POLSKA: ROŚNIE ZAGROŻENIE CYBERPRZESTĘPCZOŚCIĄ. RAPORT MSWIA

Według raportu MSWiA na temat bezpieczeństwa w Polsce w 2015 roku, mamy w kraju do czynienia ze stałym wzrostem zagrożenia cyberprzestępczością, szczególnie jeśli chodzi o przestępczość związaną z pedofilią. Odnotowano także duży wzrost cyberataków na sieci teleinformatyczne i systemy komputerowe.

Raport dotyczący przestępczości w cyberprzestrzeni został przygotowany na podstawie informacji Komendy Głównej Policji, Agencji Bezpieczeństwa Wewnętrznego, Służby Celnej, Ministerstwa Cyfryzacji i Ministerstwa Sprawiedliwości. W dokumencie podano liczbę przestępstw, ale nie ma szczegółowych informacji, czego one dotyczą. Autorzy raportu wskazują, że zagrożenie cyberprzestępczością systematycznie wzrasta. "Niepokojący jest wzrost popełnionych za pośrednictwem internetu przestępstw związanych z pedofilią" - podkreślono w dokumencie. W 2015 r. liczba tego typu przestępstw wzrosła w stosunku do roku 2014 o 89,4 proc. (w 2014 r. policja wszczęła 154 postępowania w tym zakresie, a w 2015 r. - 281).

Jak można przeczytać w raporcie, cyberprzestrzeń pozostaje obszarem działania zarówno indywidualnych przestępców, jak i zorganizowanych grup oraz środowisk ekstremistycznych i organizacji terrorystycznych. Upowszechnienie dostępu do internetu, w kontekście globalnego charakteru cyberprzestrzeni, przy jednocześnie stosunkowo dużej możliwości zachowania anonimowości i popełniania przestępstw na terenie jednego państwa z obszaru innego, sprzyja występowaniu różnego rodzaju zagrożeń zarówno dotyczących bezpieczeństwa systemów informatycznych, jak i o charakterze stricte przestępczym (przestępczość o charakterze ekonomicznym, kryminalnym i narkotykowym). Istotne jest również, że cyberzagrożenia mają charakter elastyczny i bezpośrednio zależny od kierunków rozwoju nowoczesnych technologii.

Według autorów opracowania, sprawcy przestępstw coraz częściej wykorzystują dedykowane oprogramowanie umożliwiające kamuflowanie miejsca, z którego działają, korzystają z sieci anonimizujących, m.in. TOR, czy wirtualnych systemów dokonywania płatności w internecie, np. bitcoin, pozostając poza jakąkolwiek kontrolą instytucji finansowych i pozwalających na anonimowe transferowanie korzyści uzyskanych z cyberprzestępczości.

Czytaj także: PKO BP ostrzega przed cyberatakami na konta bankowe

Wzrosła liczba wszczętych przez policję postępowań dotyczących ataków na systemy komputerowe lub sieci teleinformatyczne z 27 w 2014 r. do 52 w 2015 r., a także liczba udostępnianych urządzeń, programów lub danych służących popełnieniu przestępstw z 47 w 2014 r. do 58 w 2015 r. Spadła zaś liczba ataków na zasoby lub urządzenia informatyczne instytucji państwowych lub samorządowych - z 9 w 2014 r. do 4 w 2015 r. Dzięki współpracy z Interpolem w 2015 r., przede wszystkim z policją niemiecką, ustalono 98 polskich użytkowników, którzy sprowadzali i rozpowszechniali materiały zawierające pornografię dziecięcą. Wobec 88 osób podjęto czynności procesowe, w rezultacie czego

zatrzymanych zostało 29 osób.

Agencja Bezpieczeństwa Wewnętrznego podała z kolei, że w 2015 r. prowadziła dwa (w 2014 r. - trzy) śledztwa związane z przestępczością w cyberprzestrzeni dotyczącą zakłócenia pracy systemu komputerowego lub sieci teleinformatycznej oraz oszustwa komputerowego. Jak wskazano, w związku z tego rodzaju przestępstwami ABW nie przedstawiła zarzutów. Agencja w 2015 r. nie prowadziła śledztwa w sprawie włamania do systemów komputerowych. W 2014 r. ABW prowadziła dwa śledztwa w tych sprawach.

Zadania w zakresie koordynacji oraz przeciwdziałania cyberzagrożeniom realizuje powołany w lutym 2008 r. w ramach ABW rządowy zespół reagowania na incydenty komputerowe CERT.GOV.PL. W 2015 roku zespół ten zarejestrował 16 tys. 123 zgłoszeń (w 2014 r. - 12 tys. 17 zgłoszeń), z których 8914 (w 2014 r. - 7498) zostało zakwalifikowanych, jako faktyczne incydenty. Różnica między liczbą zarejestrowanych zgłoszeń a liczbą faktycznych incydentów wynika z tego, że część z nich to przypadki błędnej interpretacji przez zgłaszającego legalnego ruchu sieciowego lub wielokrotnego zgłoszenia tych samych incydentów. Zespół CERT.GOV.PL w 2015 r. zarejestrował 4284 incydenty dotyczące złośliwego oprogramowania działającego na stacjach roboczych podłączonych do sieci teleinformatycznych jednostek administracji państwowej (były to botnety Conficker, Tinba oraz Downadup). Zarejestrowano wzrost w stosunku do 2014 r. o około 116 proc. incydentów typu "inżynieria społeczna" z kategorii phishing (to metoda wyłudzenia informacji takich jak loginy, hasła lub PIN-y przy pomocy wiadomości e-mail).

Czytaj także: Kownacki: Bezpieczeństwo systemów MON jest zapewnione

Drugim źródłem informacji o atakach przeprowadzanych na sieci i systemy teleinformatyczne państwowych jest system ARAKIS-GOV. W systemie gromadzone i analizowane są informacje pozwalające na określenie lokalizacji geograficznej źródeł, z których podejmowano ataki na polskie sieci administracji publicznej. Zespół CERT.GOV.PL w 2015 r. odnotował 36 tys. 815 (w 2014 r. - 28 tys. 322) alarmów systemu ARAKIS-GOV. Zdecydowaną większość z nich stanowiły alarmy o priorytecie średnim – 17 tys. 548 (48 proc.) i informacyjnym – 10 tys. 880 (30 proc.). Ponadto zarejestrowano 6958 (19 proc.) alarmów diagnostycznych i testowych. Liczba alarmów o priorytecie wysokim (1429) była najniższa i stanowiła 4 proc. całości.

Ponadto w ramach prowadzonych testów bezpieczeństwa przebadano 25 witryn należących do administracji państwowej. Stwierdzono 302 błędy, w tym: 8 błędów o bardzo wysokim poziomie zagrożenia, 37 – o wysokim, 236 – o niskim oraz 21 błędów oznaczonych, jako informacyjne. W wyniku przeprowadzonych w 2015 r. kontroli przez Służbę Celną zatrzymano 393 szt. terminali internetowych, wykorzystywanych do nielegalnych gier na automatach, tj. tyle samo, ile w 2014 r. Od 2011 r. w Służbie Celnej działa Grupa Zadaniowa ds. e-kontroli, która na bieżąco śledzą portale internetowe, w celu wyszukiwania ogłoszeń dotyczących towarów wrażliwych. W wyniku tych działań wyodrębniane są m.in. strony z informacjami o sklepach lub ekspozycjach stałych z ofertami sprzedaży nielegalnych wyrobów tytoniowych. W 2015 r. zidentyfikowano w ten sposób 58 stron (w 2014 roku: 63).

Jak wynika z raportu w 2015 r. w sądach rejonowych za niszczenie lub uszkadzanie danych informatycznych osądzono łącznie 32 osoby, z czego 24 skazano. Cztery osoby osądzono, z czego 3 skazano za zakłócanie pracy systemu komputerowego lub sieci teleinformatycznej. W 2015 r. za wytwarzanie, pozyskiwanie, zbywanie, udostępnianie, urządzenia lub programu komputerowego do popełniania przestępstw osądzono łącznie 243 osoby, z czego 238 skazano. Ponadto za oszustwo komputerowe gospodarcze w 2015 r. osądzono łącznie 109 osób, z czego 97 skazano.

W większości przypadków, jak wynika z raportu MSWiA, poza atakami wymierzonymi w funkcjonowanie systemów teleinformatycznych, cyberprzestrzeń nie stwarza jednak nowego rodzaju

przestępstwa, a jedynie dostarcza nowych środków lub metod do prowadzenia przestępczej działalności lub stanowi nową przestrzeń, w której taka działalność jest prowadzona. Przykład tego stanowią przestępstwa na szkodę właścicieli dóbr intelektualnych, polegające na bezprawnym rozpowszechnianiu w internecie filmów, muzyki, gier komputerowych czy oprogramowania. Autorzy raportu podkreślają, że internet bywa nie tylko instrumentem popełnienia przestępstwa, ale również obszarem, gdzie pozostają ślady przestępstw o charakterze kryminalnym, dokonanych w świecie rzeczywistym.

PAP/MSWiA/PM