Stanowisko Sekcji Bezpieczeństwa Teleinformatycznego KI PAN
dotyczące cyberbezpieczeństwa badań naukowych w Polsce

1. Zasoby informacyjne polskiej nauki nie są obecnie chronione w systematyczny sposób. Co więcej, rozwiązania chmurowe do przetwarzania danych w działalności naukowej jest coraz szerzej stosowane. Proces ten jest pochodną niskich kosztów, dojrzałości i efektywności narzędzi oraz częstokroć braku alternatyw.
   W konsekwencji, dane które mogą być podstawą zastosowań komercyjnych, a także dane z obszaru badań o podwójnym zastosowaniu, nie znajdują się pod kontrolą polskich organizacji, ani nawet europejskich.

2. Brak jest systematycznej ochrony wyników badań o podwójnym zastosowaniu (na przykład na wzór australijskiego podejścia z Defence and Strategic Goods List). Co więcej, system ewaluacji motywuje jednostki naukowe w kierunku nieograniczonego udostępniania wyników tego typu badań. Jest to wynikiem zarówno ewaluacji w zakresie kryterium I (publikacje) jak i kryterium III („wpływ"). Wyniki badań udostępnione i wykorzystywane jedynie w Polsce automatycznie prowadzą do niskiej oceny jednostki i w konsekwencji niższego finansowania. Paradoksalnie, wykorzystanie wyników badań przez wrogie nam państwa jest podstawą do wysokiej oceny jednostki naukowej w zakresie kryterium 3.
   Możliwość prowadzenia badań w trybie niejawnym nie rozwiązuje problemu, bowiem dotyczy jedynie części badań mogących mieć strategiczne znaczenie.

3. Wobec braku systemowych rozwiązań, indywidualne zachowanie zasad cyberbezpieczeństwa przez pracowników naukowych nie rozwiązuje problemu braku kontroli nad danymi.

4. Zmiana sytuacji wymaga w co najmniej podjęcia następujących działań:
   A. Stopniowa budowa środowiska teleinformatycznego dla badań naukowych. Ze względów pragmatycznych, działania powinny być skoncentrowane na narzędziach i zasobach o największym znaczeniu i najłatwiejszych do szybkiego zrealizowania:
      - przestrzeń do przechowywania danych z zapewnieniem silnej kontroli dostępu i odporności na zniszczenie i manipulacje, z wykorzystaniem szyfrowania E2E oraz replikacji,
      - narzędzia do bezpiecznej edycji materiałów naukowych (wraz z możliwością jednoczesnej edycji, automatyczną korektą językową itp.),
      - narzędzia do bezpiecznego przetwarzania danych (np. narzędzia statystyczne),
      - narzędzia do bezpiecznej komunikacji (telekonferencje, czat) w trybie szyfrowania E2E
   B. Znalezienia rozwiązań systemowych dla ochrony badań o podwójnym zastosowaniu. Zagadnienie to jest wyjątkowo trudne ze względu na skutki uboczne tworzenia barier przepływu informacji.

5. Szereg wspomnianych powyżej zagadnień ma szerszy charakter i może być zaadresowanych poprzez stworzenie bezpiecznego ekosystemu informacyjnego w Państwie. Dla przykładu, kontrola dostępu do zasobów mogłaby być zrealizowana za pomocą narzędzi budowanych w ramach portfela cyfrowego EDIW z wykorzystaniem certyfikatów atrybutów. Wybór architektury ekosystemu i mechanizmów ochrony powinien być zrealizowany w szerszym kontekście, bez tworzenia silosa informatycznego dedykowanego dla świata nauki. Ekosystem powinien być niezależny od pojedynczego dostawcy, rozproszony i oparty o niewielka liczbę prostych i otwartych standardów.

Mirosław Kutyłowski, Wiesław Paluszyński, Józef Pieprzyk , 14.2.2025

Stanowisko wyraża poglądy Sekcji Bezpieczeństwa Komitetu Informatyki PAN i nie powinno być utożsamiane ze stanowiskiem Polskiej Akademii Nauk.