RCB
Rządowe Centrum Bezpieczeństwa

BIURO
ANALIZ I REAGOWANIA

BIULETYN

KWARTALNY

NUMER 23 KWIECIEŃ – CZERWIEC 2018

Zespół redakcyjny

Biuletynu kwartalnego Rządowego Centrum Bezpieczeństwa:

Grzegorz Świszcz – Zastępca Dyrektora RCB

Martyna Olejnik

Anna Zasadzińska-Baraniewska

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | tel./fax +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

Tąpnięcie i wypadek zbiorowy w KWK „Borynia-Zofiówka -Jastrzębie" Ruch Zofiówka w Jastrzębiu-Zdroju

Anna Swiniarska-Tadla
Wyższy Urząd Górniczy

W sobotę 5 maja br., około godziny 11.00, na poziomie 900 m w pokładzie 409/4 w kopalni „Borynia-Zofiówka -Jastrzębie" Ruch Zofiówka w Jastrzębiu-Zdroju, doszło do najsilniejszego wstrząsu w historii Jastrzębskiej Spółki Węglowej. Wstrząs o sile 1,9x10^8 J (około 3,4 stopnia w skali Richtera) spowodował tąpnięcie o bardzo rozległych skutkach. W tym czasie pod ziemią pracowało 250 osób. Siedmiu górników zostało uwięzionych w rejonie bezpośredniego zagrożenia. Dwóch z nich zostało uratowanych w pierwszych godzinach po katastrofie. Pięciu kolejnych nie przeżyło tąpnięcia, ich ciała odnaleziono i wydobyto na powierzchnię podczas trwającej 11 dni akcji ratowniczej.

To była najtrudniejsza akcja ratownicza w historii Jastrzębskiej Spółki Węglowej. Uczestniczyło w niej blisko 2500 osób. Do poszukiwań wykorzystano m.in. przygotowane do pracy w wodzie, gruzowiskach oraz zawałach psy policji i straży pożarnej. Ratownicy, przemieszczając się przez zniszczone tąpnięciem chodniki, zmagali się m.in. z fragmentami zniszczonych konstrukcji, urządzeń, wysoką temperaturą oraz ciągłym zagrożeniem metanowym. Z uwagi na wysokie ryzyko wystąpienia eksplozji, miejsce zdarzenia zabezpieczono dwiema tamami przeciwwybuchowymi, których zadaniem jest izolacja rejonu. Na skrzyżowaniu chodników H-10 i H-2 powstało rozlewisko, co dodatkowo utrudniło prowadzenie akcji. Aby spenetrować ten rejon, ratownicy musieli wypompować wodę za pomocą układu pomp na sprężone powietrze. Użycie wydajniejszych pomp elektrycznych było niemożliwe ze względu na zagrożenie wybuchem metanu. Po tygodniu akcji ratownicy wydostali z zalewiska ciała dwóch górników. Ciało ostatniego z poszukiwanych odnaleziono po 10 dniach akcji, w samym epicentrum wstrząsu.

W poniedziałek 7 maja br., jeszcze podczas trwania akcji ratowniczej, Prezes Wyższego Urzędu Górniczego Adam Mirek powołał *Komisję do zbadania przyczyn i okoliczności tąpnięcia oraz wypadku zbiorowego, zaistniałych w dniu 5 maja 2018 r. w Jastrzębskiej Spółce Węglowej S.A. KWK „Borynia-Zofiówka-Jastrzębie" Ruch Zofiówka w Jastrzębiu-Zdroju*. Komisja liczy 19 osób, a w jej skład wchodzą m.in. przedstawiciele: Głównego Instytutu Górnictwa, Akademii Górniczo-Hutniczej im. Stanisława Staszica w Krakowie, Politechniki Śląskiej w Gliwicach, Instytutu Technik Innowacyjnych EMAG, Centralnej Stacji Ratownictwa Górniczego, KGHM Polska Miedź S.A. O/Jednostka Ratownictwa Górniczo-Hutniczego, Jastrzębskiej Spółki Węglowej S.A., Okręgowego Inspektoratu Pracy w Katowicach oraz Wyższego Urzędu Górniczego. Wśród nich są geofizycy, których zadaniem jest zbadania mechanizmu wstrząsu, geomechanicy, którzy określą co go spowodowało i w jakim stopniu warunki górniczo-geologiczne mogły na to wpłynąć, a także specjaliści z zakresu wentylacji i ratownictwa, którzy zajmują się oceną przebiegu akcji ratowniczej. Pracami Komisji kieruje dyrektor Departamentu Górnictwa WUG.

Źródło: Jastrzębska Spółka Węglowa S.A.

Źródło: Jastrzębska Spółka Węglowa S.A.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | tel./fax +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

Do głównych zadań Komisji należy:

- określenie mechanizmu wstrząsu wysokoenergetycznego, zaistniałego 5 maja 2018 r. w Jastrzębskiej Spółce Węglowej S.A. KWK „Borynia-Zofiówka-Jastrzębie", Ruch Zofiówka w Jastrzębiu-Zdroju, oraz przesłanek wystąpienia tego wstrząsu, którego skutkiem było tąpnięcie oraz wypadek zbiorowy;
- analiza zagrożenia metanowego, w kontekście tąpnięcia, uwzględniająca stosowane metody prognozowania oraz działalność profilaktyczną;
- analiza wpływu prowadzonych robót na sejsmiczność w rejonie zdarzenia oraz możliwości dalszego prowadzenia ruchu zakładu górniczego w tym rejonie;
- ocena akcji ratowniczej.

W ramach Komisji wydzielono podzespoły specjalistów, mających przygotować ekspertyzy. Komisja skupi się na aspektach technicznych wypadku. Oceni także możliwość prowadzenia w przyszłości robót w rejonie zdarzenia. Na koniec sformułuje wnioski oraz zalecenia pozwalające uniknąć podobnych zdarzeń w przyszłości.

Wstępnie termin zakończenia prac Komisji wyznaczono na 10 sierpnia br. Równolegle przyczyny i okoliczności tąpnięcia oraz wypadku zbiorowego bada Okręgowy Urząd Górniczy w Rybniku.

Od stycznia 2011 r. Ruch Zofiówka jest częścią kopalni zespolonej KWK „Borynia-Zofiówka-Jastrzębie". Administracyjnie znajduje się w województwie śląskim na terenie miasta Jastrzębie, gminy Pawłowice i gminy Mszana. Od zachodu graniczy: z KWK „Jas-Mos", od północy z Ruchem „Borynia", od wschodu z KWK „Pniówek". Załoga tego zakładu górniczego liczy ponad 3 800 pracowników. Wydobycie dobowe kopalni wynosi netto ok. 8 400 t. Jest ono prowadzone na poziomie 900 m z trzech pokładów eksploatacyjnych. Ruch Zofiówka zaliczany jest do najwyższej kategorii zagrożenia metanowego oraz zagrożenia tąpaniami. Występują tu także zagrożenia: wodne, pyłowe oraz wyrzutami metanu i skał.

Informacja dotycząca sytuacji epidemiologicznej odry w związku z wzrastającą liczbą przypadków zachorowań w Europie

Izabela Kucharska
Główny Inspektorat Sanitarny

Rocznie rejestrowanych jest w Polsce około 100 przypadków odry. W 2017 r. zarejestrowano 63 przypadki, w 2016 r. – 133, w 2015 r. – 48, a w 2014 r. – 110. W pierwszej połowie bieżącego roku (tj. od 1 stycznia do 15 czerwca) odnotowano w kraju 71 przypadków odry, trzykrotnie więcej niż w analogicznym okresie roku ubiegłego, gdy zachorowało na tę chorobę 25 osób.

Wzrost liczby przypadków jest znacznie bardziej widoczny w regionie europejskim WHO, obejmującym nie tylko Europę, ale również dalekowschodnią część Rosji i kraje Azji Środkowej. Według danych WHO, w 2017 r. choroba dotknęła 21 315 osób i spowodowała 35 zgonów. Wzrost liczby przypadków obejmował duże ogniska (100 lub więcej przypadków) w 15 z 53 krajów w regionie. Według danych ECDC, na obszarze EU/EOG aż 87% przypadków odry (u osób ze znanym statusem szczepień przeciw odrze) dotyczyło osób nieszczepionych przeciwko tej chorobie.

Według danych WHO, do kwietnia/maja 2018 r., w europejskim obszarze WHO zarejestrowano prawie 36,5 tys. przypadków odry i 48 zgonów. Najwięcej osób dotkniętych chorobą odnotowano na Ukrainie (18 144), w Serbii (5 402), Rumunii (3 284), we Francji (2 306), Grecji (2 097), Anglii i Walii (1 346), we Włoszech (1 258) oraz w Rosji (1 149). Poniżej 1 tys. przypadków rejestrowano w Albanii (729), Niemczech (240), Hiszpanii (136), Portugalii (112), Polsce (68), Irlandii (61), Belgii (29), Czechach (25), Szwecji (23), Szwajcarii (23), Węgrzech (16), Słowacji (4), Finlandii (4) i Bułgarii (4). Zachorowania na odrę zgłaszane były w podobnym okresie 2018 r. również

na obszarze Ameryki Północnej i Południowej, gdzie w 11 krajach odnotowano prawie 1 200 przypadków.

Należy podkreślić, iż zachorowania na odrę w Polsce są związane przede wszystkim z zawlekaniem choroby z zagranicy i w znacznym odsetku występują u osób nie będących narodowości polskiej.

ODRA	
Rok	Liczba przypadków
2005	13
2006	120
2007	40
2008	100
2009	115
2010	13
2011	38
2012	70
2013	84
2014	110
2015	48
2016	133
2017	63
01.01-15.06.2018 r.	71

Tabela 1. *Liczba przypadków odry w Polsce w latach 2005-2018,* ***Źródło****: NIZP-PZH (www.pzh.gov.pl).*

Zachorowania o charakterze i rozmiarach ognisk epidemicznych mogą wystąpić jedynie wśród społeczności lokalnych lub środowisku szkolnym, w których stopień uodpornienia dzieci i dorosłych jest niewystarczający dla uzyskania tzw. odporności zbiorowiskowej, powstającej, gdy liczba osób uodpornionych w danym środowisku osiąga co najmniej 95%. Chorzy na odrę stwarzają wysokie ryzyko przeniesienia zachorowań na inne osoby przebywające w ośrodkach dla cudzoziemców, a także obywateli polskich, którzy nie byli szczepieni przeciw odrze ze względu na przeciwskazania o charakterze medycznym (dzieci chore na nowotwory, osoby poddane leczeniu immunosupresyjnemu) i możliwość wystąpienia związanych z tym ciężkich powikłań, a nawet zgonów. Indywidualne ryzyko zachorowania na odrę występuje bowiem u każdej osoby, która nie była szczepiona przeciw tej chorobie (lub jej wcześniej nie przechorowała). Stosowanie szczepień ochronnych ma zasadnicze znaczenie w zapobieganiu zachorowaniom na odrę i ze względu na wysoką zaraźliwość choroby oraz jej przenoszenie drogą powietrzną nie może być zastąpione jakimikolwiek innymi środkami ochrony.

Należy w tym miejscu podkreślić bardzo wysoką efektywność szczepień przeciw odrze. Po podaniu pierwszej dawki szczepionki odporność uzyskuje ok. 95-98% osób zaszczepionych. Natomiast podanie drugiej dawki szczepionki pozwala osiągnąć odporność u niemalże 100% osób zaszczepionych.

W Polsce, podobnie jak i w innych krajach, podejmowane są działania mające na celu eliminację choroby. W odniesieniu do chorób zakaźnych, które nie mają rezerwuaru zwierzęcego (tzn. występują jedynie u człowieka) i dla których dostępne są szczepionki o wysokim stopniu skuteczności, możliwe jest osiągnięcie celu jakim jest eliminacja choroby na danym obszarze (rozumiana jako brak zakażeń na terenie kraju przy możliwych zawleczeniach z zagranicy), a następnie eradykacja choroby tzn. jej całkowitego wyeliminowanie na świecie. Obecnie Polska uczestniczy w globalnym programie eliminacji odry i różyczki koordynowanym przez WHO.

Zgodnie z obowiązującym Programem Szczepień Ochronnych na rok 2018, szczepienia na odrę wykonuje się planowo u dzieci w 13-15 miesiącu życia oraz w 10. roku życia i są one obowiązkowe dla dzieci i młodzieży, które nie ukończyły 19 roku życia. System finansowania szczepień przeciw odrze nie obejmuje natomiast osób, które ukończyły 19. rok życia. W przypadku wystąpienia ognisk epidemicznych, brak nieodpłatnych szczepień dla tej grupy wiekowej stanowi istotny problem w prowadzeniu działań przeciwepidemicznych. Należy pamiętać, że każda osoba nieszczepiona w ognisku epidemicznym przyczynia się do podtrzymywania transmisji wirusa, w tym także jego przeniesieniu na dzieci w okresie niemowlęcym, które – zgodnie z kalendarzem szczepień – nie były jeszcze szczepione. Ze względu na charakterystykę epidemiologiczną odry oraz konsekwencje kliniczne choroby, szerzenie się zachorowań w społecznościach o niskim stopniu zaszczepienia wymaga podjęcia szybkich działań przeciwepidemicznych. Podanie osobom narażonym szczepionki, przed upływem 72 godzin od styczności z osobą chorą, pozwala zmniejszyć ryzyko zachorowania.

Aby umożliwić skuteczne działania przeciwepidemiczne w przypadku odnotowania rozprzestrzeniania się wirusa, w 2016 r. wydane zostało rozporządzenie Ministra Zdrowia w sprawie metody zapobiegania odrze (Dz. U. poz. 1418), które stanowi wykonanie upoważnienia zawartego

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | tel./fax +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

w art. 3 ust. 4 pkt 2 ustawy z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi (Dz. U. z 2018 r. poz. 151), umożliwiające wykonanie szczepień przeciwko odrze u osób narażonych na zachorowanie bez względu na kryterium wieku.

Z uwagi na niepokojącą tendencję jaką jest wzrost liczby osób odmawiających szczepień dzieci, a co za tym idzie nasilające się ryzyko wystąpienia zwiększonej liczby zachorowań na odrę, podejmowane są działania mające na celu upowszechnienie wiedzy na temat szczepień. Jest to przedmiotem zainteresowania, analiz i działań ze strony Ministerstwa Zdrowia, Państwowej Inspekcji Sanitarnej oraz instytutów badawczych działających na polu zdrowia publicznego. W toczonych dyskusjach podnosi się zasadnicze znaczenie świadomości lekarskiej i konieczności budowania szerokiej kampanii społecznej na temat szczepień ochronnych jako działania wielosektorowego, wychodzącego poza obszar opieki zdrowotnej. W związku z narastającymi w ostatnim czasie ruchami antyszczepionkowymi ważna jest nie tyle walka z oporem przeciwko szczepieniom, co pozytywna promocja szczepień, która powinna zaczynać się od edukacji lekarzy i pracowników ochrony zdrowia.

SMS z ostrzeżeniami – informacja na wagę bezpieczeństwa

Bożena Wysocka
Rządowe Centrum Bezpieczeństwa

Wystartował pilotaż systemu ostrzegania SMS-ami przed zagrożeniami. 29 czerwca br. został podpisany list intencyjny pomiędzy Ministrem Cyfryzacji, Ministrem Spraw Wewnętrznych i Administracji, Prezesem Urzędu Komunikacji Elektronicznej, Dyrektorem Rządowego Centrum Bezpieczeństwa oraz przedstawicielami operatorów telekomunikacyjnych. Dzięki porozumieniu, informacja o zagrożeniu dotrze do wszystkich mieszkańców zagrożonego województwa.

JAK BĘDZIE WYGLĄDAŁ MECHANIZM ROZSYŁANIA SMS-ÓW?

Po otrzymaniu informacji o zagrożeniu Rządowe Centrum Bezpieczeństwa prześle ją operatorom sieci komórkowych, którzy niezwłocznie roześlą ją do swoich abonentów. Każdy więc, kto posiada telefon komórkowy (oczywiście włączony), jeśli znajdzie się w obszarze powiadamiania alarmowego (obszar zagrożenia) dostanie na swój telefon krótką wiadomość tekstową informującą o rodzaju zagrożenia, jego lokalizacji, a także źródle ostrzeżenia. Będzie więc miał szansę na reakcję. Będzie mógł podjąć działania, aby uniknąć zagrożenia lub zminimalizować jego skutki. Komunikaty będą wydawane tylko w wyjątkowych sytuacjach, które w realny sposób zagrażają życiu i zdrowiu człowieka. Będą dotyczyły nie tylko zjawisk atmosferycznych, ale też innych zdarzeń.

DLACZEGO TO RCB BĘDZIE WYSYŁAŁO OPERATOROM INFORMACJĘ O ZAGROŻENIU DO ROZESŁANIA?

Rządowe Centrum Bezpieczeństwa pełni funkcję Krajowego Centrum Zarządzania Kryzysowego. 24 godziny na dobę monitoruje sytuację w kraju pod kątem wystąpienia różnego rodzaju zagrożeń. Informacje do Centrum wpływają od różnych podmiotów krajowych i zagranicznych. Podobny mechanizm będzie funkcjonował w przypadku komunikatów o zagrożeniu dla ludności. Ministrowie, kierownicy urzędów i instytucji centralnych np. IMGW oraz wojewodowie będą przekazywali informacje o zagrożeniu do RCB. Centrum przekaże je operatorom telefonii komórkowej do niezwłocznego rozesłania.

SKĄD IDEA INFORMOWANIA OBYWATELI O ZAGROŻENIU POPRZEZ WIADOMOŚCI SMS?

W ubiegłym roku mieliśmy do czynienia z ekstremalnymi zdarzeniami atmosferycznymi. Wtedy informacja o zagrożeniu nie dotarła do wszystkich.

Należało więc przeanalizować co nie zadziałało. Dlatego Prezes Rady Ministrów (zarządzeniem nr 101 z dnia 4 września 2017 r.) powołał Międzyresortowy Zespół do oceny funkcjonowania systemu ratownictwa i zarządzania kryzysowego. Jego przewodniczącym został ówczesny minister SWiA Mariusz Błaszczak, a dyrektor Rządowego Centrum Bezpieczeństwa Marek Kubiak – sekretarzem. Zespół przygotował dokument „Analiza i ocena funkcjonowania systemu ratownictwa i zarządzania kryzysowego w Polsce – wnioski i rekomendacje", który 17 października 2017 roku został przyjęty przez Radę Ministrów. Rada Ministrów zaleciła opracowanie – do końca roku – propozycji konkretnych działań.

We wskazanym terminie minister spraw wewnętrznych i administracji, na podstawie wniosków i rekomendacji Zespołu opracował „Propozycje zmian legislacyjnych i innych działań wynikających z rekomendacji Międzyresortowego Zespołu do oceny funkcjonowania systemu ratownictwa i zarządzania kryzysowego". Wprowadzenie ostrzegania ludności na danym obszarze poprzez wiadomości tekstowe było właśnie jedną z rekomendacji Zespołu. Do jej realizacji zostało zobowiązane Rządowe Centrum Bezpieczeństwa. W ramach prac została zmieniona ustawa Prawo telekomunikacyjne oraz niektóre inne ustawy, w tym ustawa o zarządzaniu kryzysowym. Jej nowy artykuł – 21a – zobowiązuje operatorów sieci komórkowej do wysłania komunikatu o zagrożeniu do użytkowników na określonym obszarze, aby ostrzec ludność przed nadchodzącą sytuacją kryzysową.

KIEDY SYSTEM OSTRZEGANIA SMS-AMI PRZED ZAGROŻENIAMI OSIĄGNIE PEŁNĄ FUNKCJONALNOŚĆ?

Nowe przepisy zawarte w ustawie Prawo telekomunikacyjne wejdą w życie po upływie 6 miesięcy od dnia jej ogłoszenia, czyli dopiero 12 grudnia 2018 r. Z uwagi na fakt, że data wejścia w życie przepisu dotyczącego obowiązku wysyłania przez operatorów ostrzeżeń przypada po wakacjach, a tymczasem groźne w skutkach zjawiska atmosferyczne, takie jak huragany czy gwałtowne burze, dotyczą szczególnie okresu letniego, zasadne było podjęcie działań niezwłocznie. Dlatego, w trosce o bezpieczeństwo obywateli, został uruchomiony program pilotażowy.

Działania w ramach programu pilotażowego mają charakter pionierski. Obywatele mogą zgłaszać uwagi do jego funkcjonowania na adres e-mail alert.pilotaz@rcb.gov.pl.

Standardy zapewnienia bezpieczeństwa obiektów infrastruktury krytycznej w kontekście zagrożeń terrorystycznych

Anna Zasadzińska-Baraniewska
Rządowe Centrum Bezpieczeństwa

28 czerwca br. Międzyresortowy Zespół ds. Zagrożeń Terrorystycznych (MZds.ZT) przyjął sprawozdanie Zespołu zadaniowego do spraw opracowania standardów zabezpieczeń antyterrorystycznych i reguł współdziałania dotyczących infrastruktury krytycznej oraz zasad dokonywania sprawdzenia zabezpieczeń obiektów infrastruktury krytycznej zgodnie z przepisami ustawy o działaniach antyterrorystycznych (dalej Zespół zadaniowy), w którym określone zostały minimalne, ujednolicone wymagania w zakresie zapewnienia bezpieczeństwa fizycznego, osobowego oraz teleinformatycznego dla obiektów infrastruktury krytycznej.

Wymagania, sformułowane przez Zespół zadaniowy, zostały opracowane tak, aby ograniczać podatność obiektów IK na możliwość wystąpienia incydentów o charakterze terrorystycznym oraz zwiększyć szansę na skuteczne im przeciwdziałanie. Wprowadzenie ustandaryzowanych wymagań z zakresu zabezpieczeń antyterrorystycznych wpłynie jednocześnie na odporność systemów bezpieczeństwa operatorów IK na innego rodzaju zagrożenia, w tym o charakterze hybrydowym, jak np. sabotaż.

Znaczenie działań w zakresie zapobiegania zagrożeniom o charakterze terrorystycznym dla obiektów infrastruktury krytycznej (IK)[1] zostało podkreślone w „Narodowym Programie Antyterrorystycznym na lata 2015-2019", w którym wskazano przedsięwzięcia służące podniesieniu skuteczności przygotowania państwa na tego typu zagrożenia. Rozwiązania zmierzające do zapewnienia bezpieczeństwa ww. obiektów zostały także uwzględnione w ustawie z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych. Ponadto w harmonogramie prac Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych przewidziano omówienie standardów zabezpieczeń i reguł współdziałania dotyczących infrastruktury krytycznej, a także zasad dokonywania sprawdzenia zabezpieczeń obiektów IK zgodnie z przepisami ustawy o działaniach antyterrorystycznych.

W celu usprawnienia mechanizmów współdziałania służb i organów w zakresie realizacji ww. przepisów ustawowych oraz rozwiązań programowych, Przewodniczący MZds.ZT – Minister Spraw Wewnętrznych i Administracji, powołał decyzją nr 32 z dnia 26 maja 2017 r. Zespół zadaniowy do spraw opracowania standardów zabezpieczeń antyterrorystycznych i reguł współdziałania dotyczących infrastruktury krytycznej oraz zasad dokonywania sprawdzenia zabezpieczeń obiektów infrastruktury krytycznej zgodnie z przepisami ustawy o działaniach antyterrorystycznych. Zespół działał od 26 maja 2017 r. do 31 stycznia 2018 r., a w jego skład weszli przedstawiciele Ministerstwa Spraw Wewnętrznych i Administracji, Rządowego Centrum Bezpieczeństwa, Ministerstwa Finansów, Ministerstwa Obrony Narodowej, Agencji Bezpieczeństwa Wewnętrznego, Komendy Głównej Policji, Komendy Głównej Straży Granicznej, Komendy Głównej Państwowej Straży Pożarnej oraz Biura Ochrony Rządu.

Ponadto, z uwagi na kompleksowość realizowanych zadań, do udziału w pracach zaproszeni zostali przedstawiciele Ministerstwa Cyfryzacji, Ministerstwa Energii, Ministerstwa Infrastruktury i Budownictwa, Ministerstwa Gospodarki Morskiej i Żeglugi Śródlądowej, Ministerstwa Rozwoju, Państwowej Agencji Atomistyki, Urzędu Lotnictwa Cywilnego oraz Biura Bezpieczeństwa Narodowego. Zaproszeni zostali również reprezentanci gremiów i środowisk naukowych, posiadających ekspercką wiedzę lub doświadczenie przydatne w pracach Zespołu zadaniowego, oraz wybrani przedstawiciele właścicieli i posiadaczy samoistnych lub zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej. Ze względu na specjalistyczny charakter systemów bezpieczeństwa stosowanych w obiektach IK na terenie Polski, zwrócono się również do ekspertów zewnętrznych – ośmiu uznanych w kraju specjalistów reprezentujących: Polski Komitet Normalizacyjny, Wyższą Szkołę Policji w Szczytnie, Politechnikę Poznańską, Uniwersytet Wrocławski, Naftoport S.A. oraz Polską Izbę Systemów Alarmowych.

Jednym z zadań Zespołu zadaniowego było opracowanie projektu standardu zabezpieczeń antyterrorystycznych w zakresie zapewnienia bezpieczeństwa fizycznego, osobowego oraz teleinformatycznego dla obiektów infrastruktury krytycznej oraz określenie minimalnych ustandaryzowanych wymagań dla każdego rodzaju zabezpieczeń. Przewidziano, że na sposób wdrożenia konkretnych rozwiązań mają wpływ: charakter organizacji, realizowane w niej procesy, jej wielkość i struktura, a także gotowość organizacji do wykorzystania podmiotów zewnętrznych. Czynniki te podlegają zmianom wraz z upływem czasu.

ZAPEWNIENIE BEZPIECZEŃSTWA OSOBOWEGO – WYMAGANIA MINIMALNE

Zapewnienie bezpieczeństwa osobowego to zespół przedsięwzięć i procedur mających na celu minimalizację ryzyka związanego z osobami, które poprzez autoryzowany dostęp do obiektów, urządzeń, instalacji i usług infrastruktury krytycznej, mogą spowodować zakłócenia w jej funkcjonowaniu. Wprowadzenie minimalnych wymagań standardu zapewnienia bezpieczeństwa osobowego jest niezbędne, aby zminimalizować ryzyko zakłócenia funkcjonowania IK. Istotne jest, aby zapewnienie bezpieczeństwa osobowego stanowiło integralną część procesu zarządzania ryzykiem w organizacji oraz procesu ochrony IK i było uwzględniane przy projektowaniu procesów organizacji, zgodnie z jej potrzebami. Trzeba w tym miejscu zauważyć, że wiele aspektów zapewnienia bezpieczeństwa osobowego jest nierozerwalnie związanych z innymi elementami

[1] Wymagania zawarte w niniejszym dokumencie odnoszą się wyłącznie do infrastruktury krytycznej, zlokalizowanej na terytorium kraju. W przypadku infrastruktury krytycznej zlokalizowanej poza granicami kraju, mogą być one modyfikowane z uwzględnieniem specyfiki funkcjonowania oraz przepisów prawa państwa, w którym zlokalizowana jest taka IK.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | tel./fax +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

systemu bezpieczeństwa IK, takimi jak zapewnienie ciągłości działania.

Minimalne wymagania w zakresie standardu zapewnienia bezpieczeństwa osobowego zostały sformułowane dla następujących obszarów:

- zarządzanie ryzykiem,
- polityka bezpieczeństwa osobowego,
- role, odpowiedzialność i uprawnienia,
- ustalenie tożsamości,
- weryfikacja kwalifikacji,
- weryfikacja niekaralności,
- postępowanie wobec zatrudnionych,
- niestandardowe zachowania,
- zasady dostępu,
- identyfikacja wizualna,
- postępowanie z odchodzącymi z pracy,
- postępowanie z usługodawcami/osobami z zewnątrz.

Szczegółowo rozpisane wytyczne dotyczą nie tylko elementów składających się na zapewnienie „twardego" bezpieczeństwa takich, jak np. kompetencje w zakresie weryfikacji autentyczności dokumentów, obowiązek czytelnej identyfikacji wizualnej pracowników posiadających dostęp do IK czy zasady obowiązkowej okresowej weryfikacji uprawnień i dostępów. Odnoszą się także do minimalnych wymagań postępowania wobec zagrożeń nowego typu, co zawarte zostało np. w zapisie, zgodnie z którym operator zapewnia wszystkim pracownikom szkolenia w tematyce zagrożeń socjotechnicznych. Doprecyzowano, że szkolenie powinno uświadamiać pracownikom charakterystykę zagrożenia socjotechnicznego, przykłady takich ataków, a także pokazywać metody ochrony przed ich negatywnymi skutkami. Ponadto wskazane jest profilowanie treści szkoleń w zależności od roli, jaką dana osoba pełni w organizacji.

ZAPEWNIENIE BEZPIECZEŃSTWA FIZYCZNEGO – WYMAGANIA MINIMALNE

Zapewnienie bezpieczeństwa fizycznego infrastruktury krytycznej to zespół działań proceduralnych, organizacyjnych i technicznych, mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie działań osób, które w sposób nieautoryzowany podjęły próbę dostania się lub znalazły się na terenie IK. Na działania te składają się m.in. bezpośrednia ochrona fizyczna (osobowa) oraz zabezpieczenia techniczne (elektroniczne i budowlano-mechaniczne). Zaznaczyć należy, że żadne działania zmierzające do zapewnienia bezpieczeństwa fizycznego nie gwarantują całkowitego bezpieczeństwa. Środki ochronne zwiększają jedynie szansę na skuteczne przeciwdziałanie. Podobnie jak w przypadku zapewnienia bezpieczeństwa osobowego, również zapewnienie bezpieczeństwa fizycznego powinno być integralną częścią procesu zarządzania ryzykiem w organizacji oraz procesu ochrony IK i być uwzględniane przy projektowaniu procesów organizacji, zgodnie z jej potrzebami.

Minimalne wymagania w zakresie standardów zapewnienia bezpieczeństwa fizycznego zostały sformułowane zarówno dla bezpośredniej ochrony fizycznej jak i zabezpieczeń elektronicznych i budowlano-mechanicznych. Obejmują one następujące obszary:

- zarządzanie ryzykiem,
- zarządzanie aktywami organizacji w obszarze zapewnienia bezpieczeństwa fizycznego,
- wyznaczenie osoby odpowiedzialnej za zapewnienie bezpieczeństwa fizycznego,
- organizacyjno-proceduralne środki zapewnienia bezpieczeństwa fizycznego,
- procedury reagowania,
- podział obszaru chronionego na strefy ochrony,
- przegląd systemu bezpieczeństwa fizycznego,
- szkolenia z zakresu bezpieczeństwa,
- ochronę przeciwprzepięciową technicznych systemów zapewnienia bezpieczeństwa fizycznego,
- oświetlenie obszaru objętego ochroną,
- zapewnienie fizycznej bariery pomiędzy strefą zewnętrzną a pozostałymi strefami,
- elektroniczne systemy zabezpieczeń (ESZ),
- zasilanie ESZ,
- kontrolę dostępu do chronionego obszaru,
- monitoring wizyjny,
- sygnalizację włamania i napadu,
- zasady i warunki zapewnienia ochrony przy pomocy uzbrojonych pracowników ochrony fizycznej.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | tel./fax +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

W każdym z wyżej wymienionych obszarów sformułowano szczegółowe wytyczne wraz z uwagami. W wymaganiach minimalnych odnoszących się do zabezpieczenia technicznego (elektronicznego i budowlano-mechanicznego) przywołano właściwe normy, parametry czy zasady zabezpieczenia transmisji danych. W punkcie dotyczącym uzbrojonych pracowników ochrony fizycznej umieszczono wymagania, których realizacja zapewni sprawne i rzetelne realizowanie działań ochronnych przez właściwe do tego osoby.

ZAPEWNIENIE BEZPIECZEŃSTWA TELEINFORMATYCZNEGO – WYMAGANIA MINIMALNE

Infrastruktura krytyczna jest narażona na ataki teleinformatyczne przeprowadzane zarówno przez początkujących, jak i wysoce wyspecjalizowanych cyberprzestępców, którzy mogą doprowadzić do zakłócenia jej funkcjonowania. Wpływ na IK mogą mieć również skutki zdarzeń losowych – takich jak awarie systemów, niesprawności urządzeń lub programów ją obsługujących.

Uprawnienia dostępu do systemów teleinformatycznych, wykorzystywanych do świadczenia usług krytycznych, nadawane są najczęściej pracownikom organizacji (w trakcie ich zatrudniania) oraz pracownikom usługodawców lub dostawców rozwiązań teleinformatycznych (w wyniku wzajemnych umów lub w sposób doraźny). Dostęp do systemów teleinformatycznych oraz danych w nich zgromadzonych może być nielegalnie wykorzystany i służyć zakłóceniu funkcjonowania IK lub działaniu na jej niekorzyść. Jednocześnie administratorzy dysponują największą wiedzą na temat funkcjonowania systemów teleinformatycznych IK i z reguły również najwyższymi uprawnieniami w zakresie dostępu do informacji oraz zdolności zarządczych, co powoduje, że stanowią oni potencjalne źródło zagrożenia.

Na sposób wdrożenia konkretnych wymagań w zakresie zapewnienia cyberbezpieczeństwa mają wpływ powiązane ze sobą czynniki charakteryzujące organizację, jak nasycenie systemami teleinformatycznymi czy rozwój kompetencji własnych w zakresie technologii informacyjnych. Podobnie jak w omówionych wcześniej zagadnieniach, również zapewnienie bezpieczeństwa teleinformatycznego powinno być silnie zintegrowane z procesami zarządzania ryzykiem i bezpieczeństwem w organizacji oraz ochrony IK i powinno być uwzględniane przy projektowaniu procesów organizacji, zgodnie z jej potrzebami.

Wymagania minimalne dla zapewnienia bezpieczeństwa teleinformatycznego zostały, podobnie jak w poprzednich wypadkach, sformułowane dla wyodrębnionych obszarów i obejmują:

- zarządzanie ryzykiem,
- zarządzanie zasobami teleinformatycznymi,
- zapewnienie rozliczalności użytkowników w systemach teleinformatycznych i kontroli dostępu do systemów i aplikacji,
- zapewnienie bezpieczeństwa urządzeń operatora poza siedzibą,
- mechanizmy, procedury i narzędzia bezpiecznej eksploatacji,
- bezpieczeństwo komunikacji,
- relacje z dostawcami,
- zarządzanie incydentami związanymi z bezpieczeństwem informacji,
- przeglądy bezpieczeństwa informacji.

Ze względu na możliwe skutki, największe wyzwanie w zapewnieniu bezpieczeństwa teleinformatycznego stanowią zagrożenia pochodzące z wewnątrz organizacji (insider threat). W tym kontekście istotnym zagadnieniem jest dostępność personelu wspierającego realizację krytycznych (w rozumieniu ciągłości działania) procesów organizacji – administratorów sieci i systemów. Nieobecność takiego personelu może istotnie podnieść ryzyko zakłócenia funkcjonowania IK.

Zgodnie z rekomendacją Zespołu zadaniowego, każdy operator IK miałby 24 miesiące na wdrożenie minimalnych wymagań w zakresie standardów antyterrorystycznych dotyczących zapewnienia bezpieczeństwa fizycznego, osobowego i teleinformatycznego. Ocena wdrażania ww. standardów zostałaby oparta na istniejącej procedurze uzgadniania i zatwierdzania planów ochrony infrastruktury krytycznej. Należy także podkreślić, że przy opracowaniu standardów przewidziano, iż operator IK będzie miał możliwość odstąpienia od tych minimalnych wymagań, które w danych warunkach są niemożliwe do wdrożenia (technicznie lub organizacyjnie) albo, zgodnie z przeprowadzoną przez operatora analizą ryzyka dla

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | tel./fax +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

ciągłości działania, nie mają wobec niego zastosowania, a wskazany w wymaganiu cel operator zapewnia w drodze zastosowania innych, alternatywnych środków bezpieczeństwa. Odstąpienie od spełnienia konkretnego wymagania powinno być uzasadnione, udokumentowane i zatwierdzone przez kierownictwo jednostki.

Cyberbezpieczeństwo w sektorze lotniczym – ćwiczenie „CYBER EUROPE 2018”

Marcin Napiórkowski

Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy

Cykl ćwiczeń „Cyber Europe” to przeprowadzane na dużą skalę symulacje sytuacji kryzysowych, organizowane przez Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA). Mają one formułę ćwiczeń sztabowych, w których uczestnicy testują scenariusze przygotowane na wypadek wystąpienia sytuacji kryzysowej. Dzięki temu możliwe jest jasne określenie ról i obowiązków na wypadek zaistnienia rzeczywistej sytuacji kryzysowej.

Celem ćwiczeń „Cyber Europe” jest testowanie procedur zarządzania kryzysowego w obliczu międzynarodowego kryzysu w cyberprzestrzeni (w sieciach i systemach komputerowych) – zarówno tych wewnętrznych, w państwach członkowskich i w poszczególnych sektorach i organizacjach, jak również procedur na poziomie europejskim (tzw. SOP – Standard Operating Procedures).

Źródło: NASK

W dziedzinie cyberbezpieczeństwa jest to szczególnie istotne, ponieważ kryzysy cybernetyczne mają potencjał przerodzenia się w realne zagrożenia fizyczne (np. brak prądu, problemy z łącznością). W takiej sytuacji konieczna jest sprawna współpraca zespołów reagowania na incydenty bezpieczeństwa komputerowego (CERT lub CSIRT) z zespołami i centrami zarządzania kryzysowego oraz zespołami medialnymi, a także z administracją publiczną i sektorem prywatnym (każda edycja dotyczy innego sektora gospodarki).

Dotychczas odbyły się cztery edycje ćwiczenia. Pierwsza miała miejsce w 2010 roku. W 2012 roku ćwiczenia dotyczyły sektora bankowego, w 2014 roku – sektora energetycznego i telekomunikacyjnego, natomiast w 2016 roku w ćwiczeniu wzięli udział dostawcy Internetu i firmy z sektora bezpieczeństwa IT. Obecna, piąta edycja z czerwca 2018 roku, dotyczyła sektora lotnictwa cywilnego.

Procedury wypracowane przez państwa członkowskie i ENISA w poprzednich edycjach stały się podstawą (tzw. blueprint) zaleceń Komisji Europejskiej w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę. Zalecenia zawierają ramowe procedury i organizację współpracy europejskiej na poziomie strategicznym i operacyjnym.

Źródło: Marcin Napiórkowski

Skalę ćwiczenia najlepiej zobrazować liczbami. W obecnej edycji uczestniczyło 30 państw: Unii Europejskiej i Europejskiego Stowarzyszenia Wolnego Handlu oraz 10 instytucji unijnych, zajmujących się cyberbezpieczeństwem i działających w sektorze lotnictwa cywilnego. Łącznie ćwiczyło 300 organizacji i 900 zespołów lub specjalistów z dziedziny bezpieczeństwa w cyberprzestrzeni, zarządzania kryzysowego i komunikacji społecznej. Ćwiczący

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | tel./fax +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

w ciągu dwóch dni otrzymali ponad 23 tysiące wiadomości ćwiczebnych.

W Polsce ćwiczącymi byli: Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK) z działającym w niej zespołem CERT Polska, administracja publiczna reprezentowana przez Rządowe Centrum Bezpieczeństwa, Ministerstwa: Cyfryzacji i Infrastruktury, Urząd Lotnictwa Cywilnego, a także kontrola ruchu lotniczego, podmioty z sektora lotnictwa cywilnego, dostawca sieci telekomunikacyjnej oraz stowarzyszenie Polska Obywatelska Cyberobrona. Łącznie 18 zespołów ćwiczących z 10 organizacji.

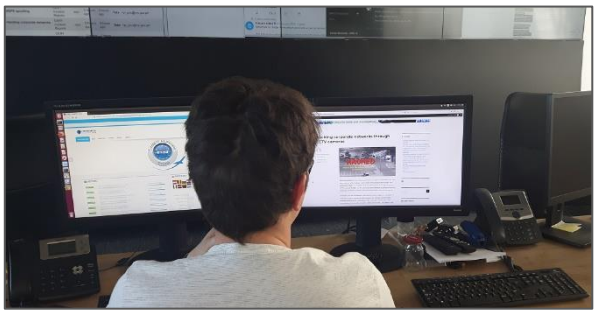
Polscy uczestnicy, w reakcji na wiadomości ćwiczebne scenariusza, wymienili między sobą ponad 500 wiadomości poprzez pocztę elektroniczną. Oprócz tego komunikowali się telefonicznie, a w sprawach technicznych (m.in. rozwiązywanie incydentów bezpieczeństwa komputerowego) za pośrednictwem formularza i komunikatora internetowego wystawionego przez CERT Polska. Ta liczba nie obejmuje komunikacji wewnętrznej w obrębie ćwiczących organizacji.

Źródło: ENISA

Reakcją na symulowane wydarzenia były także sporządzane przez uczestników krótkie analizy na potrzeby kierownictwa swojej organizacji oraz rozmowy telefoniczne z przedstawicielami ćwiczebnych redakcji mediów informacyjnych.

Kontrola i koordynacja ćwiczenia wymagała ok. 150 wiadomości elektronicznych, dziesiątek rozmów telefonicznych i bieżącej komunikacji pomiędzy moderatorami i administratorami na czacie internetowym. Koordynacja i kontrola to przede wszystkim czuwanie nad przebiegiem ćwiczenia, działaniem platformy ćwiczebnej – funkcjonowaniem wirtualnego świata i rozwiązywanie kwestii technicznych. Moderatorzy pełnili także rolę uzupełniającą dla scenariusza, ale interweniowali tylko w przypadkach szczególnych, m.in. wtedy, gdy do reakcji na zdarzenie ze scenariusza potrzebne były działania lub decyzje podmiotu, który nie brał udziału w ćwiczeniu.

Konstrukcja scenariusza zawierała incydenty bezpieczeństwa w sieciach i systemach komputerowych, ataki hybrydowe (zagrożenie bezpieczeństwa fizycznego, akcje medialne i dezinformację), które materializowały się poprzez zdarzenia w podmiotach sektora lotnictwa cywilnego i zarządzania kryzysowego. Scenariusz zawierał także potencjalne zagrożenia dla innych sektorów gospodarki, które mogły rozprzestrzenić się za pośrednictwem sieci, wraz z eskalacją incydentu. Sprawdzenie czy kooperacja na poziomie europejskim jest sobie w stanie poradzić z zażegnaniem niebezpieczeństwa było jednym z celów ćwiczenia. Testowane były plany zarządzania kryzysowego i zapewnienia ciągłości działania na wszystkich poziomach: organizacji, sektora, kraju oraz europejskiego obszaru gospodarczego.



Źródło: NASK

W warstwie medialnej scenariusz miał na celu sprawdzenie, jak organizacje i administracja lotnicza będą reagowały na zainteresowanie zagrożeniem ze strony mediów tak zwanego głównego nurtu. Drugim celem było przećwiczenie reakcji i obrony przed dezinformacją w mediach społecznościowych.

Istotnym elementem ćwiczenia były zdarzenia techniczne, wymagające od wyspecjalizowanych zespołów reagowania na incydenty bezpieczeństwa komputerowego przeprowadzania m.in. analiz powłamaniowych, analiz próbek złośliwego oprogramowania, powstrzymywania ataków z wykorzystaniem „internetu rzeczy", zautomatyzowanej analizy informacji z otwartych źródeł. Zdarzenia techniczne składały się na incydenty, a usuwanie skutków tych zdarzeń decydowało o skutecznej odpowiedzi na kryzys.

Aktualnie trwa proces formułowania wniosków i rekomendacji z ćwiczenia, które będą gotowe na przełomie października i listopada 2018 roku. W tym czasie opublikowany zostanie jawny raport

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | tel./fax +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

z organizacji i przebiegu ćwiczenia, który można będzie pobrać ze strony ENISA. Na stronie dostępne są raporty z poprzednich edycji Cyber Europe. Należy przy tym zaznaczyć, że większość obserwacji i wniosków nie jest publikowana. Stanowią one informację prawnie chronioną – informacje niejawne administracji publicznej oraz tajemnice handlowe przedsiębiorstw biorących udział w ćwiczeniu.

Ćwiczenia były doskonałą okazją do przetrenowania działania punktów kontaktowych do spraw cyberbezpieczeństwa i ich współdziałania z centrami zarządzania kryzysowego, szczególnie w kontekście prac nad rozwiązaniami zawartymi w projekcie ustawy o krajowym systemie cyberbezpieczeństwa. Przećwiczono m.in. działanie zespołu CERT Polska w roli przyszłego CSIRT NASK.

Sektorowo, w zakresie proceduralnym i technicznym, sprawdzone zostało współdziałanie podmiotów cyberbezpieczeństwa i bezpieczeństwa lotnictwa cywilnego w odpieraniu złożonego zagrożenia – przebiegającego w cyberprzestrzeni, ale mającego realny, fizyczny skutek dla podmiotów lotnictwa cywilnego.

W zakresie procedur, na poziomie krajowym, przetestowane zostało współdziałanie NASK i RCB w inicjowaniu Zespołu ds. incydentów krytycznych i jego relacji do Rządowego Zespołu Zarządzania Kryzysowego. Działanie to było jednym z celów krajowych ćwiczenia i pozwoliło na sprawdzenie jednego z zakładanych wariantów reagowania na incydenty i ich eskalowania z poziomu organizacji na poziom krajowy.

Zauważono braki i mankamenty, szczególnie w komunikacji i bieżącej wymianie informacji. Ze wstępnej analizy wynika, że większa ich część wynikała z faktu, że procedury powstały na podstawie projektu ustawy, a struktury nie są ostatecznie ustalone, w związku z czym w ćwiczeniu testowane były różne warianty działania. Braki dotyczą głównie strony technicznej i organizacyjnej kanałów komunikacyjnych, wykorzystywanych do tej pory rzadko lub w ogóle (lub wcześniej niefunkcjonujących). Dzięki wnioskom z ćwiczenia, stwierdzone niedociągnięcia będzie można usunąć przed wejściem w życie ustawy o krajowym systemie cyberbezpieczeństwa.

Źródła:

1. *https://cyberpolicy.nask.pl/cp/dobre-praktyki/cwiczenia/56,Cwiczenia-Cyber-Europe.html;*
2. *https://www.enisa.europa.eu/news/enisa-news/cyber-europe-2018-get-prepared-for-the-next-cyber-crisis/;*
3. *https://www.enisa.europa.eu/topics/cyber-exercises;*
4. *https://www.cyber-europe.net;*
5. *obserwacje własne.*

Pozytywnie oceniono współpracę w rozwiązaniu kryzysu na poziomie europejskim, z wykorzystaniem kanałów komunikacji, procedur i narzędzi, które zostały udostępnione państwom w ramach sieci CSIRT lub użyte wcześniej w czasie odpierania realnych ataków w cyberprzestrzeni. Ćwiczenie wykazało przydatność tych ustaleń i narzędzi. Polscy uczestnicy ćwiczenia zostali wstępnie bardzo wysoko ocenieni przez zespół kontrolujący ćwiczenie pod kątem reakcji na symulowane media i kontroli przekazu medialnego. Ćwiczenie Cyber Europe 2018 jest kolejną symulacją, która udowadnia, że działania zespołów medialnych i PR-owych są równie ważne jak działania techniczne i proceduralne. Mają one szczególną wartość przy odpowiedzi na zagrożenia nowego typu, takie jak działania hybrydowe czy dezinformacja.

Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | tel./fax +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l