DOŚCIGNĄĆ CYBERPRZESTĘPCÓW

W niniejszym wydaniu „Kwartalnika Policyjnego" powracamy do problematyki bezpieczeństwa w sieci. Już dawno stało się oczywiste, że żyjemy w świecie połączonym cyfrowo, jednak w ostatnim czasie dotkliwie sobie uświadamiamy, z jak wielką dynamiką cyberprzestępczości mamy do czynienia i jak ogromne straty może ona powodować.

W latach 2018–2022 prowadzone przez FBI Centrum Zgłaszania Przestępstw Internetowych (IC3) otrzymało łącznie ponad 3,2 mln skarg, które przełożyły się na stratę ponad 27,6 mld dolarów.

Według *Raportu Interpolu podsumowującego trendy przestępczości na świecie w 2022 r. (2022 Interpol Global Crime Trend Summary Report)*, opartego na danych ze 195 państw, przestępstwa finansowe i cyberprzestępczość są powodem największych obaw i przewiduje się ich największy wzrost. Interpol zaznacza, że policja musi w związku z tym nadążać za rozwojem technologicznym i dysponować niezbędną wiedzą specjalistyczną i umiejętnościami, aby radzić sobie z szybko rozwijającą się przestępczością cyfrową na szczeblu krajowym, regionalnym i międzynarodowym. Podkreśla też rolę partnerstwa i współpracy, tak by korzystać z wiedzy dostępnej w sektorze publicznym, prywatnym i akademickim.

Ze *Sprawozdania Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa za 2023 rok* wynika, że w zeszłym roku w Polsce wzrastała aktywność różnego rodzaju grup prowadzących nielegalne działania w świecie cyfrowym, w tym haktywistów, grup cyberprzestępczych o charakterze zarobkowym, grup powiązanych z innymi państwami lub wręcz bezpośrednio działających w ramach instytucji państw-adwersarzy. Pełnomocnik prognozuje ponadto, że w kolejnych latach skala cyberataków będzie się zwiększać.

W celu lepszego monitorowania zagrożeń w sieci powoływane są krajowe systemy cyberbezpieczeństwa oraz centra zgłaszania przestępstw internetowych. W Polsce CSIRT NASK przyjmuje, analizuje i podejmuje działania oraz koordynuje reakcje na incydenty dotyczące cywilnej cyberprzestrzeni RP zgłaszane przez operatorów usług kluczowych, dostawców usług cyfrowych, samorząd terytorialny, i osoby prywatne, a także na incydenty związane z publikowanymi w Internecie nielegalnymi treściami oraz zagrażającymi bezpieczeństwu dzieci. Jak wynika z raportu CERT NASK za 2023 r., liczba incydentów ciągle wzrasta. W 2023 r. było ich 80 267, czyli o ponad 100% więcej niż w 2022 r.

Najwyższa Izba Kontroli w *Informacji o wynikach kontroli „Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości"* z 2022 r. podkreśliła, iż mimo że Internet stał się nieodłączną częścią naszego życia prywatnego i zawodowego, to istnieje wiele barier, które utrudniają obywatelom uzyskanie skutecznego wsparcia w sytuacji pokrzywdzenia przestępstwem.

Wskazała też, że w jednostkach Policji nie wypracowano instrukcji dla obywateli zgłaszających tego rodzaju zdarzenia, a algorytmy przyjmowania zgłoszeń stanowiły tylko ograniczoną pomoc dla funkcjonariuszy. W zleconym przez NIK badaniu ankietowani wskazali m.in., że aż 85% cyberataków, które ich dotknęły, nie zostało wyjaśnionych, zakończyło się umorzeniem postępowania lub utratą środków finansowych i danych, a tylko w 2% spraw wykryto i skazano sprawcę lub odzyskano stracone środki.

NIK oceniła natomiast pozytywnie utworzenie w styczniu 2022 r. nowej jednostki organizacyjnej Policji, wyspecjalizowanej w zwalczaniu przestępczości internetowej – Centralnego Biura Zwalczania Cyberprzestępczości (CBZC).

Charakterystyka współczesnej cyberprzestępczości i opis jej najnowszych form, geneza utworzenia Centralnego Biura Zwalczania Cyberprzestępczości, a także jego działalność to zagadnienia, o których mowa w pierwszym artykule tego wydania. Autor, policjant CBZC, zaznacza, że Biuro zajmuje się głównie zwalczaniem najbardziej zaawansowanej i zorganizowanej cyberprzestępczości, natomiast w masowej skali z tymi przestępstwami walczą inne jednostki Policji.

Jednak aby stawić czoła błyskawicznie rosnącej lawinie cyberzagrożeń, policjanci w całym kraju potrzebują wsparcia w zakresie szkolenia i rozpowszechnienia dobrych praktyk. Niebagatelna rola w tym zakresie przypada szkolnictwu policyjnemu. Chcąc przybliżyć i zaktualizować nieco wiedzę z zakresu cyberbezpieczeństwa, zaproponowaliśmy w tym numerze artykuły dotyczące informatyki śledczej, cyberstalkingu i innych zagrożeń, a także profilaktyki w obszarze bezpieczeństwa dzieci i młodzieży w sieci.

Zapraszam również do lektury opracowań spoza tematu przewodniego tego numeru. Dotyczą one bezpieczeństwa ruchu drogowego, policji wodnej, kynologii policyjnej, a także tradycji sportu w Policji.

Redaktor naczelny
mł. insp. Agnieszka Gorzałczyńska-Mróz

Grafika na podstawie: www.pixabay.com.