SZANOWNI PAŃSTWO,

Nastał czas, który na wielu wymusił system pracy zdalnej. Jest to idealny moment dla działań przestępców działających w Internecie. Prosimy zatem w tym czasie zachować szczególną uwagę i ostrożność podczas wszelkich czynności wykonywanych w sieci. Poniżej przedstawiamy zagrożenia i działania przestępcze, na które jesteśmy narażeni oraz metody walki i zabezpieczeń.

TYPOWE ZAGROŻENIA

- Wyłudzenie danych dostępowych do systemów informatycznych tj. konta bankowe, dzienniki elektroniczne, konta pocztowe, konta witryn internetowych i sklepów internetowych itd.
- Wyłudzenie numeru telefonu, który można zainfekować i wykorzystać do przejęcia np. konta bankowego.
- Podstępne zobowiązanie do opłacania subskrypcji usługi świadczonej w sieci.
- Zainfekowanie komputera w celu np. rozsyłania spamu lub szpiegowania naszych działań
- Zaszyfrowanie dysku twardego w celu uzyskania okupu.

DZIAŁANIA MAJĄCE NA CELU ZWIĘKSZENIA BEZPIECZEŃSTWA

Przede wszystkim należy pamiętać, że żadna znana platforma czy instytucja nie prosi o podanie takich danych jak login, hasło, kod

jednorazowy, numer telefonu, czy dane wrażliwe. Prośba taka związana z aktualizacją danych jest możliwa tylko i wyłącznie po prawidłowym zalogowaniu się do systemu i może być związana jedynie z danymi teleadresowymi. W celu zminimalizowania ryzyka zainfekowania komputera nigdy nie wolno otwierać poczty e-mail od nieznanych i dziwnie brzmiących nadawców i pod żadnym pozorem nie wolno klikać w linki zawarte w treści i otwierać ewentualne załączniki. Ta sama zasada dotyczy wiadomości sms. W przypadku urządzeń mobilnych należy instalować jedynie oficjalne aplikacje i nie korzystać z publicznej sieci wi-fi. W celu zminimalizowania ryzyka przejęcia konta pocztowego, konta w sieci społecznościowej czy innego zawsze, jeśli to możliwe trzeba korzystać z podwójnej weryfikacji. Weryfikacja taka polega na wpisaniu odpowiedniego kodu w wiadomości sms lub kodu ze zintegrowanej aplikacji np. AUTHENTICATOR. Warto pamiętać, aby nie używać wszędzie tych samych haseł oraz aby hasło składało się wielkich i małych liter, cyfr oraz znaków specjalnych, jeśli to możliwe. Pod żadnym pozorem nie należy przekazywać tych danych osobom trzecim. W celu zabezpieczenia danych warto zainstalować oprogramowanie antywirusowe oraz firewall. Firewall może być sprzętowy lub w formie aplikacji tak jak ma to miejsce wsystemie Windows 10, gdzie zaimplementowano *Windows Defender*. Pamiętać należy o aktualizowaniu oprogramowania antywirusowego i systemów operacyjnych w celu usunięcia luk i błędów umożliwiających przejęcie kontroli lub zainfekowanie naszego komputera. Dodatkowo należy najważniejsze dane w postaci plików przechowywać w chmurze, co zabezpieczy je przed ewentualną utratą umożliwiając późniejsze ich odzyskanie.

Nawiązując do pracy zdalnej i wielu godzin, które dziecko spędza przy komputerze niejednokrotnie bez fizycznej kontroli rodzica warto rozważyć zasadność ustanowienia kontroli rodzicielskiej w systemie operacyjnym. System Windows jest standardowo wyposażony w możliwość ustanowienia takiej kontroli dla określonego konta dziecka lub dzieci. Warto wspomnieć, że w takim wypadku dziecko winno posiadać odpowiednie dla siebie konto różne od konta rodzica na które można nałożyć kontrolę rodzicielską. Przykładowe konfiguracje narzędzia są dostępne w sieci, a możliwości to m.in. blokada niedozwolonych treści w Internecie,

zezwolenie na używanie jedynie wpisanych przez rodzica stron internetowych lub aplikacji, kontrola historii działań dziecka.

Nie należy traktować powyższych informacji jako poradnika i zwracając uwagę na złożoność problemu należy pamiętać, że stosując się do wszystkich wymienionych działań nie ma gwarancji, że nie staniemy się ofiarą przestępstwa. Z pewnością jednak ostrożność i zachowanie zasad bezpieczeństwa zminimalizuje ryzyko korzystania z globalnej sieci Internet.