INNOWACYJNY PROJEKT POMOŻE NASK W BUDOWIE NARODOWEGO CYBERBEZPIECZEŃSTWA

Państwowy Instytut Badawczy NASK rozpoczął realizację innowacyjnego projektu, który zakłada między innymi sprawniejsze reagowanie na zagrożenia związane z cyberbezpieczeństwem na poziomie krajowym i europejskim, poprawę współpracy operacyjnej w Europie w tym zakresie oraz zwiększenie zakresu działania CERT Polska.

Projekt „Advance threat Monitoring and Cooperation on the European and national levels" (AMCE) otrzymał w ramach programu Connecting Europe Facility dofinansowanie w wysokości prawie 1 mln euro. Realizowany jest przez zespół CERT Polska, działający w strukturach Państwowego Instytutu Badawczego NASK. CERT Polska to pierwszy powstały w Polsce zespół reagowania na incydenty.

Według raportu CERT Polska w 2018 roku odnotowano ponad 3,7 tys. incydentów naruszenia cyberbezpieczeństwa. 44 proc. z nich stanowił phishing, 23 proc. wiązało się z rozprzestrzenianiem złośliwego oprogramowania, a 11 proc. z wysyłką spamu. W ten sposób przestępcy próbują pozyskać dane użytkowników do logowania się w różnych serwisach, m.in. na stronach banków.

„Cyberprzestępcy uciekają się do wymyślnych metod, które mogą zagrozić bezpieczeństwu użytkowników Internetu. Coraz częstsze są przypadki phishingu, służącego do wyłudzania danych. Można też paść ofiarą złośliwego oprogramowania typu ransomware, szyfrującego dane na dysku zaatakowanego internauty. W takiej sytuacji atakujący domaga się okupu w zamian za umożliwienie ponownego dostępu do danych. Sposoby wykorzystywane przez przestępców są też coraz trudniejsze do wykrycia. Dlatego tak istotne jest rozwijanie współpracy między CERT-ami i tworzenie nowoczesnych narzędzi, pozwalających zbierać i analizować dane na temat zagrożeń, wykrywać szkodliwe działania, a nawet je przewidywać" – mówi Krzysztof Silicki, zastępca dyrektora NASK ds. cyberbezpieczeństwa i innowacji.

Głównym celem projektu AMCE jest poprawa współpracy na poziomie operacyjnym wśród zespołów reagowania na incydenty w Unii Europejskiej poprzez powiązanie ze sobą istniejących systemów służących do monitorowania i analizowania z kluczowymi systemami zapewniającymi wymianę informacji (n6, IntelMQ, MISP). Dzięki temu wszystkie zespoły będą mogły lepiej wykrywać i reagować na zagrożenia w internecie.

Co więcej, do projektu zostanie włączona platforma SISSDEN (Secure Information Sharing Sensor Delivery Event Network), która służy do monitorowania i identyfikacji działalności cyberprzestępców w Internecie, m.in. poprzez obserwowanie aktywności botnetów i powszechnych ataków na urządzenia podłączone do internetu. Dzięki pozyskanym środkom możliwa będzie kontynuacja działania platformy zrealizowanej w ramach projektu międzynarodowego, finansowanego z programu UE: Horyzont 2020 zakończonego w pierwszej połowie tego roku, którego efektem jest system wczesnego ostrzegania o zagrożeniach w Internecie, działający w ponad 100 krajach.

NASK będzie utrzymywał system wspólnie z organizacją non-profit Shadowserver. „We współpracy z naszym partnerem merytorycznym z projektu SISSDEN - organizacją Shadowserver - uruchamiamy ten system monitorowania zagrożeń na nowo, bazując na wcześniej stworzonym oprogramowaniu oraz zdobytym doświadczeniu" – powiedział Paweł Pawliński, kierownik zespołu projektów analitycznych w CERT Polska. - „W projekcie AMCE będziemy odpowiedzialni za utrzymywanie infrastruktury i analizowanie pozyskanych danych" – uściślił. Jak zakładają specjaliści z NASK, platforma SISSDEN będzie w pełni funkcjonalna pod koniec bieżącego roku.

Koncepcja współpracy międzynarodowej ośrodków odpowiedzialnych za cyberbezpieczeństwo w oparciu o narzędzia powstałe w projektach SISSDEN i AMCE została przedstawiona jako propozycja projektu zwiększającego cyberbezpieczeństwo w regionie – w ramach inicjatywy Trójmorza (Three Seas Initiative).

W ramach SISSDEN-a w NASK powstał też system Network Telescope, który monitoruje zagrożenia w internecie w sposób pasywny. „Mamy do niego infrastrukturę i będziemy go rozwijać pod względem oprogramowania do analizy ruchu sieciowego" – zapowiedział Pawliński. W czasie prac nad poprzednim projektem powstały też dwa systemy do śledzenia złośliwego oprogramowania: jeden do obserwacji poleceń wysyłanych do zainfekowanych komputerów przez przestępców oraz drugi - sandbox służący do analizy botnetów. Jest to wyizolowany system, który można zainfekować złośliwym oprogramowaniem i następnie monitorować jego działania. W takim środowisku oprogramowanie nie może zrobić żadnych szkód, a jego zachowanie obserwuje się na przestrzeni wielu miesięcy.

Dzięki projektowi AMCE możliwy będzie też rozwój narzędzi w CERT Polska. Według Pawła Pawlińskiego istnieje szereg narzędzi, które obecnie są rozwijane, np. n6, czyli platforma, gdzie udostępniane są informacje dowolnym podmiotom w Polsce o zagrożeniach dotyczących ich sieci. Ta platforma wykorzystywana jest również do udostępniania informacji CERT-om w innych krajach. System rozwija się od wielu lat. Jak wskazuje ekspert, drugie flagowe rozwiązanie to MWDB, czyli baza informacji o złośliwym oprogramowaniu z zestawem narzędzi służących do automatycznej analizy plików. System jest przeznaczony głównie dla analityków, którzy zajmują się analizą techniczną złośliwego oprogramowania, ale używany jest też intensywnie w CERT Polska. Rozwijaniu będzie podlegało też kolejne narzędzie związane ze złośliwym oprogramowaniem: wyspecjalizowana wyszukiwarka, dzięki której analitycy mogą efektywnie i szybko przeszukiwać duże zbiory próbek złośliwego oprogramowania.

W 2020 roku rozpoczną się ponadto prace nad narzędziami do współpracy CERT Polska z innymi CERT-ami krajowymi oraz organami policji i prokuratury. Pozwolą one na udostępnienie tym podmiotom pewnego zakresu danych, którymi dysponuje CERT Polska, w sposób częściowo zautomatyzowany.

Z grantu finansowana będzie też działalność międzynarodowa zespołu CERT Polska – m.in. udział w konferencjach, grupach roboczych, podtrzymywanie kontaktów operacyjnych. Wsparte zostaną też działania w obszarze popularyzacji cyberbezpieczeństwa, na przykład w postaci organizacji Europejskiego Miesiąca Cyberbezpieczeństwa.

Projekt zwiększy też możliwości działania CERT Polska dzięki zakupowi na potrzeby operacyjne zespołu infrastruktury czy dostępów do zewnętrznych baz danych o zagrożeniach. Umożliwi to szybsze reagowanie na incydenty i proaktywne wykrywanie nadchodzących zagrożeń.

Od początku istnienia zespołu CERT Polska rdzeniem jego działalności jest obsługa incydentów bezpieczeństwa i współpraca z podobnymi jednostkami na całym świecie, zarówno w ramach działalności operacyjnej, jak i badawczo-rozwojowej. Do jego głównych zadań należy też m.in. udział w

krajowych i międzynarodowych projektach związanych z tematyką bezpieczeństwa teleinformatycznego, działalność badawcza z zakresu metod wykrywania incydentów bezpieczeństwa, analizy złośliwego oprogramowania i systemów wymiany informacji o zagrożeniach, rozwijanie własnych narzędzi do walki z zagrożeniami oraz działania informacyjno-edukacyjne.

Informacja prasowa NASK

Czytaj też: NASK znów wesprze najlepsze inicjatywy edukacyjne