

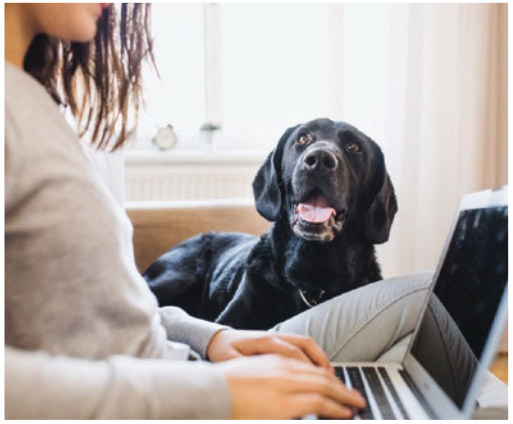

# Biznes w czasie COVID-19: Planowanie ciągłości i bezpieczeństwa

WatchGuard®

# WPROWADZENIE

W czasie, gdy społeczeństwo zmaga się z poważną pandemią, nowy Coronavirus (COVID-19) oddziałuje na prawie wszystkich ludzi na całym świecie. Szkoły są zamknięte, podróże są ograniczone, wydarzenia są odwoływane. Także biura pustoszeją — wszystko to w celu zahamowania rozprzestrzeniania się wirusa. Wielu pracowników rozpoczęło przygodę z  pracą zdalną. Obecnie więcej ludzi pracuje w swoich domach niż kiedykolwiek w historii.

W samych Stanach Zjednoczonych liczba osób pracujących zdanie wzrosła o 150% w okresie od 2005 do 2017 roku. Można śmiało przypuszczać, że obecnie liczba ta jest wielokrotnie wyższa. Chociaż wielu pracowników mogłoby korzystać z możliwości z pracy zdalnej od dawna, to obecna sytuacja jest bezprecedensowa. Jak zatem przygotować przedsiębiorstwo do zmiany panujących zasad, a nową sytuację przekuć na liczne korzyści? I przede wszystkim, jak zorganizować pracę, tak by zachować wszystkie standardy bezpieczeństwa, o które zadbaliśmy w środowisku biurowym? W tym eBooku nakreślimy strategie utrzymania ciągłości biznesowej podczas epidemii.

# COVID-19 LANDSCAPE ANALYSIS:
# Bieżące zagrożenie dla ciągłości biznesu

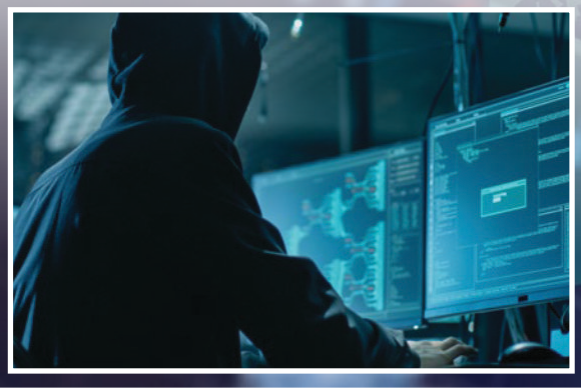
Cyberprzestrzeń codziennie stawia nas w obliczu pewnego zagrożenia. Praca zdalna, która stała się dla wielu z pracowników codziennością, zwiększa szanse na to, że padniemy ofiarą cyberataku. Brak narzędzi zapewniających bezpieczeństwo w firmowej sieci sprawia, że normalne czynności związanie z zadaniami służbowymi nie mogą być nadzorowane przez administratora sieci lub oficerów bezpieczeństwa.

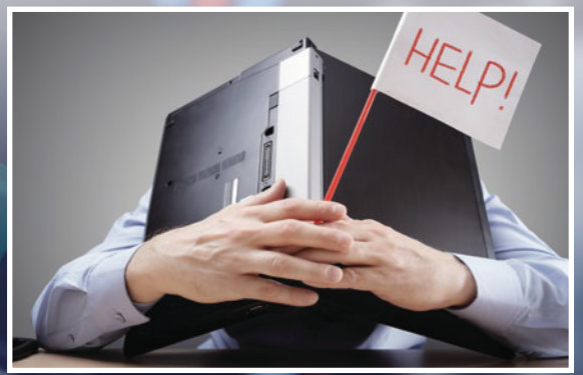
## Hakerzy wykorzystują lęki przed koronaawirusami

Wygląda na to, że hakerzy są skłonni wykorzystać każdą okoliczność do przeprowadzenia swoich ataków. W czasach wzmożonego strachu, e-maile i serwisy społecznościowe Twoich pracowników są zalewane wiadomościami, komentarzami, filmami wideo i linkami prowadzącymi dō materiałów poświęconych Covid-19. Niestety, cyberprzestępcy wykorzystują potrzebę zdobycia informacji na temat pandemii i strach, aby wyłudzać informacje od użytkowników, hakować ich systemy lub dostarczać złośliwe oprogramowanie.

**Oto tylko kilka przykładów na to, jak twórcy zagrożeń wykorzystują zamieszania związane z koronawirusem:**

- **Podszywanie się pod Światową Organizację Zdrowia (WHO)**. Światowa Organizacja Zdrowia (WHO) zgłosiła podejrzane wiadomości phishingowe, które podszywały się pod organizację i miały na celu wyłudzenie wrażliwych informacji dotyczących zdrowia. Ofiary zostały poproszone o kliknięcie linku, pobranie pliku lub podanie poufnych informacji.
- **Dostarczanie złośliwego oprogramowania.** Grupa hakerów wykorzystała pandemię wirusa do zainfekowania ofiar w Mongolii nieznanym wcześniej złośliwym oprogramowaniem, w ramach niedawno odkrytej kampanii zwanej „Vicious Panda".
- **Spam rozprzestrzeniający Trojana Emotet.** Hakerzy kuszą pozornie pomocnymi informacji o tym, jak zapobiec rozprzestrzenianiu się koronawirusa wśród użytkowników w Japonii, w ramach kampanii spamowej mającej na celu wprowadzenie trojana Emotet. Emotet jest zdolny do przejmowania kontroli nad kontami e-mail i rozsyłania wiadomości.
- **Fałszywe aplikacje do śledzenia zasięgu koronawirusa.** Aplikacja maskuje się jako mapa aktualizowana na bieżąco mapa potwierdzonych przypadków zachorowań. W rzeczywistości jest to ransomware, który szyfruje dane na telefonie ofiary. Aplikacja „COVID19 Tracker" infekuje urządzenie i żąda przekazania okupu w wysokości 100 dolarów (w Bitcoinach) w ciągu 48 godzin.



## Zdalni pracownicy

Sytuacja zagrożenia COVID-19 doprowadziła do zmiany przyzwyczajeń tysięcy pracowników, stawiając ich w nowej dla nich sytuacji. Wiele firm boryka się z trudnościami w zapewnieniu osobom pracującym w domu bezpiecznego środowiska. Najczęściej pracownicy otrzymują do domu laptopy, które będą działać wyłączone z firmowej sieci. Również po ponownym podłączeniu do sieci za pośrednictwem VPN lub po powrocie do biura należy upewnić się, że nie padły one ofiarą złośliwego oprogramowania i innych zagrożeń.

## Sieci VPN są przeciążone

W ciągu jednego tygodnia odnotowano 50% wzrost wykorzystania usług VPN. Prognozuje się, że w samych Stanach Zjednoczonych, wykorzystanie VPN wzrośnie o 150% do końca kwietnia 2020. Nagła migracja użytkowników z firm do biur domowych spowodowała, że wiele firm zaczęło korzystać z licencji VPN dla swoich pracowników. Ryzyko polega na tym, że bez łączności VPN użytkownicy nie będą mieli dostępu do potrzebnych im zasobów lub będą korzystać z niepewnych połączeń, aby uzyskać do nich dostęp.

## Szerokość pasma Bedlam

Nie tylko Twoi pracownicy zmuszeni są do pozostaniu w domu. Zamknięcie szkół i przedszkoli oznacza, że dzieci znajdują się pod opieką rodziców przez całą dobą. Oznacza to także wzrost obciążenia łączy internetowych, gdyż wszyscy domownicy chcą korzystać z sieci. Miejsca najbardziej dotknięte przez wirusa odnotowały ponad 90% wzrost wykorzystania Internetu. Na szczęście wielu dostawców usług internetowych aktualizuje swoją ofertę i oferuje klientom łącza o wyższej przepustowości lub eliminuje limity danych, aby uniknąć przestojów.

**W ciągu jednego tygodnia odnotowano 50% wzrost wykorzystania usług VPN. Prognozuje się, że w samych Stanach Zjednoczonych, wykorzystanie VPN wzrośnie o 150% do końca kwietnia 2020.**

# OSIEM PORAD DLA LIDERÓW BIZNESU: JAK UTRZYMAĆ WYDAJNOŚĆ BEZ SPADKU WYDAJNOŚCI

## 1. OCEŃ ZASOBY PRZEDSIĘBIORSTWA KTÓRYCH MOŻE WYMAGAĆ PRACA ZDALNA

Chociaż większość firm oferuje możliwość pracy na odległość, nie wszyscy pracownicy mają takie same możliwości. Dla wielu firm przejście na pracę zdalną nastąpiło z dnia na dzień, pozostawiając niewiele czasu na odpowiednie zaplanowanie zmian. Dopiero po kilku tygodniach nadszedł czas, aby przeprowadzić audyt i ocenić potrzeby firmy w zakresie dostępu do firmowych zasobów oraz rozważyć kwestie bezpieczeństwa. Dostawcy zarządzanych usług bezpieczeństwa (ang. Managed Security Services Providers, MSSP) są ekspertami w ocenie bezpieczeństwa i mogą pomóc średnim przedsiębiorstwom szybko zoptymalizować wydajność i ustanowić polityki bezpieczeństwa w nowej rzeczywistości.

Dla "sieciowych nomadów" zawsze będących w ruchu, nowe okoliczności nie zmieniają wiele. Mają oni dostęp do sprawdzonych aplikacji ułatwiających pracę zdalną. Dla ludzi, którzy nie pracują tak często z domu, pomocna byłaby lista rozwiązań, które usprawnią działanie i pozwolą zarządzać realizowanymi projektami. Współpracuj z szefami działów, aby zrozumieć unikalne potrzeby każdego zespołu i upewnij się, że ich członkowie są przygotowani na kontynuowanie rozpoczętych działań.

**Oto lista kontrolna rzeczy do rozważenia:**

- ✔ Czy pracownicy posiadają urządzenia, na które zostały nałożone ograniczenia i czy będzie potrzebował dodatkowych telefonów lub laptopów?
- ✔ Czy masz wystarczająco dużo licencji VPN, aby wydać je wszystkim, którzy ich potrzebują, czy też musisz zdobyć więcej?
- ✔ Czy pracownik ma dostęp do Internetu który pozwala na wykonywanie pracy?
- ✔ Jakich systemów potrzebuje pracownik, aby wykonywać swoją pracę?
- ✔ Czy pracownik potrzebuje bezpiecznego dostępu do wrażliwych danych?
- ✔ Z jakich aplikacji w chmurze pracownik regularnie korzysta?
- ✔ Czy pracownik jest przygotowany do korzystania z uwierzytelniania wieloskładnikowego?

# USTAL OCZEKIWANIA DOTYCZĄCE PRACY ZDALNEJ I ZAKOMUNIKUJ JE PRACOWNIKOM

Ponieważ wielu z Twoich pracowników prawdopodobnie pracuje w domu po raz pierwszy, nadszedł świetny moment, aby przedyskutować z pracownikami i nakreślić politykę firmy w zakresie pracy z domu,. Powinieneś nakreślić oczekiwania wobec pracowników pracujących zdalnie. Około 24% firm nie uaktualniło swojej polityki pracy z domu na przestrzeni ponad roku, więc wykorzystaj to jako okazję do wprowadzenia zmian. Nawet prosta wiadomość e-mail lub rozmowa konferencyjna z zespołem pomoże skrócić drogę do optymalnej polityki w firmie.

## Lista rzeczy, które powinieneś rozważyć

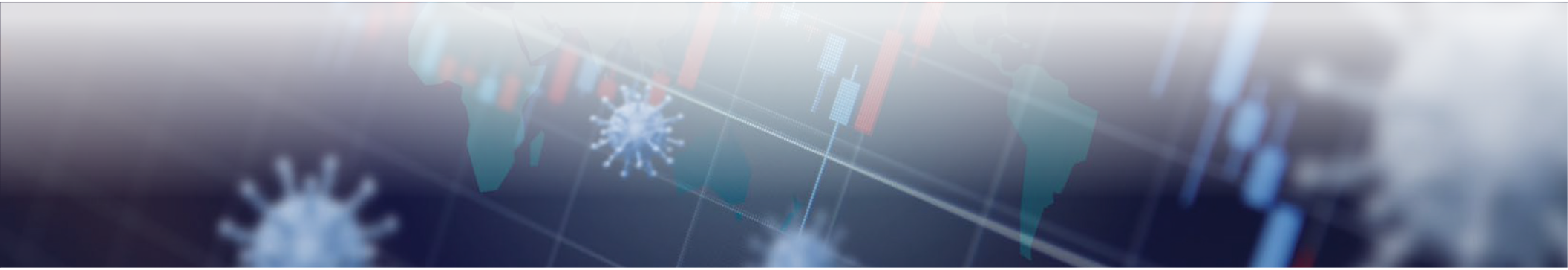
**Dostępność** - W jakich godzinach będzie pracował Twój zespół? Kiedy sam będziesz dostępny?

**Schematy reakcji** - Czy od pracowników zdalnych oczekuje się natychmiastowej reakcji? Jeśli tak, to w jaki sposób zostaną przekazane te oczekiwania? Na przykład, czy naprawdę pilne prośby będą zgłaszane tylko telefonicznie?

**Platformy** - Przypomnij swoim pracownikom, jakich narzędzi i platform powinni używać, włączając w to platformy do przechowywania danych w chmurze, narzędzia do komunikacji/konferencji wideo, narzędzia do zarządzania projektami itp. Zachęcaj swój zespół do unikania wszystkich platform spoza zatwierdzonej listy.

**Urządzenia** - Jeżeli Twój zespół posiada urządzenia wydane przez firmę, przypomnij mu o wszelkich zasadach, które ustaliłeś w zakresie ich użytkowania. Jeśli używają do pracy własnych urządzeń osobistych, udziel wskazówek, jak bezpieczenie korzystać z tych urządzeń i w jakim zakresie.

**Zgłaszanie incydentów** - Gdzie powinien się udać pracownik, jeśli ma wrażenie, że informacje firmy mogły zostać zagrożone? Komu należy zgłosić naruszenie i jakie kroki należy podjąć, aby zminimalizować skutki tego naruszenia?



# 3. BUDUJ KULTURĘ CYBERBEZPIECZEŃSTWA

Większość managerów biznesowych rozumie, że kultura miejsca pracy jest ważną częścią tego, co napędza sukces lub porażkę przedsiębiorstwa. Teraz muszą oni również zrozumieć, że taka sama dynamika istnieje w dziedzinie cyberbezpieczeństwa. Ponieważ pracownicy są zagrożeni atakami, a w niektórych przypadkach hakerzy podszywają się pod członków zespołu, kultura i standardy pracy często decydują o tym, czy atak się powiedzie.

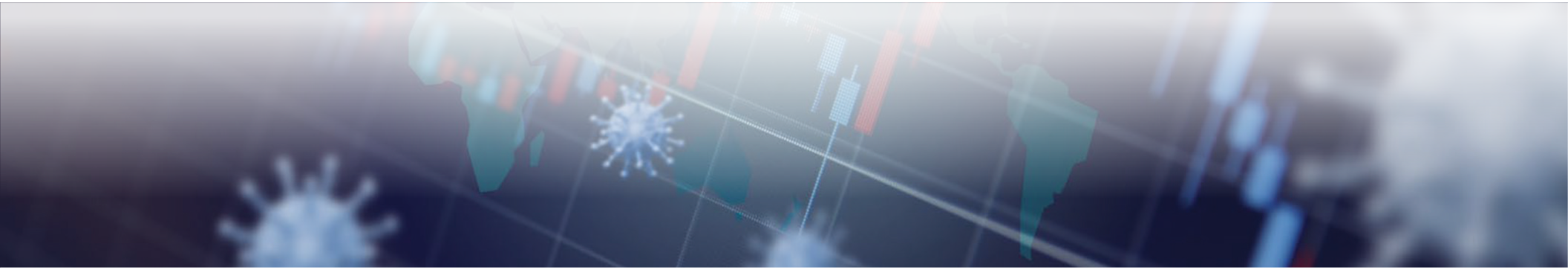
Hakerzy używają zróżnicowanych socjotechnik, aby manipulować i wpływać na użytkowników, tak aby podjęli odpowiednie działania, dzięki którym atak okazuje się skuteczny. Jako lider powinieneś zachęcać do korzystania z otwartych kanałów komunikacji. Tylko wtedy pracownik, nawet na najniższych szczeblach organizacji, będzie wiedział, że jeżeli zgłosi coś, co wzbudza jego wątpliwości, jego obawy zostaną potraktowane poważnie.

### Kilka wskazówek jak budować kulturę cyberbezpieczeństwa.

**Dziel się prawdziwymi historiami**. Pracownik złapał wiadomość e-mail informującą o phishingu, czy jego laptop został zainfekowany okupem? Dzielenie się analogicznymi historiami może pomóc w uniknąć podobnych ataków. Dlatego nie ukrywaj incydentów przed pracownikami. W przeciwnym wypadku mogą się one powtórzyć.

**Nagradzaj czujnych pracowników.** Kiedy pracownik zgłasza potencjalny atak, może oszczędzić Twojej firmie poważnego kłopotu, więc dlaczego nie nagradzać jego zachowania? Zachęcanie pracowników do zgłaszania podejrzanych działań może pomóc w zwiększeniu świadomości i zaangażowaniu innych.

**Bądź wyrozumiały.** Spójrzmy prawdzie w oczy, firmy składają się z ludzi o bardzo różnych umiejętnościach technologicznych. Nie możesz zakładać, że Twoi pracownicy będą unikać każdego zagrożenia i przestrzegać każdej polityki. Ludzie popełniają błędy.



# 4. ZAIMPLEMENTUJ WIELOSKŁADNIKOWE UWIERZYTELNIENIE

Kiedy wielu pracowników pracuje zdalnie, zabezpieczenie dostępu do narzędzi wewnętrznych stanowi duże wyzwanie. Jednocześnie hakerzy coraz częściej kierują swoje działania na dane uwierzytelniające. Z tego powodu zalecamy wszystkim użytkownikom wdrożenie wieloczynnikowej autoryzacji (MFA). W ten sposób wszyscy podłączeni do sieci użytkownicy poddani zostaną pewnej weryfikacji.

Uwierzytelnianie wieloczynnikowe pozwala również na bezpieczny dostęp do aplikacji i środowisk w chmurze, do których zdalni pracownicy mogą uzyskać dostęp bezpośrednio z przeglądarki. To ważna, dodatkowa warstwa ochrony w czasie, gdy firmy są najbardziej narażone.

**Czego należy szukać w rozwiązaniu MFA:**

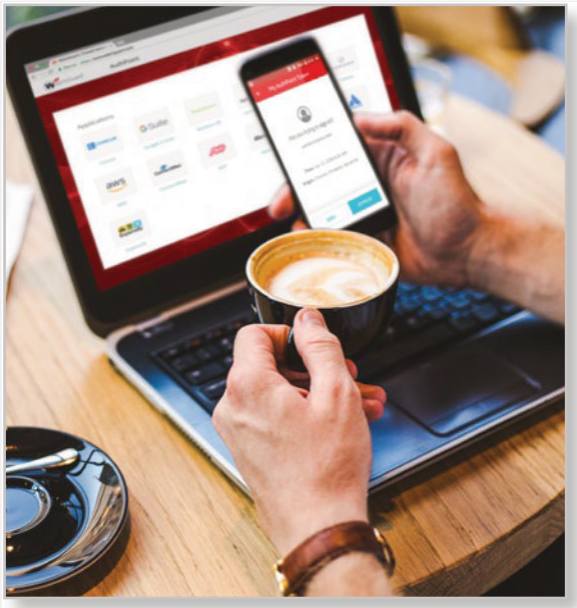
**Praca w chmurze.** W przeciwieństwie do urządzeń wielofunkcyjnych, które wymagają sprzętowego tokena, rozwiązania oparte na chmurze umożliwiają użytkownikowi pobranie aplikacji na telefon i natychmiastowe rozpoczęcie pracy.

**Wspierane aplikacje**. Twoje rozwiązanie powinno zapewniać szereg integracji, aby chronić wszystkie krytyczne aplikacje, których mogą potrzebować Twoi pracownicy.

**Prostota**. Rozwiązanie powinno być intuicyjne dla użytkowników o zróżnicowanych możliwościach technicznych.

**Wiele metod uwierzytelniania.** Obsługa wielu opcji uwierzytelniania online i offline gwarantuje, że upoważnieni użytkownicy mogą mieć dostęp do tego, czego potrzebują, kiedy jest to konieczne.

**Obsługuje wiele tokenów**. MFA jest obecnie powszechnie oferowana przez portale społecznościowe, banki, detalistów i wiele innych. Poszukaj rozwiązania, które umożliwia konsolidację tokenów do prostej aplikacji MFA, aby usprawnić dostęp dla swoich użytkowników.



# 5. ROZSZERZENIE DOSTĘPU VPN DO UŻYTKOWNIKÓW PRIORYTETOWYCH

Bezpieczna łączność z centralą firmy i krytycznymi aplikacjami jest niezbędna, jeśli Twoi pracownicy mają zamiar utrzymać wydajność pracy. Wirtualne sieci prywatne (VPN) dodają warstwę bezpieczeństwa do sieci prywatnych i publicznych, pozwalając osobom organizacjom na bezpieczne wysyłanie i odbieranie danych przez Internet.

**Twoi użytkownicy będą potrzebowali jednego z dwóch typów VPN:**

1. Sieci VPN oparte na kliencie. Działając w warstwie sieciowej, kliencka sieć VPN zapewnia użytkownikom dostęp do całej sieci.

2. Bezklientowa sieć VPN. Zazwyczaj wymagające tylko przeglądarki, bezklienckie sieci VPN łączą użytkowników z określonymi aplikacjami i usługami.

**Zazwyczaj przedsiębiorstwa dostarczają VPN tylko dla ograniczonej grupy pracowników zdalnych i często podróżujących, Oto kilka wskazówek, które pomogą Ci w zarządzaniu użytkowaniem i uniknięciu zakłóceń:**

Pierwszeństwo w dostępie do VPN należy przyznać użytkownikom wysokiego ryzyka. Niektórzy pracownicy będą wymagali większego dostępu niż inni, a jeszcze inni mogą nie potrzebować go wcale. Zrozumienie, kto i do czego potrzebuje dostępu oraz udostępnienie VPN w oparciu o listę priorytetowych pracowników pomoże uniknąć przeciążenia sieci.

Aby nadążyć za zapotrzebowaniem, można używać zapory sieciowej w chmurze. Skok zapotrzebowania na usługi VPN nie nie musi oznaczać konieczności zwolnienia miejsca w serwerowni. Firewalle w chmurze mogą pomóc w zrównoważeniu ruchu VPN w centrali i dostosować się do obsługi połączeń wymaganych przez firmę.

Obowiązkowa MFA. Bez MFA pojedynczy zestaw danych uwierzytelniających VPN może zapewnić atakującemu pełny dostęp do sieci. Użytkownicy łączący się za pomocą sieci VPN powinni być w pełni uwierzytelnieni przy użyciu co najmniej dwóch czynników.

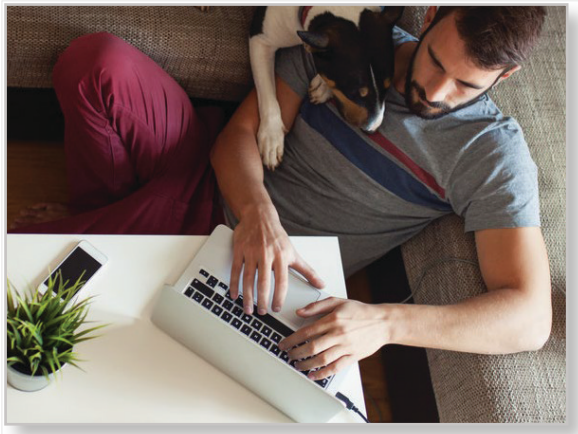
# 6. OCHRONA UŻYTKOWNIKÓW DZIĘKI FILTROWANIU DNS

Utrzymanie bezpieczeństwa użytkowników podczas poruszania się po Internecie jest trudniejsze, gdy łączą się oni z zewnątrz sieci. Ponieważ pracownicy utknęli w domu, są duże szanse, że firmowe laptopy zostaną wykorzystane do dużej ilości osobistego surfowania po sieci i sprawdzania poczty elektronicznej. Oparte na chmurze filtrowanie DNS pozwala na blokowanie połączeń i ograniczanie dostępu do ryzykownych obszarów Internetu. Klikając w złośliwe linki lub próbując połączyć się z domenami związanymi z phishingiem i złośliwym oprogramowaniem można zapobiec, bez konieczności korzystania z VPN.

### Co warto rozważyć gdy decydujesz się się na DNS:

- Produktywność i egzekwowanie polityki. W przypadku większej liczby pracowników pracujących poza siedzibą firmy może być również konieczne ograniczenie użytkownikom dostępu do niektórych rodzajów treści, takich jak serwisy społecznościowe i strony dla dorosłych. Poszukaj mechanizmów kontrolnych,- takich jak możliwość blokowania użytkowników i grup, a także ustalania godzin egzekwowania przepisów.

- Wsparcie dla inicjatyw szkoleniowych z zakresu bezpieczeństwa. Obecnie większość firm posiada pewną formę szkoleń z zakresu bezpieczeństwa cybernetycznego dla swoich pracowników, ale ponieważ migrują oni poza teren zakładu, aktualizacja takiego szkolenia jest ważniejsze niż kiedykolwiek. Niektóre rozwiązania z zakresu filtrowania DNS nie tylko blokują podejrzane połączenia, ale także dostarczają użytkownikowi informacji na temat sposobu identyfikowania podobnych zagrożeń w przyszłości.



# 7.OCHRONA PUNKTÓW KOŃCOWYCH PRZED ZŁOŚLIWYM OPROGRAMOWANEM

Zagrożenia związane ze złośliwym oprogramowaniem i ransomware uległy w czasie pandemii intensyfikacji. Ryzyko infekcji nigdy nie było wyższe, ponieważ użytkownicy zazwyczaj nie mogą  korzystać z ochrony firewalla podczas pracy w domu. Podczas gdy rozwiązania antywirusowe dla punktów końcowych wyłapują wiele zagrożeń, są one bezradne wobec złośliwego oprogramowania typu "zero-day malware". Rozwiązania typu EDR (Endpoint Detection and Response) mogą nie tylko wykryć te zaawansowane zagrożenia, ale także powstrzymać je i umożliwić dalszą, bezproblemową pracę. A to wszystko zdalnie.

### Istotne cechy rozwiązania EDR:

- **Metody detekcji**. Łapanie zaawansowanego złośliwego oprogramowania wymaga zastosowania zaawansowanych technik. Wybierz rozwiązanie które jest w stanie połaczyć kilka metod wykrywania, w tym analizę behawioralną, heurystyczną i piaskownicę.

- **Automatyzacja i SI**. Szybkie reagowanie na zagrożenia może oszczędzić poważnego bólu głowy. Automatyzacja wykrywania i reagowania może uczynić to niemal natychmiastowym.

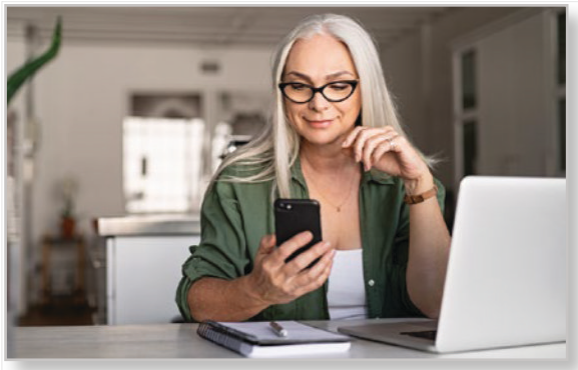
- **Izolacja zainfekowanej maszyny.** Gdy zagrożenie zostanie wykryte, zainfekowany komputer powinien zostać zablokowany, aby uniknąć rozprzestrzeniania się infekcji.

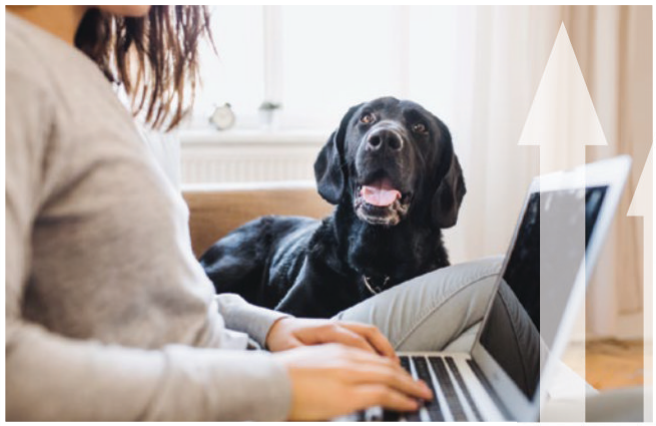
# 8. ZACHOWAJ KONTROLĘ NAD WI-FI

Praca w domu może powodować problemy związane z bezpieczeństwem w sieci Wi-Fi. Dla pracowników zdalnych pracujących w środowiskach pełnych różnorodnych urządzeń bezprzewodowych to kolejne zagrożenie. Hakerzy mogą wykorzystać to, że wielu pracowników w okolicy korzysta z dostępu do sieci i próbować podsłuchiwać ruch między pracownikiem a firmą.

**Czym się kierować wybierając rozwiązanie Wi-Fi**

- ✔ Rozważ wydanie certyfikowanych punktów dostępowych z certyfikatem Trusted Wireless Environment, aby zapewnić działowi IT pełny wgląd w wydajność klientów i sieci, co pozwoli mu lepiej obsługiwać zdalnych pracowników.
- ✔ Wstępna konfiguracja punktów dostępowych umożliwia łatwe wdrożenie dla użytkowników w domu.





W środowiskach o dużym zagęszczeniu użytkowników, np. na osiedlach, komunikacja za pośrednictwem Wi-Fi stanowi aż **50% ruchu**

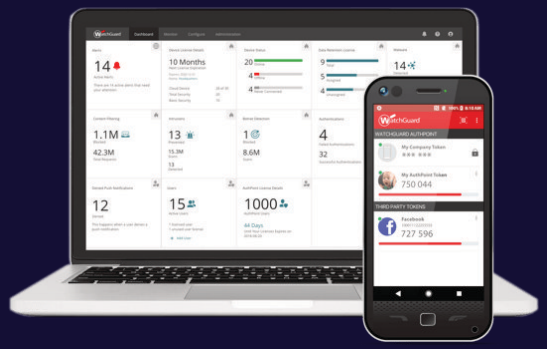
# DLACZEGO GOTOWOŚĆ DO DZIAŁANIA JEST TAK WAŻNA?

Po prostu są rzeczy, których nie można przewidzieć. Liderzy biznesu wiedzą, że na każdej drodze do sukcesu zdarzają się wyboje i nieplanowane wydarzenia. Co możesz zrobić, aby chronić przyszłość swojego biznesu? Plan gotowości nie obiecuje doskonałości, ale może dać Ci narzędzia do bezpiecznego poruszania się po wyzwaniach i zapewnić niezbędne zasoby do zapewnienia ciągłości operacyjnej.

Dziś jest to epidemia koronawirusa, ale w przyszłości czekają Cię zupełnie inne okoliczności, które mogą zagrozić Twojemu cyberbezpieczeństwu. Duże wydarzenie, takie jak mistrzostwa świata w piłce nożnej, które zakłóca normalne funkcjonowanie miasta, a nawet błąd ludzki, może popchnąć Twoją firmę do przejścia w tryb gotowości krytycznej. Każda sytuacja, która zmusza do szybkiej adaptacji do nieoczekiwanych zmian, jest ostatecznym dowodem na to, jak ważne jest, aby naprawdę zrozumieć swoją organizację i jej potrzeby.

Dlaczego? Ponieważ pokazuje Twoim pracownikom, klientom i inwestorom, że Twoja firma może rozwijać się nawet podczas bezprecedensowych wydarzeń. To ważne dla marki, którą budujesz.

**Dlaczego?** Ponieważ pokazuje Twoim pracownikom, klientom i inwestorom, że Twoja firma może rozwijać się nawet podczas bezprecedensowych wydarzeń. To ważne dla marki, którą budujesz.



**Wielsokładnikowe uwierzytelnienie**
Zarejestruj się i odbierz darmowe licencje nawet dla 250 użytkowników.

W 120 dni przekonaj się jak proste i skuteczne jest MFA od WatchGuard.

**Skontaktuj się z nami**

## Szukasz rozwiązania, które zabezpieczy Twoich pracowników w siedzibie firmy i poza nią?

Jesteśmy autoryzowanym partnerem WatchGuard. Prowadzimy szkolenia i warsztaty. Na swoim koncie mamy wdrożenia w wielu krajach Europy. **www.netcomplex.pl**

## About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by nearly 10,000 security resellers and service providers to protect more than 80,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for midmarket businesses and distributed enterprises. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

WatchGuard www.watchguard.com