# JAK ZABEZPIECZYĆ PRACĘ ZDALNĄ W TWOJEJ FIRMIE? POZNAJ NAJLEPSZE PRAKTYKI!

## TO WARTO ROBIĆ

### Edukuj i szkól pracowników w zakresie bezpieczeństwa (jak i potencjalnych zagrożeń) IT

Pomóż pracownikom zrozumieć, że jako części firmy, mają duży wpływ na jej bezpieczeństwo.
Pokaż i wytłumacz, w jaki sposób ich działania, często bardzo proste, mogą podnieść poziom bezpieczeństwa IT w Waszej organizacji. Zaprezentuj im także, jakie konsekwencje przyniosą firmie nierozważne decyzje związane z nieprzestrzeganiem ustalonych reguł i przymykanie oka na niedopełnianie procedur.

Należy pamiętać, że nawet najlepsze rozwiązanie technologiczne musi być odpowiednio wykorzystywane i wspierane przez działania użytkowników, czyli Twoich pracowników.

### Stwórz politykę zdalnego dostępu

Do odpowiedniego funkcjonowania firmy potrzeba zasad, prawda? Reguły ułatwią przystosowanie się do nowych, zdalnych warunków pracy, a przy tym będą pełniły funkcję spisu wszystkich potrzebnych oprogramowań np. do komunikacji czy łączenia się z firmową siecią za pomocą VPN. Tylko od Ciebie i Twojego zespołu zależy, jakie informacje znajdą się w Waszym dokumencie. Pamiętaj, że przede wszystkim ma on ułatwić Wam pracę i w przejrzysty sposób określić zasady pracy zdalnej.

SECURIVY

## Wprowadź kilkustopniową weryfikację podczas logowania pracowników

Obecnie logując się do popularnych portali społecznościowych, a tym bardziej do skrzynek mailowych, czy kont bankowych, możemy skorzystać z funkcji 2-Factor Authentication (2FA), więc dlaczego nie wprowadzić tego z pozoru prostego mechanizmu do usprawnienia zabezpieczeń w Twojej firmie? Logowanie dwuetapowe nie tylko dodaje kolejną warstwę zabezpieczeń, ale i pozwala upewnić się, że Twój pracownik jest tym, za kogo się podaje.

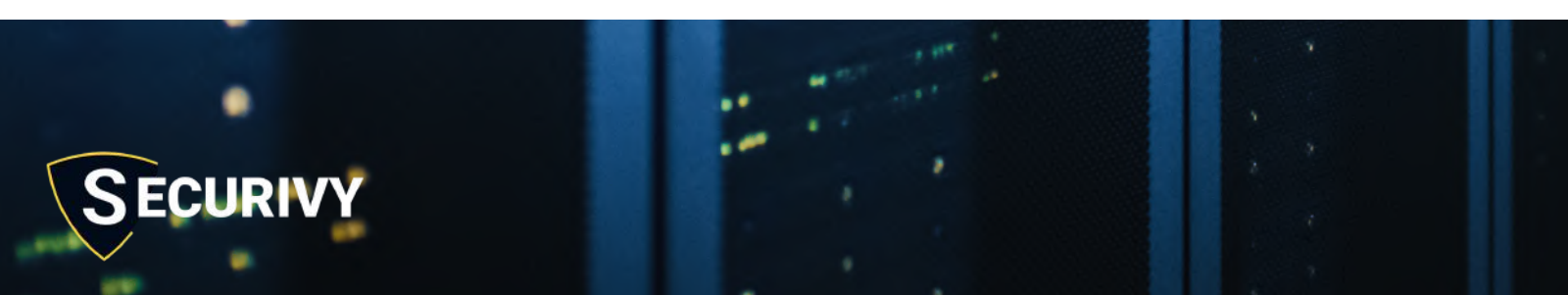
## Zapewnij pracownikom dostęp do najlepszych narzędzi ułatwiających pracę zdalną

Bezpieczeństwo IT często kojarzy się z dużymi inwestycjami, na które zazwyczaj nie mogą pozwolić sobie mniejsze firmy, ale czy to oznacza, że nie są narażone na potencjalne niebezpieczeństwo?

Dane klientów, raporty oraz różnego rodzaju projekty to jedne z najcenniejszych zasobów Twojej firmy, dlatego ich odpowiednie zabezpieczenie jest istotne bez względu na wielkość przedsiębiorstwa. Przejście na pracę zdalną wymaga od pracowników dostępu do firmowych zasobów z domu, a także wypracowania systemu przesyłania plików i danych czy sprawnej komunikacji. Upewnij się, że każdy z nich ma odpowiednio skonfigurowany VPN, zainstalowane wybrane wcześniej narzędzia, a co najważniejsze, wie jak z nich korzystać.

## Zabezpiecz swoją firmową sieć

Skupienie się na zabezpieczeniu poszczególnych komputerów, na których pracują Twoi pracownicy, jest ważne, ale tak samo istotne jest całościowe zabezpieczenie firmowej sieci. Upewnij się, że żaden spam, złośliwe oprogramowania typu malware lub ransomeware nie przedostanie się przez firewall, a wszystkie oprogramowania zabezpieczające będą aktualizowane na bieżąco (w tym celu także edukuj swoich pracowników).



## Zaplanuj przejrzyste działania... na przyszłość!

Wszystkie decyzje, które podejmujesz, zaowocują, dlatego priorytetem zawsze jest zapewnienie firmie bezpiecznej przyszłość. Planując jej rozwój, ale i udoskonalając rozwiązania technologiczne, także te związane z IT, decydujesz się na długoterminowe inwestycje, które pomogą odnieść Tobie i Twojemu zespołowi jeszcze większy sukces. Nie wahaj się z zasięgnięciem konsultacji u specjalistów IT lub testowania różnych dostępnych na rynku rozwiązań — znajdź to, co najlepiej będzie sprawdzało się w Twojej firmie i nie martw się o przyszłość.

# Chcesz wiedzieć więcej? Poznaj Securivy!

**UMÓW SIĘ NA INDYWIDUALNĄ PREZENTACJĘ ONLINE**

**SKONTAKTUJ SIĘ Z NASZYM KONSULTANTEM POD NUMEREM tel. +48 722 158 258**

**ODWIEDŹ SECURIVY.COM**

**MOŻESZ TEŻ SPRAWDZIĆ NASZE SOCIAL MEDIA, GO AHEAD :)**