Jak zadbać o cyberbezpieczeństwo pracy zdalnej w nowej rzeczywistości

Sebastian GOSCHORSKI
Business Development Partner w RSM Poland

Sytuacja, z którą mamy do czynienia obecnie kreuje zupełnie nowe podejście do sposobu zarządzania organizacją i jej zasobami. Powodzenie tych zmian, a tym samym przetrwanie organizacji jest mocno uzależnione od tego, jak zwinnie poukładamy procesy biznesowe i jak szybko przestawimy pracowników na nowy sposób pracy. W związku z ciągłymi zmianami i brakiem możliwości dokładnego zaplanowania tego procesu, organizacje naraziły się na „cyber-ryzyko" w znacznie większym stopniu, niż było to możliwe do tej pory.

Nowa rzeczywistość, czyli nauczyć się pracować inaczej

Konieczność, czy wręcz wymuszenie przez epidemię COVID-19 pracy z domu spowodowało zmianę wielu naszych nawyków i utartych ścieżek działania. Liczne procesy biznesowe „przeniosły się" z biur do naszych domów. Takie rzeczy jak wideokonferencje, praca na oprogramowaniu firmowym (np. księgowym) stały się z dnia na dzień naszą codziennością. Wymuszone pandemią wykonywanie obowiązków z domu ma też pewne zalety takie, jak chociażby dostępność, elastyczność, brak potrzeby dojazdu do firmy, możliwość większego skupienia na pracy, czy praca na własnych urządzeniach tak ważna dla użytkowników produktów firmy Apple, ale przyczyniło się ono także do wzrostu zagrożeń związanych z cyberprzestrzenią. Powód jest dość prosty. Ilość potencjalnych i łatwych „celów" upatrzonych przez hakerów internetowych wzrosła wręcz geometrycznie, a świadomość znacznej części społeczeństwa, jak się przed nimi zabezpieczyć jest niestety znikoma.

Reorganizacja cyfrowej rutyny – ważne zasady

W czasach kryzysu, kiedy większość z nas pracuje w domu i prowadzi spotkania zdalnie, bardzo ważne jest przemyślenie i reorganizacja naszej nowej cyfrowej rzeczywistości. Oto kilka zasad, które pomogą zwiększyć cyberbezpieczeństwo podczas pracy zdalnej w Twojej firmie.

1. Dostęp do systemu firmowego powinien być możliwy tylko przez wirtualną sieć prywatną (VPN), a także za pomocą uwierzytelniania 2-etapowego (np. hasło do aplikacji i kod weryfikacyjny).
2. Dostawca oprogramowania VPN powinien być wybrany przemyślanie. Nie zawsze najtańsze lub najbardziej popularne rozwiązanie jest najlepsze.
3. Zdalny dostęp przez ograniczony czas. Warto skonfigurować zdalne połączenia na ograniczony czas (minuty / godziny).
4. Aktualizacja systemu operacyjnego i wersji oprogramowania - zaleca się aktualizację organizacyjnych systemów operacyjnych i oprogramowania do najnowszych wersji, ponieważ wielokrotnie nowsze wersje są oferowane przedsiębiorstwom ze względu na naruszenia bezpieczeństwa wykryte w starszych wersjach.
5. Program antywirusowy powinien być zaktualizowany do najnowszej wersji oraz mieć pełen pakiet bezpieczeństwa, tj. możliwość sprawdzania poczty pod kątem niebezpiecznych programów czy zabezpieczenie w postaci prostego firewalla.
6. Kopia zapasowa - należy wykonać kopię zapasową dla wszystkich odpowiednich urządzeń i informacji, a kopia ta powinna być wykonywana okresowo w celu weryfikacji jej integralności.
7. Wszelkie incydenty, które wystąpiły na komputerze używanym w domu, muszą być natychmiast zgłaszane i wyjaśniane przez dedykowane temu osoby lub wsparcie IT, które obsługuje firmę.
8. Wszelkie podejrzane maile muszą być przez nas sprawdzane i w razie podejrzeń o chęć cyberataku zgłaszane wyżej wymienionym osobom lub firmom, szczególnie mailowe zlecenia przelewów.
9. Pracownicy muszą mieć świadomość dbania o bezpieczeństwo informacji, w szczególności o dane wrażliwe.

10. Posiadanie właściwej polisy od cyberryzyka, która zapewni pomoc w przypadku utraty ważnych danych osobowych oraz pokryje koszty reakcji i zarządzania kryzysowego.
11. Przestrzeganie wszystkich procedur RODO we właściwy sposób.
12. Wykupić odpowiedzenie ubezpieczanie, które w przypadku włamania,pozwoli nam pokryć jego straty oraz zapewni odpowiednie wsparcie PR.

Musimy pamiętać, że praca z domu poprzez VPN wiąże się zazwyczaj z wolniejszym dostępem do naszych zasobów firmowych zgromadzonych np. na dyskach wspólnych. Może to spowodować chęć posiadania tych dysków na własnych, dużo gorzej zabezpieczonych komputerach domowych. W tym przypadku, oprócz ryzyka uraty danych (np. w wyniku uszkodzenia dysku) „wystawiamy się" w znacznie większym stopniu na ryzyko ich kradzieży. Zabezpieczeniem jest na pewno stworzenie możliwości automatycznej synchronizacji danych na komputerze domowym z dyskiem sieciowym firmy.

Reasumując – to, co dla nas jest nowe i często przez nas pomijane w kwestii cyberbezpieczeństwa stwarza niesamowite możliwości dla potencjalnych złodziei. Brak odpowiedniego przygotowania, zaplanowania i audytu tego, w jaki sposób umożliwiamy sobie (i naszym pracownikom) pracę zdalną może kosztować nas ogromne pieniądze. Warto zatem dokładnie sprawdzić aktualnie obowiązujące zasady pracy i systemy, testując je pod kątem różnych ryzyk oraz zawczasu się zabezpieczyć lub zmienić dotychczasową taktykę dot. pracy zdalnej i „zasady gry" w nowej rzeczywistości.