Ministerstwo Cyfryzacji

Informacja Sojusznicza – US–01/2020

Advanced Persistent Threat (APT) z Korei Północnej – opis zagrożenia, przykłady działań, zalecenia bezpieczeństwa

Przeznaczenie informacji

Uwaga:

Niniejszy dokument pod pierwotnym tytułem: *„Guidance on the North Korean Cyber Threat"* jest elementem ostrzeżenia (*„DPRK Cyber Threat Advisory"*) wydanego 15 kwietnia 2020 r. przez amerykańskie instytucje: Departament Stanu (DoS), Departament Skarbu (DoT), Departament Bezpieczeństwa Krajowego (DHS) oraz Federalne Biuro Śledcze (FBI) i służy jako pomocniczy poradnik. Nie zastępuje żadnych przepisów ustawowych, ani wykonawczych. Ministerstwo Cyfryzacji otrzymało zgodę strony amerykańskiej na dystrybucję materiału. Dokument został przetłumaczony z wersji angielskiej (dołączona) oraz dostosowany do polskich warunków przez ekspertów z Departamentu Cyberbezpieczeństwa MC.

Informacja skierowana jest do specjalistów ds. cyberbezpieczeństwa, w szczególności, w następujących podmiotach:

- Organy właściwe ds. cyberbezpieczeństwa;
- Zespoły CSIRT poziomu krajowego;
- Instytucje finansowe;
- Operatorzy usług kluczowych;
- Dostawcy usług cyfrowych;
- Operatorzy infrastruktury krytycznej;
- Urzędy administracji rządowej i samorządowej.

Celem poradnika jest przedstawienie zagrożenia związanego z nielegalnym działaniem zorganizowanych grup cyberprzestępczych z Koreańskiej Republiki Ludowo – Demokratycznej (KRLD), ze szczególnym naciskiem na opis oraz analizę aktywności grupy o nazwie Lazarus Group[1]. Grupa ta jest nie tylko powiązana z rządem północnokoreańskim, lecz jest wręcz narzędziem reżimu do nielegalnego pozyskiwania dewiz.

[1] Inne nazwy: APT-38, Hidden Cobra, Gods Apostles, Gods Disciples, Guardians of Peace, ZINC, Whois Team.

Lazarus, w odróżnieniu od drugiej znanej północnokoreańskiej grupy APT-37[2], skupia się nie na cyberszpiegostwie, lecz na atakowaniu podmiotów z sektora bankowego i finansowego. Cel jest prosty – kradzież pieniędzy. Grupa opiera się w swoich działaniach na dystrybucji zaawansowanego złośliwego oprogramowania (malware) m.in. backdoorów, tunnelers, aplikacji typu dataminer, czy oprogramowania, które trwale niszczy zasoby danych zaatakowanego podmiotu. Eksperci z FireEye oceniają, że na przestrzeni ostatnich lat (od 2014 r.) przestępcy z Lazarus prowadzili nielegalne operacje w 13 państwach, a rezultatem ich działań była kradzież setek milionów USD. Natomiast sama grupa jest oceniania, jako wysoce zaawansowana i podejmująca skalkulowane działania. Jest metodyczna. Długo *„bada"* infiltrowany system przed przystąpieniem do właściwego ataku np. pozyskując wszystkie wymagane dostępy. Co istotne, grupa nie cofa się przed trwałym zniszczeniem zasobów bazodanowych zaatakowanego podmiotu, po tym jak cel przestępców został osiągnięty.

Lista aktywności cyberprzestępców z grupy Lazarus[3]:

1. Przyjmuje się, że APT-38 przeprowadziło swoja pierwszą znaną operację w lutym 2014 r.;
2. Grudzień 2015 r. – próba kradzieży w TPBank (Wietnam);
3. Styczeń 2016 r. – jednoczesny atak na liczne banki międzynarodowe;
4. Luty 2016 r. – kradzież 81 mln USD w Banku Bangladeszu (włamanie poprzez międzybankowy system SWIFT);
5. Październik 2016 r. – domniemany początek kampanii przy wykorzystaniu schematu *„watering hole"* („wodopój") nakierowanego na instytucje rządowe i media – w rezultacie w marcu 2017 r. SWIFT zakazuje dostępu bankom z KRLD (efekt sankcji ONZ);
6. Październik 2017 r. – kradzież 60 mln USD z Far Eastern International Bank (Tajwan) – mechanizm FASTCash;
7. Styczeń 2018 r. – próba kradzieży w Bancomext (Meksyk);
8. Maj 2018 r. – kradzież 10 mln USD z Banku Chile.

[2] APT-37, także znana, jako Reaper – grupa hakerów na usługach rządu KRLD. Zajmuje się zbieraniem informacji wywiadowczych (wojskowych, politycznych, ale również z sektora prywatnego) na potrzeby reżimu, Kim Dzong Una. Głównym celem APT-37 jest Korea Południowa. Jednakże zaobserwowano aktywność tej grupy także w Japonii, Wietnamie oraz na Bliskim Wschodzie. Cyberprzestępcy są przede wszystkim zainteresowani zbieraniem informacji z takich sektorów jak: zdrowie, automatyka, elektronika, lotniczy, chemiczny. Źródło – FireEye.

[3] Dane zgromadzone przez ekspertów z firmy FireEye.

Informacja rządu USA dot. cyberzagrożenia ze strony Korei Północnej

Wstęp do amerykańskiego ostrzeżenia

15 kwietnia br. Departament Stanu, Departament Skarbu, Departamentem Bezpieczeństwa Krajowego oraz Federalne Biuro Śledcze wydały ostrzeżenie na temat cyberzagrożenia związanego z nielegalnymi operacjami zaawansowanych grup cyberprzestępców z KRLD. Ponadto przedstawiono wytyczne dot. środków bezpieczeństwa oraz działań mających na celu ograniczenie tego zagrożenia.

Przestępcze działania Korei Północnej stanowią zagrożenie dla Stanów Zjednoczonych i całej społeczności międzynarodowej, a w szczególności stanowią **istotne zagrożenie dla integralności i stabilności międzynarodowego systemu finansowego**. W efekcie zdecydowanych sankcji nałożonych przez USA i ONZ, KRLD w coraz większym stopniu opiera się na nielegalnych działaniach – w tym cyberprzestępczości - by pozyskiwać fundusze na potrzeby m.in. rozwoju broni masowego rażenia
i programów rakiet balistycznych.

Stany Zjednoczone w szczególności wyrażają głębokie zaniepokojenie złośliwymi działaniami w cyberprzestrzeni prowadzonymi przez wspieraną przez reżim, Kim Dzong Una grupę APT o nazwie HIDDEN COBRA[4]. Co istotne, Amerykanie zwracają uwagę, że Korea Północna jest w stanie prowadzić niszczycielską lub zakłócającą cyberdziałalność mogącą mieć wpływ także na infrastrukturę krytyczną. Północnokoreański reżim używa również zaawansowanych narzędzi do dokonywania kradzieży środków pieniężnych z różnych instytucji finansowych. Ponadto, strona amerykańska podkreśla, że przestępcza działalność grupy APT wspieranej przez rząd KRLD jest całkowicie sprzeczna z międzynarodowym konsensusem dotyczącym odpowiedzialnego zachowania państw w cyberprzestrzeni.

Stany Zjednoczone ściśle współpracują z państwami o podobnych poglądach, aby skupić uwagę i potępić destrukcyjne lub w inny sposób destabilizujące zachowanie Korei Północnej w cyberprzestrzeni. Na przykład w grudniu 2017 roku Australia, Kanada, Nowa Zelandia, Stany Zjednoczone i Wielka Brytania publicznie przypisały rządowi Korei Północnej atak WannaCry 2.0 i potępiły szkodliwą oraz nieodpowiedzialną działalność tego państwa w cyberprzestrzeni. Dania i Japonia wydały oświadczenia popierające atrybucję ataku WannaCry 2.0, który w maju 2017 r. dotknął setki tysięcy komputerów na całym świecie.

Dla społeczności międzynarodowej, instytucji zajmujących się cyberbezpieczeństwem i społeczeństwa kluczowe znaczenie ma zachowanie czujności i współpraca w celu ograniczenia cyberzagrożenia stwarzanego przez Koreę Północną.

[4] Znana, jako Lazarus, czy APT-38.

Złośliwa cyberdziałalność Korei Północnej ukierunkowana na sektor finansowy

Wiele podmiotów działających z KRLD i prowadzących nielegalną aktywność w cyberprzestrzeni podlega bezpośrednio pod północnokoreańską agencję wywiadowczą, która zarządza tajnymi operacjami państwa tj. *Reconnaissance General Bureau*. Władze północnokoreańskie dysponują całą „gamą" wspieranych bezpośrednio przez państwo środków do prowadzenia przestępczej działalności, w tym przede wszystkim wykorzystują: hakerów, kryptologów i programistów, którzy prowadzą działalność szpiegowską, kradzieże w cyberprzestrzeni ukierunkowane na instytucje finansowe i cyfrową wymianę walut, a także motywowane politycznie działania przeciwko zagranicznym mediom. Opracowują i wykorzystują na całym świecie szeroki zakres różnych typów złośliwego oprogramowania, a ich działania stały się coraz bardziej wyrafinowane. Taktyki mające na celu nielegalne pozyskiwanie dochodów przez podmioty działające w cyberprzestrzeni sponsorowane przez Państwo obejmują m.in.:

1. **Kradzieże finansowe poprzez nielegalne działania w cyberprzestrzeni i pranie brudnych pieniędzy.** Komitet 1718 Rady Bezpieczeństwa ONZ w raporcie okresowym sporządzonym przez Panel of Experts z 2019 (raport półroczny PoE z 2019 r.) stwierdza się, że KRLD jest zdolna do generowania znacznych dochodów mimo wprowadzonych sankcji Rady Bezpieczeństwa ONZ poprzez wykorzystywanie złośliwych działań w cyberprzestrzeni do okradania instytucji finansowych przy pomocy coraz bardziej wyrafinowanych narzędzi i taktyk. W raporcie półrocznym PoE z 2019 r. odnotowano, że w niektórych przypadkach złośliwe działania w cyberprzestrzeni dotyczyły również prania pieniędzy, które ma miejsce w wielu państwach. W raporcie tym wspomniano także, że eksperci ONZ prowadzili dziesiątki dochodzeń w sprawie domniemanych kradzieży pieniędzy dokonanych przez przestępców północnokoreańskich. Ocenia się, że do końca 2019 roku Korea Północna usiłowała ukraść, aż 2 miliardy USD poprzez nielegalne działania w cyberprzestrzeni. Zarzuty zawarte w skardze na zabezpieczenie mienia Departamentu Sprawiedliwości z marca 2020 r. dotyczącej utraty pieniędzy, są zgodne z częścią ustaleń PoE. W szczególności w skardze Departamentu Sprawiedliwości stwierdzono, że północnokoreańskie podmioty prowadzące nielegalne działania w cyberprzestrzeni wykorzystywały północnokoreańską infrastrukturę w celu włamania się do giełd walut cyfrowych, kradzieży setek milionów USD w walucie cyfrowej i prania pieniędzy.

2. **Kampanie wymuszeń.** Północnokoreańscy cyberprzestępcy prowadzili również kampanie wymuszeń przeciwko podmiotom z państw trzecich poprzez atakowanie i przejmowanie systemów i sieci danego podmiotu i grożenie ich zniszczeniem chyba, że podmiot ten zapłaci okup. W niektórych przypadkach cyberprzestępcy z KRLD żądali od ofiar opłat pod pozorem długoterminowych *„płatnych konsultacji"* w celu

zapewnienia, że w przyszłości atak się nie powtórzy. Północnokoreańscy przestępcy byli opłacani również za hakowanie stron internetowych i wymuszania na zlecenie klientów zewnętrznych.

3. **Cryptojacking.** W raporcie półrocznym z 2019 r. PoE stwierdza, że prowadzi również dochodzenie w sprawie wykorzystywania przez Koreę Północną mechanizmu *„cryptojacking"*, czyli włamania do maszyny ofiary i wykorzystanie jej zasobów obliczeniowych do „kopania" waluty cyfrowej. PoE zidentyfikował kilka incydentów, w których komputery zainfekowano złośliwym oprogramowaniem do cryptojackingu, a przestępcy (przy pomocy złośliwego oprogramowania) zdobyte w ten sposób aktywa wysłali - w dużej mierze w formie zwiększonej anonimowością waluty cyfrowej (niekiedy nazywanej też *"privacy coins"*) - na serwery znajdujące się w Korei Północnej, w tym na Uniwersytecie, Kim Il Sung w Pjongjang.

Działania te podkreślają wykorzystywanie przez KRLD środków dostępnych w cyberprzestrzeni do generowania dochodów i ograniczenia tym samym skutków sankcji. Pokazują, że każdy kraj może być narażony i wykorzystany przez Koreę Północną. Zgodnie z raportem półrocznym, PoE bada również te działania pod kątem próby naruszenia sankcji Rady Bezpieczeństwa ONZ wobec KRLD.

Publiczna atrybucja cyberataków przestępców z KRLD

Korea Północna wielokrotnie celowała w amerykańskie systemy i sieci rządowe oraz wojskowe, a także systemy podmiotów prywatnych i infrastrukturę krytyczną, w celu kradzieży danych i prowadzenia działalności destrukcyjnej oraz zakłócającej w cyberprzestrzeni. Do tej pory, rząd USA publicznie przypisał następujące incydenty do podmiotów wspieranych przez reżim północnokoreański i ich współsprawców:

- **Sony Pictures**. W listopadzie 2014 r. podmioty wspierane przez rząd północnokoreański przeprowadziły cyberatak na Sony Pictures Entertainment (SPE) w odwecie za film z 2014 roku "*The Interview*"[5]. Cyberprzestępcy z Korei Północnej włamali się do sieci Sony, aby ukraść poufne dane, groziły kadrze kierowniczej i pracownikom SPE oraz uszkodziły tysiące komputerów.
  - FBI's Update on Sony Investigation (Dec. 19, 2014)
  - DOJ's Criminal Complaint of a North Korean Regime-Backed Programmer (Sept. 6, 2018)

- **Kradzież w Banku Bangladeszu**. W lutym 2016 r., jak się domniemywa, podmioty wspierane przez reżim Korei Północnej próbowały ukraść, co najmniej 1 miliard USD z

[5] Polski tytuł: *„Wywiad ze słońcem narodu"*.

instytucji finansowych na całym świecie i rzekomo ukradły 81 milionów USD z Banku Bangladeszu w wyniku szeregu nieautoryzowanych transakcji poprzez sieć SWIFT[6]. Zgodnie ze skargą, podmioty z KRLD uzyskały dostęp do terminali komputerowych Banku Bangladeszu podłączonych do sieci SWIFT. Nielegalny dostęp został uzyskany dzięki naruszeniu sieci komputerowej banku w wyniku ataku typu spearphishing – maile skierowane do pracowników banku. Północnokoreańscy cyberprzestępcy wysyłali wtedy podrobione uwierzytelnione komunikaty SWIFT, nakazujące Bankowi Rezerwy Federalnej w Nowym Jorku przelanie środków z rachunku Rezerwy Federalnej Banku Bangladeszu na rachunki kontrolowane przez sprawców.

- DOJ's Criminal Complaint of a North Korean Regime-Backed Programmer (Sept. 6, 2018).

- **WannaCry 2.0**. Wspierani przez północnokoreańscy rząd cyberprzestępcy opracowali oprogramowanie ransomware, znane jako WannaCry 2.0 (Podobnie jak dwie wcześniejsze wersje tego malware). W maju 2017 r. ransomware WannaCry 2.0, zainfekował setki tysięcy komputerów w szpitalach, szkołach, przedsiębiorstwach i domach w ponad 150 krajach. WannaCry 2.0, szyfruje dane zawarte w zainfekowanym komputerze i pozwala przestępcom na żądanie zapłaty okupu w walucie cyfrowej Bitcoin. Departament Skarbu wskazał konkretnego, północnokoreańskiego programistę, jako jednego z odpowiedzialnych za WannaCry 2.0, a także za cyberataki na Sony Pictures i dokonanie kradzieży w Banku Bangladeszu. Co więcej, wskazano także organizację, dla której ten programista pracował.
  - CISA's Technical Alert: Indicators Associated with WannaCry Ransomware (May 12, 2017);
  - White House Press Briefing on the Attribution of WannaCry Ransomware (Dec. 19, 2017);
  - DOJ's Criminal Complaint of a North Korean Regime-Backed Programmer (Sept. 6, 2018);
  - Treasury Targets North Korea for Multiple Cyber-Attacks (Sept. 6, 2018).

- **Kampania FASTCash**. Od końca 2016 r. podmioty wspierane przez reżim KRLD korzystają z fałszywego systemu wypłaty gotówki z bankomatu, znanego, jako "*FASTCash*" w celu kradzieży dziesiątek milionów USD z bankomatów w Azji i Afryce. Ataki typu FASTCash w celu ułatwienia dokonania fałszywych transakcji, umożliwiają na serwerach banków zdalne przełamanie zabezpieczeń aplikacji przełączników płatności. W jednym z incydentów w 2017 r. przestępcy z Korei Północnej umożliwili jednoczesną wypłatę gotówki z bankomatów znajdujących się w ponad 30 różnych krajach. W innym incydencie w 2018 r. przestępcy działający z KRLD umożliwili wypłatę gotówki z bankomatów w 23 różnych krajach.

[6] Society for Worldwide Interbank Financial Telecommunication.

- CISA's Alert on FASTCash Campaign (Oct. 2, 2018);
- CISA's Malware Analysis Report: FASTCash-Related Malware (Oct. 2, 2018).

- **Włamanie do giełdy waluty cyfrowej (Digital Currency Exchange Hack).** Jak szczegółowo opisano w zarzutach przedstawionych w skardze na zabezpieczenie mienia Departamentu Sprawiedliwości z kwietnia 2018 r. przestępcy wspierani przez reżim północnokoreański włamali się do giełdy cyfrowej walutowej i ukradli walutę cyfrową wartą prawie 250 milionów USD. W skardze opisano, w jaki sposób skradzione aktywa zostały wyprane poprzez setki zautomatyzowanych transakcji waluty cyfrowej, aby zatuszować źródła pochodzenia środków i tym samym uniemożliwić organom ścigania namierzenie tych aktywów. Ponadto, podejrzewa się, że dwóch obywateli Chin miało w imieniu północnokoreańskiej grupy wyprać skradzione aktywa, otrzymując około 91 milionów USD z kont kontrolowanych przez KRLD, jak również dodatkowe 9,5 miliona dolarów z włamania do innej giełdy. W marcu 2020 roku, Departament Skarbu wskazał dwie osoby w związku z reżimem sankcyjnym wobec władz północnokoreańskich, równocześnie z ogłoszeniem przez Departament Sprawiedliwości, że osoby te były uprzednio oskarżone o pranie brudnych pieniędzy i postawiono im zarzut nielegalnego transferu pieniędzy, a także, że 113 rachunków w cyfrowej walucie jest przedmiotem skargi na zabezpieczenie mienia.
  - Treasury's Sanctions against Individuals Laundering Cryptocurrency for Lazarus Group (March 2, 2020);
  - DOJ's Indictment of Two Chinese Nationals Charged with Laundering Cryptocurrency from Exchange Hack and Civil Forfeiture Complaint (March 2, 2020).

Cyberprzestępcy z KRLD w Polsce

W końcu 2016 r. także Polska stała się obiektem ataku ze strony północnokoreańskich cyberprzestępców. Atak rozpoczął się w październiku 2016 r. od wykrycia i wykorzystania podatności na stronie internetowej Komisji Nadzoru Finansowego. Atakujący pozostawili plik ze złośliwym oprogramowaniem. Przestępcy wykorzystali metodę tzw. wodopoju („*watering hole*") do dystrybucji malware do – jak się okazało – wyselekcjonowanej przez atakujących grupy podmiotów.

Odwiedzający tę część strony internetowej KNF, po tym jak jego adres IP został rozpoznany
i „*zaakceptowany*" przez złośliwy kod, był przekierowany do pobrania dedykowanego oprogramowania – oczywiście fałszywego. Z tych adresów IP mógł pobierać dodatkowe instrukcje, „co robić" i na te IP wyprowadzał wykradzione i uprzednio zaszyfrowane dane.

Kilkanaście instytucji finansowych w Polsce m.in. banki zostało zainfekowanych przez to złośliwe oprogramowanie. Co istotne, strona KNF posłużyła także to infekowania licznych instytucji międzynarodowych m.in. z USA, czy Wielkiej Brytanii.

Środki mające na celu przeciwdziałanie cyberzagrożeniom ze strony Korei Północnej

Korea Północna atakuje w skali globalnej w celu uzyskania dewiz dla swojego reżimu, w tym do finansowania programów broni masowego rażenia. Administracja USA apeluje, aby rządy, biznes, społeczeństwo obywatelskie i osoby prywatne podęły niezbędne działania w celu swojej ochrony i skutecznego przeciwdziałania cyberzagrożeniom ze strony podmiotów wspieranych przez reżim północnokoreański, takie jak:

- **Zwiększenie świadomości społecznej na cyberzagrożenia pochodzące ze strony Korei Północnej.** Podkreślenie powagi, zakresu i różnorodności złośliwych działań w cyberprzestrzeni prowadzonych przez KRLD oraz promowanie wdrożenia odpowiednich środków zapobiegawczych i ograniczających ryzyko przyczyni się do zwiększenia ogólnej świadomość zagrożenia w sektorze publicznym i prywatnym.

- **Dzielenie się informacjami technicznymi na temat cyberzagrożeń ze strony Korei Północnej.** Konieczna jest wymiana informacji zarówno na szczeblu krajowym, jak i międzynarodowym, w celu wykrywania i przeciwdziałania cyberagrożeniom pochodzącym z KRLD. Zdecydowanie zwiększy to cyberbezpieczeństwo sieci i systemów. Najlepsze praktyki powinny być dzielone z rządami i sektorem prywatnym. Zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa operatorzy usług kluczowych, dostawcy usług kluczowych, administracja rządowa i samorządowa,

podmioty publiczne, ale także podmioty prywatne i osoby indywidualne mogą zgłaszać m.in. wszelkie incydenty, wykryte podatności, zidentyfikowane cyberzagrożenia do zespołów CSIRT poziomu krajowego:

ZGŁASZANIE INCYDENTÓW W POLSCE

CSIRT GOV – zespół odpowiedzialny za koordynację obsługi incydentów m.in. w administracji rządowej oraz u operatorów infrastruktury krytycznej (w tym także u tych operatorów usług kluczowych, którzy w tym samym czasie są także operatorami infrastruktury krytycznej). Zgłoszenia należy przekazywać na adres mailowy: incydent@csirt.gov.pl. Na stronie internetowej dostępny jest formularz zgłoszenia. W sprawach pilnych możliwy jest kontakt z oficerem dyżurnym pod numerem: +48 22 58 59 373;

CSIRT MON – zespół odpowiedzialny za koordynację obsługi incydentów w sektorze militarnym. Zgłoszenia należy przekazywać na adres mailowy: csirt-mon@ron.mil.pl. Formularz do zgłoszenia jest dostępny tutaj. W sprawach pilnych możliwy jest kontakt z dyżurnym pod tel.: +48 261 87 16 41;

CSIRT NASK – zespół odpowiedzialny za koordynację incydentów m.in. u operatorów usług kluczowych, administracji samorządowej, w sektorze prywatnym oraz zgłaszanych przez osoby indywidualne. Zgłoszenie incydentu/podatności można dokonać w formie elektronicznej. Najlepiej zrobić to za pośrednictwem formularza online na stronie https://incydent.cert.pl, który podpowie, jakie informacje należy zawrzeć w zgłoszeniu. Alternatywnie, można wysłać zgłoszenie pocztą elektroniczną na adres cert@cert.pl. Ponadto, w sprawach pilnych można skontaktować się telefonicznie z dyżurem w CSIRT NASK po numerem tel. +48 22 380 82 74.

- **Wdrożenie i promowanie najlepszych praktyk w obszarze cyberbezpieczeństwa**. Wdrażanie środków wzmacniających cyberbezpieczeństwo – zarówno technicznych i podnoszących świadomość – sprawi, że infrastruktura będzie bardziej bezpieczna i odporna. **Instytucje finansowe**, w tym przedsiębiorstwa świadczące usługi pieniężne, **powinny podjąć niezależne kroki w celu ochrony przed złośliwymi działaniami Korei Północnej**. Działania takie mogą obejmować między innymi:
    - Dzielenie się informacjami o zagrożeniach poprzez kanały rządowe i/lub branżowe;
    - Przeprowadzenie segmentacji sieci, aby minimalizować ryzyko;
    - Wykonywanie regularnych kopii zapasowych danych;
    - Prowadzenie szkoleń świadomościowych dot. rozpowszechnionych taktyk wykorzystywania inżynierii społecznej;
    - Wdrażanie polityk regulujących wymianę informacji i dostępu do sieci;

- Stałe rozwijanie procedur (i planu) reagowania na incydenty[7].

Ministerstwo Cyfryzacji prowadzi i ciągle aktualizuje bazę wiedzy o cyberbezpieczeństwie. Baza wiedzy jest dostępna na portalu gov.pl (https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo) i obejmuje informacje i poradniki dotyczące zarówno podstawowych zasad cyberhigieny, jak i zestawy zaleceń dla profesjonalistów zajmujących się bezpieczeństwem IT.

Komisja Nadzoru Finansowego wydała Rekomendację D dotyczącą zarządzania obszarami technologii informacyjne i bezpieczeństwa środowiska teleinformatycznego w bankach. Natomiast na stronie internetowej zespołu CSIRT NASK dostępne są poradniki oraz materiały informacyjne o zagrożeniach, w ty także jak się przed nimi ustrzec.
Ponadto zespół CSIRT NASK wydaje m.in. w mediach społecznościowych ostrzeżenia o zidentyfikowanych zagrożeniach.

- **Zgłaszanie do organów ścigania**. Jeśli organizacja podejrzewa, że jest ofiarą cyberprzestępców pochodzących z Korei Północnej lub innego źródła, należy także niezwłocznie powiadomić organy ścigania. To nie tylko może przyspieszyć dochodzenie, ale także, w przypadku przestępstwa finansowego, może zwiększyć szanse na odzyskanie skradzionych środków. **Przestępstwa lub podejrzenia przestępstwa należy zgłaszać w najbliższej jednostce Policji lub prokuraturze**. Dla przykładu: amerykańskie organy ścigania przejęły skradzioną przez przestępców z Korei Północnej walutę cyfrową o wartości wielu milionów USD.

- **Wzmocnienie systemu przeciwdziałania praniu pieniędzy (AML)/Przeciwdziałanie finansowaniu terroryzmu (CFT)/Finansowane przeciwdziałania proliferacji broni masowego rażenia (CPF).** Państwa powinny szybko i skutecznie wdrożyć standardy przygotowane przez Financial Action Task Force (FATF) dotyczące przeciwdziałania praniu pieniędzy/finansowaniu terroryzmu/przeciwdziałaniu proliferacji broni masowego rażenia. Standardy te obejmują m.in. zapewnienie instytucjom finansowym oraz innym podmiotom stosowanie środków ograniczających ryzyko zgodnie ze standardami FATF oraz publicznymi oświadczeniami i wytycznymi FATF. W szczególności, FATF wezwał wszystkie państwa do stosowania środków w celu ochrony międzynarodowych systemów finansowych przed praniem pieniędzy, finansowaniem terroryzmu i

[7] W systemie amerykańskim zestawy dobrych praktyk i zaleceń bezpieczeństwa są zawarte m.in. w Cybersecurity Capability Maturity Model przygotowanym przez Departament Energii oraz Cybersecurity Framework opracowanym przez NIST. Ponadto, agencja CISA zapewnia dodatkowe informacje m.in. ostrzeżenia, analizy malware.

ryzykiem finansowania proliferacji broni masowego rażenia ze strony Korei Północnej[8]. Zalecenia te, obejmują m.in.: doradztwo instytucjom finansowym i innym podmiotom w celu zwrócenia szczególnej uwagi na działalność gospodarczą i transakcje z Koreą Północną, w tym z firmami północnokoreańskimi, instytucjami finansowymi i tymi, które działają w ich imieniu. Zgodnie z Rezolucją 2270 Rady Bezpieczeństwa ONZ Paragraf 33, państwa członkowskie powinny zamknąć istniejące oddziały, filie i przedstawicielstwa banków Korei Północnej i zakończyć wymianę korespondencji z północnokoreańskimi bankami.

Ponadto w czerwcu 2019 r. FATF zmieniła swoje standardy wymagając, aby wszystkie państwa regulowały i nadzorowały dostawców usług cyfrowych, w tym giełd walut cyfrowych i ograniczyły ryzyko przy zawieraniu transakcji walutami cyfrowymi. Dostawcy usług cyfrowych powinni pozostać czujni na zmiany w działaniu klientów, ponieważ ich działalność i zasoby mogą być wykorzystywane do ułatwiania prania pieniędzy, finansowania terroryzmu, czy finansowania proliferacji broni masowego rażenia. Stany Zjednoczone są szczególnie zaniepokojone platformami, które zapewniają anonimowe funkcje płatności i obsługę konta bez monitorowania transakcji, zgłaszania podejrzanych działań oraz badania rzetelności klientów[9].

- **Współpraca międzynarodowa.** Aby przeciwdziałać nielegalnej działalności Korei Północnej w cyberprzestrzeni, ważna jest regularna współpraca z krajami na całym świecie w celu zwiększenia świadomości cyberzagrożeń ze strony KRLD poprzez wymianę informacji i dowodów za pośrednictwem kanałów dyplomatycznych, wojskowych, organów ścigania, sądowych i innych. Ponadto, w 2017 r. rezolucja Rady Bezpieczeństwa ONZ zobowiązała wszystkie państwa członkowskie do repatriacji obywateli Korei Północnej uzyskujących dochody zagranicą, w tym ekspertów IT, do 22 grudnia 2019 roku.

[8] The FATF Call to Action on North Korea.

[9] Amerykańskie instytucje finansowe, w tym podmioty świadczące usługi cyfrowe z siedzibą zagranicą prowadzące działalność gospodarczą w całości lub w znacznej części na terenie Stanów Zjednoczonych oraz inne objęte przedsiębiorstwa i osoby powinny dopilnować, aby przestrzegane były przepisy prawne i obowiązki wynikające z Bank Secrecy Act. W przypadku instytucji finansowych obowiązki te obejmują rozwój i utrzymywanie skutecznych programów przeciwdziałania praniu brudnych pieniędzy, które są zaprojektowane w celu zapobiegania wykorzystywaniu sektora usług finansowych do prania pieniędzy, finansowania działalności terrorystycznej, a także identyfikacji i raportowania podejrzanych transakcji, w tym transakcji prowadzonych poprzez cyberprzestrzeń lub nielegalne finansowanie związane z aktywami cyfrowymi, w związku z podejrzanymi działaniami podlegającymi zgłoszeniu do FinCEN - Financial Crimes Enforcement Network w Departamencie Skarbu USA.

Zobowiązania oraz konsekwencje karne (zgodnie z prawem federalnym USA) udziału podmiotów amerykańskich oraz zagranicznych w nielegalnych lub podlegających sankcjom działaniach

Osoby fizyczne i podmioty zaangażowane w nielegalne działania Korei Północnej lub je wspierające, w tym przetwarzające transakcje finansowe będące efektem przestępstwa, powinni być świadomi potencjalnych konsekwencji wynikających z angażowania się w zachowania zabronione lub podlegające sankcjom.

Office of Foreign Assets Control (OFAC) Departamentu Skarbu USA jest uprawniony do nakładania sankcji na każdą osobę, która, między innymi:

- zaangażowana jest w znaczące działania wpływające negatywnie na cyberbezpieczeństwo
  w imieniu rządu KRLD lub Partii Pracy Korei,
- działa w sektorze IT w Korei Północnej,
- uczestniczyła w niektórych innych szkodliwych działaniach w cyberprzestrzeni,
- uczestniczyła, w co najmniej jednym znaczącym eksporcie/imporcie do Korei Północnej jakiegokolwiek towaru, usługi lub technologii.

Dodatkowo, jeśli sekretarz skarbu, w porozumieniu z sekretarzem stanu, stwierdza, że zagraniczna instytucja finansowa świadomie prowadziła lub ułatwiała znacząco handel z Koreą Północną albo świadomie przeprowadziła lub ułatwiła znaczącą transakcję w imieniu osoby wskazanej na mocy North Korea-related Executive Order lub Executive Order 13382 (Weapons of Mass Destruction Proliferators and Their Supporters), instytucja taka może stracić zdolność do prowadzenia korespondencji lub rachunku rozliczeniowego w Stanach Zjednoczonych (oprócz oczywiście innych możliwych restrykcji).

OFAC prowadzi dochodzenia w sprawie oczywistych naruszeń przepisów dotyczących sankcji i egzekwuje ich przestrzeganie zgodnie Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, appendix A. Osoby naruszające ww. przepisy w części 510, mogą podlegać cywilnym karom pieniężnym do najwyższej z obowiązujących maksymalnych kar lub dwukrotności wartości transakcji bazowej.

Departament Sprawiedliwości USA ściga umyślne naruszenia obowiązujących przepisów o sankcjach, zawartych m.in. w International Emergency Economic Powers Act, 50 U.S.C. §§ 1701 i kolejnych. Osoby, która umyślnie łamią prawo, mogą otrzymać karę do 20 lat pozbawienia wolności, grzywny do 1 miliona USD lub kary finansowej o łącznej wartości dwukrotnie przewyższającej zysk brutto - w zależności od tego, która z tych kar jest większa - oraz przepadek wszystkich zaangażowanych funduszy w takich transakcjach. Departament Sprawiedliwości ściga również karnie umyślne naruszenia Bank Secrecy Act (BSA), 31 U.S.C. §§ 5318 and 5322 - ustawy, która wymaga od instytucji finansowych, aby między innymi, utrzymać skuteczne programy przeciwdziałania praniu brudnych pieniędzy i zgłaszać podejrzenia do FinCEN. Osobom naruszającym BSA może grozić kara do 5 lat pozbawienia

wolności, kara grzywny w wysokości do 250 tys. USD i potencjalny przepadek mienia związanego z tym naruszeniem. Kiedy jest to możliwe, Departament Sprawiedliwości będzie również ścigał karnie korporacje i inne podmioty, które naruszają te ustawy. Departament Sprawiedliwości współpracuje również z partnerami zagranicznymi w celu dzielenia się dowodami na poparcie prowadzonych przez siebie dochodzeń i postępowań karnych.

Zgodnie z 31 U.S. Code § 5318(k), sekretarz skarbu lub prokurator generalny mogą wezwać do sądu zagraniczną instytucję finansową, która prowadzi rachunek bankowy osoby w Stanach Zjednoczonych w celu wydania rejestrów przechowywanych zagranicą. Kiedy sekretarz skarbu lub prokurator generalny powiadamia pisemnie daną amerykańską instytucję finansową, że zagraniczna instytucja finansowa nie zastosuje się do takiego wezwania, amerykańska instytucja finansowa musi wypowiedzieć umowę z bankiem tej osoby w ciągu dziesięciu dni roboczych. Niedopełnienie tego obowiązku może spowodować, że amerykańskie instytucje finansowe będą narażone na kary cywilne.

REŻIM SANKCYJNY ONZ

W raporcie półrocznym PoE z 2019 r. odnotowuje się, że Korea Północna wykorzystywała i próbowała wykorzystywać cyberprzestrzeń w celu kradzieży środków finansowych z banków oraz giełd walut cyfrowych, co mogło naruszyć wiele rezolucji Rady Bezpieczeństwa ONZ (m.in., UNSCR 1718 paragraf (OP) 8(d); UNSCR 2094, OPs 8 i 11; UNSCR 2270, OP 32).

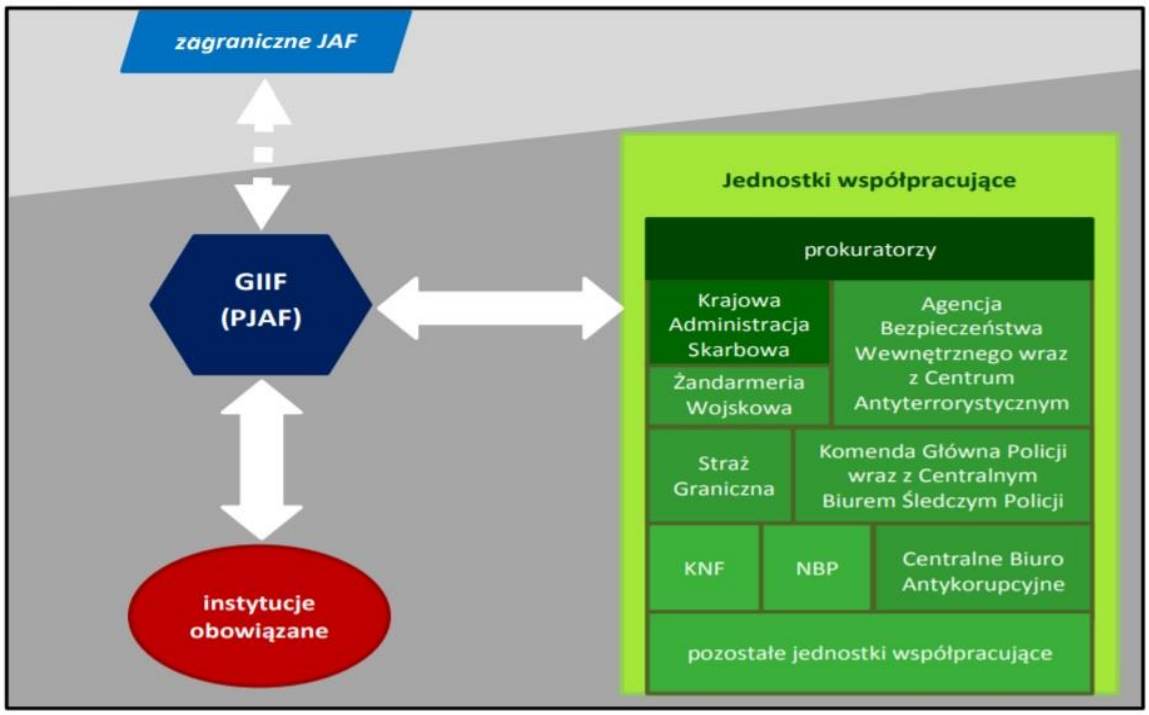
Rezolucje RB ONZ dotyczące Korei Północnej zapewniają również różne mechanizmy zachęcające do przestrzegania sankcji nałożonych przez ONZ. Na przykład Komitet 1718 Rady Bezpieczeństwa ONZ może nakładać ukierunkowane sankcje (tj. zamrożenie aktywów oraz w przypadku osób fizycznych, zakaz podróżowania) na każdą osobę lub podmiot, który angażuje się w transakcje biznesowe z podmiotami wskazanymi przez ONZ lub uchyla się od sankcji.

Nagroda dla współpracujących z rządem USA przy ściganiu cyberprzestępców z KRLD

Jeżeli jakaś instytucja lub osoba posiada informacje o nielegalnych działaniach Korei Północnej
w cyberprzestrzeni, w tym także o przeszłych lub bieżących działaniach, przekazując takie informacje za pośrednictwem Departamentu Stanu (dedykowany program nagród) może otrzymać nagrodę pieniężną w wysokości do 5 milionów USD. Szczegóły na stronie (http://www.rewardsforjustice.net/).

Przeciwdziałanie praniu brudnych pieniędzy w Polsce

Wykres nr 4 – Schemat polskiego systemu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu



SYSTEM PRZECIWDZIAŁANIA PRANIU BRUNDNYCH PIENIĘDZY W POLSCE

Podstawa prawna - ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (implementacja dyrektywy UE). Ustawa określa zadania i obowiązki Generalnego Inspektora Informacji Finansowej (GIIF), funkcjonowanie Komitetu Bezpieczeństwa Finansowego, zasady współpracy GIIF z podmiotami współpracującymi m.in. KAS, ABW, KGP, KNF, czy NBP oraz obowiązki instytucji obowiązanych, czyli podmiotów oferujących usługi lub produkty, które mogą zostać wykorzystane przez przestępców do prania pieniędzy m.in. banki, giełdy.

Istotne znaczenie w systemie mają **instytucje obowiązane**, które mają konkretne obowiązki:

- Rozpoznanie i ocena ryzyka prania pieniędzy w odniesieniu do transakcji zawieranych przez ich klientów;
- Stosowanie środków odpowiednich do oszacowanego ryzyka środków bezpieczeństwa, szczególnie polegających uzyskaniu informacji o klientach;
- Przekazywanie do GIIF informacji o transakcjach ponadprogowych tj. przekraczających równowartość 15 tys. EUR.

Główne zadania GIIF:

- Weryfikowanie zawiadomień o podejrzeniu prania pieniędzy, w tym także w oparciu o informacje otrzymane z instytucji współpracujących oraz partnerów zagranicznych;
- Zawiadamianie prokuratury w przypadku uzasadnionego podejrzenia popełnienia przestępstwa;
- Współpraca z organami ścigania, służbami specjalnymi oraz sądami;
  - Przekazanie informacji o podejrzeniu przestępstwa wraz z prośbą o podjęcie działania do organów ścigania, służb specjalnych oraz Szefa KAS;
  - Przekazanie informacji do KNF w przypadku gdy istnieje podejrzenie naruszenia przepisów rynku finansowego;
- Wymiana informacji ze swoimi odpowiednikami w innych państwach:
  - Na wniosek partnera zagranicznego może przekazywać informacje o nielegalnych operacjach w Polsce;
  - Wnioskować o informacje i dokumenty od partnerów zagranicznych;
  - GIIF może zażądać (na wniosek partnera zagranicznego) wstrzymania transakcji lub blokady rachunku

Organy ścigania:

Centralne Biuro Śledcze Policji - do jego zadań należy w szczególności planowanie, koordynowanie i podejmowanie działań ukierunkowanych na rozpoznawanie i zwalczanie przestępczości zorganizowanej krajowej i międzynarodowej, w szczególności o charakterze kryminalnym, narkotykowym i ekonomicznym oraz jej zapobieganie

Centralne Biuro Antykorupcyjne – służba do zwalczania korupcji w życiu publicznym i gospodarczym, w szczególności w instytucjach państwowych i samorządowych, a także do zwalczania działalności godzącej w interesy ekonomiczne państwa.