EKRAN®

MONITORING PRACOWNIKÓW ZDALNYCH

CO ZROBIĆ, ABY PRACA ZDALNA BYŁA EFEKTYWNA I BEZPIECZNA

W artykule znajdziesz:

- 5 najczęstszych mitów na temat pracy zdalnej
- Obawy związane z pracą zdalną
- Najlepsze praktyki w zakresie monitorowania pracowników zdalnych

SECURIVY

O PRACY ZDALNEJ

Specjaliści do spraw cyberbezpieczeństwa słusznie uważają, że praca zdalna to pole niosące ze sobą potencjalne zagrożenia oraz naruszenia zasad bezpieczeństwa. Jednak praca zdalna nie jest chwilowym trendem, który za chwilę nas opuści, a wręcz przeciwnie – model ten zostanie z nami na dłużej, dlatego też postanowiliśmy przyjrzeć się mu bliżej. Według badań sporządzonych przez US Bureau of Labor Statistics, między 2017 a 2018 rokiem, aż 36 milionów (25%) pracowników z USA przyznało, że zdarzało im się pracować z domu. Dla wielu specjalistów możliwość pracy zdalnej to również ważny aspekt, który uwzględniają podczas wyboru pracodawcy. Ponadto zdalny dostęp do zasobów firmy potrzebny jest podczas wyjazdów służbowych, korzystania z usług dostawców zewnętrznych oraz w sytuacjach awaryjnych, takich jak pandemia, problemy z transportem lub załamania pogodowe.

W takich sytuacjach kierownicy działów IT powinni być przygotowani do zapewnienia efektywnego sposobu monitorowania wszystkich pracowników oraz zagwarantowania bezpiecznego i zdalnego dostępu do firmowych zasobów. Kontrola pracowników jest bardzo ważnym aspektem każdej firmy - zwłaszcza w warunkach domowych, w których niektórzy z nich mogą być rozpraszani przez inne obowiązki, a co za tym idzie, pracować mniej efektywnie.

W tym artykule przyjrzymy się bliżej powszechnym mitom dotyczącym pracy zdalnej, a także przeróżnym cyberzagrożeniom, które ze sobą niesie oraz narzędziom i najlepszym praktykom zarządzania w przypadku pracowników na home office.

5 MITÓW NA TEMAT PRACY ZDALNEJ

Istnieje wiele fałszywych przekonań dotyczących pracy zdalnej.

Szereg pracodawców waha się przed pozwoleniem na pracę z domu, ponieważ uważają, że w takich warunkach jest ona nieefektywna, kosztowna oraz niepewna. Jednak statystyki dowodzą, że takie przekonania są w dużej mierze nieprawdziwe. Spójrzmy zatem na fakty dotyczące pracy zdalnej, które można poprzeć licznymi badanami.



MIT 1 - Pracownicy pracują mniej, gdy są poza biurem

Niektórzy managerzy uważają, że pracownicy przestają pracować, jeśli nie są pod stałą kontrolą. Mają ku temu powody, ponieważ będąc w domu, można o wiele łatwiej zostać rozproszonym przez social media lub inne czynniki zewnętrzne.

Uniwersytet w Stanford przeprowadził dwuletnie badania, które miały na celu sprawdzenie, czy pracownicy zdalni rzeczywiście pracują mniej. W ramach eksperymentu stwierdzono, że pracownicy biurowi, po rozpoczęciu pracy w formie zdalnej, wykazali znaczny wzrost wydajności. Ponadto artykuł "Stan pracy zdalnej 2019" ze strony Buffer zwrócił uwagę na fakt, że aż 22% pracowników ma problem z zaprzestaniem pracy po godzinach. Trzeba jednak pamiętać, że są również osoby, które nie potrafią wystarczająco skupić się, pracując z domu. Właśnie dlatego popularną praktyką jest wdrażanie programów mierzących i monitorujących czas pracy, w celu analizy i zwiększenia wydajności pracowników.

MIT 2 – Praca zdalna głównie na potrzeby podróżowania

Na Instagramie oraz innych mediach społecznościowych można znaleźć setki zdjęć i postów, które pokazują pracę zdalną jako leżenie na plaży lub podróżowanie do różnych krajów i miast. Trudno wyobrazić sobie, że prowadząc taki styl życia, można być produktywnym.

Jednak ten obraz jest mocno naciągany. Odnosząc się do danych ze strony Buffer, aż 84% pracowników zdalnych wykonuje swoją pracę z domu, tylko czasem zmieniając swoje środowisko pracy np. na lokalną kawiarnię. Zaledwie 3% regularnie pracuje poza miastem.

MIT 3 - Praca zdalna jest dla małych firm i startupów

Ten mit jest częściowo prawdziwy: rzeczywiście, praca zdalna jest bardziej korzystna cenowo niż wynajmowanie biura przez małe firmy oraz startupy. Jednak również sporo dużych organizacji oferuje pracę zdalną (lub częściowo zdalną), jako korzyść dla pracowników.

Poza tym sytuacja związana z koronawirusem pokazała, że firmy takie jak Oracle, Amazon, Microsoft, Google, Twitter, czy nawet NASA, w łatwy sposób mogą zmienić swój tryb pracy na zdalny zaledwie w ciągu kilku dni.

MIT 4 – Pracownicy zdalni czują się samotni i wykluczeni

Dla osób, które przyzwyczajone są do rozmów ze współpracownikami, wizja pracy z domu może wydawać się niczym izolacja społeczna. Warto pamiętać, że komunikacja z członkami zespołu nie musi kończyć się w momencie znajdowania się poza biurem.

Powołując się na wyniki ankiety TINYpulse, 52% pracowników zdalnych rozmawia ze swoim managerem codziennie. Z kolei badanie przeprowadzone przez platformę TalentLMS pokazuje, że kiedy pracownicy zdalni naprawdę czują się samotni, to aż 43% z nich wykorzystuje komunikatory internetowe, aby porozmawiać ze swoimi zespołem, a 37% odwiedza biuro.

MIT 5 – Wprowadzenie pracy zdalnej jest niepewne i kosztowne

Wprowadzenie bezpiecznego i szybkiego dostępu zdalnego rzeczywiście wymaga zakupu dedykowanych rozwiązań z zakresu cyberbezpieczeństwa. Należą do nich:

- wirtualne sieci prywatne
- firewalle
- oprogramowania monitorujące komputery
- urządzenia do mierzenia czasu pracy

Mimo to, ich zakup wiąże się ze znacznie mniejszym kosztem, niż wynajem biura wraz z dostosowaniem go do pracy.

Firmy biorące udział we wspomnianym wcześniej badaniu, przeprowadzonym przez Uniwersytet w Stanford, jednogłośnie przyznały, że dzięki wprowadzeniu pracy zdalnej, zaoszczędziły 2000 dolarów w skali rocznej na wydatkach biurowych na każdego zatrudnionego pracownika.

Praca zdalna przynosi korzyści również pracownikom, którzy rocznie mogą zaoszczędzić do 7000 dolarów na codziennych dojazdach do biura. Jednakże obawy związane ze zdalnym dostępem i kwestiami cyberbezpieczeństwa słusznie budzą niepokój. W dalszej części artykułu omówimy główne zagrożenia wynikające z pracy zdalnej i przedstawimy sposoby na ich ograniczenie.

PRACA ZDALNA W LICZBACH

OBAWY ZWIĄZANE Z PRACĄ ZDALNĄ

Zdalne połączenia znane są jako zagrożenia dla bezpieczeństwa cybernetycznego. Z badań OpenVPN wynika, że aż 73% liderów z branży IT uznaje pracowników zdalnych za potencjalnie bardziej niebezpiecznych od osób pracujących na miejscu.

Głównym powodem takich przekonań jest fakt, że pracownicy zdalni mają dostęp do zasobów firmowych, jednocześnie będąc poza standardowym obwodem bezpieczeństwa cybernetycznego firmy. Dodatkowo brak wiedzy oraz odpowiedniej ochrony komputerów sprawia, że dane, do których dostęp mają pracownicy zdalni, są bardziej narażone na ataki hakerskie oraz naruszenia.

NAJCZĘSTSZE ZAGROŻENIA SPRAWIANE PRZEZ PRACOWNIKÓW ZDALNYCH TO:

1. Używanie publicznej sieci WiFi

Połączenie z publiczną siecią WiFi nie wymaga autoryzacji, przez co podczas jej użytkowania haker może przechwycić przesyłane dane oraz naruszyć inne zasoby firmowe, takie jak wiadomości e-mail lub dane logowania.

2. Korzystanie z prywatnych urządzeń do wykonywania pracy

Stacje robocze pracowników na ogół zabezpieczane są dedykowanym programem antywirusowym, firewallem oraz algorytmem szyfrującym.

W związku z tym, dla pracownika zdalnego, najlepszym rozwiązaniem jest używanie firmowego laptopa lub instalacja specjalnego oprogramowania na prywatnym komputerze, tak aby wszystkie dane były odpowiednio chronione. Niestety zdarza się, że niektórzy pracownicy zdalni mogą mieć pokusę, aby korzystać z firmowego laptopa do celów osobistych, dzielić się nim z członkami rodziny lub używać całkiem innego urządzenia do wykonywania swoich obowiązków służbowych, które nie jest odpowiednio zabezpieczone.

3. Brak świadomości na temat wagi cyberbezpieczeństwa

Oprócz oprogramowania chroniącego komputer, pracownicy zdalni powinni mieć wiedzę na temat tego, w jaki sposób odpowiednio go używać oraz dlaczego jego instalacja jest aż tak istotna. Bez tych informacji mogą oni bowiem zignorować środki bezpieczeństwa, tak aby usprawnić i przyśpieszyć swoją pracę. Dla przykładu, wiele organizacji używa połączeń VPN z ograniczonym przesyłem danych i określoną liczbą połączeń, które mogą spowalniać pracę. Z tego właśnie powodu niektórzy pracownicy wyłączają VPN, gdy to tylko możliwe.

4. Podatność na ataki socjotechniczne

Phishing, smishing, pretexting oraz inne ataki są realnym zagrożeniem dla wszystkich zdalnych pracowników. Kiedy w nagłych przypadkach, bez uprzedniego przygotowania sprzętu, pracodawcy pozwalają na home office, często zauważa się znaczny wzrost cyberataków kierowanych na pracowników zdalnych. Doskonałym przykładem są incydenty, które miały miejsce podczas pandemii koronawirusa. Brak odpowiedniego zabezpieczenia sprzętu oraz przeszkolenia pracowników w zakresie cyberbezpieczeństwa sprawia, że pracownicy zdalni mogą być łatwym celem dla hakerów.

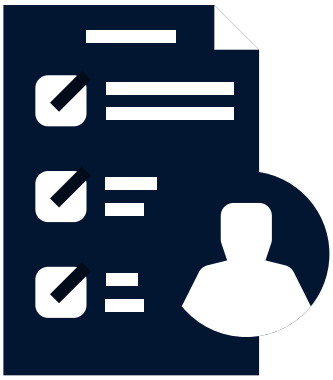
5. Brak narzędzi autoryzacji i kontroli dostępu

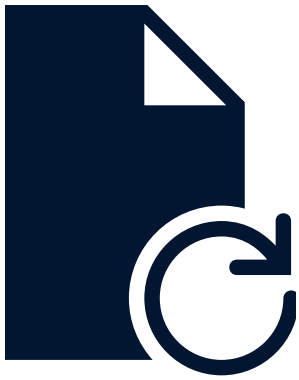
Kradzież dostępu do danych biznesowych, jest o wiele łatwiejsza w przypadku pracowników zdalnych, niż osób pracujących w biurze. Pomimo licznych statystyk i potwierdzających je sytuacji, wiele firm nadal nie korzysta z uwierzytelniania dwuskładnikowego oraz jakichkolwiek form zabezpieczania dostępu.

6. Używanie niezaktualizowanego oprogramowania

Mało osób lubi aktualizować swój komputer na bieżąco, ponieważ zajmuje to zbyt dużo czasu, zakłóca rytm pracy i wiąże się z potrzebą przyzwyczajenia się do nowej wersji oprogramowania. Jednak wychodzące aktualizacje w dużej mierze skupiają się na naprawianiu błędów w zakresie bezpieczeństwa, dlatego też ważne jest bieżące aktualizowanie sprzętu.

Właśnie z tego powodu większość przezornych administratorów IT może wymagać regularnego aktualizowania oprogramowań, zwłaszcza na punktach końcowych. Mimo zaleceń, pracownicy zdalni często je bagatelizują i niechętnie się do nich stosują. Wykorzystywanie luk w przestarzałym oprogramowaniu stanowi jeden z najbardziej efektywnych sposobów na kradzież danych przez hakerów.





7. Naruszenia danych biznesowych

Przeważnie pracownicy zdalni oraz biurowi mają ten sam poziom dostępu do danych biznesowych. Nie są oni jednak tak samo kontrolowani przez zespół IT, który skupia się przede wszystkim na osobach pracujących na miejscu. Właśnie dlatego pracownicy zdalni mogą stać się źródłem wewnętrznych ataków i doprowadzić do kradzieży danych czy wykorzystywania poufnych informacji na własne potrzeby.

8. Odpoczynek zamiast pracy

Wielu pracowników jest produktywnych, zarówno w biurze, jak i w domu. Niektórzy z nich są jednak zdecydowanie mniej efektywni na home office.

Często wynika to z braku kontroli menadżera, który pilnuje, aby pracownik pozostał skupiony na swoich zadaniach. Tacy pracownicy mogą się szybko rozpraszać lub wykonywać inne nieproduktywne czynności w czasie swojej pracy, takie jak sprzątanie, granie w gry czy używanie social mediów. Bez wdrożenia odpowiedniego oprogramowania monitorującego komputer trudno jest ocenić, czy dana osoba przebywająca na home office naprawdę pracuje.

OBAWY ZWIĄZANE Z PRACĄ ZDALNĄ

1. **Używanie publicznych sieci WiFi**
2. **Używanie prywatnych urządzeń do pracy**
3. **Brak świadomości wagi cyberbezpieczeństwa**
4. **Podatność na ataki socjotechniczne**
5. **Brak narzędzi autoryzacji i kontroli dostępu**
6. **Używanie nieaktualnego oprogramowania**
7. **Naruszenia danych biznesowych**
8. **Odpoczynek zamiast pracy**

Warto zatem pamiętać, że wdrożenie odpowiednich i sprawdzonych praktyk w zakresie cyberbezpieczeństwa oraz monitorowania pracowników zdalnych może pozytywnie wpłynąć na ich produktywność i skutecznie zabezpieczyć firmową infrastrukturę. W dalszej części artykułu dokonamy przeglądu sprawdzonych metod, które pozwolą zabezpieczyć zdalne połączenia i monitorować efektywność pracowników.

NAJLEPSZE PRAKTYKI W ZAKRESIE MONITOROWANIA PRACOWNIKÓW ZDALNYCH

Przygotowaliśmy listę, która pokazuje, jak w skuteczny sposób monitorować pracowników zdalnych oraz zabezpieczyć ich pracę. Część z naszych porad ma charakter organizacyjny, z kolei inne wymagają specjalistycznego oprogramowania do zdalnego monitorowania, takiego jak Ekran System.

1. Stwórz politykę zdalnego dostępu
2. Poinformuj swoich pracowników o atakach socjotechnicznych
3. Zabezpiecz połączenia zdalne, przy pomocy VPN
4. Egzekwuj wieloczynnikowe uwierzytelnianie
5. Ogranicz współdzielone konta lub wprowadź dodatkowe uwierzytelnianie
6. Monitoruj i rejestruj aktywność użytkowników
7. Kontroluj produktywność pracowników
8. Ustaw powiadomienia o podejrzanych i niepożądanych działaniach
9. Zarządzaj dostępem i poufnymi danymi

1. Stwórz politykę zdalnego dostępu, która będzie obejmować:

- Listę oprogramowań i środków kontroli dostępu
- Instrukcje zdalnego łączenia się do sieci
- Środki ochrony danych uwierzytelniania
- Warunki, które muszę zostać spełnione, aby zezwolić pracownikom na przejście w tryb pracy zdalnej (jeśli firma przez większość czasu nie pracuje zdalnie)

Upewnij się, że pracownicy znają te zasady i mają do nich stały dostęp,
a w razie jakichkolwiek wątpliwości, są w stanie uzyskać odpowiedzi na wszystkie pytania.

2. Poinformuj swoich pracowników o atakach socjotechnicznych

Do skutecznych ataków hakerskich bardzo często dochodzi z powodu nieuwagi pracownika oraz pośpiechu. Dlatego właśnie tak ważna jest edukacja w tym zakresie. Poinformuj pracowników o wadze cyberbezpieczeństwa i incydentach, które miały miejsce w ostatnim czasie.

3. Zabezpiecz połączenia zdalne, przy pomocy VPN

Dzięki takiemu rozwiązaniu można stworzyć bezpieczne połączenie między pracownikiem zdalnym a siecią firmową, które chronione jest za pomocą algorytmu szyfrującego i uwierzytelniania. VPN skutecznie zabezpieczy firmę w przypadku korzystania z niezaufanych i niezabezpieczonych sieci takich jak publiczne WiFi.



4. Egzekwuj wieloczynnikowe uwierzytelnianie

Uwierzytelnianie wieloskładnikowe pozwala na skuteczne weryfikowanie osób, które próbują połączyć się z siecią firmową lub zyskać dostęp do danych biznesowych. Ekran System uwierzytelnia użytkowników poprzez wysłanie jednorazowego hasła na telefon, zmniejszając tym samym ryzyko uzyskania dostępu przez niepożądane osoby.

5. Ogranicz współdzielone konta lub wprowadź dodatkowe uwierzytelnianie

Używanie wspólnych profili, zwłaszcza w przypadku kont administratorów, to duże uproszczenie dla pracowników. Niestety znacznie utrudnia ono powiązanie naruszeń cybernetycznych z konkretnym użytkownikiem. Wielu specjalistów IT blokuje możliwość zakładania takich kont, a jeśli nie mogą tego zrobić, to decydują się na użycie dodatkowego uwierzytelniania, które pozwala im powiązać konkretnego użytkownika ze współdzielonym kontem.

6. <u>Monitoruj i rejestruj aktywność użytkowników</u>

Monitorowanie działań na komputerach pracowników pozwala pracodawcy kontrolować efektywność i sprawować piecze nad poufnymi danymi. Oprogramowanie monitorujące Ekran System dostarcza takie informacje jak:

- Nagrania aktywności użytkownika
- Wejście i wyjście audio
- Naciśnięte klawisze
- Otwierane pliki oraz foldery
- Wykonywane komendy
- Oraz wiele innych

Korzystanie z oprogramowania Ekran System pozwala monitorować komputer, nawet jeśli nie jest on w danym momencie połączony z Internetem. Dzięki generowanym informacjom oraz zapisom konkretnych sesji, z łatwością będziesz znał kontekst wszystkich działań, które w razie potrzeby, będziesz mógł wykorzystać na potrzeby sądowe.



7. Kontroluj produktywność pracowników

Klasyczne aplikacje do mierzenia czasu nie dostarczają adekwatnych informacji, na temat aktywności użytkowników. Zaawansowane programy monitorujące zbierają szczegółowe dane dotyczące efektywności poszczególnych osób oraz czynności wykonywanych w czasie pracy. Analiza otwieranych plików, folderów, aplikacji, stron internetowych i nagrania ekranu, pozwalają skutecznie zweryfikować produktywność pracowników oraz sprawdzić, czy w czasie pracy nie przeglądają oni prywatnych wiadomości lub nie korzystają z serwisów społecznościowych.

Dobrą praktyką jest również organizowanie cotygodniowych lub comiesięcznych spotkań, podczas których pracownicy zdalni, zdają raporty dotyczące wykonanych w danym okresie zadań.

8. Ustaw powiadomienia o podejrzanych i niepożądanych działaniach

Alerty w czasie rzeczywistym informują o potencjalnym zagrożeniu oraz naruszeniu zasad bezpieczeństwa wewnątrz infrastruktury firmowej. Takie powiadomienie, wraz z linkiem do konkretnej sesji, umożliwia szybką reakcję administratorów i managerów na potencjalnie niebezpieczne incydenty. Powiadomienia tego typu pozwalają powstrzymać niepożądane działania. Prewencja zagrożeń, jest zdecydowanie lepszym rozwiązaniem niż radzenie sobie z ich konsekwencjami. W zakresie bezpieczeństwa wewnętrznego Ekran System:

- Powiadamia użytkownika o naruszeniu odgórnych reguł
- Blokuje niepożądane działania
- Blokuje użytkownika

9. Zarządzaj dostępem i poufnymi danymi

Przez wspomniane wcześniej powody, pracownicy zdalni są zdecydowanie bardziej podatni na kradzież danych biznesowych lub dostępów. Aby rozwiązać ten problem, można wdrożyć aplikację zarządzającą hasłami. Menadżer haseł pozwala na tworzenie, przechowywanie, przesyłanie oraz rotację loginów i haseł, dzięki czemu użytkownicy mogą korzystać z plików i aplikacji w bezpieczny sposób. Poza ochroną poświadczeń logowania, Ekran System pozwala również zarządzać hasłami Active Directory, kluczami SSH/Telnet oraz dostępem do baz danych MS SQL oraz aplikacji Web.

Poniższa grafika podsumowuje, w jaki sposób możemy załagodzić zagrożenia związane z pracą zdalną, dzięki wymienionym praktykom oraz narzędziom.

ZAGROŻENIE	ROZWIĄZANIE
Podatność na ataki socjotechniczne	Edukuj o atakach socjotechnicznych Monitoruj i nagrywaj aktywność użytkowników
Brak narzędzi autoryzacji i kontroli dostępu	Wprowadź uwierzytelnianie wieloskładnikowe Ogranicz współdzielone konta
Używanie niezaktualizowanych oprogramowań	Stwórz politykę zdalnego dostępu Zarządzaj dostępem i poufnymi danymi
Naruszenia danych biznesowych	Stwórz politykę zdalnego dostępu Monitoruj i nagrywaj aktywność użytkowników
Odpoczynek zamiast pracy	Kontroluj efektywność pracowników Monitoruj i nagrywaj aktywność użytkowników

WNIOSKI

Pracownicy zdalni mogą być równie zaangażowani, jak pracownicy biurowi, dzięki regularnemu kontaktowi ze swoim managerem. Ponadto pozwalają firmie zaoszczędzić na kosztach związanych z czynszem i utrzymaniem biura. Dodatkowo warto pamiętać, że niektóre osoby pracujące na home office bywają nawet bardziej efektywne niż te pracujące na miejscu.

Równocześnie należy wziąć pod uwagę także kwestie cybernetyczne, które są ściśle związane z pracą zdalną. Przygotowanie swojej firmy i pracowników do przejścia na home office jest istotnym elementem. Wdrożenie odpowiednich środków ochrony stanowi jeden z pierwszych kroków. Warto pamiętać, że nawet jeśli Twoja firma zatrudnia pracowników na miejscu, to zawsze mogą zdarzyć się momenty, w których będą oni musieli pracować zdalnie. Do takich sytuacji najlepiej przygotować się z odpowiednim wyprzedzeniem, aby sprawnie zapewnić bezpieczny dostęp zdalny.

W naszym artykule przedstawiliśmy główne zagrożenia, z którymi wiąże się praca zdalna. Część z nich może zostać skutecznie ograniczona poprzez wprowadzenie odpowiednich zasad cyberbezpieczeństwa oraz regularną edukację pracowników z tego zakresu.

Jednakże, aby zapewnić najwyższy poziom ochrony oraz transparentności działań, warto wdrożyć zaawansowane oprogramowanie monitorujące, takie jak Ekran System, dzięki któremu można m.in. kontrolować efektywność pracowników, ale także dodatkowo zabezpieczyć firmową infrastrukturę.

Ekran System pozwala nie tylko weryfikować tożsamość użytkowników, zarządzać ich dostępem (w tym także dostępem użytkowników uprzywilejowanych), ale również monitorować aktywność każdego użytkownika, niezależnie od tego, czy łączy się on z firmową siecią, czy pracuje zdalnie. Oprogramowanie Ekran System to uniwersalne rozwiązanie, które nie obciąża procesora, a jego wdrożenie zajmuje zaledwie kilkanaście minut, niezależnie od skali wdrożenia.