www.zyxel.com

Bezpieczeństwo w nowej normalności: jak radzić sobie z zagrożeniami związanymi z pracą zdalną

2020 rok przejdzie do historii jako ten, w którym miliony ludzi nauczyło się, jak to jest pracować zdalnie. Pandemia koronawirusa zmusiła pracodawców do zamknięcia biur i wypracowania elastycznych form pracy. Nie sposób określić, jak długo potrwają obostrzenia, dlatego warto już teraz rozważyć pracę zdalną, jako realną na dłuższy czas opcję z wieloma korzyściami zarówno dla pracowników, jak i przedsiębiorstw.

Pomimo że pandemia bez wątpienia przyspieszyła przejście na tryb zdalny, elastyczne formy pracy stopniowo zyskiwały na popularności przez całą minioną dekadę. Za sprawą postępu technologicznego zainteresowanie mobilnością i pracą w domu rosło na długo przed atakiem wirusa. Swoboda zapewniana przez coraz wydajniejsze i tańsze urządzenia mobilne, takie jak notebooki, komputery PC, Chromebooki, tablety i smartfony, umożliwia pracę z niemal dowolnego miejsca za pośrednictwem sieci Wi-Fi lub połączenia szerokopasmowego.

Kiedy jednak pracownicy cieszą się zaletami z pracy zdalnej korzystając z publicznych i domowych połączeń szerokopasmowych, cyberprzestępcy mają czas, żeby zidentyfikować i wziąć na cel luki w zabezpieczeniach sieci. Teraz kiedy pandemia znormalizowała „hybrydowe" sposoby pracy firmy na całym świecie stały się podatne na cyberataki.

Nowe wyzwania w zakresie bezpieczeństwa

Przed nadejściem pandemii, kiedy normą była praca w biurze, zabezpieczanie danych było stosunkowo łatwe, ponieważ pracownicy byli bezpośrednio podłączeni do sieci w centralnym biurze - za pomocą kabla Ethernet lub przez Wi-Fi. Teraz jednak „firmowa sieć" to coś, co istnieje w wielu lokalizacjach, zarówno w pracy, jak i w domu, a także w chmurze i w fizycznej siedzibie przedsiębiorstwa. W tym nowym hybrydowym świecie, w którym wszyscy codziennie, przez cały dzień zdalnie łączą się z siecią, pojawia się wiele potencjalnych okazji dla cyberprzestępców. Jeśli połączenia te nie są w pełni zabezpieczone, istnieje realne niebezpieczeństwo infiltracji.

Ponadto wiele osób pracujących obecnie zdalnie wykorzystuje komputery biurowe, firmowe laptopy, lub własne komputery domowe. Połączenia zdalne są zupełnie inne niż lokalne, dlatego we wszystkich trzech

przypadkach zabezpieczenia powinny być odpowiednio skonfigurowane do użytku domowego – a to bywa niełatwe.

Dodatkowo pojawiać się mogą problemy z wiekiem i przydatnością bieżącego sprzętu – zarówno na poziomie urządzeń klienckich, jak i centrum danych. Stare serwery i sprzęt sieciowy, czy nawet same urządzenia zabezpieczające, mogą nie sprostać nowym wyzwaniom.

Ze względu na pracę hybrydową zasadniczym zmianom uległa również sama infrastruktura sieciowa, co powoduje dodatkowe wyzwania. Duża liczba osób pracujących zdalnie oznacza duże rozproszenie sieci. Nie posiada ona już definitywnej, fizycznej struktury, za to ma znacznie więcej punktów wejścia. Egzekwowanie zasad bezpieczeństwa nie jest tak łatwe, jak w przypadku, gdy wszyscy znajdują się w biurze i są połączeni lokalnie. Wdrażanie aktualizacji i zmian w oprogramowaniu i usługach zabezpieczających zajmuje również więcej czasu.

Najważniejsze jest to, że rozwój i akceptacja pracy w domu zwiększyły złożoność wyzwania, jakim jest zapewnienie bezpieczeństwa sieci. Istnieje więcej możliwości powstania luk w cyfrowych zabezpieczeniach. Indywidualni użytkownicy mogą być celem ataków, a cyberprzestępcy wiedzą, że jeśli uda im się włamać do jednego urządzenia, będą mieli znacznie większą szansę na dostanie się do głównej sieci.

Cyberprzestępcy dostosowują się do zmian na rynku i w środowisku pracy. Doskonale zdają sobie sprawę ze zwiększonej podatności na zagrożenia, która jest wynikiem pracy w domu, i wykorzystują tę potencjalną słabość.

Zyxel Networks

Zyxel od ponad 30 lat zapewnia użytkownikom domowym i biznesowym dostęp do Internetu, od samego początku polegając na innowacjach i usługach zorientowanych na potrzeby klientów. W 1989 roku oznaczało to modemy analogowe. Dziś to wykorzystanie sztucznej inteligencji i chmury, by zapewniać szybkie, niezawodne i bezpieczne rozwiązania sieciowe dla domu i firmy. Zyxel jest znaczącą marką na globalnym rynku urządzeń sieciowych:

- obecny na 150 rynkach na całym świecie
- 1 mln firm pracuje lepiej, dzięki produktom marki Zyxel
- 100 milionów urządzeń łączących na globalną skalę

Obecnie, Zyxel tworząc sieci przyszłości, uwalnia potencjał i spełnia wymagania nowoczesnych miejsc pracy – wspiera ludzi w biurze, codziennym życiu i w czasie wolnym.

Dołącz do nas na Facebooku i LinkedIn!