PAŃSTWOWY INSTYTUT BADAWCZY

NASK

WSPÓŁTWORZYMY SYSTEM CYBERBEZPIECZEŃSTWA POLAKÓW

dr inż. Wojciech Kamieniecki

Dyrektor NASK
Państwowego Instytutu Badawczego

Z NASK związany od 2015 r. jako Dyrektor ds. ICT. Absolwent Wydziału Automatyki i Informatyki Politechniki Śląskiej oraz studiów doktoranckich na Uniwersytecie Szczecińskim na kierunku ekonomia i zarządzanie. Od 2017 r. doktor w dziedzinie nauk ekonomicznych.
Pełnił funkcję Dyrektora Generalnego Multimedia Polska S.A., Prezesa Zarządu Nordisk Polska Sp. z o.o., Dyrektora Projektu TETRA EXATELS.A., a ostatnio – Dyrektora Generalnego Projektu Internet dla Mazowsza.
Od 2013 r. współpracuje z CEE Equity Partners (PE) w zakresie oceny projektów związanych z budową regionalnych sieci szerokopasmowych oraz ostatniej mili. Od 2014 r. – Przewodniczący Rady Nadzorczej Mielec PV S.A. Jest autorem publikacji naukowych z zakresu strategii rozwoju i zarządzania przedsiębiorstwami oraz kształtowania wartości przedsiębiorstwa.

Skala zagrożeń związanych z używaniem internetu wymaga kompleksowej odpowiedzi. Przede wszystkim konieczna jest rozbudowa narzędzi technologicznych, np. systemów do automatycznego wykrywania zagrożeń, ich analizy i wymiany informacji, w tym międzynarodowej infrastruktury obserwacyjnej. Stanowi to obecnie jeden z ważniejszych obszarów prac badawczo-rozwojowych NASK Państwowego Instytutu Badawczego. Security Operation Center (SOC) w NC Cyber pracuje 24 godziny na dobę, korzystając z tych innowacyjnych narzędzi, aby monitorować polską sieć i w razie potrzeby przekazywać informacje do właścicieli zagrożonych sieci. Służy do tego m.in. platforma n6. Jest to usługa dla profesjonalistów – administratorów zajmujących się sieciami w biurach, na osiedlach, w szkołach, firmach.

Drugim istotnym warunkiem utrzymania bezpieczeństwa jest świadomość społeczna. Zagrożenia przychodzące z sieci często polegają na próbie oszustwa, manipulacji, podstępnego podsuwania złośliwego oprogramowania lub wyłudzania poufnych informacji (np. haseł do banku). Zapobieganie tego typu przestępstwom polega przede wszystkim na edukacji użytkowników. NASK PIB organizuje działania edukacyjne, kierowane do osób dorosłych (w tym seniorów) oraz do dzieci i młodzieży w ramach programu Komisji Europejskiej „Safer Internet" oraz w ramach działającej w instytucie Akademii NASK i portalu e-learningowego IT Szkoła.

Bezpieczeństwo wiąże się też z przeciwdziałaniem dystrybucji w internecie treści nielegalnych i szkodliwych. Tym zajmuje się zespół interwencyjny Dyżurnet.pl, który przyjmuje zgłoszenia (również anonimowe) od internautów.

WYZWANIA DLA CYBERBEZPIECZEŃSTWA JESZCZE NIGDY NIE BYŁY TAK POWAŻNE.

W 2016 r. w Europie odnotowywano ponad 4 tys. ataków dziennie z użyciem samego tylko oprogramowania typu ransomware[1], a 80% przedsiębiorstw unijnych doświadczyło co najmniej jednego incydentu związanego z bezpieczeństwem cybernetycznym.

Przewodniczący Komisji Europejskiej Jean-Claude Juncker w swoim orędziu o stanie Unii w 2017 r., wygłoszonym w Parlamencie Europejskim, wyraził opinię, że „ataki cybernetyczne mogą zagrażać stabilności systemów demokratycznych i gospodarek bardziej niż broń i czołgi"[2]. Nie sposób odmówić mu racji. Nie oznacza to, na szczęście, że nasze próby stawienia czoła temu wyzwaniu są z góry skazane na niepowodzenie. Konieczna jest jednak konsolidacja tych wysiłków, zacieśnienie wymiany informacji i doświadczeń pomiędzy ekspertami, a także w obrębie poszczególnych sektorów gospodarki – między sektorami i między państwami. Dla służb odpowiedzialnych za bezpieczeństwo, w tym Policji, współpraca z różnymi środowiskami w kraju i zagranicą jest również jednym z kluczowych warunków efektywnego działania. Niewątpliwie nasze strategie ochrony przed cyberprzestępczością muszą ulegać modyfikacji wraz ze zmianami krajobrazu zagrożeń. NASK Państwowy Instytut Badawczy od początku działania Internetu w Polsce śledzi te zmiany i dynamicznie na nie reaguje, dostosowując obszary swojej pracy do nowych warunków. Poniżej nakreślono główne obszary obecnej działalności instytutu.

Duży Internet – duży problem

Skala zagrożeń jest zależna od liczby urządzeń podłączonych do Internetu i zakresu oferowanych usług. Właśnie z rozwoju rynku internetowego wynika lawinowy wzrost liczby cyberataków, który obserwujemy od kilku lat. Niestety, stuprocentowych zabezpieczeń nie ma. Producenci sprzętu i oprogramowania, nauczeni smutnym doświadczeniem, coraz większą wagę przywiązują do kwestii bezpieczeństwa. Jednak nie wszyscy. Zresztą nawet ci, którzy troszczą się o zabezpieczenia, niekiedy popełniają błędy. W rezultacie technologie niezawodne są takimi tylko do chwili, kiedy ktoś odkryje lukę czyniącą je podatnymi na atak. Wszystkie szanujące się firmy wypuszczają aktualizacje, stale poprawiając swoje produkty i usuwając błędy, których wcześniej nie zauważyli. Luki w oprogramowaniu, które mogą wykorzystać hakerzy, są zresztą przedmiotem handlu. Bywa, że osoba, która odkryje lukę, zgłasza to do producenta, często otrzymując w zamian nagrodę pieniężną. Ale może też przekazać informację o niej przestępcom, którzy prawdopodobnie zapłacą więcej. Organizacje przestępcze niekiedy wręcz zatrudniają etatowych analityków poszukujących słabych punktów w zabezpieczeniach serwerów i innych urządzeń.

Odkrywszy lukę w popularnym produkcie – np. systemie operacyjnym lub przeglądarce internetowej, przestępcy mogą zaprojektować atak wymierzony w miliony osób na całym świecie. Często, aby zmaksymalizować efekt, hakerzy przejmują komputery nieświadomych osób, zamieniając je w tzw. boty, czyli zmuszając je do wykonywania zdalnych poleceń, np. rozsyłania spamu lub szkodliwego oprogramowania.

Sieć botów (ang. *botnet*) to jedno z aktualnie popularnych narzędzi stosowanych przez cyberprzestępców. Systemy NC Cyber do automatycznej analizy malware[3] zidentyfikowały 3344 prawdopodobne adresy serwerów zarządzania botnetami na świecie. W ubiegłym roku odnotowano też nowe zjawisko – masowe wykorzystanie do tworzenia botnetów drobniejszych urządzeń, np. kamerek internetowych i domowych lub biurowych nagrywarek DVR. Procesory tych urządzeń nie nadają się do wykonywania skomplikowanych zadań. Ale każde z nich ma własny adres IP i może połączyć się z wyznaczonym serwerem. Jeśli wiele urządzeń zrobi to jednocześnie, to serwer może zostać przeciążony. Na tym polegają ataki DDoS (ang. *distributed denial of service* – rozproszona odmowa usługi).

Jeden z rekordowych ataków z użyciem takiego botneta (o nazwie Mirai) nastąpił 21 października 2016 r. Zostały przeciążone serwery firmy Dyn świadczącej usługi internetowe, dzięki którym działało wiele popularnych na całym świecie serwisów internetowych, takich jak np. Spotify, Reddit, New York Times czy Wired. Przerwę w ich działaniu odczuły miliony internautów. Szacowana liczba botów biorących udział w tym ataku to około 100 tysięcy, a ich lokalizacja geograficzna była rozproszona. Część z nich mogła pochodzić z Polski, bo i tu eksperci zaobserwowali aktywność botnetu. W okresie od 29 października do 31 grudnia 2016 r. zespół CERT Polska (ang. *Computer Emergency Response Team*), działający w NC Cyber w NASK, obserwował średnio 7283 urządzenia przejęte przez hakerów dziennie. Rekordem było 14 054 botów jednego dnia.

Użytkownicy, poza wąskim gronem specjalistów, przeważnie nie są w stanie na bieżąco śledzić wszystkich doniesień dotyczących zagrożeń ani w porę im przeciwdziałać. Stąd potrzeba wypracowywania narzędzi do automatycznego wykrywania zagrożeń, ich analizy i wymiany informacji. Takie narzędzia umożliwiają niezwłoczną reakcję administratorów sieci na niebezpieczne zdarzenia. Jest to obecnie jeden z ważniejszych obszarów prac badawczo-rozwojowych NASK PIB. Security Operation Center (SOC) w NC Cyber pracuje 24 godziny na dobę, korzystając z tych innowacyjnych narzędzi, aby monitorować polską sieć i w razie potrzeby przekazywać informacje do właścicieli zagrożonych sieci. Służy do tego między innymi platforma **n6**. Jest to usługa dla profesjonalistów – administratorów zajmujących się sieciami w biurach, na osiedlach, w szkołach, firmach. Mogą oni, po rejestracji i uwierzytelnieniu, otrzymywać aktualne dane o incydentach zagrażających ich sieci.

Opracowana przez NASK Platforma n6 funkcjonuje w pełni automatycznie. Dostęp do niej jest bezpłatny. W ciągu roku na platformie są przetwarzane dziesiątki milionów zdarzeń dotyczących bezpieczeństwa z Polski i całego świata. Celem platformy jest efektywne, niezawodne i szybkie dostarczenie dużej liczby informacji o zagrożeniach bezpieczeństwa właściwym podmiotom: właścicielom, administratorom i operatorom sieci.

Źródłem danych systemu n6 jest wiele kanałów dystrybucyjnych przesyłających informacje o zdarzeniach bezpieczeństwa. Zdarzenia te są wykrywane w wyniku działań systemów wykorzystywanych przez różne podmioty zewnętrzne (takie jak inne CERT-y, organizacje bezpieczeństwa, producentów oprogramowania, niezależnych ekspertów od bezpieczeństwa itp.) oraz systemów monitorowania obsługiwanych przez CERT Polska. Większość informacji jest aktualizowana codziennie, niektóre częściej.

W sytuacji, gdy zagrożenia internetowe są zjawiskiem globalnym, dla którego granice państw nie stanowią bariery, narzędzia służące do obrony również muszą działać transgranicznie. NASK jest koordynatorem międzynarodowego konsorcjum firm i instytucji naukowych wspólnie budujących sieć wczesnego ostrzegania dla całej Unii Europejskiej. Projekt o nazwie SISSDEN (Secure Information Sharing Sensor Delivery Event Network) polega na budowie co najmniej 100 stacji monitorowania zagrożeń, składających się ze specjalnie przygotowanych serwerów (przynajmniej po jednym na terytorium każdego z krajów członkowskich UE) wyposażonych w innowacyjne narzędzia do wykrywania i analizy wirusów, botnetów i innych groźnych zjawisk. Ta sieć wczesnego ostrzegania ma w pełni zacząć działać w 2019 r. Już teraz niektóre jej elementy są testowane z sukcesem.

Razem przeciw fali zagrożeń

Współpraca międzynarodowa w przeciwdziałaniu zagrożeniom nie polega jedynie na tworzeniu wspólnej infrastruktury. Często równie wartościowe, lub nawet wartościowsze, jest jednoczenie wysiłków w dążeniu do wspólnego celu – chociażby był on odległy. W gronie ekspertów NASK PIB działa zespół ds. reagowania na szkodliwe i nielegalne treści w Internecie Dyżurnet.pl, który przyjmuje zgłoszenia (również anonimowe) od internautów. Do zespołu wpływają informacje o napotkanych w sieci obrazach zawierających twardą pornografię, przemoc, treści rasistowskie i ksenofobiczne, nakłanianie do przestępstw lub innych szkodliwych działań. Od lat jednak najliczniejszą grupę incydentów (22% w 2016 r.) stanowią materiały prezentujące seksualne wykorzystywanie dzieci (CSAM – ang. *child sexual abuse materials*), nazywane potocznie pornografią dziecięcą. W sytuacji, gdy materiały te znajdują się na serwerze zlokalizowanym w Polsce, Dyżurnet.pl powiadamia Policję i współpracuje z nią, udostępniając wyniki swoich analiz. O treściach umieszczonych na zagranicznych serwerach Dyżurnet.pl informuje współpracujące z nim siostrzane punkty kontaktowe zrzeszone w stowarzyszeniu INHOPE, które jest współfinansowane przez Komisję Europejską oraz firmy sektora informatycznego. Działa już ponad 50 zespołów interwencyjnych w różnych krajach. Materiały są jak najszybciej usuwane ze stron internetowych, a organy ścigania w danym państwie podejmują działania w celu wykrycia sprawców wykorzystywania dzieci, a także publikacji nagrań i zdjęć, na których to przestępstwo zostało utrwalone. Ponadto grupy eksperckie zrzeszone w INHOPE mają dostęp do prowadzonej przez Interpol bazy danych CSAM, w której zdjęcia i filmy są poddawane analizie w celu określenia miejsca przestępstwa oraz tożsamości ofiar i sprawców.

Dyżurnet.pl odnotował w 2016 r. 14 298 incydentów związanych z publikacją nielegalnych lub szkodliwych treści. Ponad trzy tysiące z nich stanowiła tzw. pornografia dziecięca. Przypadki CSAM (ang. *child sexual abuse materials*) umieszczonych na serwerach w Polsce zgłaszane są Policji. Dyżurnet.pl kontaktuje się też z Policją w sytuacjach, gdy internauta zawiadamia o zdarzeniu potencjalnie niebezpiecznym – np. uwodzeniu dziecka w sieci, szantażu internetowym, groźbach, możliwości próby samobójczej itp.

Międzynarodowa współpraca i zaawansowana technologia umożliwiają coraz częściej ściganie sprawców i ochronę ofiar przed dalszym wykorzystywaniem. Skutecznym narzędziem okazała się międzynarodowa baza danych ICSE (International Child Sexual Exploitation), do której trafiają podejrzane materiały foto i wideo z całego świata. W 2017 r. Interpol ogłosił, że w okresie funkcjonowania systemu (od 2011 r.) zidentyfikowano 10 tys. ofiar. W jednym przypadku funkcjonariuszom udało się zidentyfikować, aresztować sprawcę i oswobodzić jego ofiarę zaledwie 10 godzin po tym, jak materiał trafił do bazy danych. Były to zdjęcia, które do bazy wprowadził zespół interwencyjny w Australii. Specjaliści z USA zidentyfikowali miejsce, gdzie zostały wykonane, a następnie wytypowali podejrzanego. Wtedy wydział Interpolu ds. zwalczania przestępstw przeciwko dzieciom zawiadomił służby w kraju europejskim, w którym doszło do wykorzystania dziecka. Obecnie z bazy korzystają służby i zespoły interwencyjne w 49 krajach, również w Polsce. Ostatnio głośne w mediach przypadki aresztowań osób podejrzanych o wykorzystywanie dzieci również były efektem analizy zdjęć z bazy ICSE.

Dyżurnet.pl współpracuje z bazą od listopada 2015 r. Od tego czasu na zgłoszonych do ICSE stronach eksperci Dyżurnet.pl przeanalizowali łącznie 105 876 plików foto i wideo, spośród których zidentyfikowali 22 153 przypadków prezentujących seksualne wykorzystywanie dzieci.

Inną międzynarodową inicjatywą, w której uczestniczą eksperci NASK PIB, jest No More Ransom[4], zainicjowana przez firmy i organizacje działające na rzecz bezpieczeństwa w Internecie. Ma ona na celu ograniczenie skutków stosowania ransomware. Projekt No More Ransom skupia specjalistów, którzy analizują krążące w sieci wirusy, dostarczając wiedzy organom ścigania i – co najważniejsze – opracowują narzędzia deszyfrujące, bezpłatnie udostępniane następnie ofiarom ransomware. Grupa prowadzi też edukację na temat tego zagrożenia i radzi, jak chronić swoje dane, a także, co robić, gdy już dojdzie do ataku. CERT Polska, należący do NC Cyber zespół analityków, dołączył do tego projektu w 2017 r.

CERT Polska działa od 1996 r. Jest to najstarszy tego typu zespół ekspercki w Polsce. Powstał w instytucie badawczym NASK jako odpowiedź na nowe wyzwania bezpieczeństwa, związane z rozwojem Internetu. W momencie powstania Narodowego Centrum Cyberbezpieczeństwa, CERT Polska stał się jego częścią.

CERT Polska przyjmuje zgłoszenia o incydentach bezpieczeństwa, ponadto aktywnie bada zjawiska zachodzące w sieci pod kątem identyfikowania nowych zagrożeń, wypracowywania narzędzi analitycznych i sposobów przeciwdziałania. W ostatnim roku CERT Polska podjął m.in. badania coraz powszechniejszego zjawiska wyłudzeń z wykorzystaniem fałszywych sklepów internetowych. Opracowuje również nowe narzędzia do analizy botnetów, malware i innych zagrożeń aktualnie stanowiących wyzwanie.

Cyfrowa tożsamość w realnych sytuacjach

Wśród działań związanych z bezpieczeństwem publicznym i indywidualnym istotne są również prace NASK PIB dotyczące weryfikacji tożsamości. We współpracy z instytutem powstała i została uruchomiona niedawno przez Ministerstwo Cyfryzacji aplikacja mObywatel, umożliwiająca przechowywanie na smartfonie danych zawartych w dowodzie osobistym. Aplikacja obsługuje dane osobowe w sposób zabezpieczony, pozwalając na udostępnianie wybranej części z nich – np. tylko imienia, nazwiska i adresu zameldowania – pomiędzy użytkownikami.
Naukowcy z NASK PIB biorą też udział w pracach badawczych nad systemem do automatycznego rozpoznawania twarzy. W wyniku projektu BIOWIZ powstanie system do identyfikacji sprawców przestępstw na podstawie materiałów zdjęciowych i/lub wideo. Umożliwią one porównywanie nowych obrazów z istniejącymi w bazie danych wizerunkami sprawców, co usprawni proces analizy np. nagrań z monitoringu. System ma funkcjonować jako narzędzie interaktywne, mogące działać w kilku scenariuszach, np. detekcja twarzy, wyodrębnianie klatek z obrazami twarzy i śledzenie twarzy w materiałach wideo, identyfikacja osoby zaznaczonej na zdjęciach lub materiale wideo na podstawie profilu biometrycznego. Modułowa konstrukcja pozwoli na przyszłe uzupełnianie listy scenariuszy i technik biometrycznych. Wykorzystanie systemu będzie bardzo istotne dla pracy funkcjonariuszy identyfikujących osoby.

Międzynarodowa konferencja na temat bezpieczeństwa teleinformatycznego SECURE, która od wielu lat gromadzi najlepszych specjalistów z tego obszaru z Polski i ze świata, zarówno z sektora prywatnego, jak i publicznego (zdj. archiwum NASK).

Naukowcy rozwijają też technologie związane z biometrią w urządzeniach mobilnych (identyfikacja linii papilarnych, twarzy, wzoru tęczówki).

Narodowe Centrum Cyberbezpieczeństwa zostało powołane w strukturze NASK w lipcu 2016 r. z inicjatywy minister cyfryzacji Anny Streżyńskiej. Jednym z głównym zadań NC Cyber jest inicjowanie współpracy operacyjnej z sektorem prywatnym, w tym z dostawcami usług kluczowych. W NC Cyber funkcjonuje zespół CERT Polska – pierwszy powstały w Polsce zespół reagowania na incydenty (w strukturze NASK od 1996 r.). Głównym obszarem jego działalności jest obsługa incydentów bezpieczeństwa i współpraca z analogicznymi jednostkami na całym świecie zarówno w ramach działalności operacyjnej, jak i badawczo-wdrożeniowej. W strukturze NC Cyber funkcjonuje także centrum operacyjne, które w trybie 24/7 przyjmuje zgłoszenia od operatorów usług kluczowych. Anonimowe zgłoszenia o niebezpiecznych i nielegalnych treściach od użytkowników przyjmuje zespół Dyżurnet.pl, działający w NASK od 2005 r. Rola Narodowego Centrum Cyberbezpieczeństwa zapisana została w opracowanych pod kierunkiem Ministerstwa Cyfryzacji i przyjętych przez rząd w maju 2017 r. Krajowych Ramach Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022 oraz w projekcie ustawy o krajowym systemie cyberbezpieczeństwa, która jest obecnie na etapie konsultacji publicznych.

Humanistyczna strona cyberzagrożeń – czynnik ludzki

Zagrożenia internetowe podlegają mutacji i przekształcają się wraz z rozwojem technologii i zmianami rynkowymi. Zmiany te utrudniają klasyfikację źródeł ryzyka, jednak wyraźnie widać zaznaczający się trend, który w uproszczeniu można nazwać humanistycznym. Chociaż do przestępstwa dochodzi w środowisku nowych technologii, sprawcy często stosują jako metodę znane od starożytności socjotechniki, które w Internecie, gdzie nie dochodzi do bezpośredniego kontaktu, okazują się bardzo skuteczne. Przykładem może być zaskakująca kariera oszustwa „na prezesa" (angielski termin CEO Fraud), polegającego na wysłaniu wiadomości e-mail do pracownika firmy z prośbą o pilny przelew na wskazane konto na osobiste polecenie przełożonego. Osoba podająca się za szefa zdobywa pewną wiedzę o firmie i pracowniku, do którego kieruje korespondencję, a następnie wymyśla wiarygodny pretekst niespodziewanej dyspozycji finansowej – np. pilna zaliczka na wynegocjowany właśnie kontrakt. Według Europolu kwota oszustwa może osiągać nawet miliony euro. FBI informuje, że jego centrum powiadamiania o cyberprzestępczości otrzymało w 2016 r. nieco ponad

12 tys. zgłoszeń o tego typu atakach. Łączne straty poniesione przez poszkodowane firmy mogły wynieść ponad 360 mln dolarów. Należy przy tym pamiętać, że tylko część ofiar tego typu oszustw zgłasza się na policję, z obawy przed utratą wizerunku. Jeden z wiodących amerykańskich publicystów poruszających tę tematykę – Brian Krebs szacuje rzeczywisty „utarg" złodziei na ok. 2,4 mld dolarów.

W polskim krajobrazie cyberprzestępczości także dominują oszustwa. Ponad połowę obsłużonych przez CERT Polska incydentów bezpieczeństwa w 2016 r. stanowił *phishing*, czyli próba wyłudzenia poufnych danych. Przykładem może być e-mail przypominający korespondencję z banku, w którym klient jest proszony o potwierdzenie loginu i hasła. Banki ostrzegają klientów i przypominają, że nigdy nie proszą o wysyłanie haseł przez e-mail. Jednak złodzieje liczą na to, że internauta, rozkojarzony lub nieświadomy zagrożenia, poda dane, które później umożliwią im włamanie na jego konto i kradzież pieniędzy.

Również inne szkodliwe zjawiska internetowe, jak przemoc wśród młodzieży – tzw. *cyberbullying*, czyli prześladowanie dziecka przez grupę rówieśniczą, a także różne rodzaje szantażu, w tym coraz popularniejszy *sextortion* (zbitka angielskich słów *sex* i *extortion* – wymuszenie), opierają się na mechanizmach psychologicznych i socjologicznych, a nie na technologii.

W związku z tym tak istotna jest potrzeba edukacji, zwłaszcza młodzieży. Służy temu program Komisji Europejskiej o nazwie „Łącząc Europę", wcześniej funkcjonujący pod nazwą „Safer Internet". Koordynatorem programu w Polsce jest NASK PIB wspólnie z Fundacją Dajemy Dzieciom Siłę. Program oferuje materiały edukacyjne dla młodzieży oraz rodziców i osób pracujących w oświacie – nauczycieli, pedagogów, psychologów. NASK PIB podejmuje również własne działania w tym zakresie w ramach Akademii NASK oraz platformy e-learningowej IT Szkoła.

NASK PIB koncentruje też wiele swoich działań na promowaniu współpracy i budowaniu wzajemnego zaufania pomiędzy różnymi środowiskami, dla których ważne jest bezpieczeństwo Internetu. Doświadczenia, nie tylko polskie, pokazują, że najskuteczniejszą obroną przed poważnymi atakami jest gromadzenie specjalistycznej wiedzy i wymienianie się nią w gronie potencjalnych ofiar. Jeśli jeden podmiot padnie ofiarą hakerów, może ostrzec innych, którzy już się nie dadzą zaatakować w ten sam sposób.

Ten rodzaj współpracy jest konieczny na każdym szczeblu. Powinniśmy się dzielić informacjami o zaistniałych oraz potencjalnych zagrożeniach w obrębie branż, na poziomie krajowym oraz w sieci międzynarodowej. Unia Europejska stymuluje taką współpracę. Ma temu służyć powołanie krajowych centrów koordynacyjnych we wszystkich państwach członkowskich, wymagane przez obowiązującą od ubiegłego roku dyrektywę NIS[5]. Takim ośrodkiem w Polsce jest właśnie NC Cyber w NASK PIB. Również policja bierze udział w naszych działaniach na rzecz pogłębiania współpracy, uczestnicząc we wspólnych ćwiczeniach z ekspertami. Pokazują one w praktyce, że dopełniając wzajemnie nasze kompetencje, możemy zredukować czas potrzebny na rozwiązanie problemu i uzyskać lepsze rezultaty, niż pracując w izolacji. Wierząc, że kluczowym instrumentem przeciwdziałania zagrożeniom jest wiedza, staramy się budować sieć wymiany informacji, nie tylko między ekspertami i nie tylko na krajowym podwórku. Przyszłością globalnej sieci – jeśli ma być bezpieczna – musi być szeroko zakrojona współpraca. Zagrożenia internetowe nie respektują granic państw, więc obrona przed nimi również musi być globalna.

NASK jest Państwowym Instytutem Badawczym podległym Ministerstwu Cyfryzacji. Siedziba instytutu znajduje się w Warszawie. Instytut prowadzi działalność badawczo-rozwojową w zakresie bezpieczeństwa i efektywności systemów ICT. W strukturze NASK PIB od lipca 2016 r. działa Narodowe Centrum Cyberbezpieczeństwa, którego celem jest koordynacja działań na rzecz rozwijania współpracy w zakresie cyberbezpieczeństwa wśród podmiotów świadczących kluczowe dla społeczeństwa usługi. W instytucie działają też wyodrębnione zespoły eksperckie – Dyżurnet.pl oraz CERT Polska, które również weszły do struktury NC Cyber. NASK PIB uczestniczy w międzynarodowych inicjatywach prowadzonych przez instytucje międzynarodowe lub organizacje pozarządowe, m.in. w programie Komisji Europejskiej Safer Internet (obecnie „Łącząc Europę").

[1] Ransomware (z ang. – zbitka wyrazowa powstała ze słów *ransom* „okup" i *software* „oprogramowanie") to rodzaj szkodliwego oprogramowania, które blokuje system komputerowy lub go szyfruje, a następnie żąda od ofiary okupu za przywrócenie dostępu, https://pl.wikipedia.org/wiki/Ransomware [dostęp: 24.11.2017 r.].

[2] https://ec.europa.eu/poland/news/170913_soteu_live_pl [dostęp: 24.11.2017 r.].

[3] Złośliwe oprogramowania (z ang. *malware* – zbitka wyrazowa powstała ze słów – *malicious* „złowrogi, złośliwy" i *software* – „oprogramowanie") to wszelkie aplikacje, skrypty itp. mające szkodliwe, przestępcze, groźne lub destrukcyjne działanie w stosunku do użytkownika komputera, https://pl.wikipedia.org/wiki/Złośliwe_oprogramowania [dostęp: 24.11.2017 r.].

[4] http://www.nomoreransom.org/en/index/html [dostęp: 21.11.2017 r.].

[5] NIS – Dyrektywa Parlamentu i Rady UE w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, https://wwww.bs.net.pl/prawo/dyrektywa-nis [dostęp: 24.11.2017 r.].

Summary

Polish cyber-security system – together for common safety

The scale of threats related to the use of the Internet requires a comprehensive response. It is necessary to develop technological tools, such as systems for automatic detection of threats, their analysis and exchange of information, including international surveillance infrastructure. It is currently one of the most important areas of research and development activity of the NASK National Research Institute. SOC (Security Operation Center) in NC Cyber is working 24 hours a day using these innovative tools to monitor our network and, if necessary, relay information to endangered network owners. This is possible, for example, thanks to the n6 platform. It is a service for professionals – administrators of networks in offices, housing complexes, schools, businesses.

The second important condition for maintaining security is social awareness. Many threats involve fraud, manipulation, deceptive manipulation, or attempts to obtain security data (e.g. banking passwords). Prevention of this type of crime is done primarily by user education. NASK PIB organizes educational activities aimed at adults (including seniors) and children and youth as part of the European Commission's Safer Internet program and within the NASK Academy and e-learning portal IT Szkoła.

Security means also counteracting the distribution of illegal and harmful content online. This is the role of intervention team Dyżurnet.pl, which receives reports (also anonymous) from Internet users about disturbing content.