Biuletyn Bezpieczeństwa Komputerowego

Cyfrowa spuścizna

Wstęp

Czy zastanawialiście się kiedyś nad frapującym pytaniem: "Co stanie się z naszą obecnością w cyberprzestrzeni po śmierci lub kiedy staniemy się niezdolni do samodzielnej egzystencji?" Większość ludzi zdaje sobie sprawę z konieczności pozostawienia testamentu i listy ważny spraw dla naszych bliskich na wypadek śmierci. Lecz co się stanie z naszymi cyfrowymi danymi i kontami internetowymi? Czy nie powinniśmy rozważyć pewnego rodzaju cyfrowego testamentu? Czy nie powinniśmy stworzyć cyfrowego planu dziedziczenia?

Zastanówmy się nad naszą cyfrową obecnością. Konta bankowe, plany emerytalne, dane kredytowe, rodzinne filmy i fotografie, konta smart domów, e-maile i konta na portalach społecznościowych to tylko niektóre z przykładów, które pozostawiają nasze cyfrowe odciski palców. Na wypadek naszej śmierci lub osoby bliskiej, członkowie rodziny będą potrzebowali dostępu do naszych kont i danych. Ponadto, nasza cyfrowa spuścizna wraz z kontami internetowymi mogą stać się z czasem podatne na ataki hackerskie i tym samym staną się niebezpieczne dla rodziny i przyjaciół.

Stwórz plan

Dobrym pomysłem jest przedyskutowanie tego wraz ze swoją rodziną i zaufanymi przyjaciółmi podobnie jak inne detale na wypadek naszej śmierci. Dodatkowo podczas rozmów przedstaw w sposób zewidencjonowany twoje uczestnictwo na portalach społecznościowych, kontach internetowych i cyfrowe dokumenty. Jeśli nie zadbamy o dostęp do naszych kont internetowych na wypadek śmierci, może to stanowić dla członków rodziny poważny problem kiedy już odejdziemy z tego świata. Dla przykładu, nie chcielibyśmy żeby członkowie naszej rodziny zostali odcięci od zbieranych przez nas online prywatnych, rodzinnych fotografii i filmów.

Jednym ze sposób na zachowanie swojej cyfrowej obecności jest używanie menedżera haseł. Jest to program, który bezpiecznie przechowuje wszystkie nasze loginy i hasła, numery kart kredytowych i inne wrażliwe informacje. Menedżer haseł zaprojektowany jest do tworzenia, przechowywania i umożliwiania dostępu do haseł i pytań bezpieczeństwa, czyniąc to o wiele prostszym. W wielu przypadkach jest to potężne narzędzie do archiwizowania naszej cyfrowej obecności. Niektóre programy tego typu umożliwiają skonfigurowanie ich w taki sposób aby część haseł było dostępnych dla innych zaufanych członków rodziny. Jeśli nie czujemy się komfortowo z powyższym rozwiązaniem, zawsze możemy zapisać dostęp do menedżera haseł i zapieczętować go w kopercie, która zostanie otwarta dopiero po naszej śmierci przez wykonawce testamentu. W ten sposób, członkowie rodziny będą mieli dostęp do głównego hasła uwierzytelniającego menedżera haseł a tym samym do kont i informacji tam przechowywanych.

Ponadto, niektóre serwisy umożliwiają dodanie zaufanych kontaktów, na wypadek naszej śmierci. Na przykład serwis Facebook pozwala użytkownikom wcześniejszy wybór czy na wypadek śmierci nasze konta zostaną usunięte czy zapamiętane. Zapamiętany profil tworzy przestrzeń widoczną jedynie dla przyjaciół, gdzie mogą dzielić się swoimi wspomnieniami. Ostatecznie, możemy poradzić się prawnika lub osoby pomagającej sporządzić nam testament, która będzie miała pojęcie o dziedziczeniu naszej cyfrowej obecności.

Dziedziczenie Cyfrowych Aktywów

Możemy znaleźć się w sytuacji w której będziemy musieli uzyskać dostęp lub odzyskać dane niedawno zmarłego przyjaciela lub członka rodziny. Zalecamy aby przed podjęciem jakichkolwiek działań skonsultować się z prawnikiem lub członkami rodziny. Rodzina może się zdenerwować jeśli podejmiesz działania bez wcześniejszej konsultacji z nimi. Rozpocznij od zidentyfikowania haseł, które znasz i do których masz dostęp. Być może rodzina przechowuje gdzieś zapisane hasła? Rodzina może mieć wciąż dostęp do urządzenia, na którym osoba zmarła jest wciąż zalogowana. Jeśli nie zachodzą powyższe okoliczności najprawdopodobniej konieczne będzie odzyskiwanie po kolei dostępu do poszczególnych kont i stron internetowych. Często wymagane jest aby przedstawić akt zgonu wraz z dowodem, że jest się rodziną denata. W niektórych przypadkach nie będzie możliwe uzyskanie dostępu do kont, można wtedy jedynie wnioskować o usunięcie ich. Zróżnicowany jest czas załatwienia tego rodzaju sprawy w zależności od podmiotu do którego wnioskujemy, niemniej jednak trzeba być przygotowanym na to, że zajmie to trochę czasu.

W dzisiejszym, cyfrowym świecie powinniśmy brać pod uwagę rozporządzenie nie tylko materialnymi składnikami naszego majątku ale również tymi cyfrowymi.

Polski przekład

CERT Polska jest zespołem działającym w strukturach NASK, powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w polskiej sieci Internet. Należy do organizacji FIRST, w ramach której współpracuje z podobnymi zespołami na całym świecie.
WWW: http://www.cert.pl
Twitter: @CERT_Polska
Facebook: http://facebook.com/CERT.Polska

Redaktor gościnny

Cheryl Conley *jest ekspertem w zakresie ataków phishingowych i rozpowszechniania wiedzę z zakresu cyberbezpieczeństwa. Swoje doświadczenia zdobywała pomagając przy tworzeniu i zarządzaniu projektem phishingowym w Lockheed. Obecnie wspiera zespół SANS Security Awareness. Jest również posiadaczką certyfikatu SANS Security Awareness Professional.*

Źródła

Menedżer haseł: http://www.sans.org/u/Y5Y
Tworzenie haseł w prostszy sposób: http://www.sans.org/u/Y63

Biuletyn OUCH! powstaje w ramach programu „Security Awareness" Instytutu SANS i jest wydawany na licencji Creative Commons BY-NC-ND 4.0 license. *Powielanie treści biuletynu jest dozwolne jedynie w celach niekomercyjnych oraz pod warunkiem zachowania informacji o źródle pochodzenia kopiowanych treści oraz nienaruszania zawartości samego biuletynu. Informacje kontaktowe:* www.sans.org/security-awareness/ouch-newsletter. *Editorial Board: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Polski przekład (NASK/CERT Polska): Bartłomiej Wnuk, Konrad Purzycki, Janusz Urbanowicz*