnie" 2016, nr 70, s. 154–155.

[15] M. Kibil, I. Piecuch, *Cyberbezpieczeństwo a praca zdalna*, „Monitor Prawniczy" 2020, nr 20, dodatek: *Prawo nowych technologii – dane osobowe i prywatność, cyberbezpieczeństwo, handel elektroniczny, innowacje, internet i media, prawo IT*, red. X. Konarski, https://iuscase.pl/cyberbezpieczenstwo-a-praca-zdalna [dostęp 12.05.2023].

[16] 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 119 z 4 maja 2016 r. ze zm. [dalej: RODO].

[17] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, *op. cit.*

[18] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, tekst jedn. Dz.U. z 2017 r., poz. 2247.

[19] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2), Dz.Urz. UE L 333 z 27 grudnia 2022 r.

[20] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz.Urz. UE L 194 z 19 lipca 2016 r.

opublikowany 16 grudnia 2020 r., natomiast 27 grudnia 2022 r. dyrektywa NIS2 zastąpiła dyrektywę NIS.

Bezpieczeństwo danych w firmie – pierwsze kroki

W ramach prac nad zabezpieczeniem danych w małej firmie, zazwyczaj w pierwszej kolejności realizowane są zalecenia określone w RODO, wprowadzone Ustawą z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 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)[21]. Ustawa weszła w życie 4 maja 2019 r.

W pierwszej kolejności należy dokonać analizy przetwarzanych w firmie danych. Na tej podstawie możliwe będzie wykonanie rejestru czynności przetwarzania. Zgodnie z artykułem 30 RODO[22] w rejestrze tym zamieszcza się następujące informacje:

a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów;
b) cele przetwarzania;
c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione;
e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Ustęp 2 tego artykułu określa, co powinien zawierać rejestr kategorii czynności przetwarzania. Obydwa przypadki nie dotyczą jednak przedsiębiorstw zatrudniających mniej niż 250 osób, „chyba że przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1, lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o czym mowa w art. 10”[23].

---

[21] Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 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.U. z 2019 r., poz. 730.

[22] RODO, art. 30, ust. 1.

[23] RODO, art. 30, ust. 5.

Kolejnym krokiem jest analiza ryzyka oraz zaplanowanie środków mających na celu zapobieganie zagrożeniom. Następnie, na podstawie pełnej wiedzy na temat przetwarzanych danych, osobach odpowiedzialnych za przetwarzanie konkretnych danych na różnych etapach działalności firmy, sposobów przetwarzania, powierzania danych, a także możliwych ryzykach, stworzona może być polityka bezpieczeństwa. Jeżeli dane przetwarzane są w wersji cyfrowej, powinna powstać instrukcja zarządzania systemami informatycznymi do przetwarzania danych. W przypadku współpracy z innymi podmiotami, w ramach której dochodzi do możliwości przetwarzania danych, należy z taką firmą podpisać umowę powierzenia przetwarzania danych i informację o tym wprowadzić do rejestru powierzeń danych.

Bezpieczeństwo danych w chmurze – przykład wdrożenia w małej firmie

Jak już wspomniano – cyfryzacja procesów biznesowych doprowadziła do upowszechnienia rozwiązań chmurowych w zakresie przechowywania danych w firmach. Ważnym czynnikiem, który napędzał przejście z rozwiązań tradycyjnych do chmury, była w dużej mierze pandemia COVID-19. Obecnie – w okresie spowolnienia gospodarczego i wojny w Ukrainie – również widać wśród przedsiębiorców zainteresowanie rozwiązaniami chmurowymi. Ma na to wpływ zmieniający się rynek i przejście na pracę zdalną w okresie pandemii oraz ostatnie zmiany w polskim prawie. Pokazały to wyraźnie badania przeprowadzone od października do grudnia 2022 r. przez Deloitte[24]. Przechowywanie danych w chmurze staje się coraz popularniejsze ze względu na dużą oszczędność czasu i pieniędzy. Umieszczenie plików (zdjęć, filmów, muzyki, dokumentów) w chmurze zapewnia łatwy dostęp do danych praktycznie z dowolnego miejsca i urządzenia, które podłączone jest do Internetu.

W związku z tym przeanalizowano siedem oferowanych na polskim rynku rozwiązań chmurowych, wybranych z uwagi na dużą popularność, jaką cieszą się wśród użytkowników – głównie dzięki prostocie użytkowania. Dla przedsiębiorców korzystających z dysków chmurowych ogromną zaletą jest możliwość synchronizacji plików pomiędzy poszczególnymi urządzeniami czy pracownikami. Funkcja ta doskonale sprawdza się w przypadku korzystania z więcej niż jednego urządzenia. Wcześniej konieczne było przenoszenie danych – obecnie najczęściej robi się to automatycznie, a synchronizacja pozwala na aktualizację zawartości chmury w bardzo krótkich czasie. Przedstawione przez nas usługi przechowywania danych w chmurze posiadają opcje bezpłatnych pakietów oraz bardziej zaawansowane usługi płatne – producenci oferują różnego rodzaju pakiety z opcjami dodatkowymi. Na samym początku trzeba się

[24] *The CFO Programme. 2023 Central Europe CFO Survey*, Deloitte, https://www2.deloitte.com/content/dam/Deloitte/ce/Documents/cfo/CE_CFO_2023_Report.pdf [dostęp 12.05.2023].

jednak zastanowić, ile miejsca w chmurze tak naprawdę wykorzystamy. Przeciętnie pracownik, który zamierza przechowywać w sieci dane firmowe, powinien rozejrzeć się za opcją oferującą 100–200 GB. To przestrzeń, która powinna mu w zupełności wystarczyć. Osoby, które pracują na wielu dużych plikach, wybiorą pakiety o pojemności 1–2 TB.

Charakterystyka wybranych rozwiązań chmurowych

Dysk Google (Google Drive) – obecnie jedna z najpopularniejszych usług do przechowywania danych w chmurze. Bierze się to stąd, że wszyscy użytkownicy popularnej usługi pocztowej Gmail oraz systemu operacyjnego na urządzenia mobile Android muszą mieć aktywne konto Google. Posiadając konto Google, jesteśmy automatycznie posiadaczami Dysku Google i w wersji podstawowej mamy do dyspozycji 15 GB na dane. Użytkownicy najczęściej wykorzystują przyznaną im przestrzeń do tworzenia kopii zapasowych, przechowywania dokumentów, zdjęć, filmów, muzyki. Producent zadbał również o współdzielenie zasobów, wspólną pracę oraz synchronizację z różnego typu urządzeniami.

Microsoft OneDrive – jest doskonałym wyborem dla użytkowników pakietu Office 365. Otrzymują oni bezpłatnie 1 TB przestrzeni dyskowej z dodatkowymi funkcjami. Można też skorzystać z bardzo dobrej oferty na samą przestrzeń na dane przechowywane w chmurze. Współdzielenie zasobów, wspólna praca i synchronizacja danych to dopełnienie tego zestawu.

Dropbox – jedno z pierwszych rozwiązań dla klientów biznesowych. Dropbox oferuje świetną integracje z aplikacjami firm Microsoft i Adobe. Posiada również rozbudowane opcje zabezpieczeń przed utratą danych. W wersji bezpłatnej oferowana przestrzeń jest bardzo skromna w porównaniu z konkurencyjnymi rozwiązaniami: zaledwie 2 GB. Producent zdecydowanie jest tu nastawiony na klienta biznesowego.

Apple iCloud Drive – skierowany głównie do użytkowników innych produktów firmy Apple, ponieważ jest zaimplementowany zarówno w systemie macOS, jak i iOS. Oczywiście możemy go używać w innych środowiskach, ale jest to mało popularne rozwiązanie poza urządzeniami Apple.

Box – jest dyskiem oferującym przestrzeń chmurową do przechowywania plików dla osób indywidualnych i biznesu. Mimo dobrze działającej aplikacji do synchronizacji nie oferuje nic, czym mógłby się wyróżnić na tle konkurencyjnych rozwiązań.

Mega – oferta z korzystnymi rozwiązaniami chmurowymi. Najważniejszym atutem jest bezpieczeństwo. Szyfrowanie typu end-to-end chroni zasoby użytkowników nawet podczas przesyłania pomiędzy urządzeniem końcowym a serwerem. Mega udostępnia każdemu użytkownikowi klucze do szyfrowania, co chroni przed niepowołanym dostępem. Niestety utrata klucza uniemożliwia odzyskanie danych.

Sync – łatwe w użyciu i niedrogie rozwiązanie do przechowywania danych w chmurze. Sync oferuje bezpłatnie 5 GB miejsca oraz przesyłanie plików bez

ograniczenia. Zastosowane szyfrowanie zapewnia prywatność i nieograniczone plany przechowywania danych. Jednak użytkownicy mogą odczuwać spowolnienie kompleksowym szyfrowaniem i ograniczoną integracją aplikacji innych firm.

W tabeli 1 przedstawione zostało zestawienie najważniejszych parametrów rozwiązań chmurowych wybranych do analizy.

Tabela 1. Darmowa przestrzeń na dane w chmurze

Badany parametr	Dysk Google	Microsoft OneDrive	Dropbox	Apple iCloud	Box	Mega	Sync
Darmowa przestrzeń	15 GB	5 GB	2 GB	5 GB	10 GB	20 GB	5 GB

Źródło: zestawienie na podstawie materiałów dostawców.

Jeśli chodzi o wielkość przestrzeni na dane, przodującym rozwiązaniem jest więc Mega, oferujące 20 GB bezpłatnego miejsca. Drugi pod tym względem jest Dysk Google, a trzeci – Box.

Tabela 2. Zestawienie planów płatnych, wielkości przestrzeni na dane w chmurze wraz z ich cenami oraz średnią ceną za 1 TB*

Badany parametr	Dysk Google	Microsoft OneDrive	Dropbox	Apple iCloud	Box	Mega	Sync
Przestrzeń na dane w planach płatnych	30 GB 1 użytkownik 27 zł/miesięcznie 2 TB 1 użytkownik 54 zł/miesięcznie 5 TB 1 użytkownik 54 zł/miesięcznie	1 TB 1 użytkownik od 21 do 52 zł/miesięcznie (cena uzależniona od pakietu z dodatkowymi aplikacjami)	3 TB 1 użytkownik 75 zł/miesięcznie 5 TB min. 3 użytkowników 54 zł/miesięcznie bez limitu min. 3 użytkowników 81 zł/miesięcznie	50 GB 1 użytkownik 4,50 zł/miesięcznie 200 GB 1 użytkownik 13,50 zł/miesięcznie 2 TB 1 użytkownik 45 zł/miesięcznie	100 GB 1 użytkownik 54 zł/miesięcznie 100GB min. 3 użytkowników 27 zł/miesięcznie bez limitu min. 3 użytkowników od 81 zł/miesięcznie	Minimalny pakiet dla firm 3 TB 3 użytkowników 68 zł/miesięcznie	2 TB 1 użytkownik 36 zł/miesięcznie 6 TB 1 użytkownik 90 zł/miesięcznie
Średni koszt 1 TB na dane w chmurze	27 zł	21 zł	25 zł	22,50 zł	25 zł	22,60 zł	18 zł

* Warunki oferty i ceny z dnia 28.05.2023 r.
Źródło: zestawienie na podstawie materiałów dostawców.

Najtańszym pod względem średniej ceny za 1 TB danych jest Sync – z najbardziej ubogimi parametrami, jeśli chodzi dane przechowywane w chmurze (tabela 2). Najdroższym rozwiązaniem w tym zestawieniu jest Dysk Google, w którym oprócz miejsca na dane dostajemy pokaźną dawkę aplikacji do wykorzystania, takich jak np. Dokumenty, Arkusze czy Prezentacje. Podobnie wyposażony pakiet Microsoft 365 Business Basic otrzymamy już za 25,20 zł[25].

Tabela 3. Historia przechowywanych plików w chmurze, kompatybilność z systemami operacyjnymi

Badany parametr	Dysk Google	Microsoft OneDrive	Dropbox	Apple iCloud	Box	Mega	Sync
Historia plików*	30 dni	30 dni	180 dni	–	–	od 30 do 365 dni	od 180 do 365 dni
Aplikacje na komputer stacjonarny	Windows MacOS	Windows MacOS	Windows MacOS	Windows MacOS	Windows MacOS	Windows MacOS	Windows MacOS
Aplikacje na urządzenia mobilne wraz z ocenami Google Play	Android (4,2)	Android (4,7)	Android (4,3)	Android (3,8)	Android (4,5)	Android (4,4)	Android (3,8)

* Czas na przywrócenie usuniętych plików lub cofnięcie wprowadzonych zmian.
Źródło: zestawienie na podstawie materiałów dostawców.

Wszystkie przedstawione w tabeli 3 rozwiązania mogą być stosowane z systemem operacyjnym Windows i MacOS w przypadku komputerów stacjonarnych oraz Android na urządzeniach mobilnych.

W tabeli 4 przedstawiono porównanie usług pod względem szyfrowania danych, zgodności z RODO i korzystania z weryfikacji dwuetapowej.

Tabela 4. Parametry szyfrowania, zgodność usługi z wymogami RODO oraz dostępność weryfikacji dwuetapowej

Badany parametr	Dysk Google	Microsoft OneDrive	Dropbox	Apple iCloud	Box	Mega	Sync
Szyfrowanie	Tak	Tak	Tak	Tak	Tak	Tak	Tak
Zgodny z RODO	Tak	Tak	Tak	Tak	Tak	Tak	Tak
Weryfikacja dwuetapowa	Tak	Tak	Tak	Tak	Tak	Tak	Tak

Źródło: zestawienie na podstawie materiałów dostawców.

Opis badania

Badanie zostało przeprowadzone między wrześniem 2022 a kwietniem 2023 r. w Krakowie, w małej firmie zatrudniającej siedem osób. Do badania wykorzystano siedem

[25] Ceny z dnia 28.05.2023 r.

komputerów stacjonarnych, w tym trzy z zainstalowanym systemem operacyjnym Windows 10 oraz cztery z Windows 11. Każdy z komputerów miał zainstalowany pakiet biurowy Microsoft Office 2021, program antywirusowy ESET oraz przeglądarki Microsoft Edge, Google Chrome, Mozilla Firefox i aplikację dedykowaną do danego dysku chmurowego. W badaniu wykorzystane zostały również telefony pracowników z systemem Android, na których zainstalowane zostały aplikacje poszczególnych producentów. Do siedziby firmy doprowadzony jest światłowód i wykupiony pakiet internetowy pozwalający na osiągnięcie 2 Gb/s przy pobieraniu i 1 Gb/s przy wysyłaniu. Urządzania sieciowe są dostosowane do wyższych prędkości, niż wskazały testy szybkości łącza, a okablowanie wewnątrz firmy jest przynajmniej kategorii 6. Testy prędkości były wykonywane jednocześnie na wszystkich komputerach w firmie. Dane przetwarzane przez pracowników mieszczą się w przedziałach od 200 do 700 MB. Część danych wykorzystywanych w badaniu była współdzielona przez użytkowników. Każdy z pracowników miał założone indywidualne konto w każdej usłudze, wykorzystano pakiety bezpłatne. Badanie prowadzono na każdym oprogramowaniu, które zostało ujęte w opisie, przez około 30 dni (20 dni roboczych).

W wywiadach przeprowadzonych z użytkownikami po badaniu ustalono, że praca przebiegała płynnie, nie było problemów z synchronizacją danych. Współdzielone dane pojawiały się folderach na wszystkich komputerach i telefonach bez zauważalnych opóźnień. Aplikacje do synchronizacji danych pracowały w tle, nie powodowały opóźnienia w zapisie ani spowolnienia pracy komputerów.

Po zakończonym badaniu właściciel firmy zdecydował się na zastosowanie na stałe chmury Mega. Głównym argumentem, dla którego został wybrany ten konkretny pakiet, było to, że ma on zastosowane klucze szyfrujące i dane na serwerach są zaszyfrowane. Jest to informacja zdecydowanie premiująca to rozwiązanie w stosunku do pozostałych. Wszystkie dane w Mega są szyfrowane kluczami generowanymi na podstawie hasła użytkownika. To jest główny klucz szyfrowania. To, co sprawia, że jest to tak bezpieczne, to fakt, że nikt oprócz samego użytkownika nie ma dostępu do hasła. Mega nie posiada klucza deszyfrującego, a dane na ich serwerach przechowywane są w postaci zaszyfrowanej. Posiadacz klucza deszyfrującego, czyli użytkownik, decyduje, kto i jak może uzyskać dostęp do danych. W Mega przywrócenie dostępu do własnego konta jest to możliwe jedynie za pomocą klucza odzyskiwania. Klucz odzyskiwania chroni również konto przed cyberatakami. Takie bezkompromisowe podejście do bezpieczeństwa oznacza, że Mega nie wysyła linków do resetowania haseł. To niestety oznacza problem, gdy użytkownik zapomni hasło. Jedynym sposobem na odzyskanie dostępu do konta w Mega jest posiadanie klucza odzyskiwania. Należy więc pamiętać o tym, aby klucz odzyskiwania był przechowywany w bezpiecznym miejscu. Dodatkowym bardzo dobrym rozwiązaniem jest udostępnianie linków – domyślnie klucz deszyfrujący jest wysyłany razem z nimi, ale można zwiększyć bezpieczeństwo i wybrać eksport i wysyłanie

klucza deszyfrującego oddzielnie. Użytkownik, który otrzyma łącze, musi wprowadzić klucz, zanim będzie mógł je otworzyć. Rozwiązanie to dobrze się sprawdza przy udostępnianiu zasobów z danymi osobowymi. Mega wspiera również dwuskładnikowe uwierzytelnianie (2FA). Jest to dodatkowa warstwa ochrony konta. Po włączeniu 2FA, za każdym razem, gdy użytkownik loguje się lub dokonuje zmian na swoim koncie, musi wprowadzić 6-cyfrowy kod z aplikacji uwierzytelniającej.

Podsumowanie

Przedstawione zostały aktualne zagadnienia związane z problemami zarządzania bezpieczeństwem – w tym bezpośrednio cyberbezpieczeństwem. Jest to niezwykle istotne z uwagi na rozwój cyfryzacji w każdej dziedzinie życia, także – a może szczególnie – w procesach biznesowych. Obecnie trudno sobie wyobrazić jakąkolwiek organizację, która nie przetwarza danych w sposób cyfrowy. W niektórych przypadkach inny sposób byłby nawet niemożliwy z uwagi na ilość tych danych lub sposób prowadzenia działalności. Zapewnienie bezpieczeństwa danych i informacji staje się ważnym elementem strategii zarządzania bezpieczeństwem w organizacjach. Obowiązujące przepisy prawa regulują obowiązki podmiotów związane z bezpieczeństwem przetwarzanych danych. W obliczu coraz szerszych możliwości naruszenia bezpieczeństwa danych – ze względu na szybki rozwój technologiczny nieprzewidzianych wcześniej – przepisy te są aktualizowane i zaostrzane.

Ważnym zagadnieniem jest bezpieczeństwo rozwiązań chmurowych, które są coraz częściej wybierane jako alternatywa dla przechowywania danych na serwerach firmowych. Wybór konkretnego rozwiązania nie jest łatwy: oprócz ceny, wielkości miejsca na przechowywanie danych czy wygody podczas użytkowania, szczególną uwagę należy zwrócić na zapewnienie bezpieczeństwa. Odpowiedzialność za zapewnienie bezpieczeństwa serwera leży na dostawcy rozwiązania chmurowego. Natomiast odpowiedzialność za bezpieczne przetwarzanie danych tam zawartych spoczywa już na firmie, która z takiego rozwiązania korzysta. Dlatego warto z rozwagą wybierać rozwiązanie chmurowe, przy zapewnieniu odpowiednich mechanizmów zarządzania bezpieczeństwem w organizacji.

Bibliografia

Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006.

The CFO Programme. 2023 Central Europe CFO Survey, Deloitte, https://www2.deloitte.com/content/dam/Deloitte/ce/Documents/cfo/CE_CFO_2023_Report.pdf [dostęp 12.05.2023].

Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law" 2019, nr 2 (2), s. 7–23.

Ciborowski L., *Walka informacyjna*, Europejskie Centrum Edukacyjne, Wydawnictwo Adam Marszałek, Toruń 1999.

Huczek M., *Problematyka zarządzania bezpieczeństwem w organizacjach samorządu terytorialnego i szkołach wyższych*, „Zeszyty Naukowe Wyższej Szkoły Humanitas. Zarządzanie" 2010, nr 2, s. 96–102.

Jabłoński M., Mielus M., *Zagrożenia bezpieczeństwa informacji w organizacji gospodarczej*, [w:] *Bezpieczeństwo informacji i biznesu. Zagadnienia wybrane*, red. M. Kwieciński, Krakowskie Towarzystwo Edukacyjne sp. z o.o. – Oficyna Wydawnicza AFM, Kraków 2010, s. 23–38.

Kibil M., Piecuch I., *Cyberbezpieczeństwo a praca zdalna*, „Monitor Prawniczy" 2020, nr 20, dodatek: *Prawo nowych technologii – dane osobowe i prywatność, cyberbezpieczeństwo, handel elektroniczny, innowacje, internet i media, prawo IT*, red. X. Konarski, https://iuscase.pl/cyberbezpieczenstwo-a-praca-zdalna [dostęp 12.05.2023].

Korzeniowska H., *Edukacja dla bezpieczeństwa w systemie oświatowym Europy na przykładzie Polski i Słowacji*, European Association for Security, Kraków 2004.

Kwieciński M., *Zarządzanie bezpieczeństwem działalności przedsiębiorstwa – zarys problematyki*, „Prace Naukowo-Dydaktyczne Państwowej Wyższej Szkoły Zawodowej im. Stanisława Pigonia w Krośnie" 2016, nr 70, s. 149–170.

Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wydawnictwo Adam Marszałek, Toruń 2006.

Mąkosa G., *Zarządzanie bezpieczeństwem krajowych systemów teleinformatycznych*, „Studia Bezpieczeństwa Narodowego" 2020, R.10, nr 17, s. 129–146, https://doi.org/10.37055/SBN/144283.

Sawicka A.E., *Cyberbezpieczeństwo jako współczesne wyzwanie w zarządzaniu małym i średnim przedsiębiorstwem*, „Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie" 2022, nr 47, s. 43–59, https://znz.pcz.pl/fcp/uGBUKOQtTKlQhbx08SlkTUQJEUWRuHQwFDBoIVURNWHlBG1gnBVcoFW8SBDRKTxMWRxcBFyUJT1hLd1kIU0FYMA/_users/code_BEFIYKhdNJlY7HgMxDRFLAVVDMzgvF0MSBQ/znz/zeszyty/47/47_4.pdf [dostęp: 18.05.2023].

Szmyd J., *Bezpieczeństwo jako wartość. Refleksja aksjologiczna i etyczna*, [w:] *Zarządzanie bezpieczeństwem*, red. P. Tyrała, Wydawnictwo Profesjonalnej Szkoły Biznesu, Kraków 2000.

Šmid W., *Metamarketing*, Wydawnictwo Profesjonalnej Szkoły Biznesu Kraków 2000.

Wojciechowska K., *Cyberbezpieczeństwo – definicja*, ISPortal, 3.01.2023, https://isportal.pl/cyberbezpieczenstwo-definicja [dostęp 12.05.2023].

Akty prawne

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, tekst jedn. Dz.U. z 2017 r., poz. 2247.

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 119 z 4 maja 2016 r. ze zm.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz.Urz. UE L 194 z 19 lipca 2016 r.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. z 2018 r., poz. 1560 ze zm.

Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 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.U. z 2019 r., poz. 730.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2), Dz.Urz. UE L 333 z 27 grudnia 2022 r.

Bezpieczeństwo danych w małej firmie – wybór rozwiązań chmurowych
Streszczenie

W związku z rozwojem cyfryzacji praktycznie w każdej dziedzinie życia, cyfryzacji podlegają również procesy biznesowe. Konieczność ochrony danych, dodatkowo w zgodzie z obowiązującymi przepisami, nastręcza wielu problemów. Szczególnym przypadkiem jest kwestia cyberbezpieczeństwa w aspekcie rozwiązań chmurowych. W opracowaniu przedstawione zostały zagadnienia dotyczące bezpieczeństwa informacji, cyberbezpieczeństwa, zarządzania bezpieczeństwem, wdrażania RODO, a także wyboru rozwiązania chmurowego na przykładzie małej firmy.

Słowa kluczowe: bezpieczeństwo informacji, cyberbezpieczeństwo, zarządzanie bezpieczeństwem, RODO, rozwiązania chmurowe

Data security in a small company: choosing cloud solutions
Abstract

With the development of digitalisation in virtually every area of life, business processes are also being digitised. The need to protect data, additionally in accordance with applicable regulations, poses many problems. A special case is the issue of cyber security in terms of cloud solutions. This paper presents issues relating to information security, cyber security, security management, implementation of GDPR and the choice of a cloud solution based on the example of a small company.

Key words: information security, cyber security, security management, GDPR, cloud solutions