Bezpieczeństwo danych podczas pracy zdalnej

Praktyczne porady dla pracownika

Autor: **Mateusz Siek**

e-mail: **kontakt@bims.home.pl**

strona internetowa: **bims.info**

Warszawa, kwiecień 2020 r.

Słowem wstępu…

Stan epidemii zmusił wiele organizacji do przejścia w tryb pracy zdalnej. Te podmioty, które dotychczas przewidywały opcję tzw. home office nie są dziś zaskoczone nową sytuacją. Jest jednak sporo firm i urzędów, które stanęły przed nowym wyzwaniem. Wiąże się to zarówno z inną organizacją pracy przez pracodawcę ale również dla pracownika z pracą w nowym środowisku.

Takie „elastyczne" warunki pracy oznaczają niestety nowe ryzyka dla bezpieczeństwa danych. Transport sprzętu lub dokumentów, nadzór nad nimi w domu, kwestie związane z IT i ograniczony dostęp do wsparcia ze strony pracodawcy to obszary, na które warto zwrócić uwagę w kontekście ochrony danych. To w tych miejscach powstały nowe podatności, które dotychczas nie występowały w bieżącej pracy.

Dlatego właśnie tak istotne, by każdy pracownik wykonujący pracę zdalną zapoznał się z poniższymi radami i uwagami dotyczącymi bezpieczeństwa danych podczas pracy zdalnej. Niezależnie od trybu pracy, dane osobowe musza być właściwie chronione, tak by nie okazało się, że brak świadomości lub niewłaściwe praktyki doprowadziły do naruszenia i jego konsekwencji.

Poradnik jest przeznaczony zarówno dla osób rozpoczynających przygodę z pracą zdalną, jak również – jako przypomnienie – dla pracowników zaznajomionych już z taką formą aktywności zawodowej. Przedstawione w nim sugestie oparte są na wieloletnim doświadczeniu i dobrych praktykach zebranych z różnych źródeł. Mam nadzieję, że okażą się pomocne i pozwolą dobrze zorganizować pracę, tak by dane osobowe były bezpieczne.

Mateusz Siek

Spis treści

1. Pierwsze kroki

Zanim jeszcze rozpoczniemy naszą przygodę z pracą z domu należy się właściwie do tego przedsięwzięcia przygotować. I nie chodzi mi tylko o pogodzenie się z mejlowaniem i telekonferencjami przy płaczącym/krzyczącym/śmiejącym się dziecku, szczekającym psie, huczących bajkach, wirującej pralce, czy koncercie w kuchni. To w zasadzie tylko smaczki pracy zdalnej – natomiast to co jest szczególnie istotne, to zapewnienie w tych trudnych chwilach bezpieczeństwa powierzonym nam informacjom i urządzeniom.

1.1 Przepisy

Przepisy RODO, ani tym bardziej ustawy o ochronie danych osobowych nie regulują pracy zdalnej. Nie ma zakazu przetwarzania danych osobowych przez pracownika w domu, nie ma również wskazówek jakie środki bezpieczeństwa należy podjąć. **To administrator danych (w tym przypadku pracodawca) decyduje o zasadach jakie obowiązują w tym obszarze**. Co więcej, to **administrator danych ponosi prawną odpowiedzialność za bezpieczeństwo** tych danych osobowych.

Nie oznacza to jednak, że RODO lub Kodeks pracy nie mają tu zastosowania. Również przyjęta u pracodawcy polityka bezpieczeństwa (lub dokumenty analogiczne) będzie obowiązywała. Pracownik musi chronić powierzone mu dane w sposób określony przez pracodawcę. Natomiast niestosowanie się do tych zasad może wiązać się z **odpowiedzialnością dyscyplinarną, roszczeniem regresowym w stosunku do pracownika, a nawet odpowiedzialnością karną.**

Zasad bezpieczeństwa informacji nie można bagatelizować – zwłaszcza w przypadku pracy zdalnej!

1.2 Wewnątrzorganizacyjne regulacje

W związku z tym, że praca zdalna oznacza funkcjonowanie w zupełnie innym środowisku niż wykonywanie obowiązków u pracodawcy – w jego lokalizacji, również zasady bezpieczeństwa mogą być inaczej określone. Jest wysoce prawdopodobne, że regulacje wewnątrzorganizacyjne wskazują szczególne zasady pracy poza obszarem nadzorowanym przez administratora. Możliwe, że wydane zostały specjalne zarządzenia w tym obszarze (np. w związku z wystąpieniem stanu epidemii). **Pracownik zamierzający rozpocząć taką formę pracy musi bezwzględnie zapoznać się z tymi zasadami**!

W regulacjach wewnątrzorganizacyjnych mogą być uregulowane bardzo istotne dla nas kwestie, takie jak: posługiwanie się powierzonym sprzętem (np. laptop) poza siedzibą pracodawcy, zasady dostępu zdalnego do aplikacji i danych, transport i wynoszenie materiałów z firmy.

Ponadto warto przypomnieć sobie zasady, które zapewne obowiązują od dawna – niezależnie od formy pracy. Wśród takich obszarów przede wszystkim należy wymienić **zasady reagowania na incydenty bezpieczeństwa** (kogo i jak informować?) oraz **ogólne zasady bezpieczeństwa i przetwarzania danych osobowych** w organizacji.

Dobrą praktyką jest wyposażenie się w kopię tych zasad lub jeżeli nie jest to możliwe, to samodzielne spisanie podstawowych kwestii, tak aby np. w razie naruszenia wiedzieć kogo należy o tym poinformować… i kiedy mamy do czynienia z naruszeniem.

1.3 Sprzęt służbowy

Do najczęstszych przypadków organizacji pracy zdalnej należy oczywiście udostępnienie pracownikowi komputera służbowego. Taka stacja robocza jest zazwyczaj odpowiednio skonfigurowana, wyposażona w niezbędne do pracy programy, możliwe że zapewnia dostęp do zasobów zewnętrznych poprzez bezpieczny kanał łączności VPN. Sytuacją optymalną jest, kiedy otrzymujemy sprzęt gotowy do pracy.

Należy jednak zachować pewną powściągliwość podczas jego użytkowania:

- **nie powinniśmy na własną rękę instalować na nim oprogramowania** (może to osłabiać system bezpieczeństwa, umożliwić lub ułatwić ataki hackerskie, naruszać zasady licencyjne oprogramowania);
- **komputer powinien być wykorzystywany tylko do pracy** – oglądanie filmów, odwiedzanie portali społecznościowych itp. może być niezgodne z wewnątrzorganizacyjnymi regulacjami pracodawcy;
- jeżeli u pracodawcy wprowadzono takie **formy monitoringu** – może okazać się, że pracodawca będzie na bieżąco śledził nasze poczynania na komputerze służbowym;
- **nasze działania są zapisywane w pamięci komputera** (nawet usunięte pliki są możliwe do odzyskania) **lub konkretnie – w pamięci przeglądarki** (tu można najeść się naprawdę sporo wstydu).

Wszystkie ww. zasady odnoszą się do bezpieczeństwa pracy z wykorzystaniem służbowego sprzętu. Nieprzestrzeganie ich może doprowadzić do incydentu bezpieczeństwa, a nawet naruszenia ochrony danych osobowych.

1.4 Sprzęt prywatny

Jeżeli powierzoną pracę będziemy wykonywać na prywatnym sprzęcie – komputer stacjonarny, laptop – warto należycie się do tego przygotować. Przede wszystkim należy sprawdzić, czy **zainstalowane oprogramowanie (nie tylko to, które posłuży do pracy) jest aktualne**. Aktualizacje często dotyczą luk w bezpieczeństwie, co oznacza, że nieaktualne oprogramowanie może być furtką dla przestępcy, przez którą będzie mógł włamać się do naszego komputera.

W komputerze **powinien być wgrany i uruchomiony program antywirusowy z funkcją zapory ogniowej (tzw. firewall)**. Aby tego rodzaju oprogramowanie było skuteczne, musi posiadać aktualną bazę. To dobry moment by sprawdzić jego aktualność!

Kiedy już mamy pewność, że korzystamy z aktualnych wersji oprogramowania, dobrą praktyką jest wykonanie rutynowego przeglądu: **skan antywirusowy, defragmentacja/czyszczenie dysku**.

Następnie w komputerze **należy wydzielić przestrzeń, która będzie służyła wyłącznie do pracy (partycja dysku lub oddzielny folder plików).** Zapewni to, że pliki służbowe nie zapodzieją się gdzieś wśród prywatnych zasobów i po zakończeniu wykorzystywania prywatnego sprzętu będzie można je skutecznie wyselekcjonować i usunąć. Jeżeli z komputera korzystają również inne osoby (np. dzieci w celu nauki zdalnej) warto **dostęp do wydzielonych części dysku zabezpieczyć hasłem**.

Podczas pracy wskazane jest **nieuruchamianie programów innych niż wykorzystywane do pracy** i weryfikacja czy zbędne oprogramowanie nie działa w tle. Poza tym, że może to spowalniać komputer, jest również potencjalnym osłabieniem systemu bezpieczeństwa.

1.5 Transport: praca – dom – praca

Transport powierzonego sprzętu lub dokumentów jest tylko pozornie czynnością mało istotną. Oczywiście w 99% przypadków nie dzieje się nic złego, jednak aby nie być tym jednym procentem warto przestrzegać poniższych zasad:

- należy **unikać komunikacji miejskiej** – najlepiej skorzystać tego dnia z samochodu prywatnego/służbowego lub poprosić kogoś o podwiezienie. Przejażdżka komunikacją miejską statystycznie znacznie zwiększa ryzyko kradzieży lub zgubienia powierzonych materiałów;
- podczas transportu **nie powinno się wstępować do sklepów lub punktów usługowych**. Doświadczenie pokazuje, że są to częste miejsca zgubienia powierzonych sprzętów lub dokumentów;
- jeżeli mimo wszystko podróżujemy transportem publicznym (kolej, autobus, autokar itp.), traktujmy transportowane materiały jako szczególnie cenne – **nie zostawiajmy ich bez nadzoru**, np. w przedziale w pociągu;
- pamiętajmy też aby **nikt nie miał wglądu ani dostępu do przewożonych przez nas danych osobowych** – należy zadbać o to by nikt nie czytał nam przez ramię, ani nie słuchał naszych służbowych rozmów telefonicznych, telekonferencji).

Ponadto należy pamiętać o zasadach jakie mogły zostać wprowadzone w organizacji. Np. pracodawca mógł zarządzić obowiązek rejestrowania dokumentów wynoszonych z firmy lub wydać dyspozycje co do sposobu transportu ww. materiałów. Pracownicy muszą przestrzegać tych zasad – ich ignorowanie osłabia system bezpieczeństwa i może wiązać się z poważnymi konsekwencjami.

2. Organizacja bezpiecznej pracy

Za organizację pracy w domu *de facto* odpowiada pracownik. Tym samym to na pracowniku spoczywa również obowiązek zapewnienia by informacje, w tym dane osobowe były bezpieczne. Trzeba być świadomym, że podczas pracy zdalnej czyhają nowe, dotąd nieznane zagrożenia. Faktura zjedzona przez psa, kawa wylana na laptopa przez przebiegającego kota, ważne dokumenty pokolorowane przez dzieci, przypadkowe skasowanie jakichś plików przez domownika, który miał dostęp do komputera. To tylko przykładowe incydenty (dotyczące utraty dostępności), jakie mogą przytrafić się podczas pracy w domu. Poufność i integralność danych również jest zagrożona…

2.1. Organizacja miejsca pracy

Wszelkie niezamierzone zniszczenia dokumentów (czasem też elektronicznych) mogą stanowić naruszenie ochrony danych osobowych. Aby tego uniknąć, warto właściwie przygotować miejsce pracy. W tym celu należy zadbać o to by domownicy nie mieli dostępu do naszych służbowych materiałów. Dobrą metodą jest wyobrażenie sobie potencjalnych wypadków jakie mogą się przytrafić, a następnie podjęcie działań minimalizujących, np.: **odkładanie dokumentów w miejsca niedostępne, prowadzenie służbowych rozmów na osobności czy niepracowanie w obecności osób postronnych (goście)**. W praktyce nasze działania będą się koncentrowały na odizolowaniu pracy od życia prywatnego.

2.2. Zasada czystego biurka

Jedną z najprostszych metod podniesienia poziomu bezpieczeństwa danych osobowych jest wdrożenie polityki czystego biurka. Zgodnie z jej zasadami, po zakończeniu pracy **wszelkie dokumenty oraz inne nośniki informacji (np. laptop) powinny być należyci zabezpieczone przed dostępem osób nieuprawnionych**. Innymi słowy, należy schować je do szafy, biurka lub w inne miejsce ograniczające do nich dostęp. Dzięki przestrzeganiu tej zasady, powierzone nam materiały będą bezpieczne, a życie zawodowe oddzielimy od prywatnego. Nie chodzi jedynie o poufność dokumentów (choć też, bo domownicy nie są upoważnieni do przetwarzania tych danych osobowych), ale również o zapewnienie ich dostępności, czyli uchronienie przed ich utratą.

Stosując szerzej tę politykę, również w trakcie pracy powinniśmy **mieć „po ręką" jedynie aktualnie potrzebne materiały**. Jeżeli uczestniczymy w telekonferencji, czy po prostu rozmawiamy przez telefon, należy zadbać o odosobnienie – tak by **domownicy nie uczestniczyli mimowolnie w prowadzonych rozmowach**.

2.3. Zasada czystego ekranu

Drugą metodą zaczerpniętą z norm jakości ISO, jest polityka czystego ekranu. W myśl tej zasady, należy chronić dostęp do systemów informatycznych, w których przetwarzane są dane osobowe. Realizuje się to m.in. poprzez **każdorazowe blokowanie komputera w sytuacji, kiedy choćby na chwilę musimy zostawić go bez naszego nadzoru**. Praktycznym rozwiązaniem jest dodatkowo ustawianie automatycznego wygaszacza ekranu – blokującego komputer po określonym okresie braku aktywności. **Po zakończeniu pracy komputer służbowy należy wyłączyć**.

Ponadto monitor/ekran komputera powinien być ustawiony w sposób uniemożliwiający osobom postronnym podgląd. Należy też rozważyć zmianę haseł, jeżeli korzystamy z komputera prywatnego.

2.4. Korzystanie z Internetu

Główną osią pracy zdalnej jest zazwyczaj praca na komputerze z dostępem do Internetu. Oznacza to, że dotychczasowe zagrożenia z tym związane nadal występują, jednak my mamy ograniczone możliwości otrzymania pomocy w sytuacjach awaryjnych. Jeżeli pracujemy na własnym sprzęcie – pracodawca może nie mieć nawet możliwości zapewnienia nam bezpieczeństwa informatycznego. Dlatego tak ważne jest aby przestrzegać wszystkich zasad korzystania z Internetu i stosować powszechnie znane środki bezpieczeństwa.

Każdorazowo logując się do usług niezbędnych do wykonywania pracy (czasem są to aplikacje zwyczajowo dostępne w sieci wewnętrznej pracodawcy, a na czas pracy zdalnej – wystawione publicznie) **należy upewnić się, że połączenie z daną stroną internetową jest zabezpieczone (szyfrowane)**, tzn. nikt nie będzie mógł przechwycić wpisywanych przez nas haseł. W szczególności dotyczyć to będzie logowania się do poczty lub zasobów wewnętrznych pracodawcy. W tym celu należy weryfikować czy strona posiada wiarygodny certyfikat bezpieczeństwa (informacje w kłódce przy adresie witryny).

W czasie pracy zdalnej należy powstrzymać się od jednoczesnego korzystania z komputera w celach prywatnych. Ograniczenie aktywności na nieprofesjonalnych stronach może uchronić nas przed staniem się ofiarą przypadkowego ataku, którego skutki będą oddziaływały również na dane służbowe.

Jeżeli pracodawca udostępnił nam połączenie z wykorzystaniem kanału VPN, to absolutnie nie powinniśmy tego lekceważyć i każdorazowo powinniśmy korzystać z tej możliwości. **Połączenie VPN zapewnia nam realne podwyższenie poziomu bezpieczeństwa**, a niekorzystanie z dostarczonych mechanizmów może być niezgodne z wewnętrznymi procedurami w organizacji.

2.5. Mejle

Należy pamiętać, że skrzynki mejlowe są najczęstszym źródłem infekowania komputera. Dlatego też pracodawca do celów służbowych zazwyczaj wyposaża swoich pracowników w służbowe konta e-mail. **Za niedopuszczalne należy uznać wykorzystywanie służbowych kont mejlowych do celów prywatnych oraz prywatnych kont mejlowych do wykonywania pracy**. Poza utratą przez pracodawcę kontroli nad bezpieczeństwem informacji narażamy go również – jako administratora danych, na odpowiedzialność z tytułu naruszenia ochrony danych osobowych (usługodawcy dostarczający nam prywatne adresy e-mail nie mają zawartych z naszym pracodawcą umów powierzenia przetwarzania danych osobowych).

Ponadto należy **zachować ostrożność w przypadku otrzymania wiadomości nietypowych, z nieoczekiwanych źródeł, zawierających podejrzane załączniki** (z niewidocznym rozszerzeniem, pliki wykonalne „.exe" lub skompresowane biblioteki danych „..zip", „.rar").

2.6. Inne uwagi

Korzystanie z tzw. mobilnych nośników informacji (pendrive, karty pamięci) wymaga odpowiedniego ich zabezpieczenia. Niezależnie czy jest to nasz prywatny nośnik, czy służbowy – powinien być **zaszyfrowany i zabezpieczony hasłem dostępu**. Dzięki temu, w przypadku kradzieży lub zgubienia, przechowywane na nim dane osobowe będą bezpieczne. Przypadku z ostatnich lat pokazują, że utrata niezaszyfrowanego nośnika informacji może wiązać się z wysokimi karami pieniężnymi.

Ostatnią kwestią wymagającą wspomnienia są portale społecznościowe. Pracodawca oczywiście nie śledzi naszych poczynań na Facebooku czy LinkedIn, jednak nie zmienia to faktu, że powinniśmy w tym obszarze zachować stosowny umiar. **Upublicznianie informacji o zasadach pracy zdalnej lub co gorsza o podatnościach z tym związanych osłabia cały system bezpieczeństwa informacji**. Jeżeli mamy spostrzeżenia dotyczące możliwych ulepszeń, to dużo lepiej jest poinformować o tym pracodawcę niż użytkowników portalu społecznościowego.

3. Podsumowanie

Podsumowując najważniejsze rekomendacje z poradnika otrzymujemy poniższą listę dobrych praktyk:

1. Należy zapoznać się z regulacjami wewnątrzorganizacyjnymi, w tym m.in. z zasadami reagowania na incydenty bezpieczeństwa i zasadami związanymi z pracą zdalną.
2. Podczas pracy na komputerze służbowym:
    - nie powinniśmy na własną rękę instalować oprogramowania,
    - komputer powinien być wykorzystywany tylko do pracy,
    - pamiętajmy o stosowanych formach monitoringu – nasze działania są zapisywane w pamięci komputera.
3. Praca na komputerze prywatnym wymaga:
    - oprogramowania antywirusowego,
    - aktualizacji oprogramowania,
    - wydzielenia przestrzeni na dysku – zabezpieczonej hasłem.
4. W ramach transportu materiałów:
    - unikajmy transportu publicznego,
    - nie zbaczajmy z trasy do sklepów/punktów usługowych,
    - zachowajmy wzmożoną ostrożność.
5. Podczas pracy w domu należy odkładać dokumenty w miejsca niedostępne dla domowników, służbowe rozmowy prowadzić na osobności, unikać pracy w obecności osób postronnych (goście), każdorazowo odchodząc od komputera – wylogowywać się.
6. Jeżeli jest taka możliwość, należy korzystać z kanałów VPN.
7. Za niedopuszczalne należy uznać wykorzystywanie służbowych kont mejlowych do celów prywatnych oraz prywatnych kont mejlowych do wykonywania pracy.
8. Wszelkie nośniki informacji (pendrive, karta pamięci) powinny być szyfrowane i zabezpieczone hasłem.
9. Nie należy upubliczniać informacji o organizacji pracy zdalnej.

Powodzenia!

Mateusz Siek