CYBERATAKI. NASK CERT WSKAZUJE, JAK ZACHOWAĆ OSTROŻNOŚĆ W SIECI

Zespół CERT Polska, działający w strukturach NASK (Naukowej i Akademickiej Sieci Komputerowej) przygotował zbiór zasad, dotyczących bezpiecznego korzystania z poczty elektronicznej i mediów społecznościowych. Ma to związek z ostatnimi atakami hakerskimi na polityków.

We wtorek Agencja Bezpieczeństwa Wewnętrznego oraz Służba Kontrwywiadu Wojskowego poinformowały w oficjalnym komunikacie, że ostatnie włamanie na konta w mediach społecznościowych ministra Michała Dworczyka były częścią większego ataku hakerskiego.

„Na liście celów przeprowadzonego przez grupę UNC1151 ataku socjotechnicznego znajdowało się co najmniej 4350 adresów e-mail należących do polskich obywateli lub funkcjonujących w polskich serwisach poczty elektronicznej”.

"Co najmniej 500 użytkowników odpowiedziało na przygotowaną przez autorów ataku informacje, co istotnie zwiększyło prawdopodobieństwo skuteczności działań agresorów. Polskie służby dysponują wiarygodnymi informacjami łączącymi działania grupy UNC1151 z działaniami rosyjskich służb specjalnych" – poinformowały służby.

Prywatna a służbowa poczta elektroniczna

W związku z ostatnimi atakami zespół CERT Polska przygotował kompendium dla użytkowników internetu, dotyczące tego, jak postępować w sieci, by nie paść ofiarą ataku cyberprzestępców.

W dokumencie nadesłanym do naszej redakcji wskazano kilka podstawowych zasad, które powinny pomóc w zachowaniu bezpieczeństwa w sieci:
• Nie należy używać prywatnych kont poczty elektronicznej i komunikatorów do korespondencji służbowej.
• Lepiej nie korzystać z prywatnych komputerów i telefonów do spraw służbowych.
• Nie używać służbowych komputerów i telefonów do spraw prywatnych (w szczególności do czytania prywatnej poczty elektronicznej), nie udostępniać ich członkom rodziny.

Zasady dotyczące prawidłowego logowania się do domeny:

• Przy logowaniu się na konto, zawsze warto sprawdzić czy domena danego portalu jest prawidłowa (domena to nazwa zawierająca się między https://, a pierwszym kolejnym znakiem /).
• Lepiej ignorować wszystkie inne prośby o podanie swojego hasła, nawet jeżeli komunikat wygląda oficjalnie, wymaga natychmiastowej reakcji i grozi dezaktywacją konta.
• Wszystkie podejrzane wiadomości na skrzynce służbowej należy zgłaszać administratorom w swojej firmie/organizacji.

Najważniejsze wskazówki dotyczące haseł:

- Stosowanie długich haseł (powyżej 14 znaków).
- Hasłem może być cała fraza, składająca się z kilku słów, np. 2CzerwoneRoweryJedzaNalesniki.
- Unikać haseł, które łatwo powiązać z publicznymi informacjami na temat danej osoby np. takich, które zawierają nazwisko, datę urodzenia.
- Hasło warto zmieniać za każdym razem, kiedy istnieje podejrzenie, że mogła poznać je inna osoba. Nie ma potrzeby cyklicznej zmiany hasła.
- Nie używać tego samego hasła więcej niż raz (w szczególności do konta email, banku i innych wrażliwych kont).
- Dla ułatwienia można korzystać z menedżerów haseł. Te wbudowane w przeglądarkę czy telefon są bezpieczne i proste w użyciu.

Uwierzytelnienie dwuskładnikowe

Eksperci zalecają włączenie uwierzytelniania dwuskładnikowego (tzw. 2FA), tam gdzie jest to możliwe – jest to konieczne w przypadku poczty elektronicznej i danych do logowania do kont w mediach społecznościowych.

- Jeżeli obecny dostawca Twojej poczty nie udostępnia uwierzytelniania dwuskładnikowego, zmień go. Najlepszym drugim składnikiem uwierzytelniania i jedynym odpornym na ataki phishingowe jest token sprzętowy U2F (np. YubiKey) – czytamy w dokumencie.

Warto także zweryfikować wszystkie dane kontaktowe w ustawieniach profilu poczty elektronicznej i mediów społecznościowych; ułatwi to odzyskanie utraconego konta.

- Jeżeli podejrzewasz, że ktoś mógł włamać się na twoje konto, zmień hasło, sprawdź dostępną w profilu historię logowania i zakończ wszystkie aktywne sesje – zaznacza CERT Polska.

Potrzebna aktualizacja systemu operacyjnego

Równie istotne jest aktualizowanie systemu operacyjnego i programów na komputerze oraz posiadanie aktualnego programu antywirusowego.

VPN nie chroni przed atakami phishingowymi i złośliwym oprogramowaniem – zwraca uwagę CERT Polska i zaleca, by do wrażliwej prywatnej komunikacji używać komunikatorów szyfrowanych typu end-to-end.

Warto także używać opcji automatycznego kasowania wiadomości po upływie określonego czasu – podsumowuje eksperci.

Wszystkie podejrzane wiadomości na prywatnej skrzynce można zgłosić do CERT Polska pod adresem: incydent.cert.pl / cert@cert.pl; szczególnie te zawierające załączniki, archiwa i dokumenty Office z hasłem podanym w treści wiadomości lub zmuszające do podjęcia natychmiastowej reakcji.