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

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

Konferencja szkoleniowa dla służb państwowych połączona z wystawą sprzętu i uzbrojenia .

Hotel Novotel Szczecin Al. 3 Maja 31

Sala Konferencyjna Amber

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

09.55 - 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 Wojsk Obrony Terytorialnej i programów zbrojeniowych dla Sił Zbrojnych.
Michał Jach : Przewodniczący Sejmowej Komisji ON

10.15 - 10.35 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. 35 - 10. 50 Zarządzanie kryzysowe w przypadku konfliktu hybrydowego. Współdziałanie Wojsk Obrony Terytorialnej , służb mundurowych i cywilnych.
Mówca: dr Paweł Rodzoś , Dyrektor ds. Zarządzania Kryzysowego , Zachodniopomorski Urząd Wojewódzki , doradca Sejmowej Komisji ON

10.50 – 11. 05 Konflikt hybrydowy wyzwaniem dla bezpieczeństwa Europy Środkowej – możliwe scenariusze.
Mówca : ppłk Cezary Pawlak Centrum Doktryn i Szkolenia SZ RP

11.05 – 11.25 Dyskusja Panelowa

11.25 – 12.00 Przerwa Kawowa

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

12. 00 - 12.15 Sytuacja bezpieczeństwa w regionie - wyzwania i zagrożenia.
Mówca : Zastępca Dyrektora Agencji Bezpieczeństwa Wewnętrznego Łukasz Adamiak

12.15 – 12.35 Przyszły konflikt hybrydowy na granicy RP na przykładzie m. Gołdap. Diagnoza, program, scenariusze
Mówca : mgr J. Krysiński, Uniwersytet Szczeciński

12. 35 – 12.50 Wojna hybrydowa w cyberprzestrzeni. Scenariusze cyberataków i przechwycenia kontroli nad systemem sterowania obiektami strategicznymi w Polsce .
Mówca : Maciej Kaczkowski Prezes Zarządu Enamor International

12.50 – 13.15 Panel dyskusyjny

13.15 – 13.50 Przerwa Kawowa

Panel III Nowoczesne technologie do obrony państwa

13.50 – 14.05 Użycie zaawansowanych technologicznie systemów bojowych w działaniach hybrydowych i Wojsk Obrony Terytorialnej .
Mówca : Przedstawiciel PGZ

14.05 -14.25 Możliwość wystąpienia konfliktu hybrydowego na Morzu Bałtyckim - scenariusze.
Mówca : Kmdr por. Jarosław Keplin Centrum Doktryn i Szkolenia SZ RP

14. 25 - 14. 45 Zintegrowane zabezpieczenie obiektów strategicznych od strony morza.
Mówca : Maciej Rek Prezes Zarządu Enamor

14.45 –15.15 Panel dyskusyjny

15.15 – 15.45 Przerwa Kawowa

Panel IV Zagrożenia hybrydowe dla infrastruktury krytycznej i miejskiej

15.45– 16.00 System bezpieczeństwa II Rzeczypospolitej . Czy czegoś możemy się nauczyć ?

Mówca : Prof. H. Walczak/ Uniwersytet Szczeciński

16.00 – 16.15 Infrastruktura krytyczna miasta w III RP - Element konfliktu hybrydowego ?

prof. A. Aksamitowski/ Uniwersytet Szczeciński

16.15 - 16.30 Terroryzm bombowy a bezpieczeństwo infrastruktury krytycznej .

dr M. Cupryjak, Uniwersytet Szczeciński

16.30 – 16. 45 Rola i znaczenie infrastruktury krytycznej dla bezpieczeństwa państwa.

Mówca dr P. Chrobak, Uniwersytet Szczeciński

16.45 – 17.10 Panel

17. 15 Zakończenie/Podsumowanie

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

19 Października (Czwartek) Hotel Novotel Sala Konferencyjna Turkus .

13.50 – 17.15 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

17.15 Zakończenie