NATO Security Forum Szczecin 19 Października (czwartek) 2017 r.

Przebieg konfliktu hybrydowego w Polsce : diagnoza i możliwe scenariusze. Nowoczesne technologie dla bezpieczeństwa państwa.

Konferencja szkoleniowa .

Hotel Novotel Szczecin Al. 3 Maja 31

Sala Konferencyjna Amber

Panel I Bezpieczny Region . Bezpieczna Polska . Zagrożenia hybrydowe w regionie.

09.50 - 10.00 : Powitania:
Kmdr por. rez. Artur Bilski /think tank Nobilis Media/ Prezes Zarządu
Dr hab. Adam Makowski, prof. US – dyrektor Instytutu Historii i Stosunków Międzynarodowych Uniwersytetu Szczecińskiego

10.00 - 10.15: Znaczenie potencjału wojskowego i przemysłu zbrojeniowego Polski w regionie. Kierunki rozwoju programów zbrojeniowych dla Sił Zbrojnych jako elementy odstraszania.
Michał Jach : Przewodniczący Sejmowej Komisji ON

10.15 - 10.40 Konflikt hybrydowy. Polityczne i militarne wyzwania dla NATO w regionie Morza Bałtyckiego i Europy Środkowej.
Mówca : Przedstawiciel Kwatery Głównej NATO Robert Pszczel Senior NATO Oficer for Russia and Western Balkans

10.40 - 10.55 Północno -Wschodnia Flanka NATO – Zagrożenia Hybrydowe – Perspektywa Wielonarodowego Korpusu Północno – Wschodniego NATO
Mówca : gen. bryg. Krzysztof Król Zastępca dowódcy WKPW w Szczecinie

10:55 - 11.25 Dyskusja Panelowa

11.25 – 11.50 Przerwa Kawowa

Panel II Przebieg konfliktu hybrydowego w Polsce : diagnoza i możliwe scenariusze.

11. 50 - 12.05 Pozamilitarne zagrożenia w regionie - wyzwania.
Mówca : Zastępca Dyrektora Agencji Bezpieczeństwa Wewnętrznego Łukasz Adamiak

12.05 – 12.20 Zarządzanie kryzysowe w przypadku konfliktu hybrydowego. Współdziałanie administracji publicznej.
Mówca: dr Paweł Rodzoś , Dyrektor ds. Zarządzania Kryzysowego , Zachodniopomorski Urząd Wojewódzki , doradca Sejmowej Komisji ON

12. 20 – 12.35 Wojna hybrydowa w cyberprzestrzeni. Scenariusze cyberataków i przechwycenia kontroli nad systemem sterowania obiektami strategicznymi w Polsce . Konieczność szkolenia.
Mówca : Maciej Kaczkowski Prezes Zarządu Enamor International

12.35 – 12.50 Zagrożenia hybrydowe w perspektywie formacji chroniących infrastrukturę krytyczną.

Mówca : Rafał Batkowski Szef Służby Ochrony Lotniska Chopina , Warszawa Okęcie

12.50 – 13.20 Panel dyskusyjny

13.20 – 13.50 Przerwa Kawowa

Panel III Przebieg konfliktu hybrydowego w Polsce. Zagrożenia dla infrastruktury krytycznej i miejskiej

13.50 – 14. 05 Miasto polem bitwy .
Mówca : prof. A. Aksamitowski/ Uniwersytet Szczeciński

14. 05 - 14.20 Terroryzm bombowy a bezpieczeństwo infrastruktury krytycznej .
dr M. Cupryjak, Uniwersytet Szczeciński

14. 20 - 14. 35 Przyszły konflikt hybrydowy na granicy RP na przykładzie m. Gołdap. Diagnoza, program, scenariusze
Mówca : mgr J. Krysiński, Uniwersytet Szczeciński

14.35 – 14.50 Atak na infrastrukturę krytyczną. Prawne aspekty zarządzania sytuacją kryzysową w Polsce i Europie .
Mówca : Mirella Chomont Radca Prawny /Nobilis Media

14.50 – 15. 20 Panel dyskusyjny

15. 20 – 15.40 Przerwa Kawowa

Panel IV Zebrane doświadczenia z zarządzania sytuacją kryzysową.

15.40 – 15. 55 Rola i znaczenie infrastruktury krytycznej dla bezpieczeństwa państwa.

Mówca dr P. Chrobak, Uniwersytet Szczeciński

15.55 - 16.10 Współczesne zabezpieczenie lotnisk przed atakami terrorystycznymi

Mówca : dr Zygmunt Kozak Uniwersytet Szczeciński

16.10 – 16.25 Wpływ awarii elektrowni atomowej na infrastrukturę krytyczną państwa na przykładzie Fukushimy (wnioski i zmiany)

Mówca: dr hab. prof. Renata Gałaj – Dempniak Uniwersytet Szczeciński

16.25 – 16.40 System bezpieczeństwa II Rzeczypospolitej . Czy czegoś możemy się nauczyć. Podsumowanie.

Mówca : Prof. H. Walczak/ Uniwersytet Szczeciński , prof. dr hab. Janusz Faryś Akademia im. Jakuba z Paradyża w Gorzowie Wlk.

16.40 -17.10 Panel

17.20 Zakończenie/Podsumowanie

20.00 - 22. 00 Security Forum Szczecin Cocktail / Networking / Muzyka na żywo /Hotel Novotel

19 Października (Czwartek) Hotel Novotel Sala Konferencyjna Turkus .

13.50 – 17.20 Cyberataki na infrastrukturę krytyczną. Ataki i przechwycenia kontroli nad systemem sterowania obiektami strategicznymi i możliwości ochrony.

Mówca : Enamor International

Warsztaty przeznaczone jest dla Kadry Zarządzającej oraz Pracowników Technicznych. Szkolenie realizowane jest przez specjalistów z firmy Enamor International z Warszawy jako prezentacje teoretyczne, demonstracje i w ograniczonym zakresie ćwiczenia praktyczne. Poruszane zagadnienia dotyczą krótkiego przeglądu najnowszych zagrożeń i metod ataku oraz środków zabezpieczeń minimalizujących ryzyko związane z wykorzystaniem podatności. W szczególności poruszone są zagadnienia:

Plan szkolenia bezpieczeństwa teleinformatycznego

1. **Możliwości ochrony przed atakami przejęcia kontroli**
2. **Kontrola wycieku danych z firmy**
3. **Zbieranie i analiza danych o zagrożeniach, wstęp do SIEM**
4. **Polityki bezpieczeństwa**
5. **Security Operation Center**

Temat szkolenia: Bezpieczeństwo teleinformatyczne – wybrane aspekty
Grupa tematyczna I: ataki przechwycenia kontroli nad systemem i możliwości ochrony.
Czas trwania: 1 x 45 min
Demonstracja ataku na stację roboczą z systemem Windows 7/8.1, przejęcie kontroli nad systemem z uprawnieniami Administratora, zdalny dostęp do systemu plików, pulpitu, kamery. Dalsze przejęcie kontroli nad systemem wewnętrznym firmy. Metody ukrycie przed systemami zabezpieczeń IDS oraz End-point Protection.
Demonstracja środków zabezpieczeń IDS/End-point Protection minimalizująca ryzyko ataku (analiza behawioralna).

Grupa tematyczna II: kontrola danych w systemie teleinformatycznym (DLP).
Czas trwania: 1 x 45 min
Przedstawienie możliwości znakowania danych w systemie i wdrożenia zabezpieczenia brzegowego (bramy międzysystemowej), które umożliwia zabezpieczenie przed wyciekiem danych wrażliwych poza system TI firmy. Demonstracja przykładowego rozwiązania.
Grupa tematyczna III: zbieranie i analiza danych o zagrożeniach sieciowych – logi.
Czas trwania: 1 x 45 min
Mechanizmy kolekcji logów systemowych ze stacji roboczych (HIDS) oraz logi systemowe sensorów sieciowych (NIDS). Format i przetwarzanie logów. Korelacje zdarzeń. Wstęp do SIEM.
Grupa tematyczna IV: polityki bezpieczeństwa
Czas trwania: 1 x 45 min
Zarządzanie politykami bezpieczeństwa w rozbudowanych systemach teleinformatycznych. Możliwość formalnego zapisu polityk w formacie SCAP (XML), implementacja polityk, weryfikacja polityk.
Grupa tematyczna V: security operation center
Czas trwania: 1 x 45 min
17.20 Zakończenie