Politycy: Rozmawiają o cyberbezpieczeństwie, a sami dają się nabrać na ataki phishingowe?

- 27 kwietnia 2026 r.

Wprowadzić teraz kod bezpieczeństwa? Jasne!

„Wprowadź swój PIN”: Z pewnością przeciętny człowiek bardzo dokładnie zastanowiłby się, czy zastosować się do tej niespodziewanie wyskakującej prośby w wiadomości na Messengerze, prawda? Cóż, niemieccy politycy tego nie robią. Straszliwy „cyberatak” na członków rządu federalnego, który wszystkie media reklamują jako rosyjski atak szpiegowski, był kampanią phishingową, na którą żaden przeciętnie obeznany z internetem

obywatel nie da się już nabrać. Politycy jednak dają. I to właśnie ci sami politycy chcą ograniczyć media społecznościowe i domagają się większej „edukacji medialnej”.

Komentarz Vanessy Renner

W marcu minister ds. rodziny Karin Prien (CDU) przypuściła atak na wolny internet, wezwała do wprowadzenia zakazów korzystania z mediów społecznościowych dla młodzieży i mówiła o „edukacji medialnej”. W ten weekend ujawniono, że Prien – wraz z przewodniczącą Bundestagu Julią Klöckner (CDU) i minister Vereną Hubertz (SPD) – padli „ofiarami” ataku phishingowego za pośrednictwem komunikatora Signal. Termin „ofiary” został tu uwzględniony w cudzysłowie, ponieważ taktyka ta jest znana; politycy i wojskowi byli ostrzegani przed tą kampanią od miesięcy , a nawet Chaos Computer Club niedawno nie miał innego wyjścia, jak tylko mówić o „poważnej indywidualnej porażce”.

Chociaż Prokuratura Federalna od dawna prowadzi śledztwo w sprawie podejrzenia szpiegostwa – uważa się, że „atak” miał swoje źródło w Rosji – w internecie współczucie dla niemieckich polityków i innych ofiar pozostaje ograniczone. Koncepcja ataku jest dobrze znana: użytkownik otrzymuje wiadomość z rzekomego konta wsparcia, która sfabrykuje zagrożenie bezpieczeństwa. Następnie użytkownik jest proszony o podanie kodu PIN lub wysłanie SMS-a weryfikacyjnego w celu ochrony swojego urządzenia. Oczywiście to go nie chroni; w rzeczywistości daje atakującym dostęp do jego konta.

Takie ataki są jednym z powodów, dla których aplikacje do przesyłania wiadomości domyślnie wyświetlają ostrzeżenia o nieznanych kontaktach. Każdy może wybrać „Wsparcie” jako nazwę użytkownika. Heise.de pokazał zrzuty ekranu takich wiadomości phishingowych: Rzekome „Wsparcie Signal” jest tak oficjalne, że Signal domyślnie pyta na dole wiadomości, czy „Wsparcie Signal” ma pozwolenie na wysyłanie wiadomości i wyświetlanie imienia i nazwiska oraz zdjęcia. „Osoba nie dowie się, że widziałeś jej wiadomość, dopóki nie zaakceptujesz prośby” – kontynuuje. Brzmi to jak prawdziwe wsparcie aplikacji do przesyłania wiadomości, prawda? Błąd.

W lutym Federalny Urząd Ochrony Konstytucji i Federalny Urząd Bezpieczeństwa Informacji wspólnie ostrzegały przed tego typu próbami phishingu, dokonywanymi przez „podejrzewane o atak państwowy lub kontrolowany przez państwo”. Zgodnie z ostrzeżeniem, głównymi ofiarami byli wysoko postawieni politycy, wojsko i dyplomaci, a także dziennikarze śledczy. Jednak notatka najwyraźniej nie została przeczytana przez wszystkich narażonych. Oprócz wspomnianych polityków, były wiceprezes BND (!) Arndt Freytag von Loringhoven i kilku dziennikarzy. ofiarami ataku mieli być również

Jeden z użytkowników X wyraził się jasno: „Poważnie: ci ludzie chcą nas zbanować w mediach społecznościowych, opowiadają nam o cyberbezpieczeństwie i są tak głupi, że nie potrafią nawet rozpoznać prostej próby phishingu?”

Michał 🇩🇪
@Bundeskanz50246 ·

I po raz kolejny wiele mediów błędnie podaje informacje o rzekomym włamaniu na czat Signal, którego ofiarami padli m.in. Hubertz, Klöckner i Prien.
To nie było włamanie, a phishing; technicznie rzecz biorąc, to coś zupełnie innego. Wyglądało to tak: te trzy osoby – przepraszam za francuski – pokaż więcej

Zhakowane telefony komórkowe:

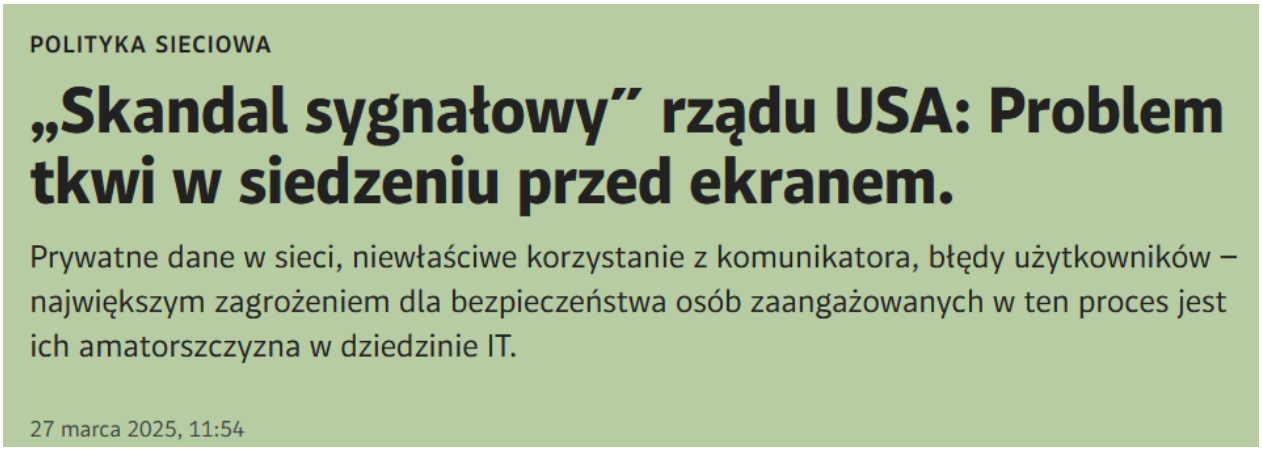
afera Signal dociera do niemieckiego rządu

25 kwietnia 2026, 20:41 | Czas czytania: 3 min. | 145 komentarzy

16:16 · 25 kwietnia 2026

Politycznie i medialnie, uwaga skupia się teraz naturalnie na złym Rosjaninie, który mógł przechwycić poufne informacje. Tymczasem przeciętny obywatel musi zadać sobie pytanie, jak bardzo powinien tolerować osoby, które pomimo stanowczych ostrzeżeń ze strony władz, tak nieostrożnie podchodzą do komunikacji i potencjalnie wrażliwych danych.

Dla odmiany, w pełni popieramy ocenę gazety „ Standard ”: **„Problem tkwi przed ekranem” –** napisali wówczas w nagłówku, odnosząc się do „afery Signal” rządu USA. Największym zagrożeniem dla bezpieczeństwa, jakie stanowili zamieszani w tę sprawę, była ich niekompetencja w zakresie IT.



Zrzut ekranu: Standard

Właśnie. Jednak ludzie nie chcą już słyszeć od tych osób nic na tematy związane z IT, mediami społecznościowymi, kompetencjami medialnymi i cyberbezpieczeństwem. Wydaje się bowiem, że nie mają oni kompetencji, by pouczać obywateli w tych kwestiach i ograniczać ich prawa.