Agencja Bezpieczeństwa Wewnętrznego
https://www.abw.gov.pl/pl/aktualnosci/2845,Cyberatak-to-nie-tylko-problem-techniczny-ABW-na-VIII-Forum-Cyberbezpieczenstwa.html
08.10.2026, 21:42

Cyberatak to nie tylko problem techniczny. ABW na VIII Forum Cyberbezpieczeństwa

Sama analiza techniczna nie zawsze wystarczy, by rozpoznać sprawcę cyberataku i jego cel. Dlatego tak ważne jest połączenie jej z wiedzą i możliwościami służby specjalnej. O znaczeniu tego połączenia mówił zastępca szefa ABW płk Adam Ciszewski podczas VIII Forum Cyberbezpieczeństwa.

30 września przedstawiciel Agencji uczestniczył w panelu „Front, którego nie widać – cyberbezpieczeństwo RP na żywo", wspólnie z reprezentantami Ministerstwa Cyfryzacji, Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni i NASK. Forum odbywa się w Pałacu Kultury i Nauki w Warszawie i potrwa do 1 października. Wydarzenie organizowane przez Ministerstwo Cyfryzacji we współpracy z m.st. Warszawą otwiera tegoroczny Europejski Miesiąc Cyberbezpieczeństwa.

Zobaczyć więcej niż pojedynczy atak

Jak podkreślił Zastępca Szefa ABW, cyberprzestępcy szukający zysku i grupy działające na rzecz obcych państw mogą korzystać z tych samych narzędzi. Sam sposób włamania nie przesądza więc, kto za nim stoi. Trzeba uwzględnić również to, kogo zaatakowano, jakich informacji szukano i czy zdarzenie ma związek z wcześniejszymi atakami.

CSIRT GOV, zespół reagowania na incydenty komputerowe będący częścią ABW, może łączyć analizę techniczną z wiedzą operacyjną Agencji oraz uprawnieniami procesowymi. Pomaga to ocenić, czy pojedyncze włamanie jest elementem szerszej operacji przeciwko Polsce. Na podstawie wieloetapowej analizy CSIRT GOV wskazuje również, z określonym poziomem prawdopodobieństwa, kto odpowiada za atak. To właśnie atrybucja. Szczegółowe informacje dotyczące konkretnych przypadków mają charakter niejawny.

Przywrócić działanie, zachować dowody

Połączenie tych kompetencji ma znaczenie także podczas reagowania na atak. Pozwala równolegle ograniczać jego skutki, przywracać działanie usług i zabezpieczać materiał dowodowy. Chodzi nie tylko o usunięcie problemu technicznego, lecz także o wyjaśnienie zdarzenia i ustalenie odpowiedzialności sprawców. Ważnym partnerem ABW w tym obszarze jest Centralne Biuro Zwalczania Cyberprzestępczości.

Płk Ciszewski podkreślił również znaczenie współpracy trzech krajowych zespołów: CSIRT GOV, CSIRT NASK i CSIRT MON działającego w Dowództwie Komponentu Wojsk Obrony Cyberprzestrzeni. Ich współdziałanie pozwala wymieniać informacje, koordynować reakcję na incydenty i łączyć kompetencje właściwe dla różnych części państwa. Zastępca Szefa ABW wskazał ten mechanizm jako przykład sprawnie działającego modelu współpracy. Obowiązek współdziałania trzech krajowych CSIRT-ów wynika również z ustawy o krajowym systemie cyberbezpieczeństwa.

Kompetencje, które widać

Jednym z widocznych sprawdzianów polskich zdolności są coroczne ćwiczenia Locked Shields, organizowane przez NATO Cooperative Cyber Defence Centre of Excellence. Polska od lat znajduje się w ich ścisłej czołówce. W 2022 r. wspólny zespół Litwy i Polski zajął drugie miejsce, rok później polski zespół był trzeci, w 2024 r. w pierwszej trójce znalazł się zespół Finlandii i Polski, a w 2025 r. drugi najwyższy wynik uzyskał zespół Polski i Francji. Jak zaznaczył płk Ciszewski, taki poziom przygotowania jest widoczny nie tylko dla partnerów Polski, ale również dla jej przeciwników.

Jednocześnie Agencja musi stale pozyskiwać nowych specjalistów. Zastępca szefa ABW mówił podczas panelu o zmianach w podejściu do rekrutacji i rosnącym znaczeniu kandydatów o profilu informatycznym. Cyberbezpieczeństwo jest dziś jednym z obszarów, do których ABW prowadzi bezpośredni nabór - m.in.

programistów, administratorów i specjalistów bezpieczeństwa systemów. Wymagania wobec przyszłych funkcjonariuszy pozostają jednak wysokie. Kandydaci przechodzą wieloetapową procedurę, obejmującą m.in. badania, weryfikację i postępowanie sprawdzające umożliwiające dostęp do informacji ściśle tajnych.

Bezpieczeństwo zaczyna się przed atakiem

Podczas dyskusji płk Ciszewski zwrócił uwagę również na znaczenie profilaktyki. ABW prowadzi działania dotyczące zarówno zagrożeń terrorystycznych, jak i radykalizacji młodych ludzi. W cyberprzestrzeni szczególnego znaczenia nabiera budowanie odporności na manipulację, dezinformację i treści prowadzące do radykalizacji.

Przykładem takiego działania jest „Broń się w necie" – projekt realizowany wspólnie przez Ministerstwo Cyfryzacji, NASK i ABW. Jego druga edycja jest skierowana do uczniów szkół ponadpodstawowych i obejmuje m.in. tematykę manipulacji w mediach społecznościowych, radykalizacji online, krytycznego myślenia i odporności cyfrowej.

Wiedzieć dużo, ujawniać tyle, ile trzeba

Płk Ciszewski zwrócił też uwagę na granice publicznego informowania o zdolnościach obronnych. Państwo powinno pokazywać, że potrafi wykrywać ataki i na nie reagować. Nie powinno jednak ujawniać szczegółów, które pomogłyby przeciwnikowi obejść zabezpieczenia.

Obecność ABW na takich wydarzeniach ma więc konkretny cel: dzielić się wiedzą, która pomaga administracji, firmom i ekspertom lepiej przygotować się do zagrożeń. Agencja wnosi do tej rozmowy nie tylko wiedzę o zabezpieczeniach systemów, ale również o przeciwniku - jego celach, powiązaniach i sposobach działania.

ABW nie musi ujawniać swoich metod, by jej wiedza pomagała innym skuteczniej się bronić.

30.09.2026

1

2

3

4

Poprzedni Strona