FUNDACJA bezpieczna cyberprzestrzeń

ZNACZENIE CYBER ĆWICZEŃ W BUDOWIE KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

31.08.2018

„Cyberbezpieczeństwo należy nie tylko do najważniejszych wyzwań, z którymi mierzy się dzisiejszy biznes, ale również w coraz większym stopniu zagrożenia te mogą dotyczyć bezpieczeństwa i obronności państwa" - tego typu stwierdzenie, choć często przywoływane, wydaje się już nieaktualne. Scenariusz, w którym zagrożone są struktury bezpieczeństwa państwa, usługi kluczowe czy obecne już w każdym obszarze życia usługi cyfrowe, jest niemalże codziennością i występuje na mniejszą, bądź większą skalę. W przeciwdziałaniu tego typu atakom mogą pomóc cyber ćwiczenia.

Złośliwe kampanie wycelowane w sferę biznesową są w stanie zakłócić normalne funkcjonowanie państwa, a przywrócenie stanu sprzed ataku bywa kosztowne i czasochłonne. Wyjątkowo pechowy pod tym względem był rok 2017, w którym po raz pierwszy pojawiły się kampanie WannaCry i NotPetya. Nie można także zapomnieć np. o poważnej awarii dostawy prądu na Ukrainie w 2015 r., spowodowanej wirusem Black Energy.

Istotnym czynnikiem mogącym zniwelować wpływ cyber ataków na bezpieczeństwo państwa, jest budowanie zdolności zespołów bezpieczeństwa, w tym CSIRT-ów (Zespoły reagowania na incydenty komputerowe) oraz SOC-ów (Security Operations Center). Jednym ze sprawdzonych sposobów takiego wsparcia jest organizacja ćwiczeń. Mogą one przybierać różne formy, mogą być bardziej techniczne (np. CTF-y, red teaming), lub skoncentrowane na realizowaniu właściwych procedur (gry decyzyjne i ćwiczenia sztabowe). Mogą mieć również ograniczenia podmiotowe, czyli dotyczyć jednej organizacji, wybranego sektora gospodarki lub weryfikować poziom współpracy między sektorowej, a nawet pomiędzy krajami.

> ISTOTNYM CZYNNIKIEM MOGĄCYM ZNIWELOWAĆ WPŁYW CYBER ATAKÓW NA BEZPIECZEŃSTWO PAŃSTWA, JEST BUDOWANIE ZDOLNOŚCI ZESPOŁÓW BEZPIECZEŃSTWA, W TYM CSIRT-ÓW (ZESPOŁY REAGOWANIA NA INCYDENTY KOMPUTEROWE) ORAZ SOC-ÓW (SECURITY OPERATIONS CENTER).

Własne ćwiczenia od wielu lat organizuje Departament Bezpieczeństwa Krajowego Stanów Zjednoczonych (Cyber Storm), Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (Cyber Europe) czy NATO (m.in. ćwiczenia Locked Shields). Organizowanie ćwiczeń krajowych, mających na celu sprawdzenie przygotowania na kryzys wywołany atakiem w cyberprzestrzeni, do niedawna nie było umocowane prawnie. Funkcjonowało raczej na poziomie dobrej praktyki i rekomendacji. Dziś, za sprawą ustawy o krajowym systemie cyberbezpieczeństwa, zadanie „inicjowania krajowych ćwiczeń w zakresie cyberbezpieczeństwa" przynależy do Pełnomocnika Rządu do spraw Cyberbezpieczeństwa. Konieczność organizowania tego typu przedsięwzięć stała się więc nie tylko ideą czy dobrą praktyką ale faktem.

Niezależnie jednak od formalnych wymagań stawianych przez polskie prawo, teraz i w przeszłości, cyber ćwiczenia w Polsce mają się całkiem dobrze. Popularne konferencje branżowe coraz chętniej organizują ćwiczenia techniczne z nagrodami (np. Security Case Study czy CONFidence), a przedstawiciele zespołów bezpieczeństwa regularnie uczestniczą w tego typu wydarzeniach organizowanych lokalnie i zagranicą. Fundacja Bezpieczna Cyberprzestrzeń od 2012 r. organizuje krajowe ćwiczenia „Cyber-EXE Polska", które są skierowane zarówno do osób technicznych, jak i menedżerów odpowiedzialnych za zarządzanie incydentami. Do tej pory odbyło się 5 edycji ćwiczeń, w które były zaangażowane takie sektory jak bankowość, finanse, telekomunikacja, consulting czy energetyka. Obecnie trwają prace nad kolejną edycją, która sprawdzi efektywność odparcia incydentu teleinformatycznego w sektorze bankowym. Jak wynika z opinii łącznie już setek osób ćwiczących podczas „Cyber-EXE Polska", cyber ćwiczenia mają m.in. wpływ na budowanie świadomości o zagrożeniach w organizacji, wzmacniają relacje z podmiotami zewnętrznymi oraz weryfikują skuteczność procesów, procedur i polityk bezpieczeństwa. Pozwalają także zidentyfikować słabe strony w komunikacji wewnętrznej, np. pomiędzy analitykami CSIRT, a działem IT.

Duża aktywność tzw. grup APT (Advanced Persistent Threat) świadczy o tym, że kolejne złośliwe kampanie ukierunkowane na infrastrukturę krytyczną z pewnością są już zaplanowane. Cyberprzestępcy nie spoczywają na laurach i analizują możliwości przeprowadzenia skutecznego ataku. Nie ma co do tego wątpliwości. Pozytywnie należy ocenić fakt, że polscy eksperci coraz chętniej biorą udział w cyber ćwiczeniach oraz fakt, że organizacja tego typu ćwiczeń jest jednym z zadań polskiego rządu. Dotychczasowe doświadczenia polskich firm i instytucji w tym obszarze mogą być cenne dla realizacji ambitnego planu budowy krajowego systemu cyberbezpieczeństwa.

Autor: Kamil Gapiński

Fundacja Bezpieczna Cyberprzestrzeń

Śledź na:
TT: @cybsecurity_org
Facebook: @FundacjaBezpiecznaCyberprzestrzen
In: cybersecurity-foundation