Wprowadzenie

Bezpieczeństwo danych osobowych. Podejście oparte na ryzyku

Wprowadzenie

Osoby prowadzące jakikolwiek biznes powinny dbać o bezpieczeństwo danych. To w zasadzie truizm, bo każdy przedsiębiorca troszczy się o to na tyle, na ile może i potrafi. Lepiej więc mówić o zarządzaniu bezpieczeństwem danych. Jednak aby zarządzać bezpieczeństwem danych osobowych, trzeba wiedzieć, jakie są możliwe ataki, jak można im zapobiegać, a jeśli już się wydarzą – jak postępować, żeby zminimalizować ich skutki. Przed tradycyjnymi zagrożeniami umiemy się bronić: montujemy zamki antywłamaniowe, wstawiamy kraty w okna, instalujemy alarm lub system nadzoru wideo, a nawet zatrudniamy służby ochrony. Uczono nas tego od pokoleń, jednak w dobie informacji cyfrowej nasza wiedza o zabezpieczeniach może okazać się niewystarczająca.

Coraz częściej do przetwarzania i przechowywania danych wykorzystuje się techniki cyfrowe: komputery, laptopy, smartfony, sieci komputerowe, usługi chmurowe. Komputery i systemy informatyczne są tak powszechne, że wspierają prawie wszystkie możliwe procesy biznesowe. *Peter F. Drucker* określa to mianem „ostrej komputerozy”[1] – i nie ma się czemu dziwić, bo **dzisiaj w systemach informatycznych gromadzi się prawie wszystkie firmowe informacje. W większości są to dane osobowe**. Zagrożenia dla informacji przetwarzanych w taki sposób nadal nie są powszechnie znane, chociaż technologia komputerowa jest z nami od mniej więcej kilkudziesięciu lat, a podczas ostatnich kilkunastu lat gwałtownie się rozwinęła. Wciąż wiele osób ma problemy z podstawową obsługą urządzeń cyfrowych, a co dopiero mówić o świadomości zagrożeń, które się z tym wiążą. Przykłady naszej nieostrożności można mnożyć. Kiedy wychodzimy z domu, zamykamy drzwi na klucz – to oczywiste. Dlaczego więc w przypadku komputera albo telefonu komórkowego nie widzimy problemu w tym, aby używać ich bez hasła? Dlaczego wielu z nas nie ma obaw, żeby podłączyć do komputera znaleziony pendrive (dysk USB) czy kartę pamięci SD[2]? Ilu z nas jest świadomych tego, że takie nośniki mogą być skażone np. wirusami komputerowymi?

Trudność poruszania się w cyfrowym świecie wynika również ze specyfiki i właściwości informacji. Kradzież portfela łatwo zauważyć – po prostu go nie ma. Ale gdy ktoś skopiuje plik z komputera, nie zauważymy, że doszło do kradzieży, ponieważ skradziony przedmiot nie zostanie usunięty z urządzenia. Wiele osób sprzedaje, oddaje lub złomuje wysłużone komputery, laptopy czy tablety. Wiemy, że przed sprzedażą trzeba usunąć wszelkie ważne dokumenty i zdjęcia (w końcu nikt nie sprzedaje mebli ze złotą biżuterią i pieniędzmi w szafie!). Zaawansowani użytkownicy formatują dodatkowo dysk lub karty pamięci. Ale i to niewiele daje, bo dane są wciąż na dysku i można je odczytać – wystarczy tylko wiedzieć, jak to zrobić!

---

1 Zob. *P.F. Drucker*, Menedżer skuteczny. Efektywności można się nauczyć, Warszawa 2014.

2 Karta SD (ang. *secure digital*) to nośnik często wykorzystywany w aparatach cyfrowych, tabletach czy telefonach komórkowych. Karty SD mają niewielkie wymiary (24 × 32 × 2,1 mm) i niską masę (ok. 2 gramów).

Brak świadomości cyfrowych zagrożeń pojawia się także w biznesie, nawet w firmach, które opierają swoją działalność wyłącznie na pracy przy komputerach. Wydawałoby się, że takie organizacje powinny mieć bardzo dobrze opracowane kwestie cyfrowego bezpieczeństwa, jednak nie zawsze odpowiednie procedury są wdrażane i zachowywane. **Dla osób prowadzących biznes ochrona informacji powinna mieć jeszcze większe znaczenie** niż dla innych użytkowników urządzeń cyfrowych. Cyberbezpieczeństwo jest bowiem jednym z narzędzi pozwalających zachować, a nawet wzmocnić pozycję konkurencyjną przedsiębiorstwa dzięki budowaniu zaufania i reputacji firmy.

Co szczególnie ważne, wiele firmowych informacji (a w niektórych organizacjach – większość) to dane osobowe. Brak odpowiednich zabezpieczeń danych osobowych nie tylko wpływa na konkurencyjność i reputację organizacji, lecz także powoduje ryzyko nałożenia na nią wysokich kar. **Od 25.5.2018 r. każdy, kto przetwarza dane osobowe, jest zobowiązany stosować się do przepisów RODO**. Nakazują one odpowiednio zabezpieczać dane osobowe, w tym posiadać mechanizmy pozwalające wykrywać sytuacje, gdy dzieje się coś niepokojącego (np. niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych). Na pewno nie jest za późno na to, aby nauczyć się, jak dbać o bezpieczeństwo danych osobowych (a przy okazji także innych firmowych informacji). **Świadomość możliwości i technik, którymi dysponują przestępcy, połączona z wiedzą o tym, jak się chronić, pozwala na sprawne zarządzanie bezpieczeństwem**.

Większe organizacje i korporacje mają łatwiej, gdyż posiadają środki finansowe na zatrudnienie specjalistów od zabezpieczeń komputerowych i bezpieczeństwa informacji. Czasami są to duże zespoły wspierające procesy biznesowe. Natomiast osoby prowadzące działalność gospodarczą, mikroprzedsiębiorstwa i małe firmy są w trudniejszej sytuacji – nie zawsze mogą zatrudnić doświadczonego profesjonalistę, który na co dzień będzie dbał o ochronę danych osobowych. Szkolenia dotyczące zabezpieczania danych są dość drogie i zajmują czas, a literatura o cyberbezpieczeństwie danych osobowych adresowana do małych przedsiębiorców w zasadzie nie istnieje. Dlatego mimo że **tę książkę kieruję do wszystkich przetwarzających dane osobowe, to skupiam się w niej przede wszystkim na mniejszych przedsiębiorstwach**. Do takiego podejścia zainspirował mnie *J. Viega*, który stwierdził: „jest wiele konkretnych rozwiązań użytecznych w środowisku korporacyjnym i niemających sensu w przypadku pojedynczego użytkownika”[3].

W tej publikacji dzielę się swoją wiedzą i wieloletnim doświadczeniem, które zdobyłem dzięki pracy w dużych organizacjach o charakterze finansowym (ubezpieczenia, bankowość, pożyczki, fundusze emerytalne, fundusze inwestycyjne) i doradzaniu mniejszym firmom. Sam prowadzę działalność gospodarczą jako osoba fizyczna, więc łatwiej mi zrozumieć, jak RODO może wpływać na niewielkie organizacje. W książce podaję praktyczne porady, uwzględniające specyfikę życia i działalności w polskich realiach. Szukam równowagi między zabezpieczeniami a wygodą funkcjonowania, bo bardzo ważne jest to, aby zabezpieczając dane osobowe, nie przesadzić. Odpowiadam nie tylko na pytanie, jak zabezpieczyć dane, lecz także – dlaczego to robić.

Naturalnym uzupełnieniem tej publikacji jest książka „Ochrona danych osobowych. Praktyczny przewodnik dla przedsiębiorców”, której jestem autorem[4]. Opisuje w niej wszystkie istotne aspekty zapewnienia zgodności z RODO, np. jakie dane można przechowywać, kiedy je usuwać, o czym informować osoby, których dane dotyczą, jak prowadzić dokumentację.

Bezpieczeństwo danych osobowych to obszerna materia, której można by poświęcić opasłe tomy. Zdaję sobie sprawę, że przedsiębiorca nie ma czasu na czytanie, a chce się skupić na prowadzeniu biznesu. Dlatego w tej publikacji przedstawiłem podstawowe zabezpieczenia, które będą dobrym fundamentem do budowania bardziej zaawansowanych zabezpieczeń na podstawie przepro-

[3] *J. Viega*, Mity bezpieczeństwa IT. Czy na pewno nie masz się czego bać?, Warszawa 2010, s. 41.
[4] *L. Kępa*, Ochrona danych osobowych. Praktyczny przewodnik dla przedsiębiorców, Warszawa 2018.

wadzonej analizy ryzyka dla praw i wolności osób fizycznych. Jestem przekonany, że książka, którą oddaję w Państwa ręce, to dobra lektura, pozwalająca rozumieć, jakie są ryzyka związane z przetwarzaniem danych osobowych, jak z nimi postępować, jakie zabezpieczenia dobierać, aby były odpowiednie, i jak zarządzać bezpieczeństwem we własnej organizacji. Życzę udanej lektury!

Leszek Kępa