Cyberdefence 24

aut. Andrzej Kozłowski 16.03.2020

BEZPIECZNA PRACA ZDALNA

Epidemia koronawirusa zmusiła pracowników do przejścia w tryb pracy zdalnej. Rodzi to nowe wzywania dla zarządzania bezpieczeństwem w firmach. Nie przestrzeganie podstawowych zasad bezpieczeństwa można doprowadzić do poważnych strat dla przedsiębiorstwa i samego pracownika. Co należy zrobić, żeby ten czas nie stał się erą złotych żniw dla hakerów?

Z badań organizacji OpenVPN wynika, że pracownicy zdalni stanowią większe zagrożenie niż pracownicy znajdujące się na miejscu pracy w biurze – uważa tak prawie 70 % ekspertów. Podjęcie odpowiednich kroków pozwoli jednak zminimalizować ryzyko wynikające z pracy na odległość.

Bezpieczeństwo sieci domowych

Pracownicy, którzy wykonują swoje obowiązki zdalnie są podłączeni do sieci domowych, które nie są w żadne sposób sprawdzone przez ekspertów ds. cyberbezpieczeństwa. Najczęściej nie są również zabezpieczone w odpowiedni sposób. Co więcej występuje również ryzyko, że mogą się w niej znajdować urządzenia niezaufane, podatne na zagrożenia jak np. elementy Internetu rzeczy (inteligentne kamerki itp.). Umożliwia to łatwiejsze włamanie się do sieci, w której znajduje się komputer służbowy. Dzięki temu przestępcy mogą podsłuchiwać i przechwytywać informacje, które najczęściej będą wysyłane w formie niezaszyfrowanego tekstu. Dlatego tak ważne jest umożliwienie pracownikom podłączenie się w bezpieczny sposób. Każdy pracujący zdalnie powinien używać VPN, a ich urządzenia końcowe z których korzystają muszą być wyposażone w najnowsze wersje oprogramowania oraz programy antywirusowe z najbardziej aktualną bazą danych. Poza używaniem VPNa ważne jest również bezpieczeństwo domowego WiFi. Konieczna jest zmiana jego domyślnej nazwy oraz utworzenie silnego hasła, które wzmocni ochronę. Należy również sprawdzić czy zainstalowane są najnowsze aktualizację oraz upewnić się, że szyfrowanie jest w standardzie WPA2 i WPA3.

Wykorzystanie służbowego sprzętu do prywatnych celów

Drugim problem, który często występuje podczas pracy zdalnej jest transfer plików pomiędzy sprzętem służbowym i prywatnym. Do takich praktyk przyznaje się 46% pracowników. Dlatego bardzo ważne jest również niepodłączenie prywatnych urządzeń zewnętrznych takich jak dyski zewnętrzne czy pendrive'y do służbowego komputera. Użytkownicy podczas pracy zdalnej powinni pamiętać o tym, żeby nie używać do komunikacji służbowej prywatnych skrzynek pocztowych czy mediów społecznościowych. Zakazane jest również granie czy oglądanie filmów na służbowym sprzęcie oraz pożyczanie go innymi domownikom. Odradza się również podłączanie służbowego sprzętu do telewizorów, które mają dostęp do Internetu.

Należy również uważać na dzieci czy zwierzęta, które mogą przez przypadek zalać firmowy sprzęt, ale również omyłkowo wysłać maila do szefa czy wprowadzić modyfikacji w projektach. Wysyłanie maili do szefa czy zabawnej wiadomości na służbowym komunikatorze może zaowocować nieprzyjemnymi konsekwencjami, a take zdradzić, że pracownik pozostawił sprzęt bez nadzoru. Innym problemem jest

również oglądanie bajek przez dzieci na komputerach służbowych przez platformy streamingowej. To również nie powinno mieć miejsca.

Silne hasła i dwuskładnikowe uwierzytelnianie

Pracownicy powinni również wykorzystywać dwuskładnikowe uwierzytelnianie logując się do swoich pracowniczych skrzynek pocztowych. Im większa liczba dodatkowych zabezpieczeń, tym mniejsze prawdopodobieństwo, że cyberprzestępcy dostaną się do systemów. Drugim ważnym elementem bezpieczeństwa jest menadżer haseł, który powinien być wykorzystywany przez pracowników. W ten bezpieczny sposób nie będą musieli pamiętać wielu różnorodnych haseł do aplikacji firmowych, ale również uniknąć tworzenia łatwych do odgadnięcia słabych haseł. Za silne bezpieczne hasła należy przyjąć konfigurację 4-5 losowo dobranych słów.

Ważnym elementem bezpieczeństwa jest również firewall, który jest istotną linią obrony przed zagrożeniami dla systemu komputerowego. Tworzoną one coś na kształt bariery pomiędzy urządzeniem i internetem, poprzez zamykanie portów komunikacyjnych. Pozwala to na zapobiegnięcie infekcji oraz wyciekowi danych. Większość systemów ma wbudowany firewall, trzeba się tylko zorientować czy jest on włączony.

Uwaga na phishing

Praca zdalna to również czas zwiększonej liczby ataków phisingowych. Nie mając koło siebie kolegów czy przełożonych, trudniej jest wykryć potencjalny phising. Niestety epidemia koronawirusa jest wykorzystywana przez cyberprzestępców do licznych wyłudzeń i podszywania się pod inne instytucje, dlatego pracownicy powinni stać się ostrożniejsi w zarządzaniu własną skrzynka mailową. Pracodawcy również na bieżąco powinni informować o wszystkich wykrytych przypadkach wyłudzeń, tak aby pracownicy jak najszybciej się o tym dowiedzieli. Dobrym rozwiązaniem jest stworzenie kanału na wykorzystywanym przez firmę komunikatorze nie tylko do informowania o organizacji pracy, ale również ostrzegania się wzajemnie o wykrytych zagrożeniach.

W trakcie pracy zdalnej pracownicy powinni również wystrzegać się drukowania służbowych dokumentów na prywatnych drukarkach czy zapisywania ich na pendrivach. Istnieje duża szansa, że mogą one nie zostać w odpowiedni sposób zutylizowane z wykorzystaniem niszczarki do papierów i w ten sposób wpaść w niepowołane ręce. Część drukarek zapisuje również drukowane dokumenty w swojej pamięci.

Nie tylko prewencja jest istotna, ale również działanie na wypadek wycieku informacji. Jeżeli pracownik podejrzewa, że informacje firmy mogły zostać naruszone przez hakera, musi to zgłosić w odpowiedni sposób. I tu jest zadanie dla firm, który muszą stworzyć odpowiednią, transparentną ścieżkę raportowania wycieków oraz służyć radom pracownikom odnośnie kroków, które mają podjąć, jeżeli przełamią zabezpieczenia.

Praca zdalna to obecnie rekomendowane rozwiązanie w trakcie epidemii koronawirusa z którego korzysta coraz więcej firm w kraju. Odpowiednie współdziałanie pomiędzy pracodawcą i pracownikiem w zakresie cyberbezpieczeństwa zdecydowanie zminimalizuje potencjalne ryzyko. Pracodawca powinien zapewnić odpowiednie narzędzia dla pracownika oraz stworzyć kanał komunikacji o potencjalnych zagrożeniach, a pracownicy muszą zachowywać się odpowiedzialnie i pamiętać, że komputery służbowe to nie zabawka.