Wiceprezes Rady Ministrów
Minister Cyfryzacji

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
Krzysztof Gawkowski

DC.WAC.5555.20.2026
Warszawa, 28 kwietnia 2026 r.

Rekomendacja Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa

dotycząca zaleceń w związku z atakami socjotechnicznymi stosowanymi przy rekrutacjach

Niniejsza rekomendacja wydana została na podstawie art. 67a ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[1], w celu zwiększania poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa (KSC), w związku z obserwowanymi atakami socjotechnicznymi związanymi z rekrutacją pracowników oraz nawiązywaniem innych relacji z danym podmiotem KSC i jego przedstawicielami.

Grupy APT (*Advanced Persistent Threat*), specjalizujące się w długofalowych i zaawansowanych cyberatakach, często powiązane ze służbami wrogich państw, zaczęły na szerszą skalę stosować metody związane z próbą przeniknięcia do podmiotu osoby rekrutującej się jako pracownik, a w rzeczywistości będącej członkiem lub przedstawicielem danej grupy APT, co ma na celu umożliwienie przeprowadzenia cyberataku, bądź kradzież danych o szczególnym znaczeniu. Przeniknięcie takiej osoby do struktur podmiotu KSC wiąże się ze szczególnym zagrożeniem dla bezpieczeństwa państwa oraz samego zaatakowanego podmiotu. W związku z powyższym rekomenduję podmiotom KSC wdrożenie następujących zaleceń.

Rekrutacja i wdrożenie do pracy

Weryfikacja kandydatów

- Prowadzić rozmowy z włączoną kamerą. Zwracać uwagę na nienaturalne pauzy, opóźnienia, wyciszenia dźwięku w momentach, gdy kandydat powinien mówić.
- Przy podwyższonym ryzyku lub podejrzeniu nadużycia uwzględnić analizę dostępnych danych telemetrycznych i diagnostycznych połączenia, realizowaną przez uprawnionych administratorów.
- Potwierdzać historię zatrudnienia bezpośrednio u poprzednich pracodawców, a nie tylko na podstawie CV i profilu LinkedIn.
- Przy rolach o podwyższonym ryzyku rozważyć weryfikację tożsamości na żywo.

Pierwsze tygodnie pracy

- Poprosić pracownika o odczytanie numeru seryjnego urządzenia, co potwierdza fizyczny dostęp do sprzętu.
- Monitorować aktywność użytkownika pod kątem nietypowych godzin pracy.
- Nadawać uprawnienia stopniowo (least privilege). Monitorować próby eskalacji.

[1] Dz. U. z 2026 r. poz. 20, z późn. zm.

telefon: +48 22 245 59 22
adres email: sekretariat.dc@cyfra.gov.pl
www.gov.pl/cyfryzacja

ul. Królewska 27
00-060 Warszawa

Po wykryciu podejrzenia lub incydentu

- Niezwłocznie zablokować konto i dostęp do wszystkich systemów.
- Przeprowadzić analizę zachowania użytkownika: historię logowań, używane narzędzia, ostatnie działania na repozytoriach i w systemach.
- Skontaktować się z właściwym zespołem reagowania na incydenty bezpieczeństwa komputerowego poziomu krajowego (CISRT NASK, CSIRT GOV, CSIRT MON) właściwym CSIRT-em sektorowym, żeby skonsultować sytuację i zlecić jej dalszą analizę.

Spotkania wideo i linki

- Weryfikować domeny linków do spotkań. Prawidłowe adresy dla popularnych narzędzi do wideokonferencji, takich jak Zoom i Teams, to odpowiednio zoom.us i teams.microsoft.com. Każda inna domena (np. teamslivc[.]com, ms-meet[.]xyz, micrusoft[.]us) stanowi sygnał ostrzegawczy.
- Nie pobierać plików ani nie uruchamiać poleceń terminalowych sugerowanych przez interfejs spotkania lub rozmówcę w trakcie połączenia wideo.
- Jeśli podczas spotkania wystąpią „problemy z dźwiękiem" i rozmówca proponuje „aktualizację" lub „naprawę" wymagającą pobrania pliku lub wklejenia komendy, należy natychmiast przerwać połączenie.
- Uwrażliwiać pracowników, że atakujący mogą kontaktować się z przejętych kont osób, które ofiara zna. Sam fakt, że wiadomość pochodzi od znanego kontaktu, nie oznacza, że jest bezpieczna.
- Zgłaszać podejrzane domeny i linki do właściwego CSIRT poziomu krajowego lub CSIRT sektorowego (jeśli został już ustanowiony w danym sektorze).

Konferencje i relacje biznesowe

- Kontakty nawiązane osobiście na konferencjach nie są automatycznie wiarygodne. Należy weryfikować firmy i osoby, które proponują współpracę techniczną lub integrację z systemami.
- Nie otwierać projektów z nieznanych repozytoriów bez wcześniejszej analizy.
- Nie instalować aplikacji dystrybuowanych poza oficjalnymi kanałami, na prośbę nowo poznanych kontaktów biznesowych.
- Zachować ostrożność wobec nowych partnerów, którzy szybko budują wiarygodność przez wpłaty własnych środków lub formalne procesy onboardingowe.
- Ograniczyć dostęp do repozytoriów i systemów wewnętrznych dla partnerów zewnętrznych. Stosować zasadę minimalnych uprawnień również wobec kontrahentów.

Ochrona pracowników technicznych i badaczy

- Informować pracowników technicznych (programistów, analityków bezpieczeństwa, badaczy) o tym, że są potencjalnymi celami spersonalizowanych kampanii rekrutacyjnych. Oferty pracy mogą być generowane przez AI na podstawie ich publikacji i aktywności online.
- Traktować z ostrożnością niezamówione oferty pracy, szczególnie jeśli: pochodzą z adresów darmowych skrzynek, odwołują się do firm, których nie można zweryfikować w publicznych źródłach lub kierują na strony zarejestrowane w ostatnich dniach.
- Weryfikować tożsamość osób proponujących współpracę badawczą, szczególnie jeśli propozycja wiąże się z uruchomieniem kodu, zainstalowaniem narzędzi.

- Rozważyć stosowanie izolowanych środowisk do analizy nieznanych projektów i narzędzi otrzymanych od osób spoza organizacji.

Rekomendacja została opracowana przy współpracy Ministerstwa Cyfryzacji oraz sektorowego zespołu reagowania na incydenty bezpieczeństwa komputerowego CSIRT KNF oraz zespołu reagowania na incydenty bezpieczeństwa komputerowego poziomu krajowego CSIRT NASK.

Szersze informacje dostępne są w raporcie CSIRT KNF pt. „Socjotechnika grup APT w procesach rekrutacyjnych i relacjach biznesowych”[2].

Z wyrazami szacunku
Krzysztof Gawkowski
Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
Wiceprezes Rady Ministrów
Minister Cyfryzacji
/dokument podpisany elektronicznie/

[2] https://cebrf.knf.gov.pl/images/Raporty/Ataki_socjotechniczne_grup_APT.pdf

telefon: +48 22 245 59 22
adres email: sekretariat.dc@cyfra.gov.pl
www.gov.pl/cyfryzacja
ul. Królewska 27
00-060 Warszawa