WĄTPLIWOŚCI KRAJÓW UE WS. SZYFROWANIA

Komisja Europejska zajęła się sprawą szyfrowania i deszyfrowania materiałów dowodowych należących do przestępców. Przedstawiciele ministerstw sprawiedliwości poszczególnych krajów odnieśli się do zadanych im w tej kwestii pytań.

Spotkanie miało charakter nieformalny, dlatego do tej pory informacja nie została podana do publicznej wiadomości. Niedawno portal Ask the EU, należący do grupy Access Info Europe, zdobył część odpowiedzi od danych krajów. Strona złożyła zapytanie w tej sprawie do Komisji Europejskiej jeszcze w październiku bieżącego roku, lecz dopiero teraz uzyskała wgląd w odpowiedzi.

Obecnie na witrynie internetowej Ask The EU znajdują się odpowiedzi z 12 państw, w tym Polski. Kwestionariusz składał się z 11 pytań dotyczących problemów oraz propozycji rozwiązań związanych z popularnością szyfrowania dokumentów, urządzeń oraz komunikacji przez osoby zamieszkujące na terenie Europy.

Pierwsze pytanie dotyczyło częstotliwości, z jaką organy ścigania spotykały się z szyfrowaniem. W przypadku Polski padła odpowiedź: "często (w wielu sprawach)", podobnie jak w Estonii. Organy ścigania w Niemczech nie prowadzą takich statystyk, natomiast Wielka Brytania odpowiedziała, że materiał jest zaszyfrowany prawie zawsze.

Kolejne pytanie dotyczyło najczęściej spotykanych rodzajów oraz mechanizmów szyfrowania w wersji komunikacji i urządzeń. Polscy przedstawiciele zaznaczyli szyfrowanie e-mail (PGP/GPG), e-komunikację (Skype, WhatsApp, Facebook i inne) oraz aplikacje szyfrujące (TrueCrypt, VeraCrypt, DiskCryptor oraz inne). Widać, że w Estonii przestępcy oraz obywatele działają na wyższym poziomie, tutaj organy ścigania napotkały takie metody jak – HTTPS, TOR, P2P/I2P, e-komunikację oraz zaszyfrowane całe urządzenia wraz z aplikacjami szyfrującymi. Niemieckie służby miały spotkać wszystkie wymienione sposoby, podobnie jak Wielka Brytania. Chodzi o te wymienione wyżej, a także metody SFTP, tunelowanie SSH oraz dane przechowywane w chmurze obliczeniowej.

Kolejne pytanie dotyczyło sytuacji, w której oskarżony, podejrzany lub świadek jest zmuszony do dostarczenia kluczy szyfrujących organom ścigania jako materiałów dowodowych. Z tych 4 krajów jedynie Wielka Brytania potwierdziła takie zapisy prawne. Wspomniane przekazanie kluczy ma być regulowane za pomocą Regulation of Investigatory Powers Act 2000 (RIPA). W przypadku Niemiec sprawa jest jednak bardziej zawiła, ponieważ podejrzany lub oskarżony nie ma obowiązku przekazywać dowodów na swoją niekorzyść. Jednak świadek w sprawie jest zobligowany do ujawnienia haseł lub kluczy szyfrujących.

Z kolei czwarte pytanie dotyczyło przekazywania kluczy przez dostawców usług. Tu ponownie niemal wszystkie głosy wskazywały na to, że nie ma takich zapisów prawnych. Niemcy dodatkowo wypowiedzieli się, że tylko operatorzy telekomunikacyjni są zobligowani do przekazywania haseł bądź kodów dostępu, o ile wcześniej mieli je w swoim posiadaniu.

W piątym pytaniu skupiono się na problemie wykorzystania podsłuchu podczas działań operacyjnych, w tym przypadku przechwytywaniu danych szyfrowanych podczas śledztwa. Tym razem to Wielka Brytania jako jedyna dała odpowiedź na "nie": prawo na Wyspach zabrania wykorzystania danych przechwyconych przez służby jako materiału dowodowego. Strona polska z kolei pozwoliła sobie zacytować ustawy związane z tym zagadnieniem, co zajęło 5 stron A4. Zwraca uwagę, że 4 strony są w języku polskim, a to jest swego rodzaju ewenement – wszystkie wymienione kraje zasadniczo tłumaczą swoje regulacje prawne na język angielski. Wśród zapisów znajdują się tam te dotyczące działania Policji, Straży Granicznej, Kontroli Skarbowej, ABW i CBA.

Kolejnym problemem poruszonym w ramach zagadnienia szyfrowania jest kwestia odszyfrowania i monitorowania takiej komunikacji. W przypadku Polski trudności wynikają z braku wystarczającego finansowania. W Estonii – niemożności odszyfrowania bez odpowiedniego klucza, podobnie jak w Niemczech, gdzie problemem jest komunikacja szyfrowana za pomocą end-to-end. Z kolei Wielka Brytania zaznacza, że ogranicza ją prawo RIPA.

W przypadku łamania kluczy widać, że polskie organy ścigania "odrobiły lekcję". Przykładowo – Wielka Brytania nadal korzysta z ataków brute force z dopasowanymi bibliotekami, zaś polscy specjaliści używają oprócz tego otwartego oprogramowania np. hashcat, gdzie wyniki zabezpieczane są później za pomocą protokołów MD5 oraz SHA1. Estonia nie zdradza swoich metod, przekazując jedynie informację, że do każdego szyfrowania dobiera odpowiednie metody łamania. Z kolei Niemcy posiadają odpowiednie zapisy dotyczące tej kwestii – Code of Criminal Procedure.

Punkt 8 skupia się na zabezpieczeniu zebranego materiału dowodowego za pomocą szyfrowania od strony prawnej. W Polsce ten problem istnieje, ma brakować wystarczająco dokładnych zapisów w tej kwestii, inaczej niż w Niemczech czy Estonii. Natomiast w Wielkiej Brytanii mają być prowadzone rozmowy, aby udało się wykorzystać odpowiednie mechanizmy szyfrowania w tej sprawie.

Kolejny punkt dotyczył głównych problemów związanych z odszyfrowaniem materiału dowodowego. Tak więc Polska ma posiadać problem w warstwie finansowej, technicznej oraz legislacyjnej. Wielka Brytania, jedynie w kwestii technicznej, Niemcy – personalnej oraz technicznej. Z kolei Estonia napotyka problemy związane z finansami, brakiem odpowiedniej ilości kadr oraz techniczne.

Czytaj też: Amerykanie boją się rządowych podsłuchów?

Przedostatnie pytanie dotyczyło zmian, jakie powinny zajść w prawodawstwie unijnym, jeżeli chodzi o szyfrowanie komunikacji. Wielka Brytania, Niemcy oraz Estonia są zgodne: potrzebna jest zwiększona współpraca prywatno-publiczna oraz lepsze narzędzia. Z kolei polska odpowiedź pokrywa się z głosami 4 innych krajów, które wzięły udział w badaniu: Chorwacji, Litwy, Włoch oraz Węgier. Mowa tutaj o zastosowaniu tzw. tylnych furtek w samym szyfrowaniu dostępnym na terenie Europy.

Znajduje się to w opozycji do odpowiedzi niemieckich przedstawicieli. Zaznaczają oni, że próba osłabienia lub zabronienia możliwości szyfrowania nie powinna mieć miejsca, ponieważ zapewnia ochronę prywatności dla obywateli oraz informacji handlowych.

O sprawie jako pierwszy napisał portal EurActiv, natomiast w Polsce – Zaufana Trzecia Strona.

Wszystkie odpowiedzi dostępne są na stronie Ask The EU.