S T U D I A N A D B E Z P I E C Z E Ń S T W E M

NR 3 **ss. 65–76** **ROK 2018**

ISSN 2543–7321

Przyjęto: 27.10.2017
Zaakceptowano: 11.01.2018

Oryginalna praca badawcza

Ewa Matuska
Akademia Pomorska
Słupsk
ewa.matuska@apsl.edu.pl

ZARZĄDZANIE BEZPIECZEŃSTWEM CYFROWYM W SEKTORZE MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTW – ASPEKTY PERSONALNE

MANAGING CYBERSECURITY IN THE SMALL AND MEDIUM ENTERPRISES SECTOR – PERSONAL ASPECTS

***Zarys treści*:** Dziedziną, w której szczególnie należy zapewnić bezpieczne przetwarzanie danych w biznesie, jest obszar procesów kadrowych oraz marketingowych związanych z relacjami z klientami. Artykuł podejmuje kwestię oceny przygotowania sektora polskich MŚP do zarządzania cyberbezpieczeństwem w kontekście upowszechniania praktyk cyfrowych w procesach przekazywania i przetwarzania danych biznesowych oraz wyzwań nowej ustawy o ochronie danych osobowych (NUODO). Opisuje luki obszarowe, w tym luki kompetencyjne menadżerów i pracowników, w sferze odpowiedzialnej ochrony procesów gospodarczych przed zagrożeniami cyfrowymi. We wnioskach sformułowano zalecenie umiejscowienia systemowej ochrony przed zagrożeniami cyfrowymi w obszarze zarządzania strategicznego oraz powierzenie jej zadań operacyjnych także działom personalnym, a nie tylko technicznym.
***Słowa kluczowe*:** biznes cyfrowy, cyberbezpieczeństwo, ochrona danych osobowych, kompetencje cyfrowe, zarządzanie strategiczne, zarządzanie zasobami ludzkimi
***Key words*:** digital business, cybersecurity, personal data protection, digital competences, strategic management, human resources management

Wprowadzenie

Cyfryzacja procesów biznesowych stwarza szansę zwiększonej elastyczności w produkcji, wyższej jakości produktów, zwiększonej produktywności i wielokierunkowej komunikacji marketingowej. Popularyzacja biznesów cyfrowych w gospodarce

wynika przede wszystkim z poszukiwań konkurencyjnych rozwiązań w związku z ostatnim kryzysem ekonomicznym, podczas którego upadło wiele przedsiębiorstw zorganizowanych w sposób tradycyjny. Stworzyło to nisze rynkowe dla pojawienia się innowacyjnych organizacji – *organizacji wirtualnych*, wykorzystujących potęgę Internetu w niskokosztowym wariancie prowadzenia działalności gospodarczej.

Niskie koszty to zwłaszcza szansa rozwoju dla małych i mikroprzedsiębiorstw oraz tworzenia start-upów. Tym samym jest to zachęta do przedsiębiorczości i kreacji innowacyjnych pomysłów biznesowych. Innowacje są niezbędne, by sprostać wymaganiom coraz bardziej świadomych klientów, którzy starannie wybierają wartości, za które płacą. Ponadto klienci coraz częściej chcą współtworzyć kupowane produkty czy usługi, dlatego chętnie uczestniczą w inicjatywach marketingowych typu *crowdsourcing*[1] organizowanych w Internecie – na portalach społecznościowych, poprzez webinaria, *open calls* czy – coraz bardziej popularne – blogi tematyczne. Na globalnej platformie ludzie i organizacje oddziałują na siebie, komunikują się, współpracują, opracowują nowe strategie, produkty i usługi. Podobnie pracownicy firm spontanicznie współtworzą wirtualny wizerunek pracodawców, zamieszczając w sieci opinie i komentarze o swoich miejscach pracy. Mobilne aplikacje dodają tym procesom niespotykanego zasięgu i tempa. Mocne strony organizacji cyfrowych to – oprócz małych nakładów – takie atrybuty, jak: złożoność, elastyczność, uspołecznienie.

Te atuty jednak niosą także istotne ryzyka związane przede wszystkim z intensywnym przetwarzaniem danych osobowych klientów, obywateli, pracowników. Digitalizacja procesów biznesowych powoduje wiele zagrożeń, które muszą być uwzględniane zarówno przy projektowaniu nowych wirtualnych start-upów, jak i w monitorowaniu funkcjonowania każdej organizacji korzystającej z narzędzi ICT (Information Communication Technology). Z narzędzi tych w komunikacji zewnętrznej i wewnętrznej korzystają powszechnie wszystkie firmy, zarówno duże, jak i te mniejsze, należące do tzw. sektora małych i średnich przedsiębiorstw (MŚP)[2]. W grupie MŚP znajdują się również mikroprzedsiębiorstwa (MMŚP), zatrudniające od 1 do 9 osób, które stanowią większość podmiotów gospodarczych w całym sektorze MŚP.

Zabezpieczenie przetwarzanych danych osobowych klientów i pracowników stało się wymogiem prawa z dniem 25 maja 2018 r., gdy zaczęły obowiązywać regulacje nowej unijnej ustawy o ochronie danych osobowych – General Data Protection Regulation (GDPR), które w Polsce jako tzw. nową ustawę o ochronie danych osobowych (NUODO)[3] zdecydowano się wprowadzić w sposób kompleksowy, tj. wraz ze zmianami w ponad 130 ustawach we wszystkich sektorach[4]. Tym samym postawiono bar-

[1] Crowdsourcing (ang. crowd – 'tłum', outsourcing – 'korzystanie z zasobów zewnętrznych') – komunikowanie się z dużą liczbą osób w celu pozyskania ich wiedzy, opinii, czasu, zasobów itp.

[2] Sektor MŚP – sektor mikro-, małych i średnich przedsiębiorstw. Obejmuje podmioty, które zatrudniają mniej niż 250 pracowników i których roczny obrót nie przekracza 50 milionów euro, a/lub całkowity bilans roczny nie przekracza 43 milionów euro. Por. *Nowa definicja MŚP. Poradnik dla użytkowników i wzór oświadczenia*, Komisja Europejska, [Bruksela] 2006, s. 5.

[3] *Nowa ustawa o ochronie danych osobowych – najważniejsze zagadnienia*, https://gdpr.pl/nowa-ustawa-o-ochronie-danych-osobowych#Nowa_ustawa_o_ochronie_danych_osobowych (dostęp: 9.09.2017).

[4] Założenia NUODO Ministerstwo Cyfryzacji ogłosiło 14.09.2017 r. jako projekt zmian kompleksowych, w odróżnieniu od praktyk innych krajów UE, gdzie najpierw ogłaszana jest nowa ustawa o ochronie danych osobowych, a dopiero później ustawy dostosowawcze w innych sektorach.

dzo wysoko poprzeczkę w dziedzinie bezpiecznego przetwarzania danych przed wszystkimi podmiotami gospodarczymi. Jest to wyzwanie szczególnie trudne dla firm z sektora mikroprzedsiębiorstw, które z uwagi na zazwyczaj mniejsze zasoby kapitałowe nie mają wystarczających środków finansowych na zakup kompleksowych, systemowych zabezpieczeń przetwarzania danych.

Stan cyfryzacji polskich firm sektora MŚP

Sektor małych i średnich przedsiębiorstw w Polsce powinien być zorientowany na wykorzystanie niskokosztowych wariantów biznesowych. Zdają się to potwierdzać dane raportu pt. „Małe i średnie firmy w Polsce – bariery i rozwój", zrealizowanego przez PI Research dla Banku Zachodniego WBK w 2016 roku. Wynika z nich, że ogólnie wzrost MŚP jest oparty na inwestycjach w znacznie mniejszym stopniu niż w przypadku dużych przedsiębiorstw[5], co sugerowałoby prawdopodobną orientację MŚP na poszukiwanie racjonalnych ekonomicznie rozwiązań inwestycyjnych. Jednakże ten sam raport podsumowuje, że „niska skłonność do zwiększania skali działalności i wysoka awersja do podejmowania ryzykownych, długoterminowych projektów inwestycyjnych"[6] mają źródło przede wszystkim w brakach wiedzy menadżerów MŚP na temat nowoczesnych narzędzi i rozwiązań. Tym samym digitalizacja mniejszych firm napotyka na barierę kompetencyjno-mentalną kadry zarządzającej. Istnieje też istotna bariera ilościowa – skali udziału sektora MŚP w gospodarce. W Polsce, na tle pozostałych krajów członkowskich Unii Europejskiej, jest on najniższy: na 1000 mieszkańców liczba MŚP (z wyłączeniem mikrofirm) w 2015 roku wynosiła tylko 1,9 (np. na Węgrzech – 2,8; w Niemczech – 4,6; średnia dla wszystkich państw UE to 3,1)[7].

Warto jednak zaznaczyć, że udział polskich MŚP w tworzeniu PKB systematycznie, chociaż powoli, rośnie – od 2008 do 2014 roku wzrósł o 2,8 p.p. (z 47 do 50%). W puli przychodów tworzonych przez wszystkie przedsiębiorstwa MŚP (bez mikrofirm) w Polsce generują ok. 36% udziału PKB (44% stanowi wkład firm dużych)[8]. W piętnastu na dwadzieścia siedem państw członkowskich UE to jednak sektor MŚP generuje większe przychody niż duże przedsiębiorstwa. Pokazuje to na stale niewykorzystany potencjał rozwojowy tego sektora w Polsce, który mógłby wiele skorzystać na wprowadzeniu biznesowych rozwiązań cyfrowych.

W marcu 2017 roku Komisja Europejska opublikowała wyniki przeprowadzanych corocznie badań w ramach Indeksu Gospodarki Cyfrowej i Społeczeństwa Cyfrowego (Digital Economy and Society Index, DESI 2017). Narzędzie to przedstawia wyniki 28 państw członkowskich, między innymi w obszarze informatyzacji przedsiębiorstw. Zgodnie z raportem DESI 2017[9]:

---

[5] A. Czerniak, M. Stefański, *Polityka Insight Research, Małe i średnie firmy w Polsce – bariery i rozwój*, Bank Zachodni WBK, 2016, https://static3.bzwbk.pl/asset/m/a/l/male-i-srednie-firmy-w-polsce2_-polityka-insight_61682.pdf (dostęp: 12.09.2017).

[6] Tamże, s. 11.

[7] Tamże, s. 5.

[8] *Raport o stanie sektora małych średnich przedsiębiorstw w Polsce*, PARP, 2017, s. 5, www.parp.gov.pl/images/PARP_publications/pdf/raport%20o%20stanie%20sektora%20msp%20w%20polsce_2017.pdf (dostęp: 10.09.2017).

[9] *Raport KE: cyfrowa przepaść*, http://ec.europa.eu/poland/news/170303_digital_pl (dostęp: 10.09.2017).

- Europejskie przedsiębiorstwa w coraz większym stopniu stosują technologie cyfrowe, wykorzystując np. oprogramowanie dla przedsiębiorstw w celu elektronicznej wymiany informacji (wzrost z 26 proc. w 2013 r. do 36 proc. w 2015 r.) lub przesyłania faktur elektronicznych (wzrost z 10 proc. w 2013 r. do 18 proc. w 2016 r.).
- Nieznacznie wzrósł również handel elektroniczny prowadzony przez małe i średnie przedsiębiorstwa (z 14 proc. w 2013 r. do 17 proc. w 2016 r.) Jednak tylko mniej niż połowa z nich sprzedaje swoje produkty do innych państw członkowskich UE.

Przyczyniły się do tego zapewne zmienione przez Komisję Europejską w 2016 r. przepisy mające pobudzić rozwój handlu elektronicznego poprzez ograniczenie blokowania geograficznego, obniżenie kosztów i poprawę transgranicznego doręczania przesyłek oraz zwiększenie zaufania klientów dzięki wzmocnionej ochronie i lepszemu egzekwowaniu przepisów. Wnioski z raportu DESI 2017 w odniesieniu do Polski jednak nie są satysfakcjonujące, bowiem wskazują na jej opóźnienie cyfrowe[10]:

- na bardzo niskim poziomie utrzymują się nowoczesne funkcje biznesowe, jak: korzystanie z mediów społecznościowych, usług w chmurze (np. hosting danych, oprogramowanie w zakresie rachunkowości, oprogramowanie do zarządzania relacjami z klientami, moce obliczeniowe);
- tylko jedno na dziesięć polskich MŚP prowadzi sprzedaż internetową[11] (dla porównania, w krajach UE sprzedaż z wykorzystaniem tego kanału prowadzi średnio 17% MŚP), a obroty w zakresie handlu elektronicznego MSP wynoszą jedynie 6,6%;
- zaledwie 3,8% polskich MŚP prowadzi transgraniczną sprzedaż internetową, a 67%[12] polskich przedsiębiorstw posiada stronę internetową;
- ogólne wyniki Polski w raporcie z 2017 r. w dziedzinie cyfryzacji pogorszyły się w porównaniu z rokiem 2016.

Wyniki te współbrzmią z innymi badaniami potwierdzającymi „cyfrowe wykluczenie" sektora MŚP w Polsce, takimi jak:

- „Monitoring kondycji sektora MMŚP", przeprowadzony w 2015 roku na zlecenie Konfederacji Lewiatan na reprezentatywnej próbie firm (N=1111), który wykazał, że:
  - 26% małych i 9% mikrofirm w Polsce nie korzysta z żadnych technologii informatycznych;
  - przedsiębiorstwa analogowe są bardziej zachowawcze pod względem strategii zarządczych (ok. 70% z nich jest zorientowanych na „przetrwanie i utrzymanie się na rynku"), biznesy cyfrowe[13] bardziej (ok. 65%) zorientowane na „dynamiczny rozwój";

[10] *Indeks gospodarki cyfrowej i społeczeństwa cyfrowego (DESI) 2018. Sprawozdanie krajowe dotyczące Polski*, https://ec.europa.eu/digital-single-market/en/scoreboard/poland (dostęp: 10.09.2017).

[11] Sprzedaż za pośrednictwem sieci informatycznej stanowiąca co najmniej 1% łącznego obrotu.

[12] Według danych raportu „Cyfryzacja gospodarki Polski", obejmującego również mikroprzedsiębiorstwa, zdecydowana większość polskich przedsiębiorstw jednak ma stronę internetową, a 60% z nich posiada internetowy katalog swoich produktów i oferuje możliwość zakupu lub zamówienia produktów przez Internet.

[13] Za cyfrowe uznawano biznesy wykorzystujące co najmniej trzy technologie informatyczne.

  - przedsiębiorstwa cyfrowe są bardziej innowacyjne – ok. 60% firm cyfrowych wprowadziło na rynek w 2014 r. i planowało wprowadzić w 2015 r. nowe lub ulepszone produkty wraz z innowacjami marketingowymi;
- badanie „Nowoczesne IT w MŚP 2015", zrealizowane przez Ipsos MORI na zlecenie Microsoft[14], które konstatuje:
  - brak mobilności pracowników – 76% pracowników MŚP w Polsce przyznaje, że muszą być obecni w biurze, aby móc w pełni efektywnie wykonać swoje obowiązki;
  - brak orientacji menadżerów na elastyczne formy pracy – 64% ankietowanych właścicieli firm z sektora MŚP uważa, że rozwiązania mobilne pomagają oszczędzać czas i wspierają produktywność, a połowa zdecydowanie zgadza się, że urządzenia i usługi mobilne pozwalają na efektywną pracę zdalną z domu oraz ułatwiają wykonywanie zadań służbowych w drodze do pracy.

Podsumowując, na tle innych krajów członkowskich Unii Europejskiej polski sektor mikro- i małych przedsiębiorstw jest w połowie drogi do cyfryzacji. Potwierdzają to dane dotyczące pozycji Polski zawarte w „Sprawozdaniu z postępów Europy w zakresie cyfryzacji za rok 2017"[15]. Wynika z niego, że obecnie e-biznes w Polsce generuje jedynie około 4,1% PKB, a dla porównania w Wielkiej Brytanii, Szwecji i Danii udział tego sektora w strukturze PKB wynosi 6–8%. Istnieje więc ryzyko, że polska działalność gospodarcza ponosi straty, nie wykorzystując wystarczająco potencjału komercyjnego technologii cyfrowych. Warto jednak dodać, że cyfryzacja biznesu, także w sektorze MŚP, jest nieuchronna w świetle realizacji kolejnych kroków krajowej *Strategii Innowacyjności i Efektywności Gospodarki „Dynamiczna Polska 2020"*[16] z roku 2013, która zakłada intensywne wsparcie rządu dla rozwoju Internetu rzeczy. Zgodnie z tą strategią w roku 2016 uruchomiono krajowy projekt fakturowania elektronicznego, aby wesprzeć wdrażanie Dyrektywy Parlamentu Europejskiego i Rady z dnia 16 kwietnia 2014 r. w sprawie fakturowania elektronicznego w zamówieniach publicznych[17] oraz rozpoczęto budowę krajowej platformy usług obsługującej fakturowanie elektroniczne dla zamówień publicznych. Strategia zakłada, że w długiej perspektywie wszystkie polskie przedsiębiorstwa skorzystają z efektu synergii wynikającej z lepszej łączności między podmiotami gospodarczymi i publicznymi oraz z rozwoju umiejętności cyfrowych swoich pracowników i menadżerów.

---

[14] Por. A. Klimczuk, *Cyfrowi bardziej konkurencyjni. Małe firmy na START do FIRMOWYCH (R)EWOLUCJI*, https://news.microsoft.com/pl-pl/2015/06/11/cyfrowi-bardziej-konkurencyjni-male-firmy-na-start-do-firmowych-rewolucji (dostęp: 1.10.2017).

[15] *Sprawozdanie z postępów Europy w zakresie cyfryzacji za 2017 (EDPR), profil krajowy Polski*, Komisja Europejska 2017, ec.europa.eu/newsroom/document.cfm?doc_id=44328 (dostęp: 2.09. 2017).

[16] Uchwała Nr 7 Rady Ministrów z dnia 15 stycznia 2013 r. w sprawie Strategii Innowacyjności i Efektywności Gospodarki „Dynamiczna Polska 2020", http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WMP20130000073&type=2 (dostęp: 12.09.2017).

[17] Dyrektywa Parlamentu Europejskiego i Rady 2014/55/UE z dnia 16 kwietnia 2014 r. w sprawie fakturowania elektronicznego w zamówieniach publicznych, http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32014L0055&from=PL (dostęp: 15.09.2017).

Bezpieczeństwo cyfrowe polskich MŚP

Stan bezpieczeństwa w zakresie danych biznesowych przetwarzanych cyfrowo jest, jak dotąd, przedmiotem dość nielicznych badań i tylko niektóre z nich poświęcono sektorowi MŚP. W celu uchwycenia trendu zmian przeanalizowano badanie ankietowe wykonane w roku 2010 przez firmę Symantec – Polska[18] na próbie 200 polskich przedsiębiorstw z sektora MŚP oraz badanie dostawcy sprzętu komputerowego Lenovo Polska pt. „Raport: Sprzęt IT – polskie MŚP cenią wydajność i nowoczesność" z roku 2017[19].

Ranking sposobów ochrony danych stosowanych przez sektor MŚP na podstawie analizy wyników obydwu badań przedstawiono w tabeli 1.

Tabela 1

Sposoby ochrony danych stosowane w polskich przedsiębiorstwach sektora MŚP

Table 1

Data protection methods used in Polish enterprises of the SME sector

Badanie Symantec z 2010 r. Które rozwiązania bezpieczeństwa i dostępu posiada Państwa firma? (pytanie wielokrotnego wyboru)	**Badanie Lenovo z 2017 r. Jakie formy ochrony bezpieczeństwa danych i prywatności są stosowane do sprzętu IT? (pytanie wielokrotnego wyboru)**
Program antywirusowy – 98%	Program antywirusowy – 69%
Tworzenie kopii zapasowych (back-up) – 85%	Bezpieczne hasła – 59%
Zapora ogniowa (firewall) – 82%	Zapora ogniowa (firewall) – 43%
Ochrona antyspamowa – 69%	Automatyczne wylogowanie – 34%
Filtrowanie treści – 37%	Tworzenie kopii zapasowych (back-up) – 25%
Archiwizacja wiadomości e-mail – 34%	Szyfrowanie danych – 22%
System IPS/IDS – 25%	Ograniczanie dostępu na podstawie IP – 21%
Ochrona przed wyciekiem danych – 16%	Podwójne hasłowanie – 17%
Szyfrowanie danych – 14%	Tokeny – 13%
Żadne z powyższych – 1%	Karty smart – 6%
–	Skanery linii papilarnych – 5%
–	Autoryzacja telefoniczna – 5%
–	Niestosowanie żadnych zabezpieczeń – 4%
–	Inne – 1%

Źródło: opracowanie własne na podstawie badań *Sektor MSP a bezpieczeństwo IT* (2010) oraz *Sprzęt IT – polskie MŚP cenią wydajność i nowoczesność* (2017), s. 13

[18] Opis wyników: *Sektor MSP a bezpieczeństwo IT* (2010), www.egospodarka.pl/ 61516,Sektor-MSP-a-bezpieczenstwo-IT,1,39,1.html (dostęp: 4.10.2017).

[19] *Sprzęt IT – polskie MŚP cenią wydajność i nowoczesność*, www.computerworld.pl/whitepaper/2833-Raport-Sprzet-IT-polskie-MSP-cenia-wydajnosc-i-nowoczesnosc.html (dostęp: 1.10.2017). Raport został opublikowany w 2017 r. w serwisie Computerworld.pl. Dane zebrane w roku 2016, nie podano wielkości próby.

Analiza powyższych danych pozwala na wysnucie następujących wniosków:

- Zauważalny jest wzrost świadomości zagrożeń bezpieczeństwa przetwarzania danych w sektorze MŚP, co potwierdza stosowanie coraz bardziej złożonych środków ochrony w roku 2017 – w porównaniu z rokiem 2010.
- Nadal najbardziej popularne środki ochrony to program antywirusowy, zapora ogniowa oraz tworzenie kopii zapasowych, jednak na drugim miejscu w 2017 roku pojawiają się już bezpieczne hasła.
- Wzrósł poziom zabezpieczenia danych w postaci takich praktyk, jak szyfrowanie danych (+8%), oraz pojawiły się niestosowane wcześniej nowe, bardziej wyrafinowane sposoby ochrony, wymagające większego wysiłku i świadomości użytkowników, jak: ograniczanie dostępu na podstawie IP, podwójne hasłowanie, tokeny, karty smart, skanery linii papilarnych, autoryzacja telefoniczna.

W raporcie z roku 2010 wyrażano zaniepokojenie faktem, że „prawie 60 proc. pracowników polskich firm wynosi dane z firmy bez zgody pracodawcy”[20] oraz że najczęstszymi powodami awarii funkcjonowania systemów IT w firmie są: po pierwsze błędy pracowników (37% wskazań), a dopiero w dalszej kolejności błędy w systemach operacyjnych (26% wskazań) czy wpływ destrukcyjnego kodu (wirusy, robaki, konie trojańskie – 24% wskazań). Jednocześnie deklarowano (70% wskazań), że wszyscy pracownicy przechodzą odpowiednie szkolenia dotyczące bezpiecznego użytkowania sprzętu i narzędzi IT. Skuteczność prowadzonych szkoleń jednak okazywała się niewystarczająca.

Raport z roku 2017 wystawia ogólnie pozytywną ocenę postępu sektora MŚP, jeśli chodzi o używanie i wykorzystanie IT, zwłaszcza w wariantach mobilnych typu smart. Jednocześnie jednak alarmuje, że w dziedzinie ochrony bezpieczeństwa sprzętu IT oraz danych stale występują wyraźne braki, zwłaszcza jeśli chodzi o mikroprzedsiębiorstwa, które:

- często w ogóle nie archiwizują danych użytkowników;
- zazwyczaj nie stosują ograniczenia dostępu na podstawie IP;
- niejednokrotnie nie stosują jakichkolwiek zabezpieczeń, co grozi im utratą wszystkich danych biznesowych.

Ponadto cały sektor MŚP niewystarczająco zabezpiecza sprzęt IT (w tym mobilny: laptopy, tablety, smartfony) przed zniszczeniem fizycznym czy kradzieżą:

- 12% w żaden sposób nie zabezpiecza swojego sprzętu przed zniszczeniem, a jako środek ochronny służą najczęściej jedynie torby czy etui, sporadycznie – folie na ekrany/monitory;
- powszechnie stosowane środki ochrony przed kradzieżą to metody pasywne: monitoring oraz dodatkowe zamki i alarmy, chociaż wzrósł odsetek firm stosujących software antykradzieżowy (15% w badaniach z 2016 wobec 9% w roku 2015), linki zabezpieczające bez alarmu (13% – wobec 7%) oraz linki zabezpieczające z alarmem (11% – wobec 6%).
- 1/3 firm MŚP nie posiada żadnej procedury zabezpieczenia przed kradzieżą.

[20] *Sektor MSP a bezpieczeństwo IT…* (komentarz: M. Iwanickiego).

Badanie operatora usług telekomunikacyjnych Orange Insights, wykonane w roku 2016[21] (pierwsza edycja badania była w 2015 r.) na próbie 500 przedstawicieli polskich MŚP[22] i w całości dedykowane zagadnieniu ochrony bezpieczeństwa informatycznego, pozwala sformułować następujące wnioski:

- Około połowy badanych przedstawicieli sektora (51%) twierdzi, że bezpieczeństwo procesów IT to kluczowy obszar, od którego zależy ciągłość działania ich firmy.
- Tylko około jednej czwartej badanych (23%) ma świadomość systematycznego wzrostu zagrożenia informatycznego w procesach biznesowych.
- Według około jednej czwartej badanych (23%) najistotniejszą tendencją w budowaniu bezpieczeństwa IT jest konieczność zapewnienia ciągłości funkcjonowania systemów.
- W rankingu największych zagrożeń dla IT wskazywano[23]: cyberprzestępczość (31% wskazań), problemy z transmisją danych przez Internet (26%), nieuczciwość pracowników oraz awarie serwerów, komputerów i łączy (po 25% wskazań).

W komentarzu do powyższych danych autorzy badania wykazują zaniepokojenie, że:

- Mobilność pracowników nie jest w ogóle postrzegana jako potencjalne zagrożenie przez ponad połowę badanych firm (61%) – pomimo faktu, że systematycznie rośnie groźba cyberataków na urządzenia mobilne (laptopy, telefony komórkowe, smartfony, tablety) w sektorze MŚP i w 2016 roku aż 13% z nich było obiektem takich zdarzeń[24], co przy dominującym udziale tego sektora w puli wszystkich przedsiębiorstw daje obraz skali zagrożenia.
- Analiza jakościowa cyberataków ujawnia, że połowa z nich (49%) to włamania na strony WWW, serwery i pocztę, 25% to szantaż finansowy, a 15% ataków to złośliwe wirusy i tzw. trojany.

Interesujące jest zróżnicowane postrzeganie ryzyk i wyzwań w zakresie bezpieczeństwa IT w odniesieniu do odmiennych sektorów działalności gospodarczej MŚP, co przedstawia tabela 2. Zawarte w niej dane wskazują, że głównym źródłem potencjalnego zagrożenia bezpieczeństwa cyfrowego w przedsiębiorstwach, niezależnie od typu działalności gospodarczej, jest człowiek. Jako główne wyzwanie w tym obszarze jest jednak postrzegane „zapewnienie ciągłości funkcjonowania systemów IT", a jedynie w sektorze usług jest to „budowanie świadomości dbania o bezpieczeństwo danych wśród pracowników".

Obserwacja ta dowodzi, że bezpieczeństwo cyfrowe w sektorze MŚP stale jest interpretowane raczej jako zagrożenie techniczne, a nie personalne, co w świetle przed-

[21] Opis wyników on-line: *Sektor MSP wobec bezpieczeństwa IT. Główne trendy i zagrożenia*, www.egospodarka.pl/130743,Sektor-MSP-wobec-bezpieczenstwa-IT-Glowne-trendy-i-zagrozenia,1,12,1.html (dostęp: 4.10.2017).

[22] Próbę badawczą stanowiło: 300 właścicieli i zarządzających, 100 specjalistów IT zatrudnionych na etacie oraz współpracujących 100 freelancerów IT, metoda: ankieta typu CATI/CAWI.

[23] Respondenci mieli możliwość wielokrotnego wyboru odpowiedzi na to pytanie, dlatego odpowiedzi nie sumują się do 100.

[24] *Sektor MSP wobec bezpieczeństwa IT…* (komentarz A. Stankiewicza).

stawionych danych stanowi błąd. Większość identyfikowanych ryzyk, takich jak: „cyberprzestępczość", „mobilność pracowników", „nieuczciwość pracowników", ma charakter *stricte* personalny, a inne, np. „awarie serwerów, komputerów i łączy", mogą pośrednio wynikać z niewłaściwego użytkowania powierzonego sprzętu (czyli braku umiejętności) lub braku świadomości pracowników w obszarze bezpiecznego posługiwania się technologią IT.

Tabela 2
Ranking ryzyk i wyzwań IT w polskich MŚP według sektorów działalności
Table 2
Ranking of IT risks and challenges in Polish SMEs by sector of activity

Handel (% wskazań)	Usługi (% wskazań)	Produkcja (% wskazań)
ryzyka IT		
Cyberprzestępczość (39)	Cyberprzestępczość (42)	Cyberprzestępczość (28)
Mobilność pracowników (32)	Awarie serwerów, komputerów i łączy (35)	Nieuczciwość pracowników (32)
Nieuczciwość pracowników (32)	–	Problemy z transmisją danych przez Internet (32)
wyzwania IT		
Zapewnienie ciągłości funkcjonowania systemów IT (18)	Budowanie świadomości dbania o bezpieczeństwo danych wśród pracowników (17)	Zapewnienie ciągłości funkcjonowania systemów IT (25)
Budowanie świadomości dbania o bezpieczeństwo danych wśród pracowników (15)	–	–

Źródło: opracowanie własne na podstawie badań Orange Insights, Orange Polska 2016[25]

Niestety, stale wielu przedsiębiorców w sektorze MŚP nie docenia korzyści z zatrudniania kompetentnych cyfrowo pracowników. Popularny w tym sektorze jest outsourcing usług IT, jednak tylko 45% badanych przedsiębiorców deklaruje, że z freelancerami podpisywane są umowy o zachowaniu poufności[26].

Wnioski

Skuteczne zarządzanie bezpieczeństwem cyfrowym w sektorze MŚP wymaga dostępu do najnowocześniejszych rozwiązań technicznych IT, ale przede wszystkim kształtowania nowoczesnych cyfrowych kompetencji zawodowych i budowania świadomości zagrożeń IT, zarówno wśród menadżerów, jak i wśród wszystkich pracowników firm. W zachodnich opracowaniach podkreśla się, że gospodarcze bez-

[25] W. Jabczyński, *Orange Insights: czyli jak wygląda informatyzacja w małych i średnich firmach w Polsce*, https://biuroprasowe.orange.pl/informacje-prasowe/Orangeinsights-czyli-jak-wyglada-informatyzacja-w-malych-i-srednich-firmach-w-polsce/ (dostęp: 10.09.2017).
[26] Tamże.

pieczeństwo cyfrowe wymaga przede wszystkim orientacji „na biznes", a nie „na technologię"[27]. Duże firmy i korporacje dawno zauważyły, że w aspekcie ochrony przed zagrożeniami IT priorytetem nie jest rozwiązywanie technologicznych luk w zabezpieczeniach, ale ochrona najważniejszych aktywów lub procesów biznesowych (np. informacji o karcie kredytowej klienta) – jest to tzw. podejście „business-back". Małe i średnie przedsiębiorstwa jeszcze bardziej muszą myśleć w ten sam sposób, bo ich „łańcuch wartości" jest zazwyczaj krótszy w porównaniu z dużymi graczami biznesowymi i łatwiej mogą stracić klientów, których transakcje czy dane nie będą należycie zabezpieczone.

Tym samym zadania w zakresie bezpieczeństwa cyfrowego powinny stać w centrum uwagi menadżerów – jako kluczowy punkt zarządzania strategicznego. Operacyjne zadania w tym zakresie mogą realizować działy personalne (kadrowe) firm przy udziale działów IT, jednak nie same działy techniczne, które nie są przygotowane merytorycznie do obsługi złożonych procesów personalnych. W większych przedsiębiorstwach procesami personalnymi zajmują się tzw. działy HR (Human Resources – zasoby ludzkie), a w przypadku mniejszych firm – najczęściej osoby zarządzające lub właściciele.

Działania HR w zakresie cyfrowego bezpieczeństwa personalnego powinny obejmować co najmniej takie elementy polityki kadrowej, jak:

- *Szkolenia stanowiskowe i szkolenia zawodowe doskonalące* – szkolenia w zakresie bezpiecznego używania systemów IT powinny mieć charakter działań systemowych, tj. powinny być: systematyczne; prowadzone w sposób zrozumiały dla pracowników nieposiadających technicznego przygotowania zawodowego; włączone w system procesów HR ukierunkowanych na poszerzanie i kontrolę kompetencji zawodowych pracowników zatrudnionych na stanowiskach.
- *Opisy stanowisk pracy* – opisy powinny uwzględniać procedury ochrony przed zagrożeniami cyfrowymi i zawierać wykaz zalecanych systemów zabezpieczeń podczas wykonywania zadań na stanowisku.
- *Dostęp do mentorów w dziedzinie IT* – stały i łatwy, dla wszystkich pracowników.
- *System okresowej oceny pracownika* – powinien zawierać kryteria ewaluacji praktycznego stosowania bezpiecznych cyfrowo praktyk biznesowych wymaganych w zadaniach wykonywanych na danym stanowisku pracy.
- *Employer branding wewnętrzny* – dbanie o dobry wizerunek pracodawcy wśród własnych pracowników poprzez różnego rodzaju benefity i działania marketingu personalnego może zmniejszyć ryzyko destrukcyjnej i/lub niefrasobliwej aktywności pracowników w sieci.
- *Kształtowanie czujności menadżerów w sferze ryzyk IT* – poprzez ich uczestniczenie w różnych formach uczenia się przez całe życie (konferencjach, seminariach, warsztatach) dedykowanych nowo pojawiającym się zagrożeniom cyfrowym i skutecznym taktykom radzenia sobie z nimi.

[27] J. Caplan, S. Sharma, A.Weinberg, *Meeting the cybersecurity challenge*, Mc Kinsey, June 2011, www.mckinsey.com/business-functions/digital-mckinsey/our-insights/meeting-the-cybersecurity-challenge (dostęp: 4.10.2017).

Człowiek stale pozostaje najsłabszym elementem systemu cyberbezpieczeństwa w sferze gospodarczej[28], ze względu na swój brak umiejętności lub świadomości zagrożeń w obszarze IT sam bardzo często prowokuje ryzykowne sytuacje. Efekt „personalnej niekompetencji" pracowników przedsiębiorstw, zwłaszcza tych mniejszych, jest doskonale znany osobom celowo działającym z zamiarem popełnienia przestępstw gospodarczych i stanowi kanwę ich cyberataków. Kevin Mitnick, nazywany „najsłynniejszym hakerem na świecie", w swojej książce[29] wyznaje, że w rzeczywistości łamał ludzi, a nie hasła. Tylko systemowe podejście menadżerów do cyberbezpieczeństwa przedsiębiorstw pozwoli planować ich rozwój, a od strony formalnej – sprostać wymogom nowej ustawy o ochronie danych osobowych.

Bibliografia

Caplan J., Sharma S., Weinberg A., *Meeting the cybersecurity challenge*, Mc Kinsey, 2011, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/meeting-the-cybersecurity-challenge (dostęp: 4.10.2017).

Czerniak A., Stefański M., *Polityka Insight Research, Małe i średnie firmy w Polsce – bariery i rozwój*, Bank Zachodni WBK, 2016, https://static3.bzwbk.pl/asset/m/a/l/male-i-srednie-firmy-w-polsce2_-polityka-insight_61682.pdf (dostęp: 12.09.2017).

Effective Cybersecurity Strategy Rests on People, Not Just Technology, 1.03.2017, www.insurancejournal.com/news/national/2017/03/01/443270.htm (dostęp: 10.10. 2017).

Indeks gospodarki cyfrowej i społeczeństwa cyfrowego (DESI) 2018. Sprawozdanie krajowe dotyczące Polski, https://ec.europa.eu/digital-single-market/en/scoreboard/Poland (dostęp: 10.09.2017).

Jabczyński W., *Orange Insights: czyli jak wygląda informatyzacja w małych i średnich firmach w Polsce*, https://biuroprasowe.orange.pl/informacje-prasowe/Orangeinsights-czyli-jak-wyglada-informatyzacja-w-malych-i-srednich-firmach-w-polsce/ (dostęp: 10.09.2017).

Klimczuk A., *Cyfrowi bardziej konkurencyjni. Małe firmy na START do FIRMOWYCH (R)EWOLUCJI*, https://news.microsoft.com/pl-pl/2015/06/11/cyfrowi-bardziej-konkurencyjni-male-firmy-na-start-do-firmowych-rewolucji (dostęp: 1.10.2017).

Mitnick K.D, Simon W.L, *Sztuka podstępu. Łamałem ludzi, nie hasła*, przeł. J. Dobrzański, Warszawa 2003.

*Nowa definicja MŚP. Poradnik dla użytkowników i wzór oświ*adczenia, Komisja Europejska, [Bruksela] 2006.

Nowa ustawa o ochronie danych osobowych – najważniejsze zagadnienia, https://gdpr.pl/nowa-ustawa-o-ochronie-danych-osobowych#Nowa_Ustawa_o_ochronie_ danych_ osobowych (dostęp: 9.09.2017).

Raport KE: cyfrowa przepaść, http://ec.europa.eu/poland/news/170303_digital_pl (dostęp: 10.09.2017).

[28] *Effective Cybersecurity Strategy Rests on People, Not Just Technology*, 1.03.2017, www.insurancejournal.com/news/national/2017/03/01/443270.htm (dostęp: 10.10. 2017).

[29] Mitnick K.D., Simon W. L, *Sztuka podstępu. Łamałem ludzi, nie hasła*, przeł. J. Dobrzański, Warszawa 2003.

Raport o stanie sektora małych średnich przedsiębiorstw w Polsce, PARP, 2017. www.parp.gov.pl/images/PARP_publications/pdf/raport%20o%20stanie%20sektora%20msp%20w%20polsce_2017.pdf (dostęp: 10.09.2017).

Sektor MSP a bezpieczeństwo IT (2010), www.egospodarka.pl/ 61516,Sektor-MSP-a-bezpieczenstwo-IT,1,39,1.html (dostęp: 4.10.2017).

Sektor MSP wobec bezpieczeństwa IT. Główne trendy i zagrożenia, www.egospodarka.pl/130743,Sektor-MSP-wobec-bezpieczenstwa-IT-Glowne-trendy-i-zagrozenia,1,12,1.html (dostęp: 4.10.2017).

Sprawozdanie z postępów Europy w zakresie cyfryzacji za 2017 (EDPR), profil krajowy Polski, Komisja Europejska 2017, ec.europa.eu/newsroom/document.cfm?doc_id=44328 (dostęp: 2.09.2017).

Sprzęt IT – polskie MŚP cenią wydajność i nowoczesność, www.computerworld.pl/whitepaper/2833-Raport-Sprzet-IT-polskie-MSP-cenia-wydajnosc-i-nowoczesnosc.html (dostęp: 1.10.2017).

Dyrektywa Parlamentu Europejskiego i Rady 2014/55/UE z dnia 16 kwietnia 2014 r. w sprawie fakturowania elektronicznego w zamówieniach publicznych, http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32014L0055&from=PL (dostęp: 15.09.2017).

Uchwała Nr 7 Rady Ministrów z dnia 15 stycznia 2013 r. w sprawie Strategii Innowacyjności i Efektywności Gospodarki „Dynamiczna Polska 2020", http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WMP20130000073&type=2 (dostęp: 12.09.2017).

Ustawa o ochronie danych osobowych, tekst jednolity, Dz.U. z 2016 r., poz. 922.

Summary

The area in which business data security is especially important is the area of human resources and customer relationship marketing. The article addresses the issue of assessing the preparation of the Polish SME sector for cyber security in the context of dissemination of digital practices in the processes of transmitting and processing business data and the challenges of the new Data Protection Act (NUODO). It describes gap areas, including – competence gaps in managers and employees in business processes responsible for protection against digital dangers. The proposals recommend the location of systematic protection against digital threats in the area of strategic management and the assignment of operational tasks to personnel departments, not just only technical ones.