Tylko dwie rzeczy są nieskończone...

Południe. Główna ulica 400-tysięcznego miasta. Spokojnie stoję w kolejce do bankomatu. Za mną ustawiła się dziewczyna z chłopakiem. Zazwyczaj nie podsłuchuję rozmów, ale mówili na tyle głośno, że ja (i pewnie jeszcze kilka innych osób) słyszałem wszystko mimowolnie.

Dziewczyna powiedziała chłopakowi, że nie pamięta PIN-u i że musi zadzwonić do koleżanki. Wzięła telefon, wykręciła numer. Rozmowa przebiegła mniej więcej tak: *Cześć Ewelina! Słuchaj, nie pamiętam PIN-u do mojej karty bankowej. Na moim biurku leży taki zielony segregator. Tam jest taka lista z wszystkimi moimi hasłami*. Lista z hasłami? Nierozsądne, ale bardzo typowe. Wiele osób tak robi. Najgorsze jednak miało dopiero nadejść. *Jak, jak? 3765? Tak – to chyba ten. Dzięki, cześć!*. Prawdziwi z nas hakierzy! Poznaliśmy numer PIN tej kobiety, chociaż tak naprawdę nic nie zrobiliśmy. W tym miejscu powinienem napisać: *co by się stało, gdyby zamiast mnie stał tam jakiś złodziej...*, ale czy to nie jest oczywiste? I gdy już myślałem, że poziom głupoty sięgnął zenitu, chłopak rzekł do dziewczyny: *Zapisz sobie ten numer w komórce*. Przecież czterocyfrowy numer telefonu w książce adresowej na pewno nie wzbudzi żadnych podejrzeń u przestępcy...

Wraz z rozwojem cywilizacji jesteśmy zmuszeni do zapamiętywania coraz to większej ilości informacji. Urodziny znajomych, terminy spotkań, ważniejsze numery telefonów. Nic dziwnego, że próbujemy różnych sposobów, aby ułatwić sobie życie. A w dzisiejszych czasach nic nie ułatwia go tak jak telefony komórkowe. W książce adresowej zapisujemy numery telefonów znajomych. Urodziny i terminy spotkań w terminarzu. Jak widać, nawet PIN do karty płatniczej możemy zapisać w komórce. Wkrótce zaczniemy wpisywać nasz adres, godziny, o których nie ma nas w domu, imię psa, rasę oraz jak go można udobruchać. Model alarmu, jakiego używamy (oczywiście wraz z numerem PIN do niego), a także to, gdzie w mieszkaniu należy szukać drogocennych przedmiotów.

Człowiek w całym łańcuchu bezpieczeństwa był, jest i będzie jego najsłabszym ogniwem.

Być może już wkrótce banki zrozumieją, jaką krzywdę robią ludziom. Pójdą swoim klientom na rękę i zaczną drukować PIN-y na kartach płatniczych. Cóż to by była za wygoda i oszczędność czasu! Już nigdy nie pomyliłby nam się PIN do karty kredytowej z PIN-em do domofonu. Nie musielibyśmy się martwić, że znowu źle wpiszemy kod i nasza karta zostanie przez bankomat zatrzymana. Zakupy w sklepie byłyby pozbawione jakiegokolwiek stresu. Gdy tylko doszłoby do płatności, wystarczyłoby podać ekspedientce kartę. Ona już sama za nas wpisałaby PIN do terminala. Nie byłoby też żadnych przeszkód, aby poprosić znajomego, żeby poszedł za nas wyciągnąć pieniądze z bankomatu. Po prostu idylla.

Zmieniając temat: czy wydawanie magazynu *Hakin9* w ogóle ma sens? Piszemy, jak poprawnie konfigurować systemy informatyczne. Uczymy o tym, jak pisać bezpieczne aplikacje. Opisujemy algorytmy kryptograficzne, których bezpieczeństwo jest zapewnione skomplikowanymi wzorami matematycznymi. Zwykły użytkownik może jednak zainstalować najlepsze i najdroższe produkty zapewniające bezpieczeństwo. Może je poprawnie skonfigurować i uruchomić wszystkie niezbędne dodatki, a i tak pozostaje wciąż narażony na niebezpieczeństwo. Bo nawet najlepsze drzwi antywłamaniowe nie powstrzymają złodzieja, jeśli klucz schowamy pod wycieraczkę. Czy jest zatem sens wymyślać coraz lepsze zabezpieczenia, kiedy problem leży zupełnie gdzie indziej?

Idealnym rozwiązaniem byłoby stworzenie takich systemów

informatycznych, które byłyby *po prostu* bezpieczne. I nieważne, czy korzystałby z nich doświadczony administrator, osoba, która nie ma pojęcia o bezpieczeństwie komputerowym, czy ktoś o inteligencji marchewki. Taki program wystarczyłoby zainstalować w swoim systemie, i już żaden haker nie mógłby dostać się do naszych zasobów. Moglibyśmy umieścić nasze kody w Internecie albo wpuścić hakera do naszego mieszkania. System i tak pozostałby niezdobyty. Niestety, takie programy pozostają jedynie w sferze marzeń. Jakbyśmy się nie starali, nie uda nam się stworzyć zabezpieczeń całkowicie *idioto-odpornych*, gdyż idioci są genialni w swojej głupocie. Jeśli nawet przewidzielibyśmy wszystkie głupstwa, jakie może popełnić użytkownik, to i tak zrobiłby on coś, na co nigdy nie wpadlibyśmy. Jakiś czas temu w większości systemów wprowadzono wykrywanie słabych haseł już w czasie rejestracji. Jednak im dłuższe i mocniejsze hasło, tym większe prawdopodobieństwo, że użytkownik karteczkę z hasłem naklei na monitor albo w ogóle zapomni, jakie hasło wpisał. Gdy zmusimy użytkownika do stworzenia profilu o ograniczonych prawach, to i tak permanentnie będzie korzystał z konta na prawach administratora. Gdy domyślnie zainstalujemy w systemie ochronę antywirusową, to użytkownik ją wyłączy (*bo przez ten program komputer wolniej działa*).

Innym rozwiązaniem (i chyba najbardziej racjonalnym) jest informowanie społeczeństwa o niebezpieczeństwach, jakie czyhają w cyberprzestrzeni. Ale przecież już to robimy! Informujemy, apelujemy, prosimy i grozimy. I co? I nic! Nie wierzę, aby bohaterka naszej historii nie wiedziała o tym, jak poufną informacją jest numer PIN. Że nie można podawać go innym i że należy chronić go jak największej tajemnicy. Że jeśli złodziej pozna PIN, to będzie mogła pożegnać się z ciężko zarobionymi pieniędzmi odłożonymi na koncie. Bo choć pieniądze w banku są ubezpieczone od kradzieży, to nie zobaczymy ani grosza, jeśli okaże się, że to my podaliśmy złodziejowi hasło do naszego konta.

Nic dziwnego, że cyfrowi przestępcy nie łamią haseł do kont bankowych. Oni po prostu grzecznie o nie proszą. Złodzieje wysyłają miliony maili, podając się za bank X i – pod pozorem na przykład świątecznej promocji – proszą o zalogowanie się na specjalnie spreparowanej stronie, wyglądającej jak strona banku X. Metoda ta nazywa się *phishingiem*. Jest ona o wiele szybsza, prostsza i skuteczniejsza niż łamanie zabezpieczeń banku. A dopóki klienci banków podają numer PIN, jakby był on numerem telefonu, to takie praktyki będą jeszcze się nasilać. I, pomimo że banki ostrzegają swoich klientów przed oszustami, ciągle słyszymy o kolejnych tego typu atakach.

Nawet Kevin Mitnick, który jest uważany za największego hakera na świecie, mówił, że łamał ludzi – nie hasła. Z kolei Albert Einstein podobno powiedział: *Tylko dwie rzeczy są nieskończone: wszechświat i ludzka głupota. Choć co do tego pierwszego to nie mam pewności.*

Czuję, że jesteśmy bezsilni w tej kwestii. Przez ostatnie 30 lat zrobiliśmy milowe kroki w kwestii zabezpieczeń. Jednak jeśli chodzi o świadomość społeczeństwa, to dalej jesteśmy tam, skąd wyruszyliśmy. Swoją drogą... pozostaje dla mnie tajemnicą, dlaczego ludzie chodzą z numerami PIN w portfelach, ale przyczepienie do klucza breloczka z adresem mieszkania uznają za totalny kretynizm? Te dwie czynności powinny wywoływać w ludziach taką samą reakcję! Różnią się między sobą tylko tym, że klucz chroni nasze mieszkanie, a PIN – nasze pieniądze.

Krzysztof Piecuch jest studentem informatyki Uniwersytetu Wrocławskiego. Interesuje się programowaniem i algorytmiką. Nie ma problemu z zapamiętaniem 4-cyfrowego numeru PIN. Kontakt: *krzysztof.piecuch@gmail.com*