**Koronawirus zmusza do pracy w domu. Lecz w domu zagrażają nam nie tylko wirusy. Jak się chronić?**

**Czy mamy do czynienia z największą w historii pandemią czy to bezpodstawne obawy? Strach przed aktualnym tempem rozprzestrzeniania się koronawirusa oraz jego następstw doprowadził firmy do zrewidowania sposobu pracy swoich pracowników. Miliony ludzi w całej Azji zaczęły pracować w domu. Pracownicy wiodących firm technologicznych takich jak Amazon, Microsoft, Facebook czy Google i innych, dostali nakaz pracy zdalnej do czasu, gdy sytuacja się poprawi i wirus zostanie opanowany. Podobne zmiany następują w Polsce - pracownicy wielu firm otrzymali w ostatnich dniach polecenie pracy zdalnej. Takie zalecenia otrzymali pracownicy wieżowca Warsaw Spire - najwyższym biurowcu w Polsce, w którym swoje siedziby mają światowe firmy i organizacje.**

Praca zdalna nie jest skomplikowana. Większość z nas robi to od czasu do czasu. Dostęp do Internetu jest powszechny, a oprogramowanie biurowe w chmurze oraz aplikacje SaaS sprawiają, że przesiadka z biura na kanapę salonu staje się banalnie prosta. Ale większość organizacji nie wspierało dotąd tak licznej rzeszy pracujących spoza biura, a sami pracownicy mogą nie być świadomi czyhających zagrożeń w sieci.

Przebywając w domu jesteśmy przeważnie bardziej zrelaksowani, szczególnie jeżeli chodzi o bezpieczeństwo. Niestety, cyberprzestępcy starają się wykorzystać tę atmosferę rozluźnienia za pomocą dopracowanych exploitów phishingowych oraz innych zagrożeń.

Z tego powodu firma Check Point Software Technologies radzi, jak zachować bezpieczeństwo pracując zdalnie.

l **Hasła są ważne:** Dobrym pomysłem jest przegląd i wzmocnienie siły (długość, zróżnicowanie znaków) haseł, których używasz do logowania się do zdalnych zasobów, takich jak mail czy aplikacje wykorzystywane w pracy

l **Uważaj na phishing:** Wystrzegaj się klikania w podejrzane linki i pobieraj pliki jedynie z zaufanych źródeł, które możesz zweryfikować. Pamiętaj, że ataki phishingowe polegają na inżynierii społecznej, więc jeżeli otrzymamy mailowo nietypową prośbę, należy sprawdzić dokładnie dane nadawcy, aby upewnić się, że komunikujemy się z kolegami z pracy, a nie przestępcami. Dział badan Check Point odkrył, że wśród [domen o tematyce koronawirusa ponad 50% jest złośliwych](https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/), więc należy upewnić się, że ostrożnie oceniamy wiadomości w skrzynce odbiorczej.

l **Uważnie wybieraj, z jakiego urządzenia korzystasz:** Wielu pracowników [wykorzystuje służbowy komputer lub laptop do prywatnego użytku](https://www.cisco.com/c/dam/global/en_ca/assets/pdf/Understanding_Remote_Worker_Security_A_survery_of_User_Awareness_vs_Behaviour.pdf), co może być narażać ich firmę na niebezpieczeństwo. Jeszcze gorzej, jeżeli wykorzystujesz prywatny komputer do celów służbowych. Jeżeli musisz korzystać z domowego komputera w pracy, porozmawiaj z działem IT, w jaki sposób poprawić jego bezpieczeństwo - przykładowo poprzez zainstalowanie dobrego antywirusa i pakietu bezpieczeństwa.

l **Czy ktoś podsłuchuje?** Czy Twoja domowa sieć Wi-Fi posiada mocne hasło czy może jest otwarta? Upewnij się, że chronisz się przeciwko przebywającym w jej zasięgu i mogącymi zyskać do niej dostęp. To samo dotyczy się sieci w kawiarniach czy hotelach - bądź ostrożny korzystając z publicznych hotspotów. Niezabezpieczone sieci ułatwiają cyberprzestępcom dostęp do Twoich maili i haseł.

**Rady dla pracodawców**

Poniżej znajdują się podstawowe zasady bezpieczeństwa dla organizacji, niezależnie czy ich dane i aplikacje są przechowywane w centrach danych, publicznych chmurach czy aplikacjach SaaS.

l **Nie ufaj nikomu:** Twój plan zdalnego dostępu powinien być zbudowany na zasadzie tzw. zero zaufania, w którym wszystko należy weryfikować i nie uznawać niczego za pewnik. Upewnij się, że rozumiesz kto ma dostęp do jakich informacji - podziel odpowiednio swoich użytkowników i wymuś korzystanie z uwierzytelniania wieloskładnikowego.

l **Każdy punkt dostępu potrzebuje uwagi:** W typowym scenariuszu Twoi pracownicy mogą pracować na komputerach stacjonarnych na terenie biura. Zakładając, że nie zabierają swoich urządzeń do domu, masz na głowie mnóstwo nieznanych urządzeń, które potrzebują teraz dostępu do danych Twojej firmy. Powinieneś przemyśleć, w jaki sposób ochronisz się przed potencjalnymi wyciekami danych, atakami mającymi źródło w jednym z urządzeń podłączonych do Twojej sieci oraz zadbać o kompletną ochronę wszystkich urządzeń w sieci firmowej.

l **Przeprowadź testy obciążeniowe infrastruktury:** W celu wprowadzenia bezpiecznego dostępu zdalnego do procesów biznesowych, kluczowym jest posiadanie VPN lub SDP. Infrastruktura ta musi być elastyczna, należy ją przetestować pod obciążeniem, aby upewnić się, że poradzi sobie z intensywnym ruchem sieciowym, podczas gdy Twoi pracownicy będą w większości pracować zdalnie.

l **Zdefiniuj swoje dane:** Poświęć czas, żeby zidentyfikować, określić swoje wrażliwe dane, aby przygotować strategię, która dopuści do nich jedynie odpowiednie osoby. Nikt nie chciałby przez przypadek udzielić dostępu do danych HR-u całej organizacji.

l **Podział na drużyny:** Dokonaj audytu aktualnej polityki firmy dotyczącej dostępu i dzielenia się różnymi rodzajami danych. Ponownie oceń zarówno politykę dostępu do danych jak i podział pracowników na zespoły, a następnie wprowadź różne poziomy dostępu skorelowane z wrażliwością danych.