dr hab. MIROSŁAW KWIECIŃSKI, prof. nadzw. KAAFM
Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
Kontakt: miroslaw.kwiecinski@wp.pl
DOI: 10.5604/01377043.1228544

Bezpieczeństwo informacji w telepracy oraz uwarunkowania bezpieczeństwa telepracy

Artykuł składa się z dwóch części. Pierwsza obejmuje zarys problematyki bezpieczeństwa informacji w ramach telepracy. Przedstawiono tu obszar aktywności pozwalający dokonywać wymiany informacji, podstawowe zagrożenia utraty informacji oraz sposoby przeciwdziałania i wykorzystanie możliwych zabezpieczeń.
Druga część odnosi się do problematyki szeroko nakreślonego bezpieczeństwa telepracy. Podobnie jak w pierwszej części, przedstawiono podstawowe zagrożenia oraz sposoby przeciwdziałania uaktywnionym zagrożeniom bezpieczeństwa pracy zdalnej.
Słowa kluczowe: telepraca, bezpieczeństwo informacji, bezpieczeństwo telepracy

Information security in telework and telework security

This article consists of two parts. The first one outlines the problems of information security in the context of telework. It presents an area of activity in which exchanging information is possible, principal dangers of losing information, and ways of counteracting this, and possible safeguards. The second part covers the problems of broadly understood telework security. Like the first part, it presents principal threats and ways to counter them.
Keywords: telework, information security, telework security

Fot. maxxyustas/Bigstockphoto

Wstęp

Chociaż telepraca funkcjonuje już od wielu lat, dopiero w ostatniej dekadzie zaczęto w Polsce doceniać nową jakość, którą ze sobą niesie. Ta forma świadczenia pracy pozwala bowiem na elastyczne planowanie jej wykonywania – zasadniczo przez pracowników wiedzy (*knowledgeworkers*). Rozwiązania organizacji pracy zdalnej pozwalają uniknąć wielu niedogodności, związanych z dotychczasowym, tradycyjnym sposobem realizacji świadczenia pracy. Wywołuje to zatem ciągłe zainteresowanie badaczy tej problematyki. Wynika ono z rosnących potrzeb zarówno firm, jak i pracowników oraz dostępności odpowiednich technologii, co sprawia, że w szybkim tempie powstają niemal idealne warunki sprzyjające dynamicznemu rozwojowi tego zjawiska.

Celem artykułu jest zarysowanie problematyki bezpieczeństwa informacji w telepracy jako jej kluczowego spoiwa, a także problematyki szeroko rozumianego bezpieczeństwa telepracy. Przedstawiono podstawowe zagrożenia bezpieczeństwa informacji w telepracy oraz samej telepracy i sposoby przeciwdziałania uaktywnionym zagrożeniom. W zakończeniu przedstawiono zasadnicze postulaty prowadzenia dalszych badań w tej dynamicznie rozwijającej się dziedzinie współczesnej aktywności człowieka.

Bezpieczeństwo informacji w telepracy

Zgodnie z powszechnie definiowanym ujęciem socjologicznym, telepraca ujmowana jest jako praca wykonywana poza lokalem pracodawcy (w domu pracownika, w telecentrum lub w innym miejscu, w którym aktualnie przebywa pracownik) z wykorzystaniem technologii informacyjnych (IT), świadczona na podstawie umowy o pracę, umów cywilnoprawnych (w tym umowy na zlecenie i o dzieło), bądź umowy o pracę nakładczą. Telepracownikiem zaś jest osoba świadcząca tak zdefiniowaną pracę.

Atrakcyjność telepracy wiąże się ściśle z zachowaniem bezpieczeństwa przetwarzania informacji przez pracownika wykonującego swoje zadania zdalnie. Kluczowe jest zatem bezpieczeństwo teleinformatyczne. W tabeli 1. przedstawiono zasadnicze różnice pomiędzy pracownikiem zdalnym, a pracownikiem w lokalnej sieci firmowej – z punktu widzenia bezpieczeństwa teleinformatycznego.

Do typowych przykładów zagrożeń bezpieczeństwa informacji w telepracy należą:

- utrata informacji firmowej, przetwarzanej przez pracownika, w wyniku uszkodzenia komputera przenośnego w trakcie przemieszczania się lub pracy w domu, gdzie sprzęt narażony jest na uszkodzenie podczas typowych prac domowych lub przez dzieci
- utrata informacji oraz sprzętu służbowego w wyniku kradzieży komputera przenośnego podczas transportu, z samochodu lub z/do domu/hotelu
- utrata informacji służbowej w wyniku zainfekowania komputera złośliwym oprogramowaniem podczas instalacji niezaufanego oprogramowania
- kradzież informacji wrażliwej z komputera pracownika przez złośliwe oprogramowanie,

Tabela 1. Zasadnicze różnice pomiędzy pracownikiem zdalnym a pracownikiem w lokalnej sieci firmowej z perspektywy bezpieczeństwa teleinformatycznego

Tabela 1. Zasadnicze różnice pomiędzy pracownikiem zdalnym a pracownikiem w lokalnej sieci firmowej z perspektywy bezpieczeństwa teleinformatycznego

Element różnicujący	Pracownik lokalny	Pracownik zdalny
Środowisko pracy		
Dostęp do Internetu	Przez router firmowy	Przez sieć osiedlową, DSL, sieć kablową, sieć WLAN, hot-spot, telefon komórkowy, kawiarenkę internetową
Komputer	Komputer stacjonarny lub laptop	Zwykle laptop
System operacyjny	Regularnie aktualizowany, często zarządzany centralnie	Nieaktualizowany lub aktualizowany nieregularnie, brak centralnego zarządzania
Aplikacje	Głównie potrzebne do pracy	Liczne niezaufane aplikacje pobrane z sieci
Zabezpieczenia		
Główne	Firmowy firewall, serwer proxy, antywirus, filtr treści	Brak centralnych zabezpieczeń sieciowych
Dodatkowe	Firewall lub/i antywirus osobisty	Firewall lub/i antywirus osobisty, często wyłączony
Opieka administratora	Dostępny na miejscu	Niedostępny na miejscu
Ryzyko		
Kradzież komputera	Ryzyko niewielkie	Ryzyko duże, w domu lub podczas podróży z notebookiem
Utrata informacji	Ryzyko niewielkie, jeśli pliki przechowywane są na udziale sieciowym i regularnie archiwizowane	Duże ryzyko np. uszkodzenia notebooka w domu lub podczas podróży
Złośliwe oprogramowanie	Ryzyko niewielkie, jeśli wdrożona jest centralna ochrona	Ryzyko duże ze względu na pracę na koncie administratora, brak centralnej ochrony i instalowanie niezaufanych aplikacji

Źródło: opracowanie własne na podstawie P. Krawczyk, Bezpieczeństwo telepracy dla MARR (dostęp: 30.05.2016).

Tabela 2. Atrybuty bezpieczeństwa informacji w organizacji

Tabela 2. Atrybuty bezpieczeństwa informacji w organizacji

Lp.	Atrybut	Właściwości
1.	Dostępność	Bycie dostępnym i użytecznym na każde żądanie upoważnionego podmiotu
2.	Poufność	Informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom
3.	Integralność	Polega na zapewnieniu dokładności i kompletności aktywów
4.	Rozliczalność	Zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi
5.	Autentyczność	Zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana
6.	Niezawodność	Oznacza stałe, zamierzone zachowanie i skutek
7.	Niezaprzeczalność	Oznacza, że dany podmiot nie może zaprzeczyć, że jest autorem lub przekazywał dane informacje

Źródło: opracowanie własne na podstawie [1]

w wyniku korzystania z niezaufanej sieci lub przez osoby postronne

• kradzież danych dostępowych do systemu firmowego (hasła) lub usług zewnętrznych (hasła bankowe, hasła do serwisów internetowych i partnerskich) przez złośliwe oprogramowanie lub osoby postronne

• możliwość przeniesienia złośliwego oprogramowania z komputera pracownika do sieci lokalnej podczas wizyty w siedzibie firmy lub korzystania z połączenia zdalnego (np. VPN)

• instalacja na komputerze służbowym pirackiego oprogramowania, pirackich kopii filmów, muzyki i innych treści mogących stanowić naruszenie przepisów prawa.[1]

Tradycyjny model zachowania bezpieczeństwa informacji organizacji, w tym także w ramach telepracy, ze względu na gwałtowne zmiany otoczenia, przechodzi do historii. W klasycznym wydaniu opiera się on na traktowaniu bezpieczeństwa informacji jako stanu zachowania poufności, integralności i dostępności informacji. Stan taki uwzględniać może dodatkowo inne własności. Współczesne atrybuty (właściwości) bezpieczeństwa informacji przedstawiono w tabeli 2.

W polskich regulacjach prawnych brakuje precyzyjnych przepisów w odniesieniu do ustalenia zasad zachowania bezpieczeństwa informacji w ramach telepracy. Rozstrzygnięcia ograniczają się do ogólników, polegających na stwierdzeniu, że pracodawca zawiera z telepracownikiem stosowną umowę o zatrudnieniu, w której można uregulować ogólne zasady zachowania bezpieczeństwa informacji. Wspomina się także o własności urządzeń, którymi posługuje się telepracownik.

Tymczasem bezpieczeństwo informacji w ramach telepracy stanowi zagadnienie niezwykle ważne z punktu widzenia samej istoty telepracy. Implementacja telepracy wymaga zastosowania zestawu kluczowych technologii obejmujących:

• bezpieczny, szerokopasmowy dostęp do sieci Internet

• obsługę poczty e-mail i przestrzeni roboczej zespołów

• obsługę wiadomości błyskawicznych (IM) i połączeń VoIP lub biznesowych linii telefonicznych (najlepiej zintegrowanych z funkcjonującą w organizacji centralą PBX)

• dostęp do konferencji internetowych i wzbogaconych narzędzi medialnych, jak np. wideokonferencje.

Należy zwrócić uwagę na to, że esencją telepracy jest zazwyczaj zlecanie zadań mających charakter pracy intelektualnej, która wymaga z kolei przetwarzania informacji mających ogromną wartość dla pracodawcy. Ta okoliczność związana jest z potencjalnymi stratami, będącymi wprost konsekwencją utraty poufności informacji. Negatywne rezultaty mogą mieć swoje konsekwencje w postaci utraty klientów na rzecz konkurencji, utraty przewagi nad konkurencją na skutek niekontrolowanego ujawnienia procesów technologicznych, bądź utraty zaufania na skutek ujawnienia poufnych danych.

W tej strukturze znacznie trudniej jest zagwarantować bezpieczeństwo zasobów znajdujących się w strefie wrażliwej. Podobnie trudno jest zagwarantować bezpieczeństwo danych w przypadku, gdy ich kopia udostępniona zostanie telepracownikowi.

Kluczową sprawą w wykorzystaniu wspomnianych technologii i udostępnieniu ich telepracownikom jest zatem bezpieczeństwo, które może być stosunkowo łatwo monitorowane, kiedy praca wykonywana jest w biurze, czyli fizycznie identyfikowalnym obiekcie. Czy jednak w pełni można zapewnić bezpieczeństwo informacji? Mamydo czynienia z pewnym paradoksem. Mianowicie wraz z wejściem w epokę Internetu bezpieczeństwo obiektów fizycznych zostało zagrożone przez próby nieautoryzowanego dostępu do poczty e-mail, rozmów telefonicznych i danych zgromadzonych na serwerach. W rzeczywistości, bezpieczeństwo jest dobre tylko na tyle, na ile skuteczne są systemy uwierzytelniania, zapory sieciowe i szyfrowanie głosu/danych, na całej ścieżce przesyłania informacji. Jeżeli systemy te stosowane są na poziomie serwera – a tak zwykle powinno być – to praca zdalna nie powoduje znaczącego podwyższenia ryzyka.

Jeżeli zatem odpowiednie rozwiązania nie zostaną opracowane kompleksowo, to raczej należy oczekiwać, że pracodawcy będą starali się eliminować potencjalne zagrożenia i ograniczać zakres usług realizowanych przez telepracowników. Mało zachęcający wpływ na zlecanie pracy zdalnej z wrażliwymi zasobami ma fakt, że w wielu przypadkach, rozważając atrakcyjność telepracy, należy pamiętać, iż to na pracodawcy ciążą obowiązki zagwarantowania ochrony danych osobowych, wynikające z ustawy O ochronie danych osobowych [2]. W wielu opracowaniach naukowych nadal nie zauważa się potrzeby uwzględniania wymogów ochrony danych osobowych, jak również znaczenia kosztów, które winien ponieść pracodawca, a które związane są z wdrożeniem *Polityki bezpieczeństwa informacji* zgodnie z zaleceniami PN ISO/IEC 17799:2003 [3]

[1] P. Krawczyk *Bezpieczeństwo telepracy dla MARR* (dostęp: 30.05.2016).

oraz kosztów opracowania i wdrożenia Systemu zarządzania bezpieczeństwem informacji definiowanego w normie ISO/IEC 27001:2005 [4].

Jedną z możliwych opcji szyfrowania transmisji głosu i danych jest wprowadzenie systemu dostępu poprzez wirtualną sieć prywatną VPN. Szyfrowanie można jednak zintegrować z każdą zdalną aplikacją (email, VoIP, konferencje internetowe, IM/Obecność). Jest to alternatywa łatwiejsza do wdrożenia, skuteczna i niewiążąca się ze skomplikowanym systemem VPN.

Uwierzytelnienie, czyli zapewnienie, że osoba logująca się do systemu jest tą, za którą się podaje, to zagadnienie nieco obszerniejsze, ale istnieje wiele możliwości, aby zminimalizować poziom ryzyka. System pojedynczego logowania (*single sign-on*) zapewnia ujednolicone uwierzytelnienie, pozwalając na dostęp do całego zestawu aplikacji, włącznie z danymi w komputerach przenośnych, rejestrując równocześnie wszelką nietypową aktywność. Dostępne są już również niedrogie urządzenia biometryczne, sprawdzające przed zalogowaniem odciski palców. Nawet funkcja „Obecność" może być wykorzystana do ochrony, przy niewielkim zaangażowaniu – jeżeli ktoś zauważy, że sygnalizowany jest status *online* innej osoby, kiedy nie powinno to mieć miejsca, wystarczy, że sprawdzi za pomocą wiadomości błyskawicznej, z kim rzeczywiście ma do czynienia.

Wystarczy zatem niewiele kroków prowadzących do skutecznego wykorzystania rozwiązań płynących z współczesnej technologii informacyjnej (IT).

Uwarunkowania bezpieczeństwa telepracy

Zagrożenia bezpieczeństwa telepracy wiążą się przede wszystkim z osobą telepracownika. Obok wielu innych istotnych zagrożeń dotyczących samego miejsca pracy (w tym także fizycznego), komfortu wykonywania telepracy, perspektyw dochowania standardów jakości, zasadniczo w określaniu bezpieczeństwa telepracy dominuje opis działań oraz ich uwarunkowań dotyczących samego pracownika zdalnego. Dotyczy to także oceny poziomu lojalności telepracownika.

Wypada zauważyć, że charakter działań w przedsiębiorstwie korzystającym z telepracy wymyka się spod kontroli przewidzianej szczegółowymi procedurami, zwłaszcza że wykorzystuje się tu przetwarzane informacje do tworzenia coraz to nowych projektów. Stąd, głównym ośrodkiem tworzenia staje się ludzki mózg, a ściślej jego zdolności do zapamiętywania kontekstów informacji, szczątkowej ich postaci, zdolności do wyłowienia z szumów tej informacji, która zdecydowanie otworzy drogę do rozwinięcia projektu o niezwykle oryginalnych: kształcie i treści. Takie podejście rodzi myśl kontrolowania wszystkiego, co pojawia się w ludzkiej wyobraźni. Wszelkie wycieki, chociażby śladowo zaznaczonych przejawów nowatorstwa, mogą być zagospodarowane przez inne mózgi, bez żadnej gwarancji, że nie zostaną wykorzystane w innych konkurencyjnych projektach, nad którymi w tym samym czasie trwają prace. Dotychczasowe procedury ochrony informacji w organizacji nie przewidują bowiem ochrony tej zawartości, która rodzi się i konstytuuje w ludzkich mózgach. Nie można przecież kontrolować tego, co zamierza powstawać i realnie powstaje w ludzkim mózgu.

Najszybszym do wdrożenia rozwiązaniem, dającym pewne przesłanki kontroli nad zachowaniem bezpieczeństwa telepracy, pozostaje wdrożenie systemu wykorzystującego technologię mikroprocesorów. W taki mikroprocesor wyposażony byłby każdy telepracownik w momencie podpisania umowy o (współ) pracę. Wszczepienie mikroprocesora stwarzałoby możliwości szerokiej kontroli pracy uczestnika organizacji, łącznie z rejestracją wszelkich rozmów, czy to w zespole, czy przy pomocy wszelkich komunikatorów. Ponadto mikroprocesory stwarzałyby okazję do:

- kontroli zachowań i rozmów telepracowników poza pomieszczeniami tworzenia projektów
- rejestracji wszelkich zmian w organizmie pracownika, które mogłyby posłużyć wykrywaniu przypadków braku lojalności, na przykład z wykorzystaniem wariografu
- bezpośredniego indywidualnego komunikowania się z pracownikiem, które pozwalałoby na uprzedzanie zagrożeń wycieku informacji, przetwarzanych w trakcie tworzenia projektów
- budowy i wykorzystywania programów poddających pod kontrolę zachowanie lojalności pracownika
- ogromną pomoc w tworzeniu profilu kreatywności, jak i map zagrożeń, wynikających z udziału każdego telepracownika w pracy zespołów tworzących projekty.

Telepraca a kultura bezpieczeństwa

Nakreślona w artykule problematyka skłania do refleksji nad koniecznym rozwijaniem kultury bezpieczeństwa, także w obszarze telepracy. Kultura bezpieczeństwa wyznacza sposób myślenia o bezpieczeństwie danego podmiotu, odczuwania bezpieczeństwa, a także sposoby osiągania bezpieczeństwa. Wyczerpującą definicję kultury bezpieczeństwa przedstawił Marian Cieślarczyk: „Kultura bezpieczeństwa to wzór podstawowych założeń, wartości, norm, symboli i przekonań charakterystycznych dla danego podmiotu, wpływających na sposób postrzegania przez niego wyzwań, szans i (lub) zagrożeń w bliższym i dalszym otoczeniu, a także sposób odczuwania bezpieczeństwa i myślenia o nim [...] oraz związany z tym sposób zachowania i działania (współdziałania), w różny sposób przez ten podmiot „wyuczonych" i wyartykułowanych, w procesach szeroko rozumianej edukacji, w tym również w naturalnych procesach wewnętrznej integracji i zewnętrznej adaptacji oraz w innych procesach organizacyjnych [...], a także w procesie umacniania szeroko (nie tylko militarnie) rozumianej obronności [...], służących w miarę harmonijnemu rozwojowi tego podmiotu i osiąganiu przez niego najszerzej rozumianego bezpieczeństwa, z pożytkiem dla siebie, ale i dla otoczenia [5].

Obok tej definicji, niejako kierując się podsumowaniem jej istoty, można przyjąć, że kulturę bezpieczeństwa stanowi ludzkie myślenie o bezpieczeństwie, zamysły projektujące i preparacyjne oraz wielostronne działania na rzecz jego osiągnięcia i utrzymania, przy wykorzystaniu wcześniej wykreowanych i kreowanych na aktualny użytek artefaktów [6].

Podsumowanie

Podsumowując, wypada zatem stwierdzić, że atrakcyjność telepracy, jako specyficznej formy zatrudnienia, rośnie wprost proporcjonalnie do wysokości poziomu bezpieczeństwa systemów informatycznych, który mogą zagwarantować dostępne rozwiązania oraz technologie teleinformatyczne wraz z kosztami, które są niezbędne do zagwarantowania wymaganego poziomu bezpieczeństwa danych.

Trzeba również zaznaczyć, że przedstawione w tekście propozycje rozwiązań z zakresu bezpieczeństwa telepracy, aczkolwiek prowadzące do zwiększenia poziomu tego bezpieczeństwa, mogą być wysoce dyskusyjne w sensie etycznym. Z jednej bowiem strony trudno jest ograniczać wolność każdego obywatela poprzez stały nadzór elektroniczny jego poczynań, z drugiej jednak strony czyni się to w imię zasady ograniczonego zaufania wobec telepracownika, który podlega odrębnym rygorom. To jednak wymaga wyrażenia jego zgody na poddanie się procedurom bezpieczeństwa informacji za pomocą technik elektronicznych.

I w końcu, w świetle informacji dotyczących relacji telepracy z kulturą bezpieczeństwa, można zauważyć, że kultura bezpieczeństwa obejmuje zasadniczo trzy sfery aktywności człowieka: mentalną (charakter subiektywny), materialną (obiektywny) i organizacyjną (subiektywno-obiektywny). Tworzy to okazje do odniesień do jak najszerzej rozumianego środowiska bezpieczeństwa.

Zasadne byłoby zatem podjęcie badań nad metodologią określania potencjału bezpieczeństwa informacji telepracy oraz samej telepracy, m.in. w kontekście kultury bezpieczeństwa.

BIBLIOGRAFIA

[1] Szomański B. *Zarządzanie bezpieczeństwem informacji – podstawy oraz znaczenie w ochronie firmy przed nieuczciwymi pracownikami, klientami i usługodawcami*, [w:] *Zarządzanie bezpieczeństwem informacji i programami antykorupcyjnymi.* Praca zbiorowa pod red. naukową T. Wawaka, Wyższa Szkoła Administracji w Bielsku-Białej, Bielsko-Biała 2007

[2] Ustawa z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych* (Dz.U. z 2015 r., poz. 2135)

[3] PN-SIO/IEC-17799:2005 *Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji*, PKN, Warszawa 2007

[4] Polaczek T. *Audyt bezpieczeństwa informacji w praktyce – Praktyczny przewodnik po zagadnieniach ochrony informacji.*HELION, Gliwice 2006

[5] Cieślarczyk M. *Teoretyczne i metodologiczne podstawy badania problemów bezpieczeństwa i obronności państwa,* Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce 2009

[6] Jarmoszko S. *Nowe wzory kultury bezpieczeństwa a procesy deterioracji więzi społecznej* [w:] E. Rekłajtis, R. Wiśniewski, J. Zdanowski (red. nauk.) *Jedność i różnorodność. Kultura vs. kultury,* Warszawa 2010