TOMASZ STEFANIUK
ORCID: 0000-0001-5769-8735
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
Wydział Nauk Społecznych

Bezpieczeństwo informacji w świadczeniu pracy zdalnej

Istota i miejsce pracy zdalnej we współczesnym świecie

Telepraca to stosunkowo nowa forma wykonywania obowiązków wynikających ze stosunku pracy. Ma ona swoje podłoże w wielu zjawiskach zachodzących we współczesnym świecie, zmieniających uwarunkowania funkcjonowania organizacji w przeciągu ostatnich lat. Gospodarka globalna i dynamiczny jej rozwój wpłynął na zmiany w komunikacji, konkurencji i współpracy pomiędzy instytucjami, podmiotami rynkowymi czy pojedynczymi osobami. Chęć uzyskania trwałej przewagi konkurencyjnej często narzuca konieczność podejmowania przez firmę współpracy z innymi podmiotami rynkowymi na różnych poziomach[1]. Coraz częściej cały zespół pracowników danego przedsiębiorstwa nie jest w stanie podołać zadaniom, jakie zostały już wyznaczone. Konieczna jest współpraca międzyorganizacyjna, tworzenie zespołów złożonych ze specjalistów wielu współpracujących ze sobą instytucji.

Tymczasem rozwój technologii teleinformatycznych umożliwił elektroniczne formy komunikacji i wymiany oraz współdzielenia danych, które otworzyły nowe możliwości podejmowania pracy uniezależnionej od odległości geograficznej. Do powyższego obrazu należy jeszcze dołożyć ogromną nieprzewidywalność otoczenia i zachodzących przemian: konflikty etniczne i religijne, zmiany ustrojowe,

[1] A. Maik, A. Godzisz, *Istota i pojęcie organizacji sieciowej*, [w:] „Studia i Materiały. Miscellanea Oeconomicae" 2013, r. 17, nr 2, s. 336.

kryzysy ekonomiczne, coraz częściej występujące stany klęski żywiołowej, czy wreszcie szybki postęp technologiczny, umożliwiający powstawanie cyfrowych produktów i będące jego konsekwencją krótkie cykle życia produktów i usług. M. Trziszka wskazuje na następujące procesy implikujące rozwój telepracy[2]:

- rozwój komputerów i powstałych z nich komputerów osobistych;
- rozwój sieci komputerowych;
- rozwój środków telekomunikacji;
- rozwój systemów zarządzania przedsiębiorstwem (klasy ERP);
- rozwój nowych koncepcji zarządzania, w tym idei outsourcingu, offsourcingu oraz modelu kosztów ABC;
- digitalizacja wielu dóbr materialnych oraz powstanie nowych, niematerialnych rynków dóbr i usług.

Polskie prawo definiuje telepracę w artykule 675 Kodeksu pracy jako pracę wykonywaną regularnie poza zakładem pracy, z wykorzystaniem środków komunikacji elektronicznej w rozumieniu przepisów o świadczeniu usług drogą elektroniczną[3]. Powyższy zapis pozwala na wyodrębnienie następujących istotnych cech telepracy[4]:

- regularność świadczenia pracy w formie telepracy;
- wykonywanie pracy poza zakładem pracy;
- wykorzystywanie środków komunikacji elektronicznej w rozumieniu przepisów o świadczeniu usług drogą elektroniczną;
- przekazywanie pracodawcy wyników pracy, w szczególności za pośrednictwem środków komunikacji elektronicznej.

Telepraca może być świadczona zarówno na podstawie zwykłej umowy o pracę lub kontraktu, jak również w ramach własnej działalności gospodarczej. Rzadko stanowi ona jedyną formę pracy danej osoby – zazwyczaj jest ona łączona z klasyczną pracą w siedzibie organizacji. Oczywiście proporcje czasu telepracy do pracy lokalnej bywają różne: od okazjonalnej, gdy pracownik jedynie ze względu na wyjątkową sytuację osobistą lub zewnętrzną (jak w przypadku epidemii

[2] M. Trziszka, *Model organizacji i zarządzania systemem pracy zdalnej w branży IT*, Rozprawa doktorska, Wyd. PP, Poznań 2019, s. 9.

[3] Art. 675 § 1. ustawy z dnia 24 sierpnia 2007 r. o zmianie ustawy – Kodeks pracy oraz niektórych innych ustaw (Dz.U. z 2007 r. Nr 181, poz. 1288).

[4] S. Wrycza, *Informatyka ekonomiczna: podręcznik akademicki*, PWE, Warszawa 2010, s. 100.

koronawirusa) kontaktuje się drogami elektronicznymi ze współpracownikami, po stałe świadczenie tej formy pracy, gdzie telepraca systematycznie stanowi większą część czasu pracy danej osoby.

Telepraca kojarzy się głównie z pracą świadczoną z domu. Jednak miejscem tej formy pracy może być również lokal pracodawcy, z którego telepracownik obsługuje klientów firmy czy telecentrum (biuro wyposażone w komputery z szybkim dostępem do Internetu) dzielone przez wielu pracodawców w celu redukcji kosztów lub prowadzone przez lokalną administrację w celu tworzenia miejsc pracy w regionie[5]. Niezależnie od miejsca jej świadczenia Kodeks pracy zobowiązuje pracodawcę do:

- wyposażenia telepracownika w sprzęt, który jest niezbędny do wykonywania przez niego pracy w systemie zdalnym;
- ubezpieczenia danego sprzętu;
- pokrycia ewentualnych kosztów, które są związane z instalacją, serwisem, eksploatacją i konserwacją sprzętu;
- zapewnienia telepracownikowi pomocy technicznej, jak i niezbędnych szkoleń w zakresie obsługi danego sprzętu.

Oczywiście powyższe ustalenia mogą przebiegać inaczej, gdyż przede wszystkim są regulowane przez umowę pomiędzy pracodawcą i telepracownikiem[6].

W przypadku gdy telepracownik do pracy udostępnia własny sprzęt, wówczas ma prawo do ekwiwalentu pieniężnego. Jeśli chodzi o jego wysokość, to ustala się ją w porozumieniu. Pracodawca zachowuje też kontrolę nad wykonywaniem przez swojego pracownika obowiązków, jednak niezbędna jest tutaj zgoda osoby kontrolowanej[7].

Telepraca przynosi korzyści zarówno dla pracodawcy, pracownika, jak również gospodarki i środowiska. Brak konieczności wspólnego przebywania w pracy, czy też fakt, iż dojazdy do pracy, stają się zbędne (lub są zdecydowanie

[5] A. Szewczak, *Telepraca – szansą czy zagrożeniem na rynku pracy?*, Wyd. Hogben, Szczecin 2002, s. 43.

[6] Ustawa z dnia 24 sierpnia 2007 r. o zmianie ustawy – Kodeks pracy oraz niektórych innych ustaw (Dz.U. z 2007 r. Nr 181, poz. 1288), art. 6711 § 1.

[7] K. Karbownik, *Korzyści i zagrożenia wynikające z zatrudnienia pracowników w formie telepracy*, „Zeszyty Naukowe Politechniki Częstochowskiej Zarządzanie" 2015, nr 20, s. 165.

rzadsze), pozytywnie wpływa na wiele kwestii: możliwość pozyskania specjalistów, obniżenie kosztów pracy, wzrost wydajności pracy czy ochronę środowiska.

Brak geograficznego ograniczenia przy angażowaniu specjalistów do współpracy daje możliwość rekrutacji najbardziej utalentowanych pracowników na świecie[8]. Z drugiej strony telepraca umożliwia zatrudnienie osobom biernym zawodowo, które w tradycyjnej formie pracy prawdopodobnie nigdy nie uzyskałyby zatrudnienia.

Kolejną zaletą pracy zdalnej, uznawaną bardzo często w literaturze za najważniejszą, jest możliwość znacznego obniżenia kosztów, zarówno po stronie organizacji, jak również pracowników[9]. Obniżenie kosztów prowadzenia działalności gospodarczej jest szczególnie ważne w okresie kryzysu – z którym, według opinii większości ekonomistów, będziemy mieli do czynienia w najbliższym czasie. J. Fort[10] twierdzi, że coraz więcej firm rozważa zastąpienie spotkań bezpośrednich w siedzibie firmy wideokonferencjami lub wręcz zamykanie biur i umożliwienie pracownikom zdalnej pracy w domu. Wszystko to oczywiście w celu obniżenia kosztów. Oszczędności płynące z takiej formy pracy wynikają przede wszystkim z niższych kosztów wynajęcia biura. Jak podaje J. Nilles[11], firmy lub instytucje rządowe zatrudniające dużą liczbę pracowników pracujących w domu, mogą łatwo uzyskać nawet do 33% oszczędności powierzchni biurowej[12]. Gdyby wykorzystano także fakt, że pracownicy przez część czasu nie korzystają z miejsc parkingowych, i gdyby zostały one przydzielone innym osobom lub były przez nie wykorzystywane, miesięczne oszczędności wynosiłyby mniej więcej jedną czwartą miesięcznego kosztu parkingu.

[8] B.J. Bergiel, E.B. Bergiel, P.W. Balsmeier, *Nature of virtual teams: a summary of their advantages and disadvantages* [w:] "Management Research News", Vol. 31 No. 2, Emerald Group Publishing Limited, United Kingdom, Bingley 2008, s. 105.

[9] T. Stefaniuk, *Komunikacja w zespole wirtualnym*, Difin, Warszawa 2014, s. 76.

[10] C. Morris, *7 ways to make working from home easier during the coronavirus pandemic*, https://fortune.com/2020/03/12/working-from-home-coronavirus-remote-work-telecommuting-wfh-covid-19/ [dostęp 24.05.2020].

[11] J. Nilles, *Telepraca, strategie kierowania wirtualną załogą*, WNT, Warszawa 2003, s. 185-186.

[12] AT&T, na przykład, szacuje, że oszczędności wynikające z ograniczenia powierzchni biurowej dzięki telepracy wynoszą 2000 USD rocznie na osobę za: "Harvard Business Review", maj-czerwiec 1998, s. 128.

Brak konieczności korzystania z dojazdów do pracy, to znaczne ograniczenie kosztów po stronie telepracowników[13]. Łączny zaoszczędzony na dojazdach do pracy czas w ciągu miesiąca może sięgać od 30 do 50 godzin.

Ograniczenie dojazdów do pracy w konsekwencji stosowania telepracy prowadzi również do zmniejszenia emisji spalin silnikowych, na co zwraca uwagę opublikowana w maju 2019 r. prognoza OECD dotycząca długookresowych perspektyw rozwoju transportu na świecie[14]. Upowszechnienie telepracy może zmniejszyć ruch pasażerów w miastach z 3% do 30%[15].

Spośród innych czynników pozwalających na zmniejszenie kosztów w wyniku stosowania zespołów wirtualnych wymienić należy także spadek fluktuacji, mniejszą ilość zwolnień chorobowych czy jednodniowych urlopów. Dla przykładu ARO Call Centre (Kansas City) zredukowało wskaźnik rotacji z 60% do 4% w ciągu roku, po tym jak osiemdziesięciu pięciu ze stu pracowników mogło pracować w domu[16]. Badanie przeprowadzone przez Telework American Association w 1999 r. pokazało, że osoby pracujące w domu rzadziej korzystają ze zwolnień chorobowych. Również w przypadkach nagłych spraw osobistych lub złego samopoczucia zwykli pracownicy najczęściej biorą cały dzień wolny, natomiast osoby pracujące w formie zdalnej wracają do pracy krótko po załatwieniu bieżących spraw[17]. Ponadto taka forma pracy eliminuje konieczność zwolnienia się z pracy, gdy firma przenosi się w inne miejsce. Cenieni pracownicy mogą być zatrzymani w charakterze pracowników elastycznych, jeśli nie chcą (nie mogą) się przeprowadzić.

[13] Zakładając, że telepracownik pracuje przeciętnie trzy dni w tygodniu w domu, zastępując jazdę samochodem tam i z powrotem na odległość 50 km i przy założeniu przeciętnego zużycia 8 litrów benzyny na 100 km, oszczędność w ciągu miesiąca wyniesie 96 litrów benzyny, co przy cenie 4.50 zł/litr daje miesięcznie 432 zł oszczędności. Do tego należy doliczyć także wydatki na odpowiednią „biurową" prezencję, lunch itp. (na podstawie własnych obliczeń). Warto pamiętać także o czasie zaoszczędzonym na dojazdach do pracy, który w ciągu miesiąca może sięgać od 30 do 50 godzin. Według szacunków dyrektora działu rozwiązań biznesowych firmy IBM, oszczędności wynikające z ograniczenia kosztów podróży i strat czasu z nimi związanych wynoszą 50 milionów dolarów, za: R. Baskerville, J. Nandhakumar, *Activating and perpetuating virtual teams*, Transactions on Professional Communication 2007, Vol. 50 No. 1, s. 20.

[14] ITF Transport Outlook 2019, https://www.oecd-ilibrary.org/transport/itf-transport-outlook-2019_transp_outlook-en-2019-en [dostęp 6.05.2020].

[15] Telepraca na odsiecz środowisku, https://www.obserwatorfinansowy.pl/bez-kategorii/rotator/telepraca-na-odsiecz-srodowisku/ [dostęp 8.03.2020].

[16] Swansea University, http://www.swan.ac.uk/psychology/patra [dostęp 19.11.2011].

[17] B. Kozłowska, J. Królikowski, P. Szczęsny, *Telepraca – podręcznik dla gminnych centrów informacji*, PARP, Warszawa 2008, s. 36.

Inną, niezwykle ważną korzyścią zdalnych form pracy, jest znaczne zwiększenie jej wydajności. Praca w domu może przynieść łączny wzrost wydajności od 10 do 60%[18]. J. Nilles, prowadząc badania nad telepracą, wykazał, iż średni wzrost wydajności osób pracujących w domu, wynikający z ich samooceny, wynosi 30%[19]. Natomiast według oceny kierowników zmiany wydajność tych osób wynosiła średnio 22%. Jak wynika z badań Uniwersytetu Stanforda, osoby pracujące z domu mogą osiągać o 13% lepsze wyniki niż ich koledzy siedzący w biurze[20].

Powyższe zalety telepracy sprawiają, że coraz więcej firm oferuje pracownikom możliwość pracy zdalnej, przy czym sytuacja kształtuje się odmiennie w zależności od kraju. Według raportu OECD ponad 51% pracowników w Danii deklaruje, że doświadczyła telepracy. Najbardziej zbliżona do Danii jest pod tym względem Finlandia (46,8% zatrudnionych czasami tak pracuje) oraz Szwecja (45,8%). Największy udział pracowników stale wykonujących telepracę posiadają takie kraje, jak Holandia (33,4%), Szwecja (30,6%) i Luksemburg (27,4%). Według badania aktywności ekonomicznej ludności udział pracowników najemnych pracujących z domu w 2018 r., w grupie wiekowej od 20 do 64 lat, wyniósł w Polsce 7,8%[21]. W każdym z powyższych przykładów widoczny jest wzrost znaczenia telepracy, a w przypadku Polski liczba telepracowników w roku 2018 zwiększyła się o 20% w stosunku do roku poprzedniego[22].

Sytuacja diametralnie zmieniła się na początku roku 2020 w związku z wybuchem epidemii koronawirusa wywołującego COVID-19. Przyjęta przez Sejm RP 2 marca 2020 r. specustawa ws. koronawirusa przewidywała, że pracodawca może zlecić pracownikowi pracę zdalną. W chwili pisania niniejszego rozdziału trudno oszacować, ile firm się na to zdecyduje, ale około 2,5 miliona Polaków jest zatrudnionych w branżach, które mają taką możliwość[23].

[18] Tamże, s. 37.

[19] J. Nilles, *Telepraca*..., dz. cyt., s. 179-186.

[20] M. Duszczyk, *Koronawirus wygania Polaków na telepracę. Czas wirtualnych biur*, https://cyfrowa.rp.pl/it/45191-koronawirus-wygania-polakow-na-teleprace-czas-wirtualnych-biur [dostęp 12.08.2020].

[21] Telepraca na odsiecz środowisku, https://www.obserwatorfinansowy.pl/bez-kategorii/rotator/telepraca-na-odsiecz-srodowisku/ [dostęp 8.03.2020].

[22] *Rocznik statystyczny Pracy 2019*, red. D. Rozkrut i in., GUS, Warszawa 2020, s. 120.

[23] Praca zdalna: 5 najważniejszych zasad. Z powodu koronawirusa w Polsce przybywa osób pracujących z domu, https://alebank.pl/praca-zdalna-5-najwazniejszych-zasad-z-powodu-koronawirusa-w-polsce-przybywa-osob-pracujacych-z-domu/ [dostęp 29.03.2020].

Badania przeprowadzone przez GfK Polonia zrealizowane w dniach 20-23 marca 2020 r. (trzy tygodnie po wprowadzeniu specustawy) wskazały, że 17% pracowników może i pracuje zdalnie (co stanowi ponad 2,8 miliona pracowników), a ponad 50% normalnie, jak zwykle przed epidemią, jeździ do pracy. Pozostała część pracowników (33%) została zmuszona do zrezygnowania ze świadczenia pracy na skutek: zawieszenia działalności przez firmę (8%), przebywania na przymusowym urlopie wypoczynkowym (5%), ze względu na konieczność opieki nad dziećmi – z uwagi na zamknięte szkoły czy przedszkola (4%) bądź z innych powodów[24].

Dodatkowo, w konsekwencji zamknięcia szkół i uczelni, w obliczu epidemii, w domach pozostało 4,5 miliona uczniów[25], 300 tys., studentów[26] oraz prawie 700 tys. nauczycieli[27] świadczących zdalne nauczanie.

Oczywiście telepraca nie posiada samych zalet. Niesie ona ze sobą ryzyka związane z występowaniem braku zaufania, rywalizacji i trudności z kontrolą efektów pracy, negatywnym wpływem na życie rodzinne, pracoholizmem i uzależnieniem od Internetu czy też problemów z bezpieczeństwem informacji i systemów teleinformatycznych.

Zagrożenia dla bezpieczeństwa informacji w pracy zdalnej oraz ich następstwa

Specyfika telepracy implikuje zależność od technologii teleinformatycznych, co prowadzi do szczególnej wrażliwości na zakłócenia dostępności informacji oraz problemy związane z ich integralnością. Ponadto poza siedzibą organizacji zdecydowanie łatwiej o utratę poufności danych, a rozdzielenie geograficzne telepracowników sprawia, iż jakakolwiek forma porozumiewania się pomiędzy

[24] G. Ułan, Tylko 17% pracowników w Polsce pracuje zdalnie, ponad połowa nadal jeździ do pracy jak zwykle, https://antyweb.pl/tylko-17-pracownikow-w-polsce-pracuje-zdalnie/ [dostęp 5.04.2020].

[25] Ilu jest uczniów w Polsce? https://www.zadluzenia.com/ilu-jest-uczniow-w-polsce/ [dostęp 4.04.2020].

[26] Potocka J., Studenci wracają na uczelnie. Dziś początek roku akademickiego 2019/2020 https://www.rmf24.pl/tylko-w-rmf24/joanna-potocka/redaktor/news-studenci-wracaja-na-uczelnie-dzis-poczatek-roku-akademickieg,nId,3233364 [dostęp 30.03.2020].

[27] Ilu jest nauczycieli w Polsce? https://www.zadluzenia.com/liczba-nauczycieli-w-polsce/ [dostęp 2.04.2020].

nimi jest możliwa tylko dzięki narzędziom teleinformatycznym. Dlatego, w przypadku świadczenia pracy zdalnie, wystąpienie incydentu naruszającego bezpieczeństwo informacji powoduje m.in. zakłócenie procedur, czego skutkiem może być brak możliwości świadczenia pracy lub zmniejszenie jej skuteczności. Dodatkowo incydenty bezpieczeństwa informacji mogą spowodować wiele innych, negatywnych konsekwencji, takich jak[28]:

- bezpośrednie straty finansowe poprzez oszustwa i kradzież informacji;
- straty finansowe będące następstwem kar oraz procesów sądowych (np. z tytułu naruszenia wolności i praw z tytułu utraty danych osobowych);
- spadek wartości dla akcjonariuszy;
- utrata reputacji powodująca dewaluację marki;
- wydatki na uszkodzone, skradzione lub utracone w wyniku incydentów aktywa bezpieczeństwa informacji;
- utrata przewagi konkurencyjnej;
- spadek rentowności.

Pierwszą kwestią, o której należy pamiętać, jest fakt, że większość domów – będących podstawowym miejscem pracy telepracowników – nie posiada takich zabezpieczeń fizycznych jak siedziba organizacji. Miejsce pracy może nie zapewniać ochrony przetwarzanych dokumentów przed utratą poufności. W niektórych przypadkach trudno o wydzielenie odpowiedniej przestrzeni, tak aby osoby postronne nie miały dostępu do dokumentów, nad którymi aktualnie prowadzona jest praca. Zdecydowanie gorsze są zabezpieczenia antywłamaniowe w porównaniu z tymi stosowanymi w siedzibie firmy: nie ma szafek zamykanych atestowanymi zamkami, alarmów, monitoringu czy osobowej kontroli wejść i wyjść itd. W efekcie nikt nie jest w stanie skontrolować, jakie osoby będzie zapraszać do domu telepracownik, z kim będzie rozmawiać i komu będzie pokazywać poufne dane ze swojego komputera. Telepracownicy w swoich domach nie posiadają gaśnic, wykrywaczy dymu czy planów ewakuacyjnych.

Co istotne, praca poza siedzibą firmy – zazwyczaj w domu – to przede wszystkim brak sieciowej infrastruktury informatycznej. Pracownicy, którzy

[28] M. Ratajczyk-Mrozek, A.I. Adamik, M. Najda-Janoszka, P. Wróbel, T. Stefaniuk, R. Niedbał, *Koncepcje zarządzania zorientowane na współdziałanie i wspomagające je narzędzia informatyczne*, TNOiK, Dom Organizatora, Toruń 2016, s. 94-95.

wykonują swoje obowiązki zdalnie, są podłączeni do sieci domowych, które nie są w żaden sposób sprawdzone przez ekspertów ds. cyberbezpieczeństwa. Najczęściej one również nie są zabezpieczone w odpowiedni sposób. Co więcej występuje ryzyko, że mogą się w nich znajdować urządzenia niezabezpieczone, podatne na zagrożenia, jak np. elementy Internetu rzeczy (inteligentne kamerki, telewizory, kuchnie, bramy garażowe itp.). Umożliwia to łatwiejsze włamanie się do sieci, w której przetwarzane są służbowe informacje. Dzięki temu przestępcy mogą podsłuchiwać i przechwytywać informacje, które najczęściej będą wysyłane w formie niezaszyfrowanego tekstu[29].

Geograficzne rozproszenie pracowników zdalnych rodzi wymagania co do dostępności informacji i wiedzy poza siedzibą organizacji. Istnieje wiele sposobów zapewnienia dostępności informacji telepracownikom. Może to być przekazanie istotnych danych na pamięciowych urządzeniach przenośnych, zapewnienie zdalnego dostępu do danych przechowywanych w sieciowej infrastrukturze organizacji bądź ich przechowywania w zewnętrznej chmurze (cloud computing). Każde z nich rodzi poważne zagrożenia dla bezpieczeństwa.

Przenośne nośniki danych wynoszone poza siedzibę organizacji mogą być łatwo zgubione lub skradzione. Jak pokazują badania przeprowadzone przez Kingston Technology w 2016 r., aż 70% przedsiębiorstw nagminnie gubi nośniki pamięci. Warto dodać, że często znajdują się tam kluczowe dla organizacji dane, szczegóły realizowanych projektów, a także dane osobowe. To może się okazać bardzo kosztowne dla firm, pracowników oraz osób, których dane były na dyskach. Wg badań przeprowadzonych przez firmę Kingston prawie 24% osób przyznało, że pamięci USB w firmie nie są w żaden sposób zabezpieczane, a co więcej ponad połowa decydentów (kadra kierownicza) w firmach przyznaje się do utraty pamięci USB z ważnymi danymi[30]. Dane tracone są najczęściej z powodu uszkodzeń pamięci USB (61,2%) oraz zgubienia (31,1%) czy kradzieży pamięci USB (3,0%). Aż w 4,1% przypadków ankietowani nie mają pewności co do przyczyny utraty danych lub jest ona nieznana. Nie dość, że pamięć USB łatwo jest utracić, to w dodatku pracownicy nie zgłaszają tego typu zdarzeń w swojej firmie. Co

[29] A. Kozłowski, *Bezpieczna praca zdalna*, https://www.cyberdefence24.pl/bezpieczna-praca-zdalna [dostęp 3.04.2020].

[30] Pamięć USB – używasz prywatnie lub służbowo? Przeczytaj!!!, https://blogspeclab.pl/pamiec-usb-uzywasz-prywatnie-lub-sluzbowo-przeczytaj/ [dostęp 28.03.2020].

gorsza, dane w podręcznej pamięci najczęściej nie są zaszyfrowane ani chronione hasłem. Szyfrowanie sprzętowe zastosowane jest tylko w 21% przypadków. Szyfrowanie programowe – w 37% przypadków. Należy pamiętać, że niezabezpieczone pamięci stwarzają ryzyko nie tylko opisanego powyżej wycieku danych, ale również niebezpieczeństwa infekcji szyfrującej (ransomware) lub innego ataku wirusowego (nie mówiąc o oprogramowaniu szpiegującym backdoor).

Według ankiety firmy Apricorn 8. na 10. pracowników używa w pracy obcych napędów, np. otrzymanych na eventach branżowych[31]. W przypadku telepracowników korzystanie z prywatnych nośników pamięci jest trudne do zweryfikowania, stąd i skala ryzyka jest większa. Zespół CERT.GOV.PL informuje o ciągłym wzroście aktywności szkodliwego oprogramowania wyspecjalizowanego w rozprzestrzenianiu się za pomocą wymiennych nośników pamięci (pendrive'y, karty pamięci, zewnętrzne dyski twarde). Dotyczy to w szczególności przenośnych pamięci typu flash USB, które są najpopularniejszym medium przenoszenia danych[32].

Inne rozwiązanie – zapewnienie telepracownikom zdalnego dostępu do zasobów sieciowych (danych lub aplikacji) otwierają organizację na różnorodne zagrożenia cyberbezpieczeństwa. Aby ustanowić połączenia zdalne, organizacje często używają wirtualnej sieci prywatnej (Virtual Private Network – VPN), w celu umożliwienia użytkownikom interakcji z ich systemami. Jednak sieci VPN można porównać z jednej strony do drzwi frontowych, które umożliwiają uprawnionym użytkownikom dostęp do danych, a z drugiej strony – do tylnych drzwi, którymi osoby bez uprawnień mogą dostać się do krytycznych danych i aplikacji. W związku z tym połączenia VPN są często wykorzystywane do uzyskania nieautoryzowanego dostępu do systemów, przyciągając uwagę hackerów. Analiza danych dotyczących incydentów wykazuje, że prawie każde poważne naruszenie bezpieczeństwa IT w ciągu ostatnich kilku lat w Polsce wiązało się z pewnym sposobem nieautoryzowanego dostępu zdalnego. 86% menedżerów uważa, że naruszenia danych są bardziej prawdopodobne, gdy pracownicy pracują zdalnie[33].

[31] 8 praktyk dla bezpiecznego zarządzania nośnikami danych, https://logsystem.pl/blog/8-praktyk-dla-bezpiecznego-zarzadzania-nosnikami-danych/ [dostęp 3.04.2020].

[32] CSIRT: Nośniki USB- zapobieganie zagrożeniom, https://www.csirt.gov.pl/cer/wiadomosci/zagrozenia-i-podatnosc/110,Nosniki-USB-zapobieganie-zagrozeniom.html [dostęp 3.04.2020].

[33] T. Smug, *Niebezpieczeństwa związane z VPN i jak zminimalizować zagrożenia zdalnego dostępu za pomocą PAM?*, https://emspartner.pl/beyondtrust/niebezpieczenstwa-zwiazane-z-vpn-i-jak-zminimalizowac-zagrozenia-zdalnego-dostepu-za-pomoca-pam/ [dostęp 6.04.2020].

Trzecim, wcześniej wymienionym, rozwiązaniem udostępniania danych telepracownikom jest technologia przetwarzania w chmurze (cloud computing), która stała się jednym z coraz częściej stosowanych rozwiązań w wielu obszarach biznesowych[34]. Organizacja, korzystająca z takiej usługi, swoje zasoby wiedzy przechowuje na zewnętrznych serwerach, do których częściowy dostęp przydziela telepracownikom.

Pomimo wielu zalet takiego rozwiązania, organizacja godzi się na przynajmniej częściową utratę kontroli nad danymi oraz sposobami ich zabezpieczenia. Przechowywanie danych na zewnętrznych serwerach sprawia, że są one narażone na wyciek lub utratę, a ponadto łatwiejsze staje się przejęcie konta albo aplikacji przez osoby nieuprawnione. Pojawiają się problemy z kompatybilnością wspólnie używanych narzędzi, serwery przeciążają się, zabezpieczenia interfejsów są niedostateczne[35]. Według międzynarodowego badania, w którym wzięło udział 676 praktyków bezpieczeństwa informacji, to właśnie zwiększająca się ilość usług cloud computing została uznana za jedno z największych obecnie zagrożeń dla organizacji w dziedzinie bezpieczeństwa informacji, przy czym odsetek respondentów, którzy zidentyfikowali wykorzystanie zasobów cloud computing jako główny problem wzrósł w przeciągu roku z 28% do 44%[36].

Według Cloud Security Alliance największe zagrożenia dla danych w chmurze są następujące[37]:

1) naruszenie danych (kradzieże, oglądanie lub używanie przez osobę do tego nieupoważnioną);
2) niedostateczna identyfikacja tożsamości i zarządzanie dostępem;
3) niebezpieczne interfejsy API;
4) luki w systemie;
5) przejęcie konta;
6) ataki od wewnątrz (malicious insiders);
7) zaawansowane długotrwałe ataki (APT);
8) utrata danych;

[34] PWC, 2016 *W obronie cyfrowych granic, czyli 5 rad, aby realnie wzmocnić ochronę firmy przed Cyber ryzykiem*, s. 16, https://www.pwc.pl/pl/pdf/raport-pwc-gsiss-cyberzagrozenia-2016.pdf [dostęp 26.11.2016].

[35] M. Hołyński, *Bezpieczeństwo w Chmurach*, „Elektronika" 2012, vol. 53, nr 8, s. 119.

[36] 2014 State of Endpoint Risk Report, Ponemon Institute LLC, Traverse City 2014, s. 4.

[37] Cloud Security Alliance*, Top Threats in 2016*, https://cloudsecurityalliance.org/group/top-threats/ [dostęp 12.11.2016].

9) brak należytej staranności przy wyborze odpowiedniej technologii;
10) nadużywanie oraz niefrasobliwe korzystanie z usług Cloud.

Wystąpienie incydentu dotyczącego wiedzy przechowywanej w chmurze skutkować może utratą reputacji, wyższymi kosztami i potencjalnie nawet likwidacją firmy[38].

Kolejnym następstwem pracy zdalnej jest konieczność zapewnienia sprzętu komputerowego telepracownikom i realizowana jest na dwa sposoby:

1) korzystanie ze sprzętu służbowego w domu;
2) praca na prywatnym komputerze.

Obydwa przypadki niosą za sobą negatywne konsekwencje dla bezpieczeństwa informacji. Z jednej strony praca na służbowym sprzęcie poza siedzibą organizacji stwarza większe ryzyko jego kradzieży (choćby podczas transportu). Łatwiej w przestrzeni prywatnej o dostęp osób trzecich do urządzeń służbowych lub o celowe ich udostępnienie (np. domownikom). Jak wynika z przeprowadzonych badań, około 50% wszystkich pracowników deklaruje, że z ich firmowego laptopa korzysta rodzina[39]. Dodatkowe ryzyka mogą stwarzać dzieci czy nawet zwierzęta, które mogą przez przypadek zalać firmowy sprzęt lub go uszkodzić, ale również omyłkowo wysłać e-maila służbowego czy wprowadzić modyfikacje w dokumentacji. W środowisku domowym służbowe komputery nie posiadają osłony firewall, a często pozbawione są także aktualizacji programów antywirusowych.

Z drugiej strony korzystanie z komputerów prywatnych to jeszcze większe zagrożenie dla bezpieczeństwa informacji. Bardzo często urządzenia prywatne pozbawione są większości zabezpieczeń stosowanych tradycyjnie w sprzęcie firmowym. Nie posiadają one kont zabezpieczonych hasłami, aktualnych programów antywirusowych czy ograniczeń ruchu sieciowym (np. firewall). Dodatkowo częściej są zainfekowane wirusami. Podczas prywatnego wykorzystywania tych urządzeń pracownicy lub ich domownicy wchodzić mogą na niebezpieczne strony internetowe lub instalować niebezpieczne aplikacje, sprowadzając ryzyko na dane służbowe i systemy wewnątrz firmy, z którymi telepracownik będzie się łączył z prywatnego komputera.

W związku z powyższym transfer plików pomiędzy sprzętem służbowym i prywatnym niesie za sobą poważne ryzyko naruszeń i ataków hackerskich, a jak

[38] Tamże, s. 4.
[39] Infowatch, http://www.InfoWatch.com [dostęp 4.02.2010].

wynika z prowadzonych badań, do takiego transferu przyznaje się 46% pracowników zdalnych[40].

Coraz częściej do komunikacji z innymi pracownikami lub do pracy w sieci służbowej wykorzystywane są również prywatne smartfony i tablety. Trend powyższy nazwany jest BYOD (Bring Your Own Device). Specyfikacja współczesnych urządzeń mobilnych umożliwia pracownikom dostęp do sieci korporacyjnej i biznesowych aplikacji z dowolnego miejsca. W konsekwencji duża ilość poufnych informacji firmowych jest zatem narażonych na utratę lub kradzież. Jak łatwo się domyśleć, crackerzy chętnie wykorzystują fakt, że coraz więcej urządzeń łączy się z globalną siecią. Dla samego systemu Android, tylko w drugim kwartale 2018 r., specjaliści odnotowywali pojawianie się nowych zagrożeń co 7 sekund. Natomiast w pierwszej połowie roku 2018 naliczono ponad 2 miliony przykładów złośliwego oprogramowania działającego w systemie stworzonym przez Google'a [41].

Pomimo że smartfony i tablety są wszechobecnym narzędziem pracy telepracowników, a informacje o zagrożeniach z nimi związanych są obecne w czołówkach serwisów informacyjnych, to organizacje nie spieszą się z wprowadzaniem zabezpieczeń mających przeciwdziałać zagrożeniom ze strony urządzeń przenośnych[42].

Analogiczne ryzyka, jak w przypadku korzystania z urządzeń teleinformatycznych, istnieją podczas wykorzystywania prywatnych nośników informacji. Według analizy przeprowadzonej w 2016 r. przez Kaspersky Lab ICS Cert, przenośne pamięci masowe są drugim z najczęstszych źródeł wnikania złośliwego oprogramowania. Podłączając prywatne przenośne urządzenie do komputera służbowego, możemy przenieść do niego (lub nawet do całej infrastruktury IT) np. złośliwy kod znajdujący się na pendrivie. Jego źródłem są zwykle zainfekowane, pobierane z sieci pliki (zwłaszcza pornografia)[43]. Inną kwestią istotną dla bezpieczeństwa

[40] A. Kozłowski, *Bezpieczna...*, dz. cyt.

[41] D. Długosz, *Nowy wirus na Androida pojawia się co 7 sekund. Tak źle jeszcze nie było*. https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/nowy-wirus-na-androida-pojawia-sie-co-7-sekund-tak-zle-jeszcze-nie-bylo/s68yx49 [dostęp 5.04.2020].

[42] Jedynie nieco ponad połowa organizacji na świecie (54%) wdrożyło strategię bezpieczeństwa dla urządzeń przenośnych. Źródło: *The Global State of Information Security® Survey 2015*, PWC, s. 25.

[43] Dekra, Nie używaj prywatnych pamięci przenośnych w pracy, https://hi-in.facebook.com/DEKRAwPolsce/photos/dlaczego-nie-powiniene%C5%9B-u%C5%BCywa%C4%87-prywatnych-pendrive%C3%B3w-na-komputerach-s%C5%82u%C5%BCbowych-%EF%B8%8F/2753828461301721/ [dostęp 6.04.2020].

danych w pracy zdalnej jest fakt, iż osoba pracująca w domu, pozbawiona jest bezpośredniego wsparcia ze strony administratora czy specjalisty bezpieczeństwa informacji. W takiej sytuacji łatwiej o zachowania niezgodne z polityką bezpieczeństwa firmy bądź o zwykłą pomyłkę. Nie mając w pobliżu siebie kolegów czy przełożonych, trudniej jest wykryć potencjalny atak przy użyciu socjotechniki – phishing. Jak pokazuje przypadek epidemii koronawirusa, powszechna praca zdalna jest łatwo wykorzystywana przez cyberprzestępców do licznych wyłudzeń lub podszywania się pod inne instytucje.

Już od wielu lat wszystkie badania poświęcone bezpieczeństwu informacji wskazują na człowieka jako głównego sprawcę incydentów zagrażających bezpieczeństwu informacji. Należy zauważyć, że aż 70% wszystkich nadużyć w roku 2014 było popełnionych przez pracowników organizacji (z czego 48% przez obecnych, a 22% przez byłych pracowników)[44]. Jednak w większości przypadków pracownicy są wykorzystywani jedynie jako środek do przenoszenia złośliwego oprogramowania czy jako obiekt ataku phishingowego i wykorzystującego socjotechnikę, stając się w ten sposób narzędziem w ręku rzeczywistych sprawców. Zdecydowanie łatwiej bowiem cyberprzestępcom wykorzystać naiwność człowieka niż złamać coraz to doskonalsze zabezpieczenia sprzętowo-programowe. Takich pracowników można podzielić na trzy kategorie: beztroskich i niedoświadczonych, wprowadzonych w błąd lub padających ofiarą ataków typu: inżynieria społeczna.

Bardzo często pracownicy wykonują lwią część pracy cyberprzestępców, stosując np. te same loginy i hasła w różnych serwisach, które nie są równie dobrze zabezpieczone. Wystarczy więc, że włamywacz wydobędzie informacje z bazy danych, z tego teoretycznie nieistotnego portalu, aby chwilę później, wykorzystując zdobyte dane, zalogować się do skrzynki pocztowej lub wykraść dane znajdujące się na firmowym dysku wirtualnym.

Jest to szczególnie istotne w pracy zdalnej, w której pracownicy nie mogą liczyć na szybkie wsparcie ze strony administratora czy serwisanta w miejscu swojej pracy. Rzadkością są również szkolenia dla wirtualnych pracowników dotyczące zagrożeń bezpieczeństwa informacji. W efekcie 70% ekspertów w dziedzinie bezpieczeństwa uważa, że pracownicy zdalni stanowią większe zagrożenie niż pracownicy wykonujący swe obowiązki w siedzibie pracodawcy[45].

[44] Tamże, s. 16.
[45] A. Kozłowski, *Bezpieczna*..., dz. cyt.

Zestawienie głównych zagrożeń dla bezpieczeństwa informacji wynikających ze specyfiki pracy zdalnej przedstawiono w tabeli 1.

Tabela 1. Zagrożenia w obszarze bezpieczeństwa informacji w pracy zdalnej

Cechy pracy zdalnej	Zagrożenie dla bezpieczeństwa informacji
Brak wydzielonego stanowiska pracy	- przeglądanie lub kopiowanie danych przez osoby trzecie - kradzież danych - modyfikacja danych
Brak adekwatnych zabezpieczeń fizycznych	- kradzież danych - kopiowanie danych
Stała obecność osób trzecich (domowników)	- ryzyko nieuprawnionego dostępu do danych - usunięcie danych - modyfikacja danych
Brak wsparcia ze strony administratora	- zwiększone ryzyko ataków phishingowych - błędna reakcja na incydenty bezpieczeństwa - dłuższy brak dostępu do danych w przypadku incydentu bezpieczeństwa
Korzystanie ze służbowych urządzeń w domu	- kradzież urządzeń - ryzyko nieuprawnionego dostępu do danych - ryzyko uszkodzenia sprzętu
Korzystanie z prywatnych urządzeń w celach służbowych	- nieautoryzowany dostęp do danych - zainfekowanie plików zawierających informacje służbowe - zainfekowanie systemów informatycznych organizacji
Praca w domowej sieci internetowej	- przechwycenie informacji / podsłuch informacyjny - włamanie się do sieci organizacji
Korzystanie ze służbowych nośników danych	- kradzież nośnika - nieautoryzowany dostęp do danych
Korzystanie z prywatnych nośników danych	- utrata danych - nieautoryzowany dostęp do danych - zainfekowanie plików zawierających informacje służbowe - zainfekowanie systemów informatycznych organizacji - ataki hackerskie na systemy informatyczne organizacji
Dostęp do danych w chmurze	- naruszenie danych (kradzież, wgląd w dane) - ataki hackerskie - brak dostępu do danych
Korzystanie z wirtualnej sieci prywatnej (Virtual Private Network – VPN)	- ataki hackerskie na systemy informatyczne organizacji

Źródło: opracowanie własne.

Ochrona informacji w organizacji pracy zdalnej

Z perspektywy bezpieczeństwa informacyjnego w pracy zdalnej optymalnym rozwiązaniem jest posiadanie przez organizację Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), który kompleksowo obejmuje wszystkie obszary zagrożeń i sposoby przeciwdziałania im. Wdrożenie SZBI jest obligatoryjne w organizacjach, w których istnieje konieczność zachowania zgodności ze standardami, wytycznymi branżowymi takimi jak SOX, Basel II czy Cobit oraz zgodności z przepisami prawa, co szczególnie dotyczy podmiotów publicznych podlegających Ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących działania publiczne[46]. Jednak rosnąca świadomość w zakresie potrzeby ochrony informacji, szczególnie tych dotyczących know-how, danych osobowych czy też danych klientów sprawiają, że po SZBI coraz częściej sięgają organizacje chcące uchodzić w oczach swoich klientów za bezpiecznych i wiarygodnych partnerów.

Tworzenie i modyfikacja systemu zabezpieczeń oparte na cyklicznej analizie ryzyka – charakterystyczne dla SZBI – są szczególnie istotne podczas pracy zdalnej, zależnej od technologii teleinformatycznych. Z kolei kompletność podejścia oznacza zajęcie się całą organizacją i wszystkimi procesami przetwarzania informacji. SZBI oparty o normę PN ISO/IEC 27001 obejmuje m.in. takie obszary istotne z perspektywy bezpieczeństwa informacji, a kluczowe dla pracy zdalnej, jak:[47]

- polityka stosowania urządzeń mobilnych;
- telepraca;
- dostęp do sieci i usług sieciowych;
- zarządzanie dostępem użytkowników;
- uświadamianie, kształcenie i szkolenie z zakresu bezpieczeństwa informacji;
- przekazywanie nośników informacji;
- bezpieczeństwo sprzętu i aktywów poza siedzibą;
- bezpieczeństwo komunikacji i przesyłania informacji drogą elektroniczną;

[46] Są one zobowiązane do wdrożenia zasad zarządzania bezpieczeństwem informacji, co wynika z Rozporządzenia 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.

[47] PN ISO/IEC 27001:2014-12- *Systemy zarządzania bezpieczeństwem informacji – wymagania*, s. 16-27.

- ochrona przed szkodliwym oprogramowaniem;
- zarządzanie usługami świadczonymi przez dostawców;
- zgłaszanie incydent;
- zapewnienie ciągłości działania;
- zapewnianie zgodności z prawem.

Oczywiście zabezpieczenia w poszczególnych obszarach są opisane w normie na dużym poziomie ogólności. Każda organizacja w oparciu o zapisy normy tworzy zestaw procedur opisujących szczegółowy sposób postępowania w powyższych obszarach uwzględniający specyfikę danej organizacji.

Jeśli w danej organizacji nie funkcjonuje SZBI, zasady dotyczące bezpiecznej pracy zdalnej powinny zostać opracowane oddzielnie i uwzględniać następujące kwestie:

1) Zaopatrzenie telepracownika w komputer służbowy zabezpieczony wcześniej przez administratora w: system antywirusowy, firewall, konto zabezpieczone hasłem, ustawione blokowanie komputera po pewnym krótkim czasie bezczynności. W przypadku niemożności skorzystania z komputera służbowego – komputer prywatny powinien zostać poddany takiemu samemu reżimowi bezpieczeństwa jak sprzęt służbowy.
2) Zaopatrzenie telepracownika w szyfrowane służbowe dyski przenośne.
3) Opracowanie zasad bezpiecznego łączenia się ze służbową infrastrukturą informatyczną z wykorzystaniem szyfrowanych metod łączenia.
4) Wprowadzenie zakazu zapisywania na prywatnych nośnikach informacji i prywatnych komputerach jakichkolwiek plików z danymi wrażliwymi (dane osobowe, informacje niejawne lub inne istotne z punktu organizacji dane).
5) Opracowanie zasad bezpiecznego korzystania z poczty elektronicznej, zawierających min:
   a) zakaz korzystania z systemu poczty elektronicznej dla celów prywatnych oraz z adresów prywatnych do celów służbowych;
   b) nakaz szyfrowania informacji wrażliwych, a szczególnie danych osobowych przed wysłaniem.
6) Opracowanie zasad przechowywania dokumentów w przestrzeni domowej.
7) Politykę haseł dostępu (określającą ich siłę, częstotliwość zmian czy sposoby przechowywania).

8) Pomoc techniczną telepracownikom.
9) Sposób postępowania w przypadku wykrycia incydentu bezpieczeństwa informacji.

Należy równocześnie pamiętać, że samo opracowanie odpowiednich zasad i procedur działania nie sprawi, że będą one stosowane. Każdy incydent naruszenia bezpieczeństwa informacji w organizacji jest mniej lub bardziej zależny nie tylko od zapisanych procedur czy technologii, ale przede wszystkim od ludzi. Niewłaściwe postępowanie lub brak działania ze strony pracowników prowadzi do większości incydentów związanych z bezpieczeństwem informacji. W związku z powyższym telepracownicy muszą być zaznajomieni z obowiązującymi procedurami i rozumieć konsekwencje swoich zachowań. Dlatego nieodzowną częścią organizacji pracy zdalnej muszą stanowić szkolenia, które nie tylko zwiększają wiedzę na temat bezpieczeństwa informacji, ale przede wszystkim posiadają istotny wpływ na faktyczne zachowania pracowników w tym obszarze[48].

Podsumowanie

Praca zdalna ze swej istoty jest uzależniona od wykorzystania systemów teleinformatycznych. Technologie te umożliwiają dostęp do niezbędnych informacji i wiedzy, wspólne podejmowanie decyzji, przesyłanie efektów pracy, konsultacje czy dyskusje. Jednym słowem pozwalają na realizację zadań. Charakterystyka tej formy pracy sprawia, że pojawiają się w niej nowe – liczne – zagrożenia dla bezpieczeństwa informacji. Z kolei wystąpienie incydentu bezpieczeństwa informacji powoduje zakłócenia procedur i procesów bądź uniemożliwia ich realizację, a w efekcie zmniejsza skuteczność całej organizacji.

W konsekwencji zasadne wydaje się wdrożenie w organizacjach stosujących pracę zdalną systemu zarządzania bezpieczeństwem informacji. W przypadku niewielkich podmiotów zawiłe procedury i działania SZBI mogą wydawać się zbyt zbiurokratyzowane czy wręcz zbędne. Jednak z perspektywy potencjalnych kosztów, wynikających z naruszenia bezpieczeństwa informacji, posiadanie zasad bezpieczeństwa pracy zdalnej staje się koniecznością.

[48] T. Stefaniuk, *Training in shaping employee information security awareness*, "Entrepreneurship and Sustainability Issues" 2020, No. 7 (3), s. 1843.

Bibliografia

8 praktyk dla bezpiecznego zarządzania nośnikami danych, https://logsystem.pl/blog/8-praktyk-dla-bezpiecznego-zarzadzania-nosnikami-danych/ [dostęp 3.04.2020].

2014 State of Endpoint Risk Report, Ponemon Institute LLC, Traverse City 2014.

Baskerville R., Nandhakumar J., Activating and perpetuating virtual teams, [w:] Transactions on Professional Communication 2007, Vol. 50, No.1.

Bergiel B.J., Bergiel E.B., Balsmeier P.W., *Nature of virtual teams: a summary of their advantages and disadvantages,* [w:] "Management Research News", Vol. 31, No. 2, Emerald Group Publishing Limited, United Kingdom, Bingley 2008.

Cloud Security Alliance, *Top Threats in 2016*, https://cloudsecurityalliance.org/group/top-threats/ [dostęp 12.11.2016].

CSIRT: Nośniki USB- zapobieganie zagrożeniom, https://www.csirt.gov.pl/cer/wiadomosci/zagrozenia-i-podatnosc/110,Nosniki-USB-zapobieganie-zagrozeniom.html [dostęp 3.04.2020].

Dekra, *Nie używaj prywatnych pamięci przenośnych w pracy*, https://hi-in.facebook.com/DEKRAwPolsce/photos/dlaczego-nie-powiniene%C5%9B-u%C5%BCywa%C4%87-prywatnych-pendrive%C3%B3w-na-komputerach-s%C5%82u%C5%BCbowych-%EF%B8%8F/2753828461301721/ [dostęp 6.04.2020].

Długosz D., *Nowy wirus na Androida pojawia się co 7 sekund. Tak źle jeszcze nie było*, https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/nowy-wirus-na-androida-pojawia-sie-co-7-sekund-tak-zle-jeszcze-nie-bylo/s68yx49 [dostęp 5.04.2020].

Duszczyk M., Koronawirus wygania Polaków na telepracę. Czas wirtualnych biur, https://cyfrowa.rp.pl/it/45191-koronawirus-wygania-polakow-na-teleprace-czas-wirtualnych-biur [dostęp 5.04.2020].

GfK Corona Mood, *Dynamika zachowań konsumenckich na rynkach FMCG, dóbr trwałych i usług finansowych*, https://www.gfk.com/pl/aktualnosci/press-release/polowa-respondentow-51-proc-deklaruje-ze-chodzi-do-pracy-jak-zwykle/, https://antyweb.pl/tylko-17-pracownikow-w-polsce-pracuje-zdalnie/ [dostęp 5.04.2020].

"Harvard Business Review", maj-czerwiec 1998, s. 128.

Hołyński M., *Bezpieczeństwo w Chmurach*, „Elektronika" 2012, vol. 53, nr 8, s. 119.

Ilu jest nauczycieli w Polsce?, https://www.zadluzenia.com/liczba-nauczycieli-w-polsce/ [dostęp 04.04.2020].

Ilu jest uczniów w Polsce?, https://www.zadluzenia.com/ilu-jest-uczniow-w-polsce/ [dostęp 4.04.2020].

Infowatch, http://www.InfoWatch.com [dostęp 4.02.2010].

ITF Transport Outlook 2019, https://www.oecd-ilibrary.org/transport/itf-transport-outlook-2019_transp_outlook-en-2019-en [dostęp 6.05.2020].

Karbownik K., *Korzyści i zagrożenia wynikające z zatrudnienia pracowników w formie telepracy*, „Zeszyty Naukowe Politechniki Częstochowskiej Zarządzanie" 2015, nr 20.

Kozłowska B., Królikowski J., Szczęsny P., *Telepraca – podręcznik dla gminnych centrów informacji*, PARP, Warszawa 2008.

Kozłowski A., *Bezpieczna praca zdalna*, https://www.cyberdefence24.pl/bezpieczna-praca-zdalna [dostęp 3.04.2020].

Maik A., Godzisz A., *Istota i pojęcie organizacji sieciowej*, [w:] „Studia i Materiały. Miscellanea Oeconomicae" 2013, r. 17, nr 2.

Morris C., *7 ways to make working from home easier during the coronavirus pandemic,* https://fortune.com/2020/03/12/working-from-home-coronavirus-remote-work-tele-commuting-wfh-covid-19/ [dostęp 24.05.2020].

Nilles J., *Telepraca, strategie kierowania wirtualną załogą*, WNT, Warszawa 2003.

Pamięć USB – używasz prywatnie lub służbowo? Przeczytaj!!!, https://blogspec-lab.pl/pamiec-usb-uzywasz-prywatnie-lub-sluzbowo-przeczytaj/ [dostęp 28.03.2020].

PN ISO/IEC 27001:2014-12-2014 – *Systemy zarządzania bezpieczeństwem informacji – wymagania*.

Potocka J., *Studenci wracają na uczelnie. Dziś początek roku akademickiego 2019/2020*, https://www.rmf24.pl/tylko-w-rmf24/joanna-potocka/redaktor/news-studenci-wra-caja-na-uczelnie-dzis-poczatek-roku-akademickieg,nId,3233364 [dostęp 30.03.2020].

Praca zdalna: 5 najważniejszych zasad. Z powodu koronawirusa w Polsce przybywa osób pracujących z domu, https://alebank.pl/praca-zdalna-5-najwazniejszych-zasad-z-powodu-koronawirusa-w-polsce-przybywa-osob-pracujacych-z-domu/ [dostęp 29.03.2020].

PWC, 2016, *W obronie cyfrowych granic, czyli 5 rad, aby realnie wzmocnić ochronę firmy przed Cyberryzykiem*, https://www.pwc.pl/pl/pdf/raport-pwc-gsiss-cyberzagroz-enia-2016.pdf [dostęp 26.11.2016].

Ratajczyk-Mrozek M., Adamik A.I., Najda-Janoszka M., Wróbel P., Stefaniuk T., Nie-dbał R., *Koncepcje zarządzania zorientowane na współdziałanie i wspomagające je narzędzia informatyczne*, TNOiK, Dom Organizatora, Toruń 2016.

Rocznik statystyczny pracy 2019, GUS, Warszawa 2020, s. 120.

Smug T., *Niebezpieczeństwa związane z VPN i jak zminimalizować zagrożenia zdalnego dostępu za pomocą PAM?*, https://emspartner.pl/beyondtrust/niebezpieczenstwa-zwiazane-z-vpn-i-jak-zminimalizowac-zagrozenia-zdalnego-dostepu-za-pomoca-pam/ [dostęp 6.04.2020].

Stefaniuk T., *Komunikacja w zespole wirtualnym*, Difin, Warszawa 2014.

Stefaniuk T., *Training in shaping employee information security awareness*, „Entrepreneurship and Sustainability Issues" 2020, nr 7 (3).

Swansea University, http://www.swan.ac.uk/psychology/patra [dostęp 19.11.2011].

Szewczak A., *Telepraca – szansą czy zagrożeniem na rynku pracy*? Wyd. Hogben, Szczecin 2002.

Telepraca na odsiecz środowisku, https://www.obserwatorfinansowy.pl/bez-kategorii/rotator/telepraca-na-odsiecz-srodowisku/ [dostęp 8.03.2020].

The Global State of Information Security® Survey 2015, PWC.

Trziszka M., *Model organizacji i zarządzania systemem pracy zdalnej w branży IT*, Rozprawa doktorska, Wyd. PP, Poznań 2019.

Ustawa z dnia 24 sierpnia 2007 r. o zmianie ustawy – Kodeks pracy (Dz.U. z 2007 r. Nr 181, poz. 1288).

Wrycza S., *Informatyka ekonomiczna: podręcznik akademicki*, PWE, Warszawa 2010.

Information security in the provision of remote work

Summary: Remote work, also referred to as teleworking, involves performing tasks entrusted by the employer to be performed outside the company headquarters - usually at home. It has many advantages both from the employee's and employer's perspective. As the teleworker moves outside the parent company's headquarters, the information and IT systems necessary to do the work move. This results in a much easier materialization of information security threats. This chapter presents the essence and advantages of remote work and the main threats to information security resulting from the specifics of this form of employment. Attention was also paid to key issues related to the security of information and ICT systems.
Keywords: *information security, remote work, teleworking, information security management system (ISMS)*