Cyberdefence 24

aut. Szymon Palczewski 25.09.2020

AMERYKANIE SPRAWDZILI ODPORNOŚĆ STRATEGICZNYCH PORTÓW NA CYBERATAKI. CZAS NA POLSKĘ

Amerykanie przetestowali jakość zabezpieczeń elementów infrastruktury krytycznej w strategicznych portach USA, a także zdolność do reagowania na cyberataki podmiotów odpowiedzialnych za ich bezpieczeństwo. Wszystko odbyło się w ramach zaawansowanych ćwiczeń, które zakładały wywołanie tzw. mieszanego kryzysu. Polska powinna iść śladami Stanów Zjednoczonych i regularnie testować zdolności w zakresie cyberbezpieczeństwa? Nad Wisłą zrobiono już pierwszy krok.

Jack Voltaic to inicjatywa skoncentrowana bezpieczeństwie na infrastruktury krytycznej oraz partnerstwie publiczno-prawnym w Stanach Zjednoczonych. Seria ćwiczeń sprawdza przede wszystkim zdolności władz lokalnych oraz przemysłu do reagowania na zaawansowany cyberatak.

Jednym z celów cyklu symulacji (zapoczątkowanym w 2016 roku) jest wywarcie wpływu na podmioty z wielu sektorów oraz sprawdzenie ich skoordynowanej reakcji na zagrożenie. Równie istotne jest wskazanie nieprawidłowości i stworzenie przyjaznego środowiska „uczenia się", aby w ten sposób umożliwić wszystkim uczestnikom zdobycie niezbędnego doświadczenia na wypadek wystąpienia incydentu. Niemniej ważnym celem pozostaje ocena jakości wymiany informacji między podmiotami – czytamy w komunikacie amerykańskiego Army Cyber Institute, jednego ze współorganizatorów wydarzenia.

Najnowsza odsłona symulacji trwała od 22 do 24 września br. Inicjatywa skupiła ponad 150 uczestników, a jej głównym zadaniem było sprawdzenie zdolności w zakresie reagowania na cyberataki wymierzone w infrastrukturę krytyczną – poinformował Instytut na Twitterze.

> Our final day of #JackVoltaic is kicking off! This completely virtual, distributed event provides more than 150 participants from the @cityofsavannah to exercise their "whole-of-community" approach and response to #cyberattacks against critical infrastructure. #ThursdayMotivation pic.twitter.com/zTWAdqkYIL
>
> — Army Cyber Institute (@ArmyCyberInst) September 24, 2020

3 edycja Jack Voltaic była zgodna z serią ćwiczeń Defender 2020 i zakładała scenariusz, w którym cywilna infrastruktura miała wpływ na rozmieszczenie sił U.S. Army oraz ich operacje. Głównym obszarem symulacji był Charleston w Karolinie Południowej i Savannah w stanie Georgia. „Dzięki Jack Voltaic 3.0 oba miasta miały możliwość przećwiczenia, udoskonalenia i zademonstrowania swoich zdolności w zakresie reagowania na zagrożenia w cyberprzestrzeni" – stwierdzono w komunikacie

Army Cyber Institute.

Głównym założeniem najnowszej odsłony symulacji było opracowanie ram reagowania na cyberataki oraz konwencjonalne operacje wrogich podmiotów. Inicjatywa pozwoliła również sprawdzić poziom zdolności lokalnych władz w zwalczaniu incydentów w sieci, zarówno w celu zapewnienia nieprzerwanego świadczenia usług publicznych oraz ochrony infrastruktury krytycznej.

Bardzo ważnym aspektem było także wzmocnienie odpowiedniej reakcji „całego narodu" na incydenty w wirtualnej domenie poprzez trwałe, wielopoziomowe partnerstwa między sektorami – przemysłem, środowiskiem akademickim oraz rządem. Ponadto inicjatywa Jack Voltaic 3.0 miała na celu sprawdzenie procesu koordynacji działań amerykańskich sił zbrojnych w kontekście cyberbezpieczeństwa, a także ocenę wpływu cyberataków na cywilną infrastrukturę krytyczną na zdolności armii do skutecznego prowadzenia wojskowych operacji – wskazano w czytamy w komunikacie Instytutu.

W ramach ćwiczenia posłużono się scenariuszem, w którym na cele znajdujące się w portach w Charleston oraz Savannah przeprowadzono serię cyberataków z udziałem oprogramowania ransomware. Podmioty biorące udział w symulacji dodatkowo musiały zmierzyć się z fikcyjnym wypadkiem statku towarowego, powodzią oraz awarią systemów 911. Założeniem twórców inicjatywy było wywołanie tzw. mieszanego kryzysu.

„Naprawdę staramy się zrozumieć, jaki jest wpływ cyberataków na infrastrukturę krytyczną, w szczególności jak wpływa to na reakcję i jakie są luki w kluczowych elementach" – wskazał na łamach CyberScoop ppłk Doug Fletcher, główny planista ćwiczenia z Army Cyber Institute.

Miejsce przeprowadzenia symulacji nie było przypadkowe. Jak zaznaczył ppłk Doug Fletcher, porty w Charleston i Savannah to dwa strategiczne obiekty z punktu widzenia amerykańskich sił zbrojnych.

Podczas ćwiczeń wykorzystano Emotet, czyli popularny rodzaj złośliwego oprogramowania, który może łatwo rozprzestrzeniać się w sieciach. Jak informowaliśmy na naszym portalu, początkowo Emotet był uznawany za trojana bankowego, jednak z biegiem czasu znacznie ewoluował.

Obecnie złośliwe oprogramowanie pozwala między innymi na przejęcie haseł przechowywanych w systemach ofiar, w tym przeglądarkach internetowych oraz poczty, a także kradzież danych pochodzących z e-maili (np. plików z załącznikach czy listy kontaktów). Emotet łatwo rozprzestrzenia się w docelowej sieci, ponieważ wykorzystuje luki w zabezpieczeniach oraz pozyskane hasła dostępu.

Czytaj też: Najpierw Francja, teraz Japonia i Nowa Zelandia. Seria cyberataków trwa

Według Departamentu Bezpieczeństwa Wewnętrznego USA wirus jest obecnie jednym z najbardziej destrukcyjnych rodzajów złośliwego oprogramowania, wykorzystywanego przeciwko władzom stanowym. Stąd też decyzja o uwzględnieniu trojana „w głównej roli" przeprowadzonej symulacji.

W ramach ćwiczenia uczestnicy początkowo musieli zmierzyć się z „usterkami technicznymi" w sferze zarządzania ładunkiem. Z czasem pojawiał się kolejny problem – cyberatak z udziałem Emotet. Następnie zaangażowane podmioty zostały sparaliżowane przez ransomware. W efekcie incydent spowodował regionalne przerwy w dostawie prądu – donosi CyberScoop.

W tym miejscy należy podkreślić, że większość infrastruktury portowej należy do własności prywatnej. Dlatego też uczestnikami ćwiczenia obok władz obu miast, Army Cyber Command, US Coast Guard, South Carolina i Georgia National Guards były także takie firmy jak Dominion Energy, Southern

Company, Chubb Insurance, Verizon oraz AT&T.

Porty morskie są nie tylko kluczowym elementem z punktu widzenia sił zbrojnych, ale także gospodarki państwa. Według American Association of Port Authority porty zapewniają amerykańskim firmom około 5,4 biliona dolarów przychodów w skali roku.

Obecnie nie przedstawiono żadnych konkretnych wniosków płynących z symulacji. W nadchodzących dniach Army Cyber Command będzie analizować pozyskane dane, aby zweryfikować oraz ocenić działania uczestników. Wówczas zostaną opublikowane szczegóły oraz rekomendacje.

Polska idzie śladami Amerykanów?

W tym samym czasie (22-23 września br.) w Polsce odbyły się ćwiczenia sprawdzające Krajowy System Cyberbezpieczeństwa „KSC-EXE 2020". W ramach inicjatywy eksperci zweryfikowali jak w praktyce działają podstawowe elementy Systemu, w tym między innymi procedury reagowania na incydenty oraz współpraca zespołów reagowania na incydenty - CSIRT.

Jak wówczas informowaliśmy, były to pierwsze tego typu ćwiczenia cyberbezpieczeństwa nad Wisłą. Głównym celem symulacji stanowiło sprawdzenie w praktyce skuteczności obowiązujących w kraju rozwiązań i procedur.

Inicjatywa KSC-EXE 2020 miała charakter międzysektorowy, co oznacza, że sprawdzała współpracę podmiotów z różnych obszarów gospodarki narodowej. Wzięły w niej udział podmioty z takich branż jak: bankowość, infrastruktura rynków finansowych, energia oraz telekomunikacja.

Ćwiczenia mają mieć swoją kontynuację w kolejnych latach, co zadeklarował minister cyfryzacji Marek Zagórski. „Planujemy, aby takie ćwiczenia z udziałem ekspertów i praktyków z różnych dziedzin, odbywały się przynajmniej raz w roku" – podkreślił szef resortu cyfryzacji.

Czytaj też: Jak działa Krajowy System Cyberbezpieczeństwa? Ćwiczenia KSC-EXE 2020