Za nami 22. konferencja SECURE

Nowoczesne rozwiązania techniczne, wyniki badań i analiz oraz rekomendacje w budowie systemu cyberbezpieczeństwa – przez dwa dni konferencji SECURE 2018 specjaliści w dziedzinie bezpieczeństwa komputerowego wymieniali się wiedzą i doświadczeniami. Konferencję, organizowaną przez NASK i CERT Polska po raz 22. odwiedziło ponad 600 gości. Prezentacje przygotowało 50 prelegentów, a stoiska firmowe 20 wystawców.

Liczba i różnorodność urządzeń, korzystających dziś z internetu, wymaga rozwoju nowych usług bezpieczeństwa teleinformatycznego. Na konferencji SECURE można poznać wszystkie nowości w tej dziedzinie. W tegorocznym programie nie brakowało też specjalistów, prezentujących analizy, dotyczące najbardziej aktualnych wyzwań i wskazujących bardzo praktyczne rekomendacje w budowie kompleksowego systemu cyberbezpieczeństwa w organizacjach i w państwie – mówi p.o. dyrektora NASK Krzysztof Silicki.

Wśród tych najbardziej aktualnych zagadnień na tegorocznym SECURE obecna była sztuczna inteligencja. Ten temat omawiała dr Aleksandra Przegalińska z Akademii Leona Koźmińskiego i MIT. Rozwój tej technologii, jej zdaniem, wiąże się z wieloma szansami na stworzenie zupełnie nowych narzędzi do rozwiązywania problemów w niedostępny dotychczas sposób. Jako przykład takiej technologii podała komputer Alpha Go, który pokonał koreańskiego arcymistrza w tradycyjnej chińskiej grze go Lee Sedola. Jest to komputer, wyposażony w wielowarstwową sieć neuronową i inne systemy uczącego się oprogramowania. „Alpha go, kiedy już nauczył się grać w go, zaczął stosować ruchy z puli, z której ludzcy gracze nie korzystają. Kombinacja ruchów w go jest olbrzymia. Ludzie podczas gry korzystają tylko z pewnych typów tych ruchów. Program wykroczył poza tę strefę i dokonywał zaskakujących zagrań. Te ruchy istniały oczywiście wcześniej, ale ludzie nie zwracali na nie uwagi. Alpha Go zaczął grać w

sposób ‘nieludzki’, co dało mu przewagę” – mówiła specjalistka. Jej zdaniem, właśnie z tą zdolnością do wykroczenia poza nasze schematy myślowe możemy wiązać nadzieję na największe korzyści ze stosowania systemów opartych na sztucznej inteligencji. Ekspertka mówiła również o wyzwaniach – jednym z nich jest trudność w ustaleniu sposobu w jaki głęboka sieć neuronowa dochodzi do rezultatu. To tzw. problem black-boxa, czyli skrzynki, do której wkładamy dane i otrzymujemy wynik, ale szczegóły procesu oceny tych danych i uzyskiwania wyniku są dla nas ukryte. Taka sytuacja może być niekorzystna, a nawet potencjalnie groźna. Dlatego specjaliści w dziedzinie AI starają się przeciwdziałać, poszukując narzędzi do „rozplątywania” zawiłych sieci neuronowych.

Wyzwania, z którymi na co dzień mierzą się specjaliści w dziedzinie cyberbezpieczeństwa są zwykle związane z bardziej tradycyjnymi technologiami. Wiele miejsca na konferencji poświęcono więc zabezpieczeniom operacji w chmurze, poczty elektronicznej, kont zdalnego dostępu do różnych usług oraz urządzeń mobilnych. Omawiane były różne techniki i metody działania, które mogą wykorzystać specjaliści w dziedzinie bezpieczeństwa w firmach.

Podczas konferencji prezentowano badania dotyczące metod wykrywania cyberataków. Piotr Bazydło, kierownik Zespołu Metod Bezpieczeństwa Sieci w NASK przedstawił wyniki prowadzonych obserwacji złośliwych aktywności w teleskopie sieciowym, zwanym również darknetem. Zespół pracuje nad projektowaniem narzędzi do automatycznych analiz ruchu sieciowego, w tym analiz do wykrywania zainfekowanych urządzeń (botnetów) oraz ataków DoS.

Wiele mówiono również o organizacji cyberbezpieczeństwa na poziomie krajowym i międzynarodowym. W Polsce w tym roku zaczęła obowiązywać ustawa o krajowym systemie cyberbezpieczeństwa, która opisuje procedury wymiany informacji, raportowania incydentów i reagowania na nie w celu uniknięcia poważniejszych skutków. Wszystkie podmioty, uznane za kluczowe dla funkcjonowania społeczeństwa, w branżach takich jak energetyka, dostawy wody pitej, usługi finansowe czy szpitale, mają obowiązek zgłaszania wszystkich incydentów naruszenia cyberbezpieczeństwa do odpowiedniego zespołu reagowania (CSIRT) na poziomie krajowym. Trzy takie zespoły działają w NASK, ABW oraz MON. Większość firm oraz indywidualne osoby, a także samorządy terytorialne będą zgłaszać zaobserwowane przez siebie incydenty do CERT Polska w NASK. Szczegółowo system ten omawiał na SECURE 2018 Krzysztof Silicki.

Podczas konferencji odbyła się również debata, poświęcona praktycznemu wdrożeniu nowych regulacji. Z kolei o organizacji współpracy międzynarodowej mówił Jean

Baptiste Demaison z francuskiej agencji ANSSI, przewodniczący Rady Zarządzającej ENISA.