FUNDACJA bezpieczna cyberprzestrzeń

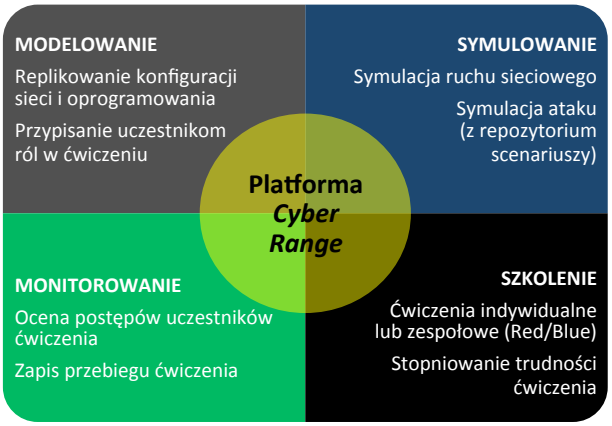
CYBERPOLIGONY – NOWA GENERACJA SZKOLEŃ DLA SPECJALISTÓW BEZPIECZEŃSTWA IT

23.05.2017

Pojawianie się nowych, coraz bardziej zaawansowanych cyberzagrożeń pokazuje, że zapewnienie bezpieczeństwa IT wymaga nie tylko inwestycji w odpowiednie technologie zabezpieczeń, ale co równie ważne – w szkolenia cyberspecjalistów, którzy zapewnią ich właściwą implementację i obsługę.
Tradycyjne metody szkoleń okazują się często niewystarczające i dlatego powstają nowatorskie rozwiązania, w tym specjalne platformy szkoleniowo-ćwiczeniowe typu *Cyber Range*, zwane *cyberpoligonami*.

Każdego dnia, na całym świecie, cyberprzestępcy opracowują nowe sposoby infiltracji informatycznych sieci administracji rządowej, sektora prywatnego i różnych organizacji. Wobec coraz bardziej złożonych i różnorodnych cyberzagrożeń, nawet najbardziej nowoczesne i zaawansowane technologie bezpieczeństwa są obecnie niewystarczające bez odpowiednio wyszkolonej kadry specjalistów. Skuteczne wdrażanie zabezpieczeń a także identyfikacja i reagowanie w czasie rzeczywistym na wyrafinowane, często ukierunkowane cyberataki, wymaga specjalistycznej wiedzy, doświadczenia i odpowiednich umiejętności.

Wysoko wykwalifikowany zespół specjalistów w obszarze cyberbezpieczeństwa staje się obecnie krytycznym elementem każdej większej organizacji. Rosnące zapotrzebowanie na takich ekspertów a także konieczność szybkiego podnoszenia ich kwalifikacji i przygotowania na coraz bardziej złożone zagrożenia powoduje, że większe organizacje zaczynają poważnie inwestować w szkolenia. Konwencjonalne metody szkoleń cyberspecjalistów okazują się często niewystarczające i dlatego powstają nowatorskie rozwiązania, w tym specjalne platformy szkoleniowo-ćwiczeniowe typu *Cyber Range*, zwane *cyberpoligonami*.



Platforma *Cyber Range* to wirtualne środowisko symulacyjne, które pozwala uczestnikom szkolenia rozwinąć, udoskonalić i przetestować umiejętności potrzebne do odpierania prawdziwych cyberataków, w możliwie najbardziej realistycznych warunkach. Modelowanie dynamiczne pozwala szkolonym zespołom dostosować symulacje do własnych potrzeb, poprzez replikowanie konfiguracji ich własnej sieci, oprogramowania oraz symulację typowego ruchu sieciowego w ich organizacji. Platforma umożliwia symulowanie całego spectrum cyberataków, pobieranych z aktualizowanej na bieżąco biblioteki scenariuszy. Podczas symulowanego ataku, poszczególni członkowie szkolonego zespołu są przydzielani do ról, które wykonują w swojej codziennej pracy. W trakcie szkolenia, uczestnicy przechodzą przez różne scenariusze ataków, o coraz większym stopniu trudności. Ćwiczenie przybiera często formę gry, w której testowana jest skuteczność zespołu obrony (*Blue Team*) przed cyberatakami, rywalizującego z zespołem atakującym (*Red Team*). Co istotne, platforma umożliwia zapis „w locie" całego przebiegu szkolenia, osobno dla każdego członka zespołu. Pozwala to, po zakończeniu szkolenia, przeanalizować i wskazać obszary, które należy poprawić zarówno w zakresie reakcji jak i komunikacji.

W ostatnich latach powstało na świecie bardzo dużo platform *Cyber Range*. Wśród istniejących platform znajdują się rozwiązania zarówno komercyjne, rządowe, militarne, jak i akademickie. Własne rozwiązania *Cyber Range* posiadają w swojej ofercie zarówno duże międzynarodowe firmy informatyczne, jak i mniejsze, specjalizujące się w technologiach i usługach bezpieczeństwa IT. Wśród rozwiązań komercyjnych znajdują się m.in. platformy firm: IBM, Cisco, Cyberbit, CyberGym, JYVSECTEC, ixia, Raytheon, Sypris Solutions.

> WŚRÓD ISTNIEJĄCYCH PLATFORM SZKOLENIOWYCH TYPU *CYBER RANGE* ZNAJDUJĄ SIĘ ROZWIĄZANIA KOMERCYJNE, RZĄDOWE, MILITARNE I AKADEMICKIE

Dostępne rozwiązania różnią się od siebie poziomem zaawansowania. Te najbardziej zaawansowane wzbudzają zainteresowanie rządów i organizacji oraz są wykorzystywane przy tworzeniu ośrodków do szkolenia cyberspecjalistów. Jednym z rozwiązań jest platforma Cyber Range izraelskiej firmy Cyberbit, stosowana m.in. w amerykańskim ośrodku ETA Cyber Range w Baltimore od kwietnia 2017 roku oraz w ośrodku tworzonym od lutego 2017 roku w Tokio, dla japońskiej firmy Ni Cybersecurity. Ośrodek w Japonii ma pomóc m.in. w uzupełnieniu niedoboru specjalistów przed zbliżającą się Olimpiadą w 2020 roku. Europejskim przykładem jest centrum szkoleniowe CyberGym Europe w Czechach (pod Pragą), które powstało w 2016 roku. Jest to wspólne przedsięwzięcie czesko-izraelskie, które dostarcza szkoleń z zakresu ochrony infrastruktury krytycznej. Z końcem 2016 roku, także IBM otworzyło swój pierwszy ośrodek Cyber Range w Cambridge, a na początku 2017 roku, Cisco zainwestowało w ośrodek Cyber Range Lab w Indiach.

Wśród rozwiązań szkoleniowych dla celów rządowych i militarnych, znajduje się m.in. amerykańska platforma NCR (*National Cyber Range*). Ta wielkoskalowa platforma została opracowana w latach 2009-2012 przez organizację DARPA (*Defense Advanced Research Projects Agency*) a następnie przekazana do centrum TRMC (*Test Resources Management Center*) Departamentu Obrony USA (*DoD*). Innym przykładem jest platforma JCOR (*Joint Cyberspace Operations Range*) z symulatorem SIMTEX (*Simulator Training Exercise Network*), opracowana dla Sił Powietrznych USA (*US Air Force*). Na potrzeby sił zbrojnych USA, powstaje specjalny cyberpoligon PCTE (*Persistent Cyber Training Environment*). Do przykładów europejskich rozwiązań należy m.in. cyberpoligon szkoleniowo-badawczy dla Departamentu Obrony przed Cyberatakami holenderskiego Ministerstwa Obrony, powstający w ramach umowy z firmą Thales, która zabezpiecza m.in. łącza komunikacyjne NATO.

Centrum operacyjne Sił Powietrznych USA (źródło: www.af.mil)

Należy wspomnieć, że Polska ma również swój sukces w tym zakresie. W ubiegłym roku, platforma CDeX polskiej firmy Vector Synergy została wybrana przez NATO do zastosowania jako jedno z rozwiązań szkoleniowo-ćwiczeniowych w zakresie cyberobrony. Powstają również mniejsze polskie projekty, z dużym potencjałem rozwoju, jak na przykład platforma CERT GAMES. Jest to wspólny projekt Fundacji Bezpieczna Cyberprzestrzeń i firmy ComCERT SA, z sukcesem wykorzystany przy szkoleniu specjalistów z zespołów CERT (Computer Emergency Response Team) z kilkunastu krajów.

Ćwiczenia „Cyber-EXE Polska”
(źródło: www.cyberexepolska.pl)

Platformy *Cyber Range* są wykorzystywane w przeprowadzanych regularnie, na całym świecie, międzynarodowych i krajowych ćwiczeniach testujących umiejętności odpierania cyberataków a także współpracy w tym zakresie. Do międzynarodowych, największych i najbardziej zaawansowanych technicznie ćwiczeń należą Locked Shields, organizowane corocznie, od 2012 roku, przez Centrum Doskonalenia Obrony Cybernetycznej NATO w Tallinnie. Przeznaczone są dla wojskowych i cywilnych ekspertów ds. bezpieczeństwa, chroniących krajowe systemy informatyczne. Amerykańskie ogólnokrajowe ćwiczenia Cyber Storm są przeprowadzane co dwa lata, od 2006 roku, przez Departament Bezpieczeństwa Wewnętrznego (*DHS - Departament of Homeland Security*). Innym przykładem są ogólnoeuropejskie ćwiczenia Cyber Europe, organizowane przez agencję ENISA (*European Network and Information Security Agency*) **a także ćwiczenia Cyber-EXE Polska, które od kilku lat przeprowadza Fundacja Bezpieczna Cyberprzestrzeń dla polskich sektorów infrastruktury krytycznej i administracji państwowej.**

Ośrodki akademickie i badawczo-rozwojowe coraz częściej rozwijają swoje projekty w zakresie symulacyjnych platform szkoleniowych. Interesującym przykładem jest platforma SCEPTRE (*Substrate for Cybersecurity Education; a Platform for Training, Research and Experimentation*), która, od 2016 roku, powstaje w ramach wspólnego projektu Cyber Academy na Uniwersytecie J.Waszyngtona oraz organizacji Merit Networks. Platforma MCR (*Michigan Cyber Range*) tej organizacji zostanie zintegrowana z akademicką siecią komputerową w celu stworzenia środowiska edukacyjnego, testowego oraz platformy badawczej, dedykowanej tworzeniu kursów akademickich oraz certyfikatów w zakresie cyberbezpieczeństwa.

> CYBERPOLIGONY SĄ SZANSĄ NA SZYBSZE ROZWIĄZANIE PROBLEMU ROSNĄCEGO DEFICYTU CYBERSPECJALISTÓW

Nowatorskie rozwiązania w zakresie szkoleniowych platform symulacyjnych bardzo zyskują na znaczeniu na całym świecie. Upatruje się w nich m.in. możliwość szybszego rozwiązania problemu rosnącego niedoboru ekspertów ds. bezpieczeństwa IT. Z pewnością, stanowią one ogromną szansę na zintensyfikowanie i skrócenie procesu podnoszenia i doskonalenia umiejętności zarówno obecnych cyberspecjalistów, jak i edukacji przyszłych adeptów kierunków bezpieczeństwa IT. Wśród dostępnych platform szkoleniowych, dominują jednak kosztowne rozwiązania komercyjne. Na pewno zwiększenie ogólnodostępnych rozwiązań akademickich, nawet o dużo niższym poziomie zaawansowania, poprawiłoby jakość i efektywność procesu nauczania w tym zakresie. Dodatkowo, organizowanie regionalnych lub krajowych konkursów i gier „Zdobądź flagę” (*Capture the flag*), z wykorzystaniem takich platform, mogłoby być skutecznym sposobem na „łowienie talentów”, już na wczesnym etapie nauczania.

NAZWA PLATFORMY	TYP PLATFORMY	ORGANIZACJA	KRAJ
BreakingPoint	komercyjna	ixia	USA
Cisco Cyber Range	komercyjna	Cisco	USA
CyberGym's Training Area	komercyjna	CyberGym	Izrael
Cyber Range	komercyjna	Cyberbit	Izrael
IBM Cyber Range	komercyjna	IBM	USA
Michigan Cyber Range	komercyjna	Merit Networks	USA
Raytheon's Cyber Range	komercyjna	Raytheon	USA
RGCE (*Realistic Global Cyber Environment*)	komercyjna	JYVSECTEC	Finlandia
Sypris Cyber Range	komercyjna	Sypris Solutions	USA
CDeX	wojskowa (NATO)	Vector Synergy	Polska
NCR, NCRC (*National Cyber Range Complex*)	rządowo-wojskowa (Departament Obrony USA)	DARPA/ Lockheed Martin	USA
SIMTEX (Simulator Training Exercise Network)/JCOR (Joint Cyberspace Operations Range)	wojskowa (Siły Powietrzne USA)	EADS North America Defense Security and Systems Solutions (Airbus Group)	USA
Thales' Cyber Range	rządowo-wojskowa (holenderskie Ministerstwo Obrony)	Thales	Holandia
RINSE (*Real Time Immersive Network Simulation Environment*)	akademicka	University of Illinois	USA
SCEPTRE (*Substrate for Cybersecurity Education; a Platform for Training, Research and Experimentation*)	akademicka	George Washington University/ Merit Networks	USA

Wybrane przykłady platform szkoleniowych typu Cyber Range

Platformy *Cyber Range* mogą stać się także wsparciem podczas procesu rekrutacji specjalistów, pozwalając na efektywne testowanie praktycznych umiejętności kandydatów a także sprawniejszą certyfikację z zakresu cyberbezpieczeństwa. **To wszystko sprawia, że takie platformy zaczynają być postrzegane jako rozwiązania przyszłości w zakresie cyberbezpieczeństwa, pozwalając na tworzenie symulowanej cyberprzestrzeni, w której umiejętności i narzędzia cyberobrony mogą być bezpiecznie trenowane i testowane w kontrolowanym środowisku. Analogicznie, jak to się odbywa na symulatorach lotu czy na wojskowych poligonach.**

—

Autor: Elżbieta Nowicka

Kierownik Projektu
Fundacja Bezpieczna Cyberprzestrzeń

———

Śledź na:
TT: @cybsecurity_org
Facebook: **@FundacjaBezpiecznaCyberprzestrzen**