Wirusy i włamania do sieci komputerowych to plaga XXI wieku. Hakerzy i internetowi przestępcy rozsyłają na skrzynki pocztowe i przez SMS fałszywe wiadomości w celu wyłudzenia danych osobowych lub danych logowania do banku, zawierające często złośliwe oprogramowanie lub linki to pobrania tego oprogramowania. Przestępcy podszywają się pod strony internetowe banków lub instytucji publicznych, które łudząco podobne są do oryginalnych stron. Nieświadomy użytkownik logując się przez taką stronę, podaje poufne dane lub dane do logowania do banków przestępcom.

Często zdarza się, że na stronach internetowych w oknach reklam pojawiają się niesamowite, mające przykuć naszą uwagę wiadomości. Przykładowe tytuły to: „Niesamowite! Ten człowiek jest portierem a znalazł prosty sposób na zarabianie 2000 tysięcy złotych dziennie", „Apple iPhone 6s już za 50 zł dzięki prostemu trikowi", „Najnowsza wiadomość! Prezydent miał poważny wypadek - jest w szpitalu". Klikając w taki link narażamy się na zainfekowanie komputera szczególnie, gdy nie jesteśmy chronieni przez oprogramowanie antywirusowe. Ok. 6 lat temu mój brat Maciek po zalogowaniu się do komputera zobaczył ogłoszenie wypełniające cały ekran i uniemożliwiające dalszą pracę na komputerze: „Na twoim komputerze znaleziono pirackie oprogramowanie - jeżeli nie wpłacisz 300 dolarów na numer konta podany poniżej zawiadomimy organy ścigania w tym Prokuratura Generalnego". Było to złośliwe oprogramowanie typu *ransomware*. Szyfruje ono cały dysk i zgromadzone na nim dane takie jak zdjęcia, muzykę i ważne pliki. Mój brat, mimo że oprogramowanie na naszych domowych komputerach jest legalne łącznie ze wszystkimi grami, bardzo się przestraszył i zadzwonił do pracy do naszego taty. Tata natychmiast polecił wyłączyć komputer i wypiąć go z sieci. Na szczęście wszystkie ważne pliki takie jak ważne dokumenty i zdjęcia z wakacji były zgromadzone na komputerze rodziców. Na komputerze Maćka były zainstalowane tylko gry, których oryginały w postaci płyt CD Maciek trzymał na półce. Przestępcy liczyli na to, że komputer który zaatakowali zawiera cenne dla właściciela dane i chętnie zapłaci im okup. Ale się przeliczyli. Tata po przyjściu do domu sformatował dysk i ponownie zainstalował system *Windows*. Maciek z powrotem wgrał swoje gry z oryginalnych nośników i na tym cała sprawa się skończyła. Od tego czasu zwracamy szczególną uwagę, aby oprogramowanie antywirusowe, które mamy na naszych komputerach posiadało moduł zwalczający *ransomware*.

Od kiedy pamiętam mój tata zawsze dbał o to, aby na naszych wszystkich domowych komputerach (jest ich 4) zawsze było aktywne oprogramowanie antywirusowe i zapora sieciowa (tzw. *firewall*). Od 2 lat stosujemy płatną wersję programu *Bitdefender Family Pack*. Program umożliwia ochronę komputerów PC oraz telefonów komórkowych w systemach

Android i iOS. Program w chwili obecnej chroni 4 komputery (2 desktopy, 2 laptopy) i 4 telefony komórkowe w naszej rodzinie. Posiada moduł skanowania komputera i podpiętych dysków, *firewall*, moduł chroniący przed oprogramowaniem *ransomeware,* moduł chroniący przed *phishingiem*, moduł do transakcji bankowych oraz sejf plików. Sejf plików programu *Bitdefendr* tworzy specjalne, szyfrowane miejsce na dysku, w którym rodzice przechowują ważne pliki jak np. rozliczenia podatkowe, skany wyników badań lekarskich czy inne ważne dokumenty. Wiemy bowiem, że te dokumenty są szczególnie ważne przede wszystkim dlatego, że zawierają nasze dane osobowe. Program antywirusowy ma również moduł kontroli rodzicielskiej i tzw. niszczarkę plików. Wiadomo przecież, że po standardowym wykasowaniu ważnego pliku można go z powrotem przywrócić z pomocą odpowiedniego oprogramowania. Aby tego uniknąć i aby przestępcy po ewentualnym włamaniu do komputera nie odtworzyli tych ważnych, skasowanych plików – stosuje się tzw. niszczarki plików. Programy te, w miejscu wykasowanego pliku wgrywają i kasują generowane sztucznie dane powtarzając ten proces kilka razy. Po takim zabiegu (już po siedmiokrotnym wgraniu i wykasowaniu sztucznych danych w miejsce usuwanego pliku) odzyskanie jego kopii jest już niemożliwe. Tata również regularnie przeprowadza skanowanie każdego komputera raz w miesiącu oraz czyści zawartość systemu z podwójnych plików, plików śmieci i historii aktywności sieciowej.

Cieszę się, że moi rodzice tak świadomie dbają o bezpieczeństwo danych osobowych całej naszej rodziny. Dzięki temu razem z bratem czujemy się bezpiecznie, a przede wszystkim nabywamy właściwych nawyków niezwykle ważnych we wciąż rozwijającym się świecie technologii.