Dziesięć wskazówek dotyczących cyberbezpieczeństwa podczas pracy zdalnej

Jeszcze nigdy nie byliśmy aż tak uzależnieni od technologii, zarówno w życiu prywatnym, jak i zawodowym. Wraz ze wzrostem tej zależności rośnie liczba zagrożeń w cyberprzestrzeni. Ponadto im więcej ludzi pracuje lub studiuje z domu, tym większa szansa na to, że dojdzie do incydentu związanego z cyberbezpieczeństwem, w ten lub inny sposób.

Cyberprzestępcy wiedzą, że większa liczba osób komunikujących się on-line oznacza większe zróżnicowanie sposobów interakcji z technologią. Niektórzy użytkownicy korzystają z sieci czy oprogramowania po raz pierwszy w życiu. Cyberprzestępcy często próbują wykorzystać takie sytuacje, podstępem uzyskując dostęp do chronionych informacji. Jednocześnie firmowe działy IT i administracji koncentrują się na tym, aby zapewnić bezproblemowe działanie sieci, przez co ich zdolność do szybkiego wykrywania złośliwych działań jest obniżona.

To sprawia, że ochrona informacji poufnych jest trudniejsza niż kiedykolwiek wcześniej. W firmie Chubb staramy się w jak największym stopniu pomóc naszym klientom, np. poprzez wskazywanie sposobów na unikanie tego typu problemów. Przestrzeganie poniższych dziesięciu wskazówek może pomóc Państwa firmie i Państwa pracownikom poruszać się bezpiecznie w Internecie, także w obecnych, niepewnych czasach.

Najlepsze praktyki dla Twojej firmy

1 Przygotuj się na problemy z zasobami IT, zarówno ludzkimi, jak i technologicznymi.

Obecnie więcej ludzi pracuje zdalnie, więc centra obsługi technicznej mogą być przeciążone ilością napływających zgłoszeń i konieczne może okazać się zapewnienie większej liczby konsultantów poza normalnymi godzinami pracy. Sytuacja ta wystawia również na próbę przepustowość sieci, możliwości w zakresie przechowywania danych oraz moc obliczeniową. Pomimo tak dużego natężenia ruchu nie wolno pomijać pozornie drobnych szczegółów. Firmy powinny zwrócić szczególną uwagę na powyższe potrzeby, przygotować plan ewentualnej realokacji zasobów i być przygotowane na to, że ta zależność może z czasem być coraz większa.

2 Upewnij się, że Twoje oprogramowanie, aplikacje i sieć są na bieżąco aktualizowane.

Powszechnie wiadomo, że technologie zdalnego dostępu mają swoje słabe punkty i bardzo często zdarza się, że cyberprzestępcy właśnie za ich pośrednictwem uzyskują dostęp do chronionych informacji. Upewnij się, że całe oprogramowanie i wszystkie aplikacje są na bieżąco aktualizowane oraz usuwaj wszelkie wykryte słabości systemu.

3 Zadbaj o skoordynowanie swoich zasobów, zanim dojdzie do incydentu.

Firmy i instytucje powinny zadbać o odpowiednią koordynację swoich planów ciągłości działania (business continuity plan - BCP), planów odtworzenia systemów po awarii (disaster recovery plan - DRP) oraz planów reagowania na incydenty cybernetyczne (cyber incident response plan). Cyberprzestępcy zdają sobie sprawę, że zależność od sieci firmowej i jej dostępności jest największa w momencie, gdy korzysta z niej zdalnie dużo osób, i będą próbować wykorzystać tę sytuację.

4 Przeanalizuj aktualne zasady polityk obowiązujących w firmie i dokładnie monitoruj wszelkie niezbędne wyjątki dotyczące bezpieczeństwa.

Kiedy zasoby IT są wykorzystane do granic możliwości, firma lub instytucja może być zmuszona do wprowadzenia pewnych wyjątków dotyczących obowiązujących zasad polityk, standardów lub praktyk w zakresie bezpieczeństwa. Należy wdrożyć procedurę szczegółowej analizy w celu zapewnienia ścisłego monitorowania i traktowania tego typu wyjątków. Większość zasad dotyczących pracy z domu nie została opracowana pod kątem obecnego masowego przejścia na pracę zdalną, dlatego firmy i instytucje powinny dokładnie przeanalizować również ten obszar.

5 Korzystaj z uwierzytelniania wieloskładnikowego (multifactor authentication) – jeżeli jeszcze go nie wdrożyłeś, warto zrobić to teraz.

Tradycyjne konta, do których użytkownik loguje się z użyciem loginu i hasła, to łatwy cel dla cyberprzestępców. Jeżeli tylko jest to możliwe, należy stosować uwierzytelnianie wieloskładnikowe. Wymaga to podania minimum dwóch składników uwierzytelniania przed uzyskaniem dostępu do chronionych danych. W ten sposób tworzone są dwie linie obrony przed przestępcami. Ten dodatkowy poziom ochrony jest szczególnie ważny w sytuacji, gdy więcej osób uzyskuje zdalny dostęp do sieci, w wyniku czego cyberprzestępcy mają więcej możliwości przeniknięcia do znajdujących się w niej zasobów.

Najlepsze praktyki dla Twoich pracowników

6 Łącz się z Internetem tylko za pośrednictwem bezpiecznych sieci.

W przypadku podłączenia do sieci publicznej wszelkie informacje udostępniane w Internecie lub przez aplikacje mobilne mogą zostać przechwycone przez osoby postronne. Zawsze korzystaj z wirtualnej sieci prywatnej (Virtual Private Network - VPN) do szyfrowania swojej aktywności. Większość firm i instytucji zapewnia pracownikom połączenie VPN gwarantujące bezpieczeństwo zdalnej pracy, a indywidualne konta VPN są dostępne u różnych dostawców usług internetowych.

7 Używaj silnych haseł.

Większość ludzi używa takiego samego lub nieco zmodyfikowanego hasła do wszystkiego, zarówno w pracy, jak i prywatnie. Niestety oznacza to, że kradzież jednego hasła pozwala hakerom uzyskać dostęp do szeregu różnych kont. Zapamiętanie bezpiecznych i złożonych haseł do poszczególnych kont jest trudne, a czasem wręcz niemożliwe. Korzystaj z oprogramowania do zarządzania hasłami pozwalającego ustawić silne i unikalne hasła do wszystkich kont, ponieważ hasła są podstawą dobrych praktyk zapewnienia bezpieczeństwa w Internecie.

8 Klikaj w łącza, otwieraj załączniki i pobieraj oprogramowanie wyłącznie z zaufanych źródeł.

Większość ludzi chce być na bieżąco z nowymi informacjami, zwłaszcza w niepewnych czasach. Cyberprzestępcy o tym wiedzą i próbują wykorzystać sytuację, prezentując złośliwe łącza jako zawierające treści mogące zaciekawić użytkownika. Kliknięcie złośliwego łącza może dać im dostęp do prywatnych informacji danej osoby lub firmy, a także sparaliżować pracę komputerów lub całej sieci. Jeżeli masz wątpliwości co do źródła, zajrzyj na stronę podmiotu, która wysłał Ci dane materiały. Jeżeli to coś ważnego, informacje będą opublikowane także tam.

9 Zanim udostępnisz informacje poufne, sprawdź adres URL strony.

Cyberprzestępcy mogą tworzyć fałszywe strony internetowe, których adres URL lub strona główna wygląda niemal identycznie jak strona, do której masz zaufanie – np. Twojego systemu opieki medycznej, banku czy dostawcy poczty elektronicznej. Zamiast klikać łącze podane w wiadomości e mail, wpisz ręcznie adres URL w przeglądarce. Dodatkowo upewnij się, że adres URL strony, którą odwiedzasz, zaczyna się od HTTPS – takie strony są bezpieczniejsze niż strony z adresem zaczynającym się od HTTP.

10 Nie odpowiadaj na zapytania dotyczące informacji pochodzące z nieznanych źródeł, zwłaszcza jeżeli dotyczą one danych osobowych lub haseł.

Cyberprzestępcy starają się nakłonić ludzi do ujawnienia informacji poufnych, podszywając się pod osoby, które znasz lub z którymi pracujesz. Bardzo dokładnie sprawdzaj, komu udostępniasz informacje, nawet jeżeli sądzisz, że zapytanie pochodzi ze źródła lub od podmiotu, któremu ufasz. Nie działaj pod presją czasu – zweryfikuj starannie zapytanie, zanim odpowiesz.

Zminimalizuj swoje ryzyko cybernetyczne i zareaguj na incydent

Każda cyber polisa zawarta w Chubb zapewnia dostęp do usług, które pomogą Twojej firmie szybko zareagować na incydent cybernetyczny.

Dowiedz się więcej na chubb.com/pl-pl/products/cyber.aspx

Chubb. Insured.℠