Cyfrowa luka pokoleniowa

Wstęp

Próba jak najlepszego wykorzystania dzisiejszej technologii może być przytłaczająca dla prawie każdego z nas. Szczególnie trudna może być dla członków rodziny, którzy nie są do niej przyzwyczajeni oraz nie są dobrze z nią obeznani. Dlatego pragniemy podzielić się kluczowymi krokami, aby pomóc zabezpieczyć członków rodziny, którzy mogą mieć problem z technologią i mogą źle zrozumieć ryzyko związane z jej używaniem.

Skoncentruj się na podstawach

Zazwyczaj najlepszym sposobem, aby pomóc w zabezpieczeniu członków rodziny, jest maksymalne uproszczenie bezpieczeństwa. Skoncentruj się na tych najmniejszych krokach, które będą miały największe znaczenie.

1. **Socjotechnika:** Ataki socjotechniczne są jednym z podstawowych sposobów, w jaki większość z nas jest atakowana. Wyjaśnij, że oszustwa i oszuści istnieją od tysięcy lat i ataki tego typu to nic nowego. Jedyną różnicą jest to, że teraz używa się do tego Internetu. Przedstaw przykłady popularnych ostatnimi czasy wiadomości e-mail podszywających się pod bank lub firmę kurierską z przesyłką. Upewnij się, że członkowie rodziny rozumieją, że nigdy nie powinni nikomu podawać swojego hasła, numeru kart kredytowej czy danych osobowych. Zwróć uwagę, że im większe poczucie pilności w wiadomości e-mail, tym większe prawdopodobieństwo ataku. Niektórzy przestępcy żerują na uczuciach, polując na naszych bliskich, którzy stęsknieni miłości, są ich wymarzoną perspektywą. Ponadto niech wiedzą, że jeśli czują się nieswojo lub mają zastrzeżenia do wiadomości e-mail lub kogoś dzwoniącego, najpierw powinni zadzwonić do Ciebie zanim zdecydują się podać jakiekolwiek informacje.
2. **Domowa sieć Wi-Fi:** Poświęć chwilę aby upewnić się, że sieć Wi-Fi w ich domu jest bezpieczna a hasło dostępowe jest inne niż domyślne. Możesz też rozważyć skonfigurowanie sieci Wi-Fi tak, aby używać bezpiecznego DNS takiego jak https://www.opendns.com. Bezpieczne usługi DNS nie tylko pomagają powstrzymać użytkowników przed odwiedzeniem zainfekowanych stron internetowych, ale także dają kontrolę nad wyborem, które strony internetowe będzie można odwiedzić lub nie, co może być szczególnie przydatne kiedy z Internetu korzystają dzieci.
3. **Aktualizacja:** Utrzymanie aktualnego oprogramowania jest kluczowe i znacząco utrudnia przestępcom złamanie zabezpieczeń. Upewnij się, że automatyczne aktualizacje są włączone, jeśli

nie, włącz je wszędzie gdzie to tylko możliwe. Jeśli urządzenie lub system, z którego korzystasz jest przestarzały i producent już go nie wspiera, pomyśl o zakupie nowego urządzenia, który obejmuje aktualizację bezpieczeństwa.

4. **Hasła:** Silne i bezpieczne hasła są kluczem do ochrony zarówno urządzeń, jak i wszelkich kont online. Przeprowadź członków rodziny przez proces tworzenia silnych haseł. Wyrażenia hasłowe mogą być dla nich najprostsze w użyciu i łatwe do zapamiętania. Innym pomysłem jest zainstalowanie menedżera haseł i nauczenie ich jak go używać. Dzięki temu pomysłowi, bliscy nie będą musieli pamiętać wszystkich haseł, a jedynie tylko to do menedżera haseł. W zależności od używanej wersji menedżera haseł, niektóre umożliwiają zdalne nimi zarządzanie, co może być ułatwieniem jeśli będziesz chciał pomóc na odległości. Jeśli natomiast używanie menedżera haseł jest dla nich za trudne, w ostateczności można zasugerować im aby zapisywali hasła i przechowywali je w bezpiecznym miejscu. W przypadku kluczowych kont takich konto bankowe, sugerujemy skonfigurowanie dwuskładnikowe uwierzytelnianie. Ponadto upewnij się, że posiadasz plan dziedziczenia dla każdego konta online w ten sam sposób, w jaki przygotowałbyś testament dla aktywów fizycznych.
5. **Kopie zapasowe:** Kiedy wszystko inne zawiedzie, tylko kopie zapasowe mogą uratować sytuację. Upewnij się, że członkowie rodziny mają prosty i niezawodny system do tworzenia kopii zapasowych swoich plików. Ostatnimi czasy rozwiązanie oparte na chmurze są bardzo popularne i często lepsze od tradycyjnego przechowywania danych na dysku twardym.

Jeśli członkowie rodziny czują się przytłoczeni, pomóż im koncentrując się tylko na podstawach zachowujących możliwie najlepszą ochronę. Bądź również cierpliwy, daj czas i przestrzeń na popełnianie błędów i pomóż innym, aby ich nie powtarzali. Zastanów się również nad zapisaniem ich do OUCH! komputerowego biuletynu informacyjnego.

Redaktor gościnny

Chris Dale (Twitter @chrisadale) jest głównym konsultantem w River Security, europejskiej firmie konsultingowej zajmującej się bezpieczeństwem oraz jest certyfikowanym instruktorem SANS (https://www.sans.org/profiles/chris-dale/). Znajdź Chrisa na LinkedIn: https://www.linkedin.com/in/chrisad/

Źródła

Ataki socjotechniczne: https://www.sans.org/security-awareness-training/resources/social-engineering-attacks
Menedżer haseł: https://www.sans.org/security-awareness-training/resources/password-managers-0
Aktualizacje: https://www.sans.org/security-awareness-training/resources/power-updating
Czy robisz kopie zapasowe: https://www.sans.org/security-awareness-training/resources/got-backups
Cyfrowa spuścizna: https://www.sans.org/security-awareness-training/resources/digital-inheritance

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz