Polacy pracujący z domu łatwym celem dla cyberprzestępców

Kategoria: Styl życia
Opublikowano: środa, 21, październik 2020 10:17
Alicja Cisowska

Praca zdalna zmniejsza ryzyko zarażenia koronawirusem, zwiększa natomiast zagrożenie wyciekiem danych osobowych. Powodem takiego stanu rzeczy jest fakt, że większość spraw załatwiamy teraz za pośrednictwem Internetu. Nie pomagają również: brak procedur w firmie, nieprzeszkoleni pracownicy oraz niewystarczająca liczba służbowego sprzętu do pracy. Krajowy Rejestr Długów oraz serwis ChronPESEL.pl sprawdzili, jak pracując zdalnie, dbamy o bezpieczeństwo danych osobowych. Wyniki badania są alarmujące.

Jak wynika z danych GUS, w II kwartale 2020 r. w związku z pandemią pracę zdalną wykonywał co dziesiąty pracownik. W przeprowadzonym przez Krajowy Rejestr Długów i serwis ChronPESEL.pl badaniu, 70% Polaków pracujących z domu zadeklarowało, że taka forma daje im większe możliwości i ułatwia pogodzenie obowiązków domowych i rodzinnych z zawodowymi. Z powodu niskich zabezpieczeń i braku uwagi samych pracowników nowe możliwości otwierają się również przed cyberprzestępcami.

Grzech ignorancji

Przestępcy starają się wykorzystać fakt, że większość spraw załatwiamy obecnie za pośrednictwem Internetu. Amerykańskie Federalne Biuro Śledcze (FBI) poinformowało niedawno, że od początku pandemii liczba cyberataków wzrosła o 400%. Jak na nowe okoliczności przygotowana są firmy, które wysłały dużą część zespołu do domu? Według przeprowadzonego we wrześniu 2020 r. badania, pracujący zdalnie nie zostali odpowiednio przeszkoleni pod kątem ochrony danych osobowych. Wpływ na to ma fakt, że tylko niespełna połowa (48%) firm opracowała odpowiednie procedury na tę okoliczność. Równocześnie 52% pracowników nie wie, w jaki sposób ich pracodawca zabezpiecza dane osobowe. To pierwszy sygnał ostrzegawczy.

Brak odpowiedniego przeszkolenia widać również w innych sytuacjach. Pomimo zaleceń ze strony pracodawcy, co czwarta osoba w trakcie pracy wyłącza szyfrowanie połączenia sieciowego na swoim komputerze. Warto też dodać, że z takich zabezpieczeń w postaci szyfrowanej sieci VPN korzysta tylko niespełna 2/3 firm. To, w połączeniu z większą liczbą ataków hakerów, zwiększa zagrożenie wycieku danych osobowych pracownika, który korzysta z niezabezpieczonego komputera.

- W przypadku ochrony danych osobowych w sieci możemy mówić o dwóch liniach obrony. Pierwszą jesteśmy my sami – użytkownicy Internetu. To od naszych decyzji zależy, czy narazimy się na niebezpieczeństwo klikając na przykład w podejrzany link albo otwierając wiadomość od fikcyjnego sklepu internetowego. Drugą linią obrony są zabezpieczenia na urządzeniach, z których korzystamy. Programy antywirusowe i szyfrowanie sieci pomogą w przypadku, gdy pobierzemy niewłaściwy plik lub jeśli pracujemy z zastrzeżonymi dokumentami. Firmy, które nie edukują swoich pracowników oraz nie inwestują w odpowiednie zabezpieczenia sprzętu otwierają drzwi cyberprzestępcom, którzy tylko czekają na takie okazje. Trzeba sobie również zdawać sprawę, że ryzyko dotyczy nie tylko naszych pracowników, ale także naszych klientów, których dane osobowe są przetwarzane przez osoby pracujące z domu – ostrzega Bartłomiej Drozd, ekspert serwisu ChronPESEL.pl.

Lekcje online na służbowym komputerze

Jak pokazują wyniki badania, tylko niewiele ponad 30% pracowników może wykonywać swoje obowiązki korzystając ze sprzętu służbowego. Co piąty nie ma w ogóle takiej możliwości. Powoduje to sytuację, w której osoby pracujące zdalnie zmuszone są pracować na swoim prywatnym komputerze, a

firmy nie mają kontroli nad tym, czy są one odpowiednio zabezpieczone.

Prawie połowa pracowników (46%) przyznaje się do tego, że wykorzystuje sprzęt służbowy nie tylko do czynności związanych z pracą. Wśród aktywności ankietowani najczęściej wskazali sprawdzanie prywatnych e-maili (80%), załatwianie spraw bankowych (65%), zakupy online (51%) oraz korzystanie z mediów społecznościowych (47%). Co dziesiąty pracownik przyznał się do tego, że z jego sprzętu firmowego korzystają również pozostali domownicy. Co trzeci taki przypadek związany jest z koniecznością udziału dzieci w zajęciach online. W tym czasie rodzice tracą kontrolę nad komputerem i nie mają wpływu na to, jak ze sprzętu będzie korzystała ich pociecha. To bardzo nieostrożne w sytuacji, w której największe banki oraz instytucje publiczne codziennie ostrzegają o oszustach podszywających się pod nich w Internecie.

Pracownicy udostępniają swoim domownikom nie tylko służbowe komputery. 45% ankietowanych korzysta w pracy również z firmowych przenośnych nośników danych. Co piąty z nich użycza ich w razie potrzeby swoim bliskim. W przypadku nieodpowiednio zabezpieczonego komputera (stary, nieaktualny program antywirusowy bądź jego darmowa wersja) lub braku nawyku skanowania za każdym razem dysku zewnętrznego, może się to wiązać z zainfekowaniem sprzętu wirusem lub instalacją oprogramowania, dzięki któremu cyberprzestępcy zyskają do niego dostęp.

- *Niestety, zapominając o podstawowych zasadach bezpieczeństwa, ułatwiamy cyberprzestępcom dostęp do naszych komputerów i narażamy na kradzież nasze dane osobowe. Odpowiednie zabezpieczenie komputera, tabletu lub telefonu, z którego na co dzień korzystamy, powinno być priorytetem. Należy również pamiętać o tym, by zachować czujność podczas obecności w sieci. Zatem, nie klikajmy w podejrzane linki otrzymane w mailach lub SMS-ach, a zakupy i transakcje bankowe róbmy tylko za pośrednictwem oficjalnych stron lub aplikacji. Nie stosując się do tych zasad, możemy narazić się na poważne konsekwencje. Przestępcy mogą próbować wykorzystać zdobyte w ten sposób dane osobowe, żeby podszywając się pod ich właściciela, wyłudzić pożyczkę, kupić drogi sprzęt elektroniczny na raty lub wziąć w leasing samochód. Dodatkowo, myśląc o ochronie swoich danych osobowych musimy mieć na uwadze również to, że nawet najlepiej zabezpieczony komputer i daleko posunięta ostrożność nie ustrzeże nas w sytuacji, w której do wycieku dojdzie, w którejś z firm lub urzędu, które przetwarza informacje na nasz temat* – ostrzega Bartłomiej Drozd, ekspert serwisu ChronPESEL.pl.

Badanie „Ochrona danych osobowych w trakcie pracy zdalnej" zostało przeprowadzone we wrześniu 2020 roku na próbie 303 osób, przez Krajowy Rejestr Długów i serwis ChronPESEL.pl.

Źródło: ip