RCB
Rządowe Centrum Bezpieczeństwa

BIURO ANALIZ I REAGOWANIA

BIULETYN

KWARTALNY

NUMER 18 STYCZEŃ – MARZEC 2017

Zespół redakcyjny

Biuletynu kwartalnego Rządowego Centrum Bezpieczeństwa:

Grzegorz Świszcz – Zastępca Dyrektora RCB

Martyna Olejnik

Anna Zasadzińska-Baraniewska

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

Atak teleinformatyczny na polski sektor finansowy

Artur Maciąg, Ireneusz Tarnowski
Polska Obywatelska Cyberobrona

„W Urzędzie Komisji Nadzoru Finansowego zidentyfikowana została próba ingerencji z zewnątrz w system informatyczny obsługujący stronę internetową www.knf.gov.pl. Wewnętrzne systemy raportowania przez podmioty nadzorowane funkcjonują niezależnie od systemu informatycznego obsługującego stronę internetową i pozostają bezpieczne. Prace Urzędu przebiegają w sposób niezakłócony. W sprawie tej zostało złożone zawiadomienie do właściwych organów ścigania, z którymi Urząd ściśle współpracuje. Strona internetowa www.knf.gov.pl została wyłączona przez administratorów z UKNF w celu zabezpieczenia materiału dowodowego. Urząd pozostaje w bieżącym kontakcie z przedstawicielami nadzorowanych sektorów, w tym bankowego, których działalność nie jest w żadnym stopniu zagrożona."

Komentarz Komisji Nadzoru Finansowego dotyczący ataku teleinformatycznego

„Warszawska prokuratura okręgowa prowadzi postępowanie sprawdzające w sprawie cyberataku na system informatyczny Komisji Nadzoru Finansowe. Sprawa jest badana w kierunku art. 267 Kodeksu karnego, zgodnie z którym, kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie podlega karze grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2."

prokurator Magdalena Sowa

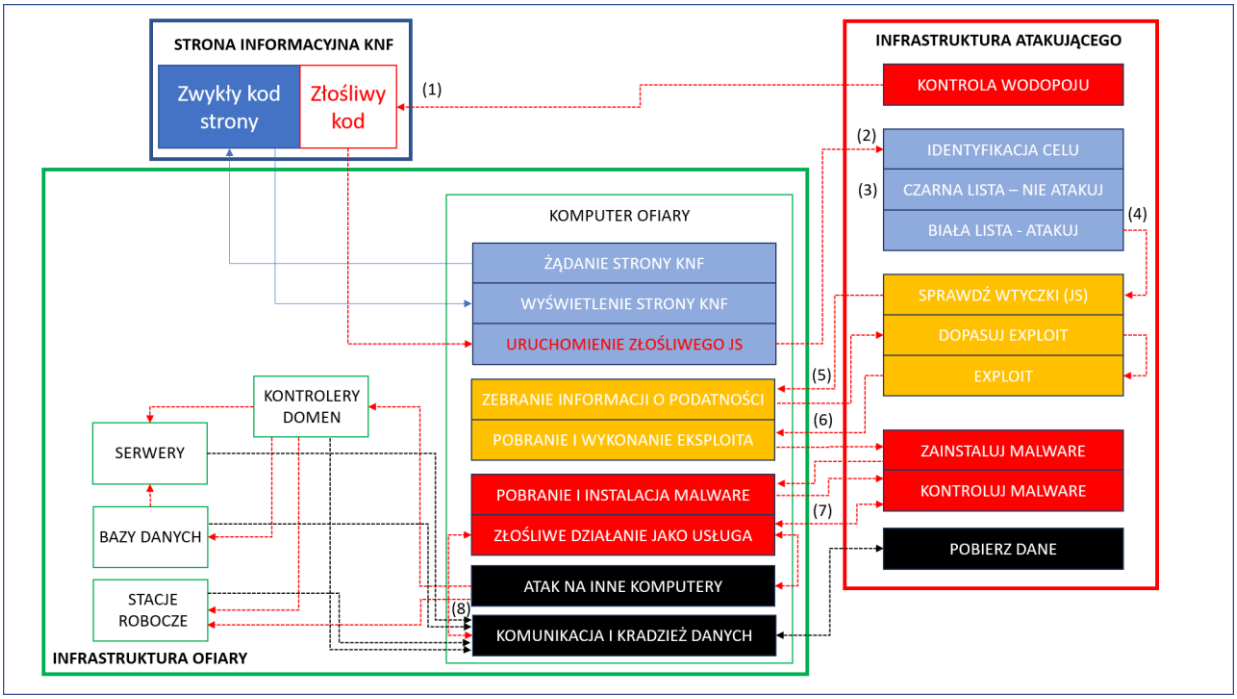
W ostatnim czasie znacząco wzrosła liczba zagrożeń, ataków oraz incydentów komputerowych. Niemal codziennie każda organizacja spotyka się z atakami komputerowymi. Wiele z nich nie jest świadomych tego, że są przedmiotem ataku, inne nie są przygotowane na atak podejmując działanie dopiero w sytuacji wystąpienia incydentu, natomiast organizacje o wysokim poziomie świadomości planują swoją reakcję na zagrożenie z wyprzedzeniem zachowując ciągłą gotowość do aktywnej obrony swoich zasobów i interesów ich klientów.

CO SIĘ STAŁO?

Polska cyberprzestrzeń nie stanowi „samotnej wyspy" na globalnym oceanie informacji. Kwestią czasu było, po głośnych atakach na międzynarodowe systemy finansowe, uderzenie skierowane w banki obecne na polskim rynku. Choć cele atakujących do dzisiaj nie są jawne, jednym z nich było przedostanie się do zaufanej sieci wewnętrznej systemów bankowych, przejęcie kontroli nad komputerami tam umieszczonymi i ustanowienie komunikacji pomiędzy systemami ofiary a infrastrukturą kontrolowaną przez przestępców. W niektórych przypadkach cel ten został osiągnięty przy wykorzystaniu kilku na pozór niezwiązanych ze sobą błędów, jakie popełniono. Aby cały atak się powiódł trzeba było pokonać kilka poziomów zabezpieczeń jakie są stosowane w bankowych systemach informatycznych. Wdrożone rozwiązania techniczne oraz organizacyjne (m.in. stosowanie norm oraz rekomendacji regulatorów krajowych oraz organizacji międzynarodowych) znacząco utrudniają uzyskanie informacji, a tym bardziej dostępu do wewnętrznego systemu banku. Skuteczni przestępcy od wieków wiedzą, że nie warto tracić czasu na „frontalny atak", bo zazwyczaj istnieją mniej strzeżone drogi do wnętrza. Intruzi postanowili dotrzeć do chronionej warstwy infrastruktury poprzez stacje robocze pracowników, co jest ostatnio najskuteczniejszą metodą „przeskoczenia muru". Kompromitacja stacji roboczych wymaga pokonania dwóch mechanizmów: czujności użytkownika i ochrony stacji końcowej. Pracownicy zatrudnieni w sektorze bankowym posiadają zazwyczaj wiedzę na temat bezpieczeństwa i potrafią rozpoznać proste ataki socjotechniczne jak np. phishing, dlatego użytkownika zaatakowano wykorzystując relację zaufania, jaka łączy bank z nadzorcą, którym jest Komisja Nadzoru Finansowego (dalej KNF). Serwis internetowy (informacyjny) KNF stał się narzędziem w rękach przestępców. Kimkolwiek był ten, kto uznał, że serwis informacyjny nie wymaga szczególnych mechanizmów ochrony, nie wymaga aktualizacji, czy nawet reakcji na zgłoszenia dotyczące nieprawidłowości, powinien był solidniej podejść do analizy ryzyka „łańcucha dostaw" w polskim systemie finansowym. Strona ta stanowi źródło informacji dla pracowników banków, skąd czerpią wiedzę nt. najnowszych komunikatów KNF. Atakujący szukał słabego miejsca w całym systemie w sposób zorganizowany i systemowy (po końcowej analizie incydentu okazało się, że ten sam scenariusz ataku został przeprowadzony w innych krajach, m.in. Urugwaju i Meksyku). Strona KNF została

„zatruta", to znaczy wykorzystując nieaktualizowaną aplikację strony umieszczono w niej dodatkowy kod, który był wykonywany na każdym komputerze odwiedzającym daną stronę, oprócz wyświetlenia jej standardowej zawartości. Tego typu dystrybucja malware nosi nazwę metody wodopoju (ang. watering hole). Polega na tym, że przestępca zamiast próbować bezpośrednio dotrzeć do ofiary, kompromituje miejsca, które ona zazwyczaj zna, przez co atakowany nie zachowuje typowej podejrzliwości i realizuje scenariusz zgodnie z oczekiwaniami agresora („każdy kto przyjdzie i skorzysta z zatrutego źródła zostanie zatruty"). Ta metoda infekcji wykorzystuje przeświadczenie użytkownika internetu o tym, że serwis, z którego korzysta jest bezpieczny. W tym konkretnym przypadku wykorzystano zaufanie użytkowników do regulatora rynku (jakim jest KNF). W ramach relacji zaufania założono bez weryfikacji, że skoro KNF opracowuje, egzekwuje oraz kontroluje standardy (w tym bezpieczeństwo) w podmiotach mu podległych, to on sam będzie bezpieczny i będzie spełniał wszystkie regulacje jakie wprowadza. W opisywanym przypadku nie musiało to być prawdą. Serwis informacyjny KNF był zainfekowany od 5 października 2016 roku do 2 lutego 2017 roku (kiedy to już incydent został ujawniony w mediach). W serwisie zmodyfikowano istniejący kod JavaScript, który nakłaniał każdy komputer gościa do pobrania i uruchomienia skryptu ze złośliwego serwera. Skrypt ten weryfikował czy ofiara stanowi cel jaki wyznaczył sobie atakujący, a dokładniej czy jego adres IP należy do grup adresowych, które były celem. Tutaj trzeba zauważyć, że atakujący wcześniej przeprowadził rekonesans i uzyskał informacje o swojej ofierze (instytucji finansowej, banku). Atak nie był przeprowadzany metodą na chybił trafił, tylko dokładnie zaplanowany. Co więcej, przeprowadzano również weryfikacje, czy aktualnie atakowana sieć nie znajduje się na liście zakazanych sieci, aby jak najdłużej uniknąć wykrycia ataku. Jeśli komputer ofiary pozytywnie przeszedł oba testy, otrzymywał ze złośliwego serwera stronę internetową z JavaScript, który badał przeglądarkę odwiedzającego pod kątem stosowania technologii podatnych na przygotowany przez agresora atak. W kolejnym kroku, jeżeli sieć ofiary należała do kręgu zainteresowań intruza, a środki techniczne zabezpieczeń stacji roboczej celu (jak i ochrona sieciowa) nie wykryły i zablokowały podejrzanej aktywności przeglądarki, następowało pobranie ze złośliwego serwera jednego z czterech exploitów, które wykorzystywały znane podatności we wtyczce Silverlight oraz wtyczce Flash w przeglądarce internetowej. Podatności, które zostały wykorzystane w ataku, ujawnione były już w 2015 oraz w kwietniu 2016 roku i znane były poprawki (aktualizacje oprogramowania), które eliminowały te podatności (poprawki były opublikowane 28 grudnia 2015, 5 kwietnia 2016 oraz 2 maja 2016). Poprawne wykonanie eksploita pozwalało atakującemu na uzyskanie dostępu do systemu komputera ofiary pobranie oraz uruchomienie narzędzi służących do zbierania informacji o kontrolowanym środowisku i przekazaniu ich na serwer przestępców. Opisane fazy ataku miały charakter automatów, nie wymagających interakcji atakującego. Nie były również możliwe do zaobserwowania ze strony użytkownika odwiedzającego „zatruty wodopój". W kolejnej fazie ataku, intruz oznaczał komputery do infekcji docelowym złośliwym oprogramowaniem, które unikając wykrycia instalowane było w systemie użytkownika jako usługa. To oprogramowanie, choć korzystało z zestawu znanych złośliwych narzędzi było niewykrywane przez systemy antywirusowe i zostało przygotowane tak, aby utrudnić jego analizę przez systemy, czy analityków bezpieczeństwa. Na tym etapie ataku intruz praktycznie kontrolował zaatakowane środowisko, zabezpieczenia techniczne zostały przełamane lub ominięte. Zainstalowany złośliwy program sterowany był zdalnie przez przestępcę komendami, które między innymi pozwalały na przeglądanie zasobów komputera i sieci, komunikację z innymi zainfekowanymi komputerami, zaszyfrowanie kopii interesujących plików, po czym wysłanie ich na zdalny serwer. Wiadomo, że przestępcy używali pierwotnie zainfekowanego komputera do ataku na inne obecne w sieci, tworzyli sieć zainfekowanych komputerów i wybierali wśród nich takie, które nie wzbudzając podejrzeń mogły być używane do komunikacji z internetem – w celu sterowania taką przejętą siecią komputerów – botnetem jak i kradzieży danych. W tej chwili trudno ocenić czy była to końcowa faza ataku, czy agresor dotarł do celu i pobrał interesujące go dokumenty. Nie można wykluczyć, że był to kolejny etap, przygotowanie do innego ataku, np. takiego, którego skutkiem mogło być wytransferowanie znacznych wartości pieniężnych.

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l



Rys. 1. Diagram ataku na infrastrukturę ofiary.

Obecny stan wiedzy nie pozwala jednoznacznie stwierdzić jakie były motywacje, co było celem atakujących, jakie dane zostały pobrane i ile tych danych było.

Jak powyżej widać, atak był dobrze zaplanowany, skoordynowany i wieloetapowy, a intruz po wniknięciu do systemu pozostawał w nim nie wykryty.

Atak się powiódł, gdyż popełniono wiele błędów:

- utrzymywano serwis informacyjny w środowisku aplikacyjnym, które było podatne na ataki,
- zignorowano ostrzeżenia, iż strona KNF zawiera zatruty kod źródłowy,
- utrzymano komputery z nieaktualnym i podatnym oprogramowaniem,
- nie monitorowano ruchu sieciowego z infrastruktury zawierającej chronione informacje.

Po tak spektakularnej akcji (w Polsce celowano w kilkanaście banków), specjaliści bezpieczeństwa zastanawiają się kto jest inicjatorem tego ataku. Jednoznaczna atrybucja nie jest możliwa do ustalenia (przynajmniej na podstawie informacji wynikających z analizy incydentu, narzędzi i taktyk). Jednak w analizie przypadku zauważono znaczne podobieństwa do ataku grupy Lazarus (analitycy z Symantec mają pewność). Grupa ta łączona jest z atakami na Sony Pictures (rok 2014) oraz na system transferowy centralnego banku Bangladeszu (rok 2016, skradziono 81 mln $). To właśnie tej grupie przypisuje się autorstwo narzędzi ataku, natomiast nie jest jednoznaczna afiliacja atakującego i dokładny cel. Pewne ślady wskazują na rosyjskojęzycznych hackerów, jednak ten trop traktuje się jako próbę wprowadzenia w błąd analityków – tzw. false flag, znane z innych cyberataków. Stopień zaawansowania oraz techniki operacyjne nie są typowe dla cyberprzestępców, którzy kierują się kryterium finansowym w swoich atakach. Technika, taktyka oraz rozmach (poza Polską było to kilkadziesiąt innych celów w kilkunastu krajach) stanowią obecnie najgroźniejszą kategorię ataków – są to ataki związane z cyberszpiegostwem, gdzie atrybucja wskazuje na kraj o znacznym potencjale w dziedzinie cyberataków.

KONSEKWENCJE

Informacje o tym, iż występuje poważny incydent w (wielu) systemach bankowych została udostępniona przez jeden z banków w postaci IoC (ang. Indicator of Compromise, zbiór technicznych informacji o ataku) w Systemie Wymiany Ostrzeżeń o Zagrożeniach (SWOZ). Informacja uzyskała status ochrony TLP: Amber co oznacza, iż odbiorcy mogą dzielić się informacjami jedynie w obrębie swojej organizacji z osobami, które muszą poznać wiadomości oraz jedynie w zakresie niezbędnym do podjęcia stosownych działań. Narzucenie takiego statusu w znaczący sposób chroni informację, jednak w tym przypadku istotnie utrudniło wymianę informacji

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

między zainteresowanymi instytucjami. Analitycy z zespołów reagowania na incydenty komputerowe (bankowych, rządowych, operatorskich) wymieniali się strzępkami informacji o tym co się dzieje, starając się poznać mechanizmy działania intruza, ocenić skalę włamania oraz oszacować szkody (np. określić jakie systemy padły ofiarą, jakie informacje zostały wytransferowane). 3 lutego pojawiła się pierwsza publikacja prasowa a później kolejne. Zakres niektórych publikacji wprost ujawniał dane z systemu SWOZ, które objęte były klauzulą ochronną. Zdarzenie odbiło się szerokim echem wśród specjalistów ds. bezpieczeństwa. Poza mediami branżowymi pojawiły się informacje w mediach ogólnopolskich, jak również zagranicznych. Wszyscy zaangażowani w obsługę tego incydentu dosyć zdawkowo dzielili się informacjami. Natomiast osoby postronne mogły zauważyć, iż w polskim środowisku nastąpiła blokada informacji.

Przypadek ten pokazuje kilka ważnych aspektów:

- Wykorzystano zaufanie do organu rządowego, aby zaatakować wybrany cel. Zauważono, że systemy ochrony w sektorze rządowym nie są adekwatne do zagrożeń. Wykorzystano niewłaściwą klasyfikację systemów informatycznych i niewłaściwą ich ochronę. Tym samym znacząco zmniejszyło się zaufanie w internecie (zwłaszcza do dostarczycieli treści).
- System Wymiany Ostrzeżeń o Zagrożeniach, który z niemałym wysiłkiem był budowany i w ostatnim czasie był dobrze wykorzystywany – w tym przypadku zawiódł. Informacja z systemu nie trafiła do właściwych osób, nie podjęto w porę działań ograniczających incydent. A w momencie, gdy w systemie znalazły się wartościowe informacje, to nastąpił wyciek informacji do mediów. Wyciek ten sprawił, że obecnie wszyscy użytkownicy systemu jeszcze bardziej będą ograniczać dzielenie się informacjami bojąc się kolejnych wycieków.
- Wyciek danych (w znaczeniu upublicznienia wszystkich adresów IP uczestniczących w incydencie) na początkowym etapie analizy znacząco utrudnił pracę badaczy. Na tym etapie wiedzę powinni posiadać wszyscy zajmujący się badaniem przypadku oraz zespoły bezpieczeństwa w organizacjach (aby móc szukać obecności intruza u siebie lub skutecznie się bronić). Intruz już miał pewność, że został zauważony, posiadł wiedzę, gdzie i w jakim zakresie poznano jego działalność. To mogło mu pozwolić na przekonfigurowanie scenariusza ataku i lepsze ukrycie się lub konsekwentne zacieranie śladów i tworzenie mylnych tropów.
- Po analizie zdarzenia nie można ustalić motywów i pełnych narzędzi atakujących. A brak tych informacji nie pozwala określić zagrożenia i konsekwencji. Jednocześnie są duże trudności w ustaleniu czy zagrożenie zostało opanowane.
- Poza informacjami, których źródłem były wycieki do mediów z banków oraz SWOZ, nie było żadnych oficjalnych komunikatów (zarówno w sektorze, branży jak i do obywateli jako ogółu). Oficjalnie nikt się nie przyznał do zdarzenia, do jego skali i konsekwencji. Nawet KNF nie przyznał się do tak poważnych uchybień, a jedynie wydał oświadczenie informacyjne, iż nastąpiła „próba ingerencji".
- Ze względu na problem z wymianą informacji (nawet na poziomie technicznym) analitycy mieli ograniczone możliwości pełnego badania przypadku. Okazało się, że znacznie więcej informacji można uzyskać od zewnętrznych podmiotów, najczęściej zagranicznych. Kilka firm specjalizujących się w badaniach cyberbezpieczeństwa pozyskało bardzo dużą wiedzę na temat tego przypadku w innych środowiskach, w których dzielenie się informacjami technicznymi funkcjonuje w sposób właściwy (jak wspomniano przypadek dotknął wiele innych instytucji w innych krajach). Firmy te dzieliły się wynikami swoich badań. Wiedza ta pozwoliła w pełni zrozumieć mechanizmy ataku oraz wprowadzić dane (sygnatury, polityki) do systemów ochronnych.

CO DALEJ?

Incydent związany z naruszeniem bezpieczeństwa systemów informatycznych w skali ogólnopolskiej oraz cały tok postępowania w odniesieniu do tego zdarzenia powinien zostać wykorzystany do głębszej analizy. Należy wyciągnąć wnioski i przygotowywać się na kolejne ataki na dużą skalę.

Wnioski z incydentu dotyczą wszystkich: zespołów bezpieczeństwa, CERT, CSIRT, operatorów telekomunikacyjnych, dostawców usług informatycznych, służb państwowych. A są to:

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | www.rcb.gov.pl

- Konieczność znaczącej poprawy współpracy i wymiany informacji w ramach swoich kompetencji (między sobą, ale również podmiotami prywatnymi i zewnętrznymi).
- Prowadzenie działań proaktywnych oraz weryfikacja zabezpieczeń.
- Wdrażanie i stałe stosowanie polityk bezpieczeństwa, norm, standardów (m.in. budowanie bezpiecznych architektur, wdrażanie rozwiązań klasy Security by Design, Defense in Depth).
- Przygotowanie oraz przetestowanie procedur obsługi incydentów, eskalowania tych incydentów i powiadamiania innych elementów obrony cybernetycznej.
- Nie można pozostawić żadnego obszaru poza kontrolą bezpieczeństwa, gdyż nawet na pozór nieistotne miejsca w cyberprzestrzeni mogą stanowić punkt wejściowy do ataku.
- W skali ogólnopolskiej powinien powstać Plan Reagowania na Incydenty Komputerowe (Incident Response Plan – IRP).

Należy zastanowić się jakie są możliwości powtórzenia ataku – na sektor bankowy, czy na inne sektory gospodarki lub usług publicznych (np. służbę zdrowia). Prawdopodobieństwo jest bardzo duże. Przestępczość tradycyjna przenosi się w świat cybernetyczny, szpiegostwo tradycyjne przenosi się do świata cyfrowego, cenne informacje są przechowywane w systemach komputerowych, posługujemy się wirtualnymi walutami. To wszystko sprawia, że staliśmy się celem. Ważne byśmy (jako obywatele, jako specjaliści od systemów informatycznych, bezpieczeństwa) zdali sobie sprawę z tego zagrożenia i wyciągnęli wnioski z ataku, który miał miejsce. Wart podkreślenia jest fakt, iż atakujący nie niszczą danych, nie chcą okupu – ich głównym celem stała się informacja. Nie wiemy czy to co zostało zaobserwowane to cały atak, czy raczej przygotowanie do jakiegoś większego i bardziej celowanego ataku. Jak widać atakujący przygotowują precyzyjne plany i scenariusze, a obywatele i informacje o nich stały się celem. To może skutkować złożonymi atakami na infrastrukturę administracji publicznej, czy też infrastrukturę krytyczną, taką jak sektor finansowy, ale nie tylko. Nie tak trudno sobie wyobrazić przejęcie w podobnym ataku systemów zarządzania ruchem, czy powiadamiania kryzysowego.

Kampania Ratankba, którą zaobserwowaliśmy w polskim sektorze finansowym wg badaczy z wielu ośrodków dotyczyła ponad 104 podmiotów w 31 krajach, nie ograniczała się jedynie do jednego sektora, finansowego - złośliwą aktywność zaobserwowano w firmach z branż: ubezpieczeń, telekomunikacji, lotnictwa, edukacji, usług teleinformatycznych (hostingi), usług doradczych [6]. Rozważając wpływ każdej z tych branż na infrastrukturę krytyczną Polski, zaryzykować można wniosek, że usługi finansowe jako jedyne tak intensywnie inwestujące w nowe technologie i uzależniające od nich swoich klientów, są atrakcyjnym celem adwersarzy, których interesem mogłaby być destabilizacja sytuacji społecznej i gospodarczej w kraju. Próby podważenia zaufania do polskiego systemu finansowego, dzisiaj szczęśliwie nieskuteczne, powinny zostać uwzględnione w planach zarządzania kryzysowego, tak aby powstały i zostały przetestowane okresowo testy odporności systemu finansowego na zagrożenia płynące z nowoczesnych technologii informatycznych. Tak samo jak to ma miejsce w innych obszarach infrastruktury krytycznej.

Czy gdyby dziś nastąpił atak o podobnym stopniu skomplikowania, bylibyśmy w stanie go wykryć? Jak byśmy zareagowali? To podstawowe pytania na jakie instytucje odpowiedzialne za bezpieczeństwo obywateli muszą odpowiedzieć.

Źródła:

1. http://www.cashless.pl/wiadomosci/bezpieczenstwo/2243-knf-zrodlem-cyberinfekcji-sektora-finansowego-bankowcy-uspokajaja-pieniadze-klientow-sa-bezpieczne
2. http://www.money.pl/gospodarka/wiadomosci/artykul/atak-na-banki-hakerzy-abw-wlamania-do-bankow,220,0,2256604.html
3. http://www.polskieradio.pl/5/3/Artykul/1723781,Atak-na-strone-KNF-Byl-zaawansowany-technicznie-i-profesjonalny
4. http://www.money.pl/gospodarka/wiadomosci/artykul/cybera tak-na-knf-prokuratura-sledztwo-hakerzy,162,0,2259362.html
5. https://zaufanatrzeciastrona.pl/post/wlamania-do-kilku-bankow-skutkiem-powaznego-ataku-na-polski-sektor-finansowy/
6. https://zaufanatrzeciastrona.pl/post/techniczna-analiza-scenariusza-przebiegu-ataku-na-polskie-banki/
7. https://zaufanatrzeciastrona.pl/post/polityka-komercja-i-niekompetencja-czyli-echa-ataku-na-polskie-banki/
8. http://blog.trendmicro.com/trendlabs-security-intelligence/ratankba-watering-holes-against-enterprises/
9. http://www.cashless.pl/wiadomosci/bezpieczenstwo/2376-po-cyberataku-knf-zbuduje-swoja-nowa-strone-internetowa
10. http://baesystemsai.blogspot.in/2017/02/lazarus-watering-hole-attacks.html
11. http://baesystemsai.blogspot.in/2017/02/lazarus-false-flag-malware.html

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

12. https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware-0
13. https://badcyber.com/several-polish-banks-hacked-information-stolen-by-unknown-attackers/
14. https://blog.cyber4sight.com/2017/02/technical-analysis-watering-hole-attacks-against-financial-institutions/
15. http://www.welivesecurity.com/2017/02/16/demystifying-targeted-malware-used-polish-banks/
16. http://www.pcworld.com/article/3169413/security/recent-malware-attacks-on-polish-banks-tied-to-wider-hacking-campaign.html
17. http://www.polskieradio.pl/42/273/Artykul/1744444,Hakerzy-z-Korei-Polnocnej-odpowiadaja-za-probe-ataku-na-20-polskich-bankow-Zastosowali-taktyke-wodopoju
18. https://www.nytimes.com/2017/03/25/technology/north-korea-hackers-global-banks.html?_r=0

KOMENTARZ

Właściwe podejście do reakcji na atak powinno znaleźć swoje odzwierciedlenie w planach postępowania na wypadek jego wystąpienia. Aby być przygotowanym na atak i podjąć właściwe kroki organizacja musi mieć opracowany całościowy plan postępowania na wypadek wystąpienia incydentu. Każdy trwający atak powinien wyzwolić działania, które zostały przewidziane w procedurach. Należy umożliwiać również elastyczne korzystanie z dostępnej wiedzy i specjalistów, a w szczególności dopasowanie procedur do scenariusza ataku. Odpowiadając za cyberbezpieczeństwo trzeba mieć świadomość, iż atakujący może mieć wiele prób i może popełnić wiele pomyłek. Zespół broniący cyberbezpieczeństwa nie może się pomylić ani razu, gdyż skutki pomyłki „blue team'u" zawsze są kosztowne.

ABC cyberbezpieczeństwa na podstawie wymogów dyrektywy NIS

Anna Cuch
Rządowe Centrum Bezpieczeństwa

Gwałtowny rozwój technologii informacyjnych sprzyja zwiększeniu efektywności komunikacji, powstawaniu innowacji oraz ułatwieniu świadczenia usług. Staje się on równocześnie ogromnym zagrożeniem głównie, ze względu na coraz powszechniejsze i wyrafinowane ataki na sieci informatyczne. Przygotowany przez firmę Check Point Software Technologies Ltd. „2016 Security Report"[1] pokazuje, że co 4 sekundy ściągane jest nieznane złośliwe oprogramowanie, co 32 minuty dane wrażliwe wysyłane są poza serwery przedsiębiorstwa, a straty przedsiębiorstw związane z utratą danych wzrosły w ostatnich 3 latach o 400%.

W trosce o poziom cyberbezpieczeństwa, starając się zmniejszyć podatności poszczególnych krajów na zagrożenia w cyberprzestrzeni, Parlament Europejski przyjął 6 lipca ub. roku dyrektywę w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (2016/1148/UE), dalej jako Dyrektywa NIS. Weszła ona w życie w sierpniu ub. roku, a kraje UE mają 21 miesięcy na jej implementację.

Cele dyrektywy mają zostać osiągnięte poprzez:

- ustanowienie obowiązków dla państw członkowskich dotyczących przyjęcia krajowej strategii cyberbezpieczeństwa,
- utworzenie sieci Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego (tzw. CSIRT),
- stworzenie grupy współpracy zapewniającej strategiczne współdziałanie oraz wymianę informacji,
- ustanowienie wymogów dotyczących bezpieczeństwa sieci i informacji oraz zgłaszania incydentów,
- ustanowienie obowiązków dotyczących wyznaczania przez państwa członkowskie organów krajowych, punktów kontaktowych oraz CSIRT, którym powierzone zostaną zadania związane z cyberbezpieczeństwem.

Zgodnie z informacjami Ministerstwa Cyfryzacji (MC), projekt Strategii Cyberbezpieczeństwa Polski na lata 2017-2022 poddano uzgodnieniom międzyresortowym

[1] http://pages.checkpoint.com/security-report.html.

oraz przedstawiono na Komitecie Rady Ministrów ds. Cyfryzacji. Obecnie procedura legislacyjna jest kontynuowana. Według zapowiedzi MC, dokument powinien zostać przyjęty w drodze uchwały RM na początku drugiego kwartału br. Jednak to dopiero początek drogi do osiągnięcia pełnej zdolności państwa do wykonywania nałożonych na nie funkcji. Istotne są dalsze działania, które będą prowadziły do stworzenia efektywnego systemu zarządzania cyberbezpieczeństwem. Tu główną rolę będzie odgrywała sieć Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego (sieć CSIRT). Na mocy postanowień Dyrektywy NIS państwa członkowskie obowiązane są zapewnić, aby operatorzy usług kluczowych oraz dostawcy usług cyfrowych (sektor prywatny), zgłaszali właściwemu organowi krajowemu lub CSIRT[2] incydenty związane z bezpieczeństwem ich sieci informatycznych. Utworzone 1 lipca 2016 r. Narodowe Centrum Cyberbezpieczeństwa NASK (NC CYBER NASK) ma pełnić rolę security operation center (SOC) w dziedzinie cyberbezpieczeństwa, realizując audyty tych przedsiębiorstw i organów administracji publicznej, w których znajdują się elementy infrastruktury krytycznej.

Ponadto w ramach struktury NC CYBER NASK działa CERT Polska, do którego zadań należą:

- rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci,
- aktywne reagowanie w przypadku wystąpienia bezpośrednich zagrożeń dla użytkowników,
- współpraca z innymi zespołami CERT w Polsce i na świecie,
- udział w krajowych i międzynarodowych projektach związanych z tematyką bezpieczeństwa teleinformatycznego,
- działalność badawcza z zakresu metod wykrywania incydentów bezpieczeństwa,
- analizy złośliwego oprogramowania i systemów wymiany informacji o zagrożeniach;
- rozwijanie własnych narzędzi do wykrywania, monitorowania, analizy i korelacji zagrożeń,
- regularne publikowanie Raportu CERT Polska o bezpieczeństwie polskich zasobów internetu,
- działania informacyjno-edukacyjne zmierzające do wzrostu świadomości w zakresie bezpieczeństwa teleinformatycznego, w tym:
  - publikowanie informacji o bezpieczeństwie na blogu cert.pl oraz w serwisach społecznościowych Facebook i Twitter,
  - organizacja cyklicznej konferencji SECURE,
  - niezależne analizy i testy rozwiązań z dziedziny bezpieczeństwa teleinformatycznego.

Pozostałe wyznaczone Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego zakresem swojego działania objęłyby wszystkich wyznaczonych operatorów usług kluczowych i dostawców usług cyfrowych. Wymagania i zadania dla tych zespołów zawiera załącznik do Dyrektywy NIS. Zespoły te mają stanowić kolejną linię wsparcia dla operatorów i dostawców. Warto zaznaczyć, że dyrektywa nie ustanawia obowiązku wyznaczenia jednego zespołu o charakterze narodowym. Dlatego też można dostrzec potrzebę powołania sektorowych zespołów reagowania na incydenty bezpieczeństwa komputerowego lub sektorowych centrów wymiany i analizy danych (Information Sharing and Analysis Center, ISAC)[3].

Jednocześnie na poziomie europejskim utworzona zostanie sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego. W tym przypadku rolę sekretariatu będzie pełnić Europejska Agencja Bezpieczeństwa Sieci i Informacji ENISA[4]. Do europejskiej sieci zespołów należeć będą CSIRT wybrane przez władze krajów członkowskich, a także CERT-EU.

W zakresie organizacji systemu cyberbezpieczeństwa, skupiającego poszczególne zespoły reagowania na incydenty bezpieczeństwa komputerowego, należy przywołać opinie ekspertów, którzy wskazują na możliwość wykorzystania doświadczeń Stanów Zjednoczonych, gdzie sektorowe zespoły reagowania

[2] CSIRT – Computer Security Incident Response Team.

[3] https://www.cybsecurity.org/9-faktow-o-dyrektywie-nis-ktore-powinienes-znac/.

[4] Europejska Agencja Bezpieczeństwa Sieci i Informacji (ENISA, ang. European Network and Information Security Agency) – agencja Unii Europejskiej odpowiedzialna za zapewnienie wysokiego i efektywnego poziomu bezpieczeństwa w sieciach i systemach informatycznych w Unii Europejskiej. Formalnie powołana do życia 15 marca 2004 roku na mocy Rozporządzenia (WE) nr 460/2004 Parlamentu Europejskiego i Rady służyć ma jako centrum doradztwa państwom członkowskim Unii Europejskiej w kwestiach związanych z szeroko rozumianym bezpieczeństwem w Internecie oraz przyczyniać się do rozwoju społeczeństwa informacyjnego.

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

na incydenty już funkcjonują. Tego typu rozwiązania systemowe pozwalają oszczędzić czas i pieniądze, gdyż są budowane i finansowane przez sektor prywatny. Z uwagi na większą elastyczność w zakresie zatrudniania i wynagradzania gromadzą najlepsze kadry, na których utrzymanie nie mogłyby pozwolić sobie pojedyncze firmy czy też administracja rządowa. Chodzi zarówno o specjalistów analizy wstecznej złośliwego oprogramowania, jak i ekspertów zajmujących się testami penetracyjnymi, aż do osób, których jedynym zadaniem jest prowadzenie działań wywiadowczych w Internecie i darknecie[5]. Zdaniem ekspertów problematyki, powołanie takich zespołów powinno być obowiązkowe i stanowić jeden z podstawowych punktów implementacji Dyrektywy NIS. Takie też zapisy znajdują się w projekcie Strategii Cyberbezpieczeństwa Polski na lata 2017-2022.

Koncepcja budowy CSIRT sektorowych jest jak najbardziej słuszna. Problemem może stać się wyegzekwowanie udziału poszczególnych sektorów w jej realizacji. Często są to firmy i instytucje konkurujące ze sobą. Utworzenie jednego wspólnego dla nich ośrodka skupiającego dane wrażliwe, informującego m.in. o podatnościach, atakach, incydentach w użytkowanych przez nie systemach i sieciach teleinformatycznych, może stać się czynnikiem uniemożliwiającym budowę takiego zespołu. Dlatego też konieczne wydaje się nałożenie ustawowego obowiązku tworzenia sektorowych CSIRT na poszczególnych operatorów usług kluczowych oraz dostawców usług cyfrowych.

Reasumując, przed Polską, a w szczególności przedstawicielami instytucji zaangażowanych w opracowanie Strategii Cyberbezpieczeństwa RP oraz ustawy o krajowym systemie cyberbezpieczeństwa wiele zadań. Wśród najistotniejszych dla realizacji projektu można wyróżnić:

- uchwalenie Strategii Cyberbezpieczeństwa RP na lata 2017-2022 – to zadanie jak już wspomniano jest prawie zrealizowane,
- rzetelną implementację Dyrektywy NIS – jakość jej wdrożenia będzie świadczyć o determinacji w budowaniu cyberbezpieczeństwa,
- klarowne i jednoznaczne określenie ról, odpowiedzialności oraz kompetencji poszczególnych podmiotów w zakresie cyberbezpieczeństwa,
- uchwalenie ustawy o krajowym systemie cyberbezpieczeństwa regulującej najważniejsze kwestie związane z tym obszarem (projekt jest opracowywany w Ministerstwie Cyfryzacji),
- aktywny udział Polski na arenie międzynarodowej w najważniejszych debatach odnoszących się do cyberbezpieczeństwa,
- rozbudowę niezależnych, narodowych zdolności w obszarze cyberbezpieczeństwa (np. program Park Enigma),
- dostosowanie systemu kształcenia w celu pozyskiwania większej ilości specjalistów w obszarze cyberbezpieczeństwa,
- zaprojektowanie mechanizmów dobrze funkcjonującej współpracy prywatno-publicznej,
- zapewnienie odpowiednich środków finansowych w budżecie państwa[6].

[5] jw.

[6] http://www.cyberdefence24.pl/288295,10-przykazan-dla-polskiego-rzadu-w-zakresie-cyberbezpieczenstwa.

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

Wojska amerykańskie w Polsce

Maria Wągrowska
Rządowe Centrum Bezpieczeństwa

Jedno z istotniejszych założeń polskiej polityki bezpieczeństwa i obrony się spełnia. Bezpośrednie zaangażowanie najważniejszego sojusznika z NATO w bezpieczeństwo Rzeczypospolitej staje się bowiem faktem. Od początku 2017 roku przybywają do naszego kraju oddziały amerykańskie. Jednakże całkowitej pewności co do trwałego charakteru obecności jednostek USA jeszcze nie ma.

Zarówno w ocenie rządu RP jak i ekspertów oraz opinii publicznej wojskowa obecność USA w naszym kraju (a jednocześnie przybycie sił z innych państw sojuszniczych i umiejscowienie kilku struktur NATO) uchodzi za znaczące wzmocnienie wschodniej flanki obszaru euroatlantyckiego oraz za czynnik odstraszający potencjalnego wroga od ataku. Niekoniecznie uważana jest natomiast za wystarczającą na wypadek konieczności obrony terytorium. Decyzja Waszyngtonu, dzięki której do Polski trafia Pancerna Brygadowa Grupa Bojowa (ABCT) wspomagana przez Brygadę Lotnictwa Bojowego (CAB) i pododdziały logistyczne zapadła za prezydentury demokraty Baracka Obamy. Tymczasem – biorąc pod uwagę nieukształtowaną jeszcze w pełni politykę administracji republikańskiej pod wodzą prezydenta Donalda Trumpa wobec NATO i zaangażowania w bezpieczeństwo Europy – należy się liczyć z modyfikacjami. Innym – raczej stałym – elementem obecności amerykańskiej ważnej dla obrony Polski i części Europy jest powstająca w Redzikowie baza USA integrowana z sojuszniczym systemem chroniącym przed rakietami balistycznymi.

Siły Stanów Zjednoczonych rozmieszczane u wschodnich granic obszaru objętego gwarancjami bezpieczeństwa wynikającymi z Traktatu Północnoatlantyckiego[1] mają szczególne znaczenie nie tylko w sytuacji współczesnych zagrożeń dla bezpieczeństwa Polski (zwłaszcza na najbardziej wrażliwych terenach) i jej sąsiadów – trzech państw bałtyckich. Liczy się też kilka innych aspektów, jak głównie powstawanie z udziałem USA wojskowej infrastruktury we wschodniej części obszaru sojuszniczego, dzięki czemu zanika w Polsce wcześniejsze poczucie bycia państwem członkowskim NATO drugiej kategorii. Sprzyja to lepszej interoperacyjności pomiędzy oddziałami wojsk amerykańskich i polskich osiąganej przy okazji ćwiczeń, transportu, przerzutu ciężkiego sprzętu jak np. ostatnio drogami w rejonie przesmyku suwalskiego. Usprawnia również łańcuch dowodzenia, komunikowania się i łączności pomiędzy komponentami wojskowymi pochodzącymi z różnych państw.

Należy mieć na uwadze, że amerykańska obecność wojskowa jest „dwuczłonowa". Oznacza to, że część sił jest tu rozmieszczanych na podstawie decyzji jedynie administracji USA, aczkolwiek wpisujących się w politykę NATO, a inna część w ramach sojuszniczych. I tak w przypadku wojsk amerykańskich dyslokowanych stopniowo i rotacyjnie w Polsce na bazie ABCT[2] ową podstawą jest postanowienie Waszyngtonu o wzmocnieniu regionu Europy Środkowo-Wschodniej (European Reassurance Inititative, ERI) podjęte w roku 2014 z planowanym wówczas budżetem 3,4 mld. dol. Inicjatywa ta powstała pod wpływem pogarszającej się sytuacji bezpieczeństwa w naszym regionie i po okresie zmniejszania obecności wojskowej USA na kontynencie europejskim. W odniesieniu do Polski, w ramach ERI, chodzi o ok. 4 tysiące żołnierzy wyposażonych w 87 czołgów M1 Abrams, 144 bojowe wozy piechoty Bradley, 419 samochodów HMMWV w różnych wariantach, a także 18 samobieżnych haubic M109 Paladin. Następnym komponentem, trafiającym do naszego kraju z miejsca stałego

[1] Jednakże podporządkowane dowództwu US Army Europe.

[2] Pancerna Brygadowa Grupa Bojowa (Armored Brigade Combat Team, ABCT) będzie rozmieszczana w cyklu 9-miesięcznym. Pierwszą rotację zapewnia 3 Pancerna Brygadowa Grupa Bojowa z 4 Dywizji Piechoty z Fort Carson (stan Colorado). Dowództwo brygady, batalion inżynieryjny, 3. batalion 29 Pułku Artylerii i 4 Batalion 10 Pułku Kawalerii zostaną rozmieszczone w Żaganiu (gdzie usytuowane będzie dowództwo), Świętoszowie, Skwierzynie i Bolesławcu, a więc w Polsce zachodniej, natomiast będzie ćwiczyć i szkolić się na terenie całego naszego kraju oraz będzie przerzucana do innych krajów flanki wschodniej. Brygada posiada gotowość operacyjną.

bazowania w RFN jest ok. 1800 żołnierzy CAB[3] dysponującej 60 statkami powietrznymi (śmigłowcami CH-47 Chinook, UH-60 Blackhawk, a ponadto 400-osobowym kontyngentem bojowym z 20 śmigłowcami AH-64 Apache)[4]. Jednostka ta może być użyta celem wsparcia ACTB, ale też sił sojuszniczych.

Stany Zjednoczone są bowiem – niezależnie od realizacji ERI – tzw. państwem ramowym (wiodącym) dla batalionowej grupy bojowej NATO[5], która jest rozmieszczana w następstwie sojuszniczej decyzji o tzw. wzmocnionej wysuniętej obecności (enhanced Forward Presence, eFP). W tych ramach w Orzyszu znajdzie się ponad 900-osobowy 2 Batalion 2 Pułku Kawalerii z transporterami Stryker i wsparciem ogniowym armatami 105 mm, współdziałający z naszą 15 Brygadą Zmechanizowaną[6]. Według źródeł amerykańskich[7] w razie ataku jednostka ta będzie gotowa do natychmiastowego działania (ready for fight tonight). Decyzja o eFP zapadła na warszawskim szczycie NATO w lipcu 2016 roku.

W 2018 roku ma zacząć działać amerykańska baza antyrakietowa, zapewniająca obronę przed ograniczonym atakiem rakiet balistycznych na terytorium Polski i część europejskiego obszaru NATO. To zarazem jeden z zasadniczych elementów powstającej sojuszniczej obrony przeciwrakietowej (Ballistic Missile Defence, BMD).

Łącznie na polskiej ziemi znajdzie się 7 tysięcy oficerów i żołnierzy Stanów Zjednoczonych ze sprzętem, który – jak się spekuluje – może być uzupełniany szczególnie z myślą o osłonie wojsk z powietrza.

Amerykańska obecność wojskowa w naszym regionie, zarówno w wymiarze dwustronnym jak i sojuszniczym, stanowić może – pod warunkiem pełnej realizacji jej założeń i kontynuacji – bardzo istotny czynnik wzmocnienia bezpieczeństwa i obronności Polski, zwłaszcza dzięki swemu odstraszającemu charakterowi. Zasadniczą wątpliwością zgłaszaną przez polityków i ekspertów w trakcie planowania ich pobytu była, i pozostaje, przyjęta zasada rotacyjności. Polsce zależałoby na obecności stałej i trwałej, a przynajmniej na razie, brakuje przesłanek wskazujących, aby została podjęta taka decyzja. Będzie ona zależała od wielu czynników: od samej administracji waszyngtońskiej i stopnia jej zaangażowania w bezpieczeństwo i obronę europejskiej części obszaru NATO, od rozwoju sytuacji geopolitycznej, relacji USA z Federacją Rosyjską i perspektyw dialogu o kontroli zbrojeń i środkach budowy zaufania.

KOMENTARZ

Za jeden z ważnych czynników mogących mieć wpływ na przyszłe decyzje można uznać zdolność ze strony Polski, państw bałtyckich i innych położonych na wschodniej flance do współpracy z goszczącymi w naszym regionie wojskami Stanów Zjednoczonych. Wyrażać się ona powinna w bezkolizyjnym współdziałaniu w sferze wojskowej, ale nie tylko. Polska, spełniając rolę państwa-gospodarza (Host Nation Support, HNS), winna wprowadzać wszystkie możliwe ułatwienia i usprawniać procedury, aby Amerykanie mogli efektywnie działać wówczas, gdyby Polsce przyszło się zmierzyć z bezpośrednim zagrożeniem.

[3] Najpierw przybywa do Polski 10 Brygada Lotnictwa Bojowego 1 Górskiej Dywizji z Fort Drun (stan Nory Jork), wchodząca w skład Brygady Lotnictwa Bojowego (Combat Aviation Brigade, CAB), która będzie umiejscowiona w Powidzu.

[4] ERI przewiduje – poza obecnością wojskową – wiele innych przedsięwzięć, ale niekoniecznie na polskim terytorium. Można się z nimi zapoznać np. na stronie www Ośrodka Studiów Strategicznych i Międzynarodowych z Waszyngtonu (Center for Strategic and International Studies, http:/csis.org).

[5] Z udziałem 150 żołnierzy brytyjskich i 150 rumuńskich.

[6] Działania czterech batalionowych grup bojowych rozmieszczanych w Polsce i państwach bałtyckich w ramach eFP mają być koordynowane przez Wielonarodową Dywizję Północny-Wschód w Elblągu (najprawdopodobniej z wykorzystaniem struktur 16. Pomorskiej Dywizji Zmechanizowanej).

[7] Patrz: https://pl.usembassy.gov.pl.

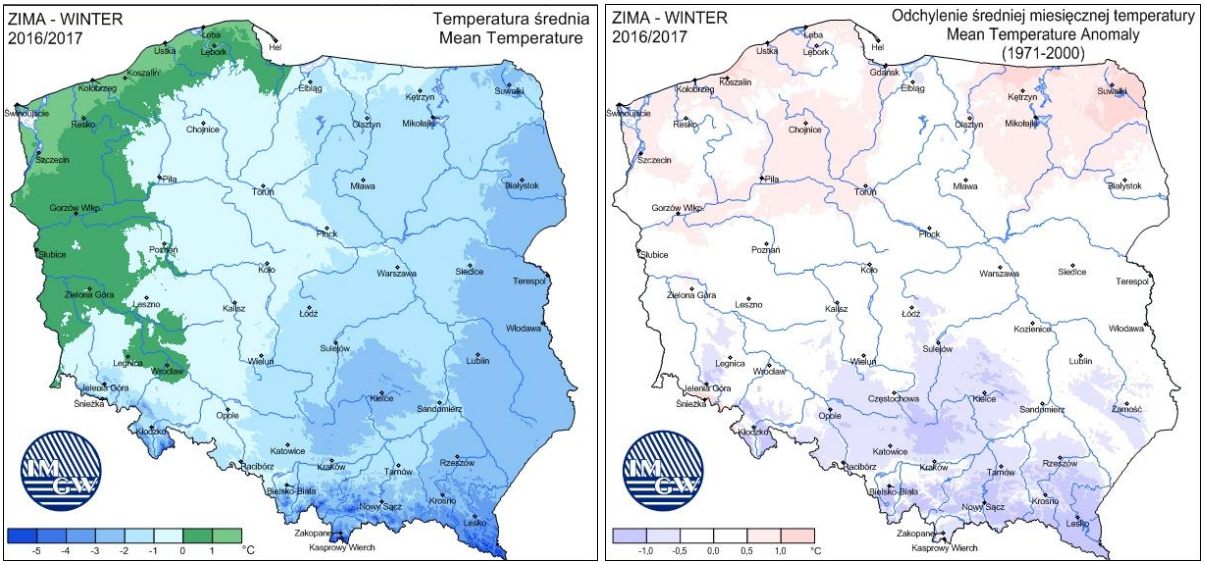
Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | www.rcb.gov.pl

Zima 2016/2017 – podsumowanie sezonu

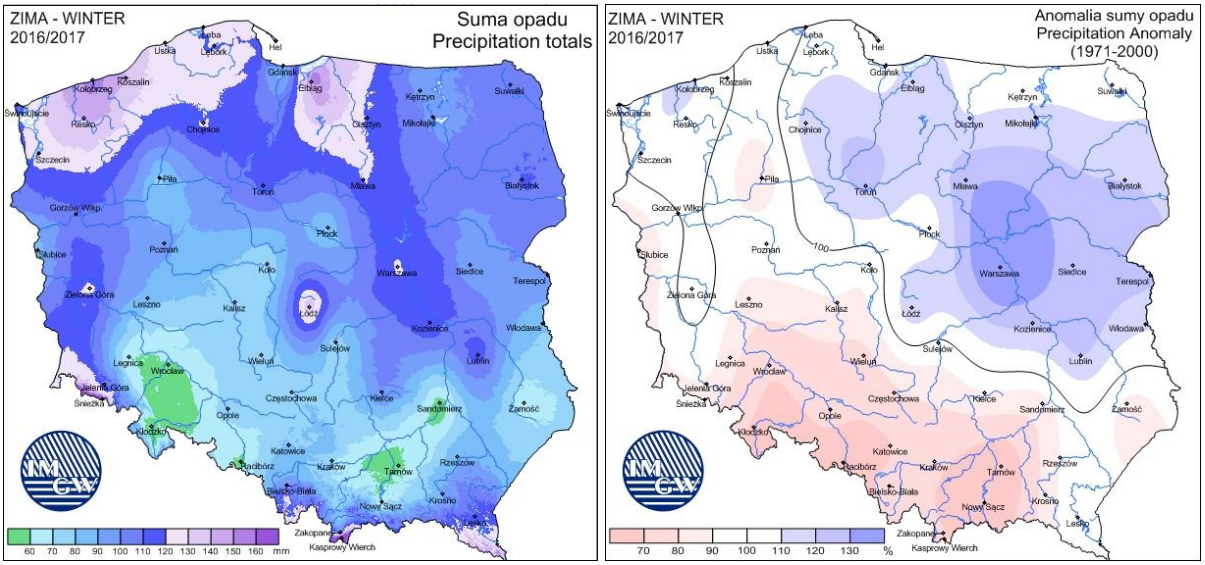
Anna Zasadzińska-Baraniewska
Rządowe Centrum Bezpieczeństwa

Artykuł opracowany we współpracy z ekspertami Centrum Nadzoru Operacyjnego IMGW – PIB

Przebieg warunków meteorologicznych i hydrologicznych w sezonie zimowym 2016/2017 był zróżnicowany w zależności od regionu. Według oceny IMGW okres grudzień 2016 – luty 2017 można sklasyfikować jako: lekko ciepły w północnej części kraju oraz chłodny w południowej połowie kraju (Rys. 1). Opady natomiast można sklasyfikować dla tego sezonu jako: w normie lub powyżej normy w centralnej, północnej i północno-wschodniej Polsce oraz poniżej normy w południowej i południowo-zachodniej części kraju (Rys.2). Podsumowując, można stwierdzić, że na północny kraju zima była ciepła i wilgotna, a na południu chłodna i sucha w stosunku do wartości średnich z wielolecia. Negatywne skutki dla ludności i infrastruktury wywołane były przede wszystkim niską temperaturą powietrza (przypadki zgonów z wychłodzenia) oraz silnym wiatrem, który kilkakrotnie w ciągu sezonu powodował uszkodzenia sieci elektroenergetycznych, budynków i drzewostanu.



Rys. 1. Anomalie średniej miesięcznej temperatury powietrza w zimie 2016/2017 w stosunku do średniej wartości wieloletniej 1971-2000 i średnia miesięczna temperatura powietrza w zimie 2016/2017.



Rys. 2. Sezonowa suma opadu atmosferycznego i anomalie miesięcznej sumy opadu atmosferycznego w zimie 2016/2017 w stosunku do okresu normalnego 1971-2000.

PODSUMOWANIE WARUNKÓW HYDROLOGICZNO-METEOROLOGICZNYCH

Zgodnie z oceną Centrum Nadzoru Operacyjnego IMGW, w grudniu i lutym przeważała pogoda ciepła z opadami znacznie powyżej normy w centralnej oraz północnej i północno-wschodniej części kraju oraz lekko lub znacznie poniżej normy w południowej i zachodniej części kraju. W styczniu natomiast na terenie całej Polski przeważała zdecydowanie pogoda chłodna z opadami poniżej normy wieloletniej.

Styczeń był najchłodniejszym, a zarazem najsuchszym miesiącem minionej zimy. Na przeważającym obszarze kraju sumy miesięczne opadów, głównie w postaci śniegu, nie przekraczały normy wieloletniej, a temperatury średnie dla tego miesiąca były poniżej średniej na wszystkich stacjach synoptycznych (w południowej i południowo-wschodniej Polsce znacznie poniżej normy). W styczniu również notowane były najniższe temperatury tej zimy – silne mrozy utrzymywały się przez wiele dni we wschodniej Polsce. Zanotowano także największą liczbę dni z pokrywą śnieżną, a w znacznej części kraju pokrywa utrzymywała się niemalże przez cały miesiąc. Czas utrzymywania się pokrywy śnieżnej był dwu, a w niektórych regionach nawet trzykrotnie dłuższy niż w sezonie zimowym 2015/2016.

Opady występujące w grudniu i lutym miały postać najczęściej deszczu i deszczu ze śniegiem, rzadziej samego śniegu. Również w tych miesiącach pokrywa śnieżna utrzymywała się krócej, bądź następowało jej topnienie. Najwyższe sumy miesięczne opadu, w odniesieniu do norm z wielolecia, zanotowano zarówno w grudniu jak i w lutym. W miesiącach tych temperatura powietrza przekraczała wartości normalne, a pod względem odchylenia od średniej to luty okazał się najcieplejszym miesiącem tej zimy.

Pierwsze zjawiska lodowe pojawiły się w dorzeczu Wisły pod koniec grudnia, następnie utrzymywały się w styczniu i lutym. Silne mrozy w pierwszej dekadzie stycznia przyspieszyły rozwój zjawisk lodowych na rzekach w całym kraju, przede wszystkim dorzecze Wisły, górnej Odry oraz zlewnie rzek Przymorza – utworzyła się tam stała pokrywa lodowa. W trzeciej dekadzie lutego odnotowano zdecydowane ocieplenie. Temperatury powyżej zera występowały zarówno w ciągu dnia jak i nocy, a dodatkowo wystąpiły intensywne opady deszczu. W tym okresie następowało szybkie topnienie pokrywy śnieżnej oraz zanikanie zjawisk lodowych na rzekach.

W grudniu sytuacja hydrologiczna przez większą część miesiąca była stabilna, a notowane wzrosty i wahania stanu wody najczęściej ograniczały się do strefy wody średniej, lokalnie były wyższe i sięgały strefy wody wysokiej. Na niektórych odcinkach rzek wystąpiły przekroczenia stanu ostrzegawczego, sporadycznie alarmowego. Po wysokich opadach, zanotowanych na początku miesiąca, na Wiśle obserwowano przemieszczanie się niewielkiej fali wezbraniowej (o kulminacji w górnej strefie wody średniej). Podobne dwie niewielkie fale wezbraniowe powstały na górnej Wiśle na początku drugiej dekady miesiąca oraz w trzeciej dekadzie grudnia. Wahania i wzrosty stanu wody w dorzeczu Odry były relatywnie niższe niż w dorzeczu Wisły, przeważnie notowano stan wody na granicy wody średniej i niskiej.

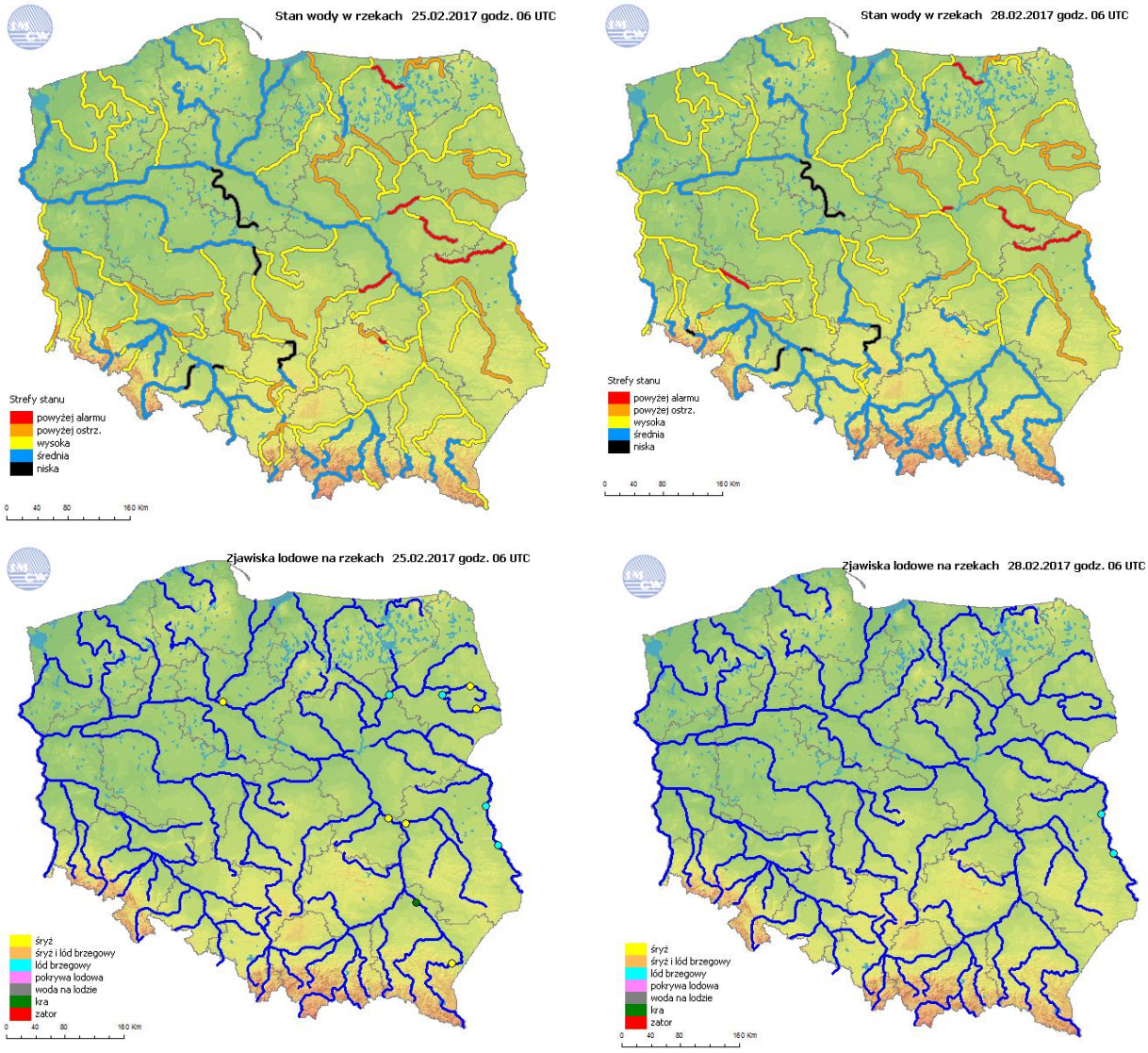
W styczniu na rzekach obserwowano przewagę spadków stanu wody. Tylko na początku stycznia odnotowano na stacjach wodowskazowych na Bałtyku oraz w ujściach rzek do Bałtyku wzrosty stanu wody sięgające 1 m, spowodowane silnym wiatrem od strony morza oraz opadami. W dniach 5-7 stycznia na stacjach tych zanotowano kilka niewielkich przekroczeń stanu alarmowego. W styczniu na rzekach wystąpiły również niewielkie, kilkudniowe lokalne wzrosty, spowodowane rozwojem zjawisk lodowych, głównie pokrywy lodowej oraz opadami. Na niektórych odcinakach rzek stan wody sięgał strefy wody wysokiej, lokalnie notowano przekroczenia stanu ostrzegawczego.

W lutym przez niemal dwie dekady stan wody rzek był ustabilizowany. Począwszy od końca drugiej dekady lutego, w wyniku wzrostu temperatury powietrza powyżej 0°C i opadów deszczu, nastąpiło topnienie pokrywy śnieżnej oraz zanikanie zjawisk lodowych na rzekach. Spływ wód roztopowych wywołał wzrost stanu wody. Najwyższy stan na rzekach notowano 24 i 25 lutego. Wystąpiły liczne przekroczenia stanu ostrzegawczego oraz niewielkie (do 50 cm) stanu alarmowego. Maksymalne wartości przekroczeń stanu alarmowego, rzędu 50-60 cm, nie stworzyły zagrożenia powodziowego.

Występujące w lutym opady deszczu powyżej normy oraz topnienie pokrywy śnieżnej wpłynęły korzystnie na sytuację hydrologiczną przed zbliżającym się sezonem wiosennym i letnim. W czasie sezonu zimowego obserwowano stopniowe wzrosty stanu wody, które nie stwarzały zagrożenia powodziowego, natomiast wpłynęły korzystnie na odbudowę niedoboru

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

wód podziemnych. Największe wzrosty stanu wody wystąpiły w trzeciej dekadzie lutego (Rys. 3). Wówczas miejscami przekroczone zostały stany ostrzegawcze oraz alarmowe. Przekroczenia stanów alarmowych były lokalne, spowodowane topnieniem pokrywy śnieżnej (dodatnie temperatury w ciągu dnia i nocy) przy intensywnych opadach deszczu.



Rys. 3. Strefy stanu wody w rzekach w dniu 25.02.2017 (największa liczba przekroczeń stanów ostrzegawczych i alarmowych w trakcie zimy 2016/2017) i w dniu 28.02.2017 (ostatni dzień sezonu zimowego) oraz notowane w tych dniach zjawiska lodowe.

W końcu sezonu (koniec lutego 2017) stan wody układał się następująco:

- w dorzeczu Wisły – w strefie wody średniej i wysokiej,
- w dorzeczu Odry – w strefie wody średniej i wysokiej,
- rzeki Przymorza – w strefie wody wysokiej.

Z przeprowadzonej przez ekspertów IMGW analizy sytuacji hydrologicznej wynika, że niedobór zasobów wodnych, obserwowany w ostatnich sezonach, został częściowo odbudowany. Poprawa warunków hydrologicznych nastąpiła początkowo w grudniu, a następnie zdecydowanie w lutym. Pomimo, że styczeń był miesiącem suchym to opady w postaci śniegu zostały zmagazynowane i zaczęły topnieć podczas lutowych roztopów. Gwałtowne ocieplenie pod koniec lutego oraz towarzyszące mu opady tylko w niewielkim stopniu stwarzały zagrożenie powodziowe, jedynie na mniejszych rzekach. Notowane w tym czasie stany alarmowe były stosunkowo krótkotrwałe. Początek marca z punktu

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | www.rcb.gov.pl

hydrologicznego był korzystnym stanem wyjściowym dla zbliżającego się ciepłego sezonu zarówno pod względem braku zagrożenia powodziowego jak również wystąpieniem niżówki hydrologicznej.

SKUTKI SYTUACJI HYDROLOGICZNO-METEOROLOGICZNEJ

Głównym zjawiskiem, które minionej zimy wywoływało okresowe negatywne skutki dla ludności i funkcjonowania infrastruktury był silny wiatr, a także lokalnie, zwłaszcza w styczniu, spadki temperatury.

Ogółem w sezonie zimowym, czyli od 1 listopada 2016 r. do 21 marca br., Komenda Główna Policji odnotowała 111 zgonów z powodu wychłodzenia organizmu. Komenda Główna Państwowej Straży Pożarnej od 1 września 2016 r. do 23 marca br., odnotowała 61 zgonów spowodowanych zatruciem tlenkiem węgla (czadem).

Na samym początku sezonu, w dniach 25-27 grudnia ub.r. obserwowano nasilające się porywy wiatru, zwłaszcza na wybrzeżu. 26 grudnia na wybrzeżu i zachodzie występował wiatr silny i bardzo silny (do 55 km/h), w porywach do 100 km/h. W zachodniej połowie kraju porywy wiatru dochodziły do 70-90 km/h, a wysoko w górach do 110 km/h. Straż Pożarna odnotowała ponad 2 200 interwencji, przede wszystkim w woj. mazowieckim, zachodniopomorskim oraz pomorskim. Polegały one głównie na usuwaniu powalonych drzew i konarów. Lekko ranne zostały 2 osoby (m. Czerwonak, woj. wielkopolskie, na samochód upadło drzewo). Ze względu na uszkodzenia linii elektroenergetycznych w godzinach nocnych i wcześnie rano 27 grudnia ub.r. na terenie kraju bez prądu pozostawało około 97 tys. odbiorców (zachodniopomorskie – 36,5 tys., woj. mazowieckie – 34,5 tys., wielkopolskie – 8,1 tys., warmińsko-mazurskie – 3,7 tys., pomorskie – 2,8 tys., lubuskie – 2,6 tys., łódzkie – 2,5 tys., kujawsko-pomorskie – 1,8 tys., podlaskie – 1,7 tys., dolnośląskie – 1,3 tys., podkarpackie – 500, małopolskie – 500, świętokrzyskie – 400). W portach na Bałtyku wprowadzono pogotowia przeciwsztormowe. Usuwanie skutków silnego wiatru trwało do 28 grudnia.

Gwałtowne wichury przeszły nad krajem również 2 marca. Silny wiatr spowodował śmierć jednej osoby (przygniecenie powalonym drzewem) oraz szkody materialne, w tym uszkodzenia linii energetycznych. W kulminacyjnym momencie bez prądu pozostawało 70 tys. odbiorców. Przerwami w dostawie najbardziej dotknięte były województwa: dolnośląskie (30 tys. odbiorców), lubelskie, (23 tys.), mazowieckie (15 tys.) i łódzkie (12,5 tys.).

Kolejny raz silne porywy wiatru spowodowały zniszczenia w ostatnich dniach zimy – 18 marca i 19 marca w godzinach nocnych Państwowa Straż Pożarna interweniowała w sumie 954 razy – w woj. wielkopolskim – 215 razy, śląskim – 131, lubuskim – 130, małopolskim – 104, dolnośląskim – 97, łódzkim – 91, opolskim – 35. Działania związane były głównie z usuwaniem powalonych drzew i konarów oraz przy zabezpieczaniu zerwanych/uszkodzonych poszyć dachowych. Nie było osób poszkodowanych. W szczytowym okresie energii elektrycznej pozbawionych było łącznie około 38 480 odbiorców: lubelskie – 19 000, lubuskie – 8810, opolskie – 3500, łódzkie – 2500, zachodniopomorskie – 2250, małopolskie – 1760, kujawsko-pomorskie – 660. Uszkodzonych zostało 65 budynków: opolskie – 33, łódzkie – 9, małopolskie – 8, podkarpackie – 3, świętokrzyskie – 2 oraz wielkopolskie – 1.

Silny mróz odnotowano w tygodniach 2-8 stycznia i 9-15 stycznia br. Temperatura spadła lokalnie do -25°C w woj. małopolskim – subregion południowy i do -15°C na terenie województw: małopolskiego (subregion północny), podkarpackiego, śląskiego, opolskiego, łódzkiego (subregion piotrkowski), świętokrzyskiego i lubelskiego. W tym okresie również Komenda Główna Policji odnotowała najwyższą liczbę zgonów z powodu wychłodzenia organizmu: w dniach od 2 do 8 stycznia zmarły 24 osoby, natomiast w kolejnym tygodniu – 17. Odnotowano też intensywne opady śniegu, które w połączeniu z porywami wiatru wywoływały zawieje i zamiecie śnieżne. Mimo rozwoju zjawisk lodowych na rzekach oraz niskiej temperatury powietrza, sytuacja w elektrowniach: Kozienice, Stalowa Wola, Połaniec i Ostrołęka była stabilna – nie odnotowano ograniczeń w produkcji wynikających z sytuacji hydrologicznej. W Elektrowni Kozienice trwało ciągłe rozmrażanie ujęcia, jednak tam również nie wystąpiły zakłócenia w wytwarzaniu. Sytuacja na szlakach komunikacyjnych – mimo opadów śniegu – nie stwarzała utrudnień, na drogach pracowały pojazdy zimowego utrzymania. Wszystkie drogi krajowe były przejezdne.

W ostatnich tygodniach zimy wraz z ociepleniem występowały intensywne opady deszczu. Po nocnych opadach, jakie miały miejsce 5 marca br., powstało osuwisko zagrażające drodze prowadzącej do miejscowości Glinka (powiat żywiecki) i dalej

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

do przejścia granicznego ze Słowacją. Osunęła się skarpa podtrzymująca korpus drogi wraz z murem oporowym. 12 marca zaobserwowano powiększenie się osuwiska. Mur oporowy podtrzymujący korpus drogi powiatowej został naruszony, pojawiły się także ubytki powyżej i poniżej uszkodzenia. Konieczne było podjęcie natychmiastowych robót budowlanych, ponieważ dalsze zniszczenie drogi mogło doprowadzić do odcięcia miejscowości Glinka od reszty gminy z powodu braku możliwości wytyczenia objazdu. 13 marca na miejscu zdarzenia odbyło się posiedzenie Powiatowego Zespołu Zarządzania Kryzysowego.

ZACHOROWANIA NA GRYPĘ SEZONOWĄ

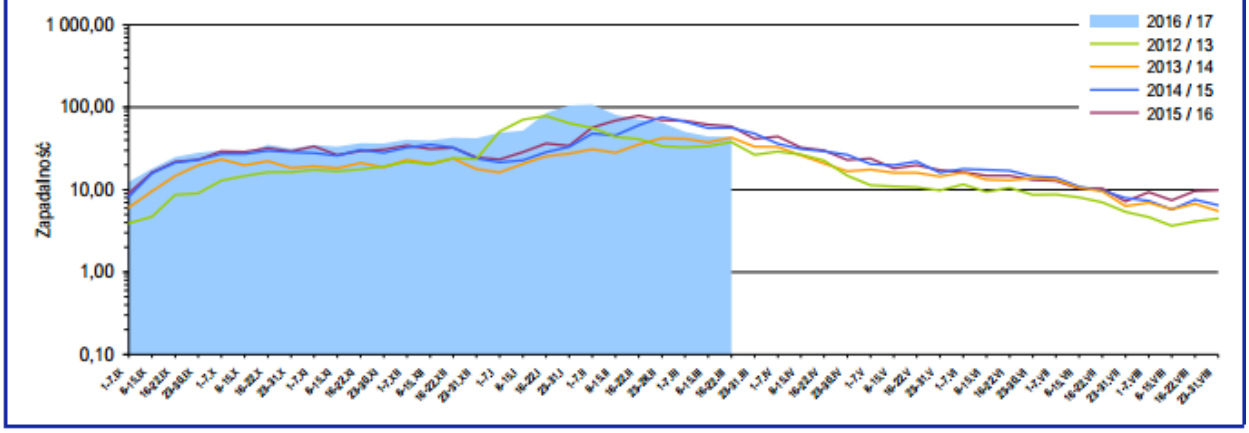
Sezon epidemiologiczny 2016/2017 pod względem zachorowań na grypę charakteryzował się podobną dynamiką jak sezon poprzedni (2015/2016), jednakże jego szczyt wystąpił nieco wcześniej (druga połowa stycznia) i cechował się nieco wyższym poziomem średniej zapadalności.

Największa liczba przypadków zachorowań i podejrzeń zachorowań na grypę została zgłoszona między 8 stycznia a 7 lutego br., przy czym najwyższy wzrost zapadalności odnotowano w okresach meldunkowych 16-22 stycznia oraz 23-31 stycznia br. Zgodnie z danymi epidemiologicznymi NIZP-PZH, najwyższa w skali kraju liczba bezwzględna przypadków i podejrzeń przypadków grypy wystąpiła w okresach:

- 8-15 stycznia: 160 476;
- 16-22 stycznia: 228 451;
- 23-31 stycznia: 363 583;
- 1-7 lutego: 290 771.

Z kolei najwyższą dynamikę zapadalności odnotowano w okresach: 16-22 stycznia wzrost zapadalności na poziomie 32,70 oraz 23-31 stycznia wzrost zapadalności 20,19. Najwyższą przeciętną dzienną zapadalność – 108,02 na 100 tys. ludności – stwierdzono natomiast w okresie 1-7 lutego, gdy ogólna liczba bezwzględna przypadków i podejrzeń przypadków grypy w skali kraju zaczęła już stopniowo spadać.

Zapadalność [1)] na grypę i podejrzenia grypy w sezonie epidemicznym 2016/2017 w porównaniu z poprzednimi sezonami wg okresowych meldunków



Źródło: NIZP-PZH http://wwwold.pzh.gov.pl/oldpage/epimeld/grypa/2017/G_17_03C.pdf.

KOMENTARZ

Sezon zimowy 2016/2017 należy ocenić jako typowy. Nie wystąpiły szczególnie gwałtowne zjawiska atmosferyczne, również niewiele było dni z silnym mrozem. Negatywne skutki warunków pogodowych dla ludności i infrastruktury zaznaczyły się kilkakrotnie, jednak ich nasilenie nie spowodowało wystąpienia sytuacji kryzysowej. Uszkodzenia linii elektroenergetycznych na skutek silnego wiatru wywołały przejściowe, lokalne braki w dostawach energii do odbiorców indywidualnych, jednakże awarie były na bieżąco usuwane. Warunki hydrologiczne i meteorologiczne nie miały wpływu na funkcjonowanie Krajowego Systemu Elektroenergetycznego.

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

Smog – czyli epizody wysokich stężeń pyłu zawieszonego w powietrzu

Barbara Toczko
Główny Inspektorat Ochrony Środowiska

W styczniu i lutym bieżącego roku w południowej i centralnej Polsce wystąpiły epizody wysokich stężeń pyłu zawieszonego w powietrzu zwane smogiem. W takcie trwania epizodów smogowych na 59 stacjach pomiarowych monitoringu jakości powietrza, funkcjonujących w ramach Państwowego Monitoringu Środowiska, odnotowano co najmniej jedno przekroczenie poziomu informowania dla pyłu zawieszonego PM10, w tym na 22 stacjach przekroczony został poziom alarmowy dla pyłu zawieszonego PM10. Najwyższe stężenia pyłu zawieszonego odnotowano w województwie śląskim.

Smog aerozolowy (zimowy) to zjawisko występowania wysokich stężeń pyłu zawieszonego w powietrzu. Można go zaobserwować głównie w okresie jesienno-zimowym. Składają się na niego jednocześnie trzy czynniki. Pierwszym, kluczowym czynnikiem, jest pierwotna emisja pyłu do powietrza. Drugim to emisja zanieczyszczeń gazowych do powietrza i powstawanie pyłu wtórnego w wyniku reakcji chemicznych zachodzących w atmosferze. Trzecim czynnikiem są warunki meteorologiczne sprzyjające kumulacji zanieczyszczeń takie jak cisza wiatrowa, silna inwersja termiczna, zamglenie czy średnia dobowa temperatura powietrza poniżej 5˚C. Sytuacje takie mogą mieć charakter lokalny, regionalny, a nawet ponadregionalny, gdy dotyczą znacznego obszaru Polski lub Polski i krajów ościennych. Mogą trwać od jednego do kilku dni, a w przypadkach ekstremalnych nawet kilkanaście dni.

Pył PM10 jest to frakcja pyłu zawieszonego o średnicach cząstek poniżej 10 µm będąca zawiesiną cząstek stałych i ciekłych w powietrzu.

Poziomy dopuszczalne dla pyłu zawieszonego PM10 w powietrzu pod kątem ochrony zdrowia ludzi

Okres uśredniania wyników pomiarów	Wartość	Dopuszczalna częstość przekraczania normy w roku kalendarzowym	Termin osiągnięcia poziomu celu długoterminowego
rok kalendarzowy	40 µg/m³	–	2005 r.
24 godziny	50 µg/m³	35 razy	2005 r.

Progi ostrzegawcze

wartość progowa informowania społeczeństwa o ryzyku wystąpienia przekroczenia poziomu alarmowego dla pyłu PM10	200 µg/m³	Okres uśredniania wyników – 24 godziny
poziom alarmowy	300 µg/m³	Okres uśredniania wyników – 24 godziny

Problem wysokich stężeń zanieczyszczeń powietrza został zdiagnozowany już kilkanaście lat temu. Duża zawartość w pyle zawieszonym PM10 wielopierścieniowych węglowodorów aromatycznych, w tym benzo(a)pirenu wskazuje, iż głównym źródłem zanieczyszczenia powietrza pyłem w Polsce jest spalanie paliw stałych w wysokoemisyjnych piecach. Według danych Krajowego Ośrodka Bilansowania i Zarządzania Emisjami, sektor komunalno-bytowy jest odpowiedzialny za emisję ok. 49% pyłów emitowanych do atmosfery i emisje te mają bezpośredni wpływ na występowanie smogu. Emisja zanieczyszczeń odbywa się na małej wysokości, dlatego też zanieczyszczenia oddziałują najbardziej na ludzi, którzy zamieszkują w bezpośrednim sąsiedztwie takich źródeł.

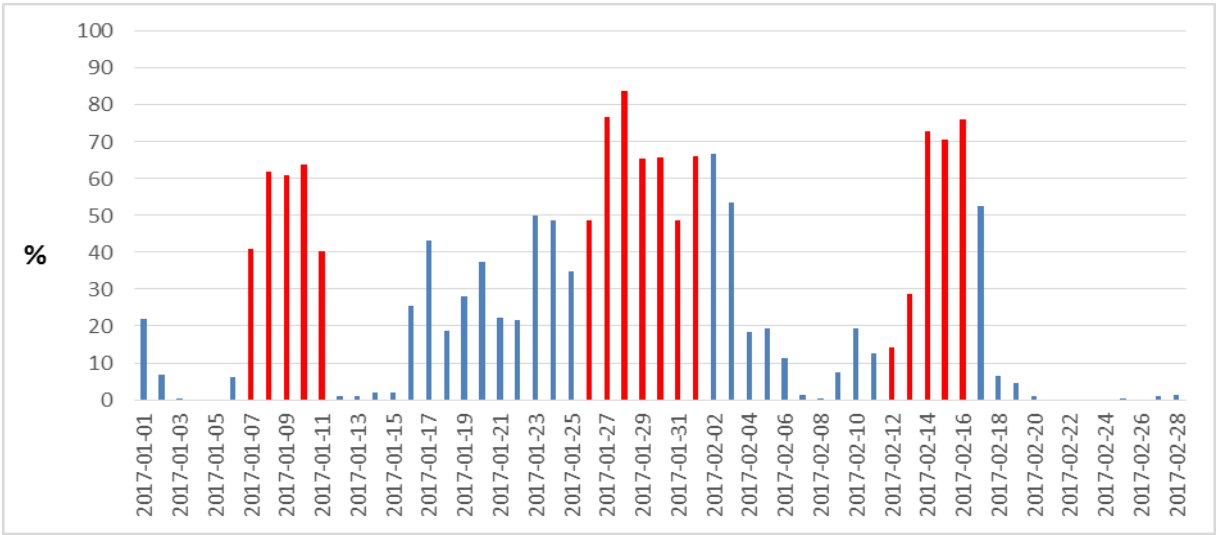
EPIZODY WYSOKICH STĘŻEŃ PYŁU ZAWIESZONEGO W ROKU 2017

Od 1 stycznia do 22 lutego bieżącego roku w południowej i centralnej Polsce wystąpiły epizody wysokich stężeń pyłu PM10 o charakterze ponadregionalnym. Stężenia pyłu PM10, przekraczające poziom informowania, wystąpiły w dniach:

- 7-11 stycznia (województwa objęte epizodem: śląskie, małopolskie, opolskie, łódzkie, mazowieckie, świętokrzyskie, wielkopolskie, dolnośląskie, kujawsko-pomorskie);
- 26 stycznia – 1 lutego (województwa objęte epizodem: śląskie, małopolskie, lubelskie, dolnośląskie, kujawsko-pomorskie);
- 12-16 lutego (województwa objęte epizodem: śląskie, małopolskie, opolskie, łódzkie, mazowieckie, świętokrzyskie, wielkopolskie, dolnośląskie, kujawsko-pomorskie, lubuskie).

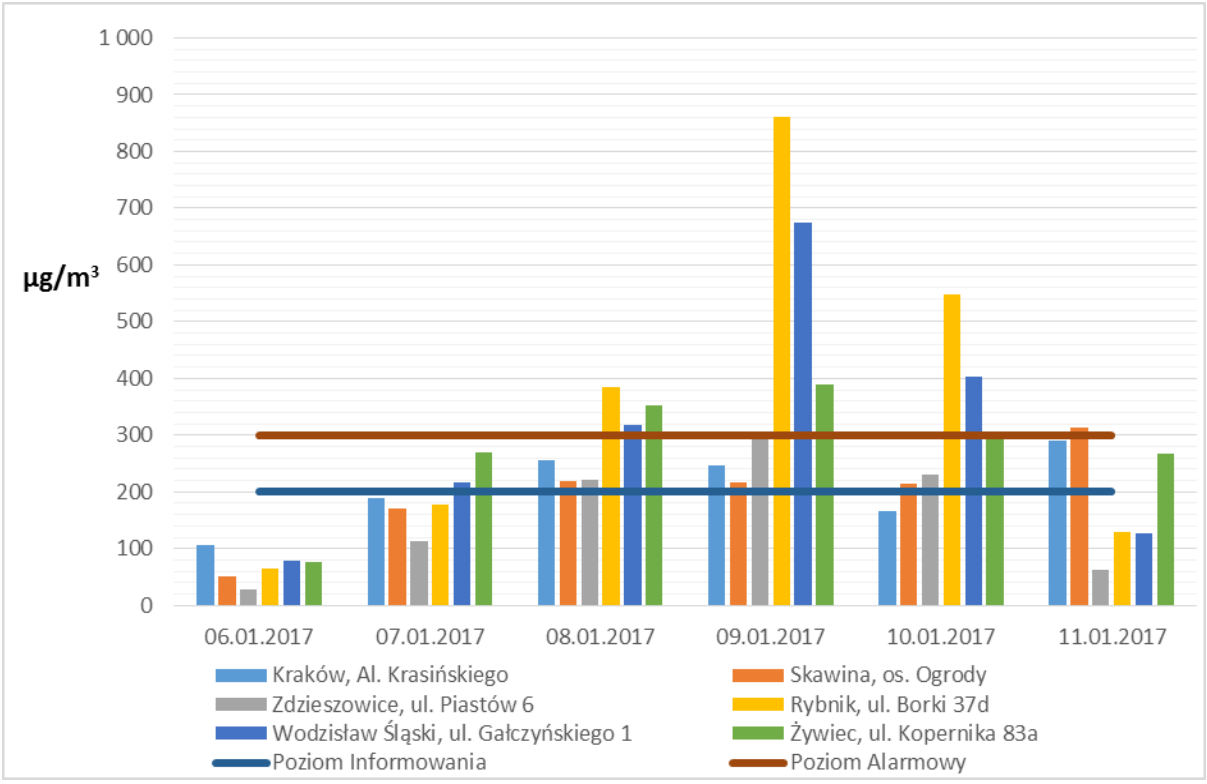
Spośród ww. epizodów (zaznaczonych na rysunku 1 czerwonym kolorem) najwyższe stężenia pyłu zawieszonego PM10 odnotowano od 7 do 11 stycznia na obszarze województwa śląskiego, opolskiego i małopolskiego (rysunek 2). Najwyższe dobowe stężenia pyłu PM10 wystąpiły w Rybniku, gdzie w dniu kulminacyjnym średnie dobowe stężenie pyłu PM10 wyniosło 860 µg/m^3, bardzo wysokie stężenia wystąpiły w wielu innych miastach, np. w Ząbkowicach Śląskich (736 µg/m^3), Wodzisławiu Śląskim (675 µg/m^3), Pszczynie (503 µg/m^3), Częstochowie (499 µg/m^3), Brzeszczach (428 µg/m^3), Gliwicach (424 µg/m^3), Łodzi (399 µg/m^3), Radomsku (394 µg/m^3) i Żywcu (390 µg/m^3).

W trakcie powyższego epizodu wysokie stężenia pyłu PM10 wystąpiły nie tylko w miastach, ale również na obszarach podmiejskich i pozamiejskich. Na stacji tła regionalnego zlokalizowanej w Złotym Potoku (województwo śląskie), w dniu kulminacyjnym stężenie średniodobowe pyłu PM10 wynosiło 95,5 µg/m^3 i było prawie dwukrotnie wyższe od stężenia dopuszczalnego. Oznacza to, iż w trakcie tego epizodu przekroczenia poziomu dopuszczalnego wystąpiły na całym obszarze południowej i centralnej Polski, nie tylko na obszarach miejskich. W przypadku epizodów o ponadregionalnym charakterze, do których zaliczyć należy wszystkie ww. epizody, podwyższone stężenia pyłu zawieszonego są obserwowane na większości stacji monitoringu jakości powietrza w Polsce (rysunek 1).



Rys. 1. Procent stanowisk pomiarowych pyłu PM10, na których stężenie 24-godz. pyłu PM10 w styczniu i w lutym 2017 r. przekraczało wartość 75 µg/m^3, czyli o ponad 50% przekraczało średniodobowy poziom dopuszczalny dla pyłu PM10 (spośród wszystkich stanowisk, na których w danym dniu pomiary były prowadzone).

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l



Rys. 2. Średnie dobowe stężenia pyłu zawieszonego PM10 na wybranych stacjach monitoringu jakości powietrza w Polsce od 6 do 11 stycznia 2017 roku.

INFORMOWANIE SPOŁECZEŃSTWA I ORGANÓW PAŃSTWA O STĘŻENIACH PYŁU ZAWIESZONEGO

O każdym przypadku przekroczenia poziomu informowania lub poziomu alarmowego dla pyłu PM10 właściwy wojewódzki inspektorat ochrony środowiska informuje:

- wojewódzki zespół zarządzania kryzysowego za pomocą poczty elektronicznej na uzgodniony wcześniej adres e-mail, a jeżeli istnieje taka potrzeba, również w inny sposób uzgodniony z wojewódzkim zespołem zarządzania kryzysowego, nie później niż do godz. 10:00 dnia następnego;
- Głównego Inspektora Ochrony Środowiska nie później niż do godziny 10:00 danego dnia roboczego za pomocą modułu bazy danych.

Przekroczenia poziomów informowania i poziomów alarmowych dla pyłu PM10 są ogłaszane wyłącznie w oparciu o wyniki pomiarów automatycznych (łącznie do tego celu wykorzystuje się wyniki pomiarów ze 132 stanowisk pomiarowych). Pomiary automatyczne pyłu zawieszonego ze względu na dostępność wyników w trybie on-line są wykorzystywane dla potrzeb informowania społeczeństwa. Oprócz pomiarów automatycznych do pomiarów stężenia pyłu zawieszonego w powietrzu stosuje się pomiary manualne. Manualna metoda pomiaru pyłu jest metodą referencyjną, jednak wyniki pomiarów pyłu z tych stanowisk są dostępne dopiero po ich oznaczaniu metodą wagową w laboratorium wojewódzkich inspektoratów ochrony środowiska. W Polsce, w ramach Państwowego Monitoringu Środowiska, funkcjonuje ok. 300 stacji monitoringu jakości powietrza. Na 248 z nich prowadzone są pomiary pyłu PM10, przy czym na 72 prowadzone są jedynie pomiary pyłu PM10 metodą automatyczną, na kolejnych 60 prowadzone są pomiary pyłu PM10 zarówno metodą automatyczną jak i manualną, a na kolejnych 116 stacjach pomiary prowadzone są jedynie metodą manualną za pomocą poborników.

Wyniki pomiarów automatycznych pyłu zawieszonego są prezentowane przez Główny Inspektorat Ochrony Środowiska w trybie on-line poprzez „Portal Jakości Powietrza" (www.powietrze.gios.gov.pl) oraz poprzez aplikację na urządzenia mobilne „Jakość powietrza w Polsce". Dane aktualizowane są co godzinę i są dostępne wraz z informacją o potencjalnym wpływie stężeń pyłu zawieszonego na zdrowie ludzi, ze szczególnym uwzględnieniem grup ludzi wrażliwych (dzieci, osoby chore, kobiety w ciąży, osoby starsze). Wyniki pomiarów manualnych pyłu są prezentowane na ww. portalu w Banku Danych Pomiarowych.

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l

Rys. 3. Stacja monitoringu jakości powietrza w Krakowie przy ul. Bujaka, na której prowadzone są m.in. manualne i automatyczne pomiary pyłu PM10 i PM2,5. (autor zdjęcia B. Toczko).

Rys. 4. Pobornik do pomiarów pyłu zawieszonego PM2,5 we Wrocławiu przy ul. Na Grobli. (autor zdjęcia B. Toczko).

Rys. 5. Pobornik do pomiarów pyłu zawieszonego PM10 w Busku Zdroju. (autor zdjęcia B. Toczko).

KOMENTARZ

Mając na uwadze wpływ zanieczyszczenia powietrza na jakość życia, zarówno na poziomie samorządowym jak i rządowym podejmuje się obecnie szereg działań mających na celu ograniczenie emisji zanieczyszczeń. W ramach działań mających na celu poprawę jakości powietrza prowadzone są m.in. prace legislacyjne w zakresie wprowadzenia norm jakościowych dla paliw stałych oraz wymagań emisyjnych dla kotłów na paliwo stałe. Komitet Ekonomiczny Rady Ministrów opracował Program działań na rzecz poprawy jakości powietrza pn. „Czyste Powietrze" – zawierający rekomendacje dla Rady Ministrów. Program jest jednym z projektów strategicznych realizowanych w ramach przyjętej 14 lutego 2017 r. przez Radę Ministrów „Strategii na Rzecz Odpowiedzialnego Rozwoju". W ramach tego programu przygotowanych zostało 14 propozycji działań niezbędnych do podjęcia w związku z występowaniem na znacznym obszarze kraju wysokich stężeń zanieczyszczeń powietrza.

Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | tel./fax +48 22 236 59 75
e-mail: poczta@rcb.gov.pl | w w w . r c b . g o v . p l