Cyberdefence 24

aut. Sylwia Gliwa 21.05.2019

LENISTWO UŻYTKOWNIKÓW SPRZYJA CYBERPRZESTĘPCOM [WYWIAD]

O konsekwencjach utraty smartfonu, co zrobić, gdy stracimy dostęp do naszych mediów społecznościowych oraz zachowaniu użytkowników w sieci, które sprzyja przestępcom mówią Weronika Bartczak i Piotr Derlecki z CyberRescue

Codziennie do komunikacji w celach biznesowych i prywatnych używamy smartfonów które obecnie są już naszym małym mobilnym centrum zarządzania komunikatorami, mediami społecznościowymi, aplikacjami podpiętymi pod nasze konto bankowe czy skrzynkami pocztowymi. Utrata smartfonu może pociągnąć za sobą dużą stratę finansową oraz również umożliwi wejście w posiadanie naszych danych osobowych. Jakie powinny być pierwsze kroki przy utracie telefonu? Czy zgłoszenie sprawy do organów ścigania ma jakikolwiek sens?

Tak naprawdę pierwsze kroki powinniśmy podjąć jeszcze przed utratą telefonu. Zarówno system Android, jak i iOS pozwalają na zadbanie o nasze dane i odzyskanie telefonu zanim to jeszcze się wydarzy. Po utracie telefonu można spróbować go zlokalizować, można na nim umieścić wiadomość dla osoby, która go znajdzie, a także można zdalnie usunąć dane z telefonu. Na to pozwalają ustawienia konta Google oraz usługi takie jak “Znajdź mój iPhone”. – wyjaśnia Weronika Bartczak, specjalista ds. cyberbezpieczeństwa CyberRescue. Warto także ustawić blokadę ekranu, dzięki czemu trudno będzie dostać się do danych telefonu.

Myślę, że zawsze warto jest zgłosić kradzież policji. Na szczęście mam dobrą wiadomość dla czytelników - kradzieży telefonów jest coraz mniej (60 tys. w 2005r., 14 tys. w 2018r., wg UKE) właśnie przez to, że łatwiej go obecnie zlokalizować, a trudniej się do niego włamać, przez co staje się bezużyteczny dla złodzieja.

Newralgicznym z punktu widzenia biznesu, ale i dość stresującą sytuacją dla osoby prywatnej jest podszywanie się i publikowanie treści na przeróżnych portalach społecznościowych. Przejęcie naszego wirtualnego „ja” może nieść za sobą skutki zarówno zawodowe jak i dotkliwe straty społeczne. W wypadku tego typu działań, podobnie jak w wypadku internetowego nękania, organy ścigania raczej nie są dość efektywne. W jaki sposób użytkownik może reagować na tego działania? Jak zablokować dostęp do swoich kont społecznościowych, kiedy doszło już do ich przejęcia?

Rzeczywiście, zdarzały nam się nawet przypadki, w których podszywanie się pod osobę prywatnie w Internecie miało wpływ na jej życie zawodowe i wizerunek. To bardzo stresująca sytuacja, bo my traktujemy to jak nękanie, ale według polskiego prawa osoba jest winna wtedy, kiedy jej zamierzeniem był uszczerbek na zdrowiu fizycznym, psychicznym lub sytuacji finansowej ofiary.

Zabezpieczeniem kont powinniśmy zająć się zanim cokolwiek się stanie. Czasami wystarczy 5 minut -

stworzenie skomplikowanego hasła oraz włączenie weryfikacji dwuetapowej może uchronić nas przed przejęciem konta na mediach społecznościowych. Podszywanie możemy zgłosić bezpośrednio na portalu i z reguły duże portale (Facebook, Instagram) szybko się tym zajmują. Niestety, jeśli ktoś chce nam zrobić krzywdę to będzie po prostu tworzył kolejne profile. W takim przypadku przede wszystkim powinniśmy ostrzec naszych znajomych, że ktoś się pod nas podszywa, by być czujnym na podejrzane wiadomości oraz zgłosić się na policję. Może ona zwrócić się bezpośrednio do portalu i spróbować namierzyć atakującego np. po lokalizacji logowania. Trochę gorzej bywa z odzyskaniem konta, jeśli oszust zmieni nasze hasło oraz e-mail: trzeba przejść przez weryfikację ze strony portalu, która może trochę potrwać.

Załóżmy, że utraciliśmy kontrolę nad naszymi mediami społecznościowymi czy prywatną lub służbową skrzynką mailową. W jaki sposób jesteśmy w stanie sprawdzić jakiego rodzaju i w jakiej skali wyrządzono szkody?

Jeśli nasz klient odzyska dostęp do profilu przechodzimy z nim przez tzw. “kontrolę szkód”. Trzeba przejrzeć opublikowane posty, ustawienia profilu (np. czy został dodany inny pomocniczy mail), dodanych znajomych, jakie aplikacje (z jakimi uprawnieniami) mają dostęp do konta, wysłane wiadomości. Nie jesteśmy w stanie sprawdzić wszystkiego, przede wszystkim dlatego, że niektóre rzeczy można ukryć - np. skasować wysłane wiadomości. Podobnie ze skrzynką mailową: wysłane wiadomości, dodane kontakty, ale przede wszystkim jakiego rodzaju dane były na skrzynce. Warto wyszukać frazy typu: “PESEL”, “numer dowodu”, “hasło”, “umowa najmu”. Jeśli trzymaliśmy dane osobowe lub poufne na skrzynce to warto je zabezpieczyć przed ich nielegalnym wykorzystaniem.

Dużo mówi się o edukacji użytkowników sieci w zakresie „higieny” działania w sieci o zasadach zachowania bezpieczeństwa, weryfikowania, gdzie i jakie dane o sobie udostępniamy. Jakie zachowania użytkowników sprzyjają przestępcom i jak się ich ustrzec?

Internet pełen jest okazji, jest także najszybszym medium, wszystko jest w nim dostępne w zasadzie od momentu, kiedy się wydarzyło. Wszelkie premiery filmów, gier, seriali czy maile oferujące nowe darmowe smartfony to pole do popisu dla przestępców. To czas ich wzmożonej aktywności, ponieważ chcemy zobaczyć ten film już, teraz, najlepiej za darmo i na własne życzenie ściągamy wirusa. Jesteśmy także przyzwyczajeni do tego, że wirus od razu da o sobie znać, że go zauważymy, a wcale tak nie jest - obecnie wirusy często zaczynają działać dopiero kilka dni po pobraniu, w tle, rejestrując np. to, co wpisujemy na klawiaturze (hasła do portali i bankowości).

Kolejnym zachowaniem, które im sprzyja jest nasza niechęć do wysiłku ;) Nie chce nam się wymyślać trudnych haseł, innych dla każdego portalu, więc często używamy tego samego do kilku stron, co ułatwia włamanie. To tak, jakby każdy lokator w bloku używał takiego samego klucza do każdego z mieszkań: zgubienie przez jedną osobę klucza skutkowałoby zagrożeniem włamania do każdego mieszkania.

Nie winię nas, spamiętanie wszystkich haseł byłoby naprawdę trudne. Dlatego polecam manager haseł. To program/aplikacja, która pomaga generować trudne hasła oraz bezpiecznie je przechowuje.

CyberRescue, którą Państwo reprezentuje jest ściśle powiązana z działalnością bankową. Jak rozumiem zamysłem w pierwszej kolejności było stworzenie narzędzia do ochrony i pomocy klientom banku. Jakiego rodzaju problemy, wyzwania, ale i przejawy dobrych praktyk rokujących na przyszłość dostrzegają Państwo obecnie w polskim systemie regulacyjnym w kontekście bezpieczeństwa klientów bankowości elektronicznej?

Głównym zamysłem oferowania usługi CyberRescue przez bank jest to, że klienci, którzy będą bardziej bezpieczni prywatnie będą też bardziej uważać na bezpieczeństwo swoich finansów. Na

pewno wyzwaniem zawsze jest wprowadzenie jakiejkolwiek zmiany, ponieważ jesteśmy przyzwyczajeni do pewnych rzeczy (np. papierowych kart z kodami uwierzytelniającymi transakcje), a nagle powinniśmy to zmienić.

Kolejnym wyzwaniem może być to, że świat Internetu bardzo szybko się zmienia; pojawiają się nowe technologie, nowe rozwiązania, a regulacje prawne mogą za nimi nie nadążać. Natomiast to, co bardzo mnie cieszy to podejmowanie działań mających na celu polepszenie zabezpieczeń przede wszystkim użytkowników indywidualnych, ponieważ zawsze najsłabszym ogniwem jest człowiek. Banki mają dobrze zabezpieczone infrastruktury, ale nie są w stanie przypilnować każdego klienta. Dlatego mBank obecnie testuje tzw. biometrię behawioralną spółki Digital Fingerprints, która pozwoli na ciągłą weryfikację użytkownika podczas jego sesji online w banku. Pozwoli to na wykrycie zarówno programów, które mogą chcieć przejąć sesję, jak i oszustów mających dane logowania klienta. To ogromny krok w kierunku zabezpieczenia użytkowników.

Wywiadu udzielili:

Weronika Bartczak - specjalista ds. cyberbezpieczeństwa CyberRescue

Piotr Derlecki - specjalista ds. cyberbezpieczeństwa CyberRescue