Cybernetyczna wojna i bezpieczeństwo wewnętrzne

Zwycięstwo i porażka są dalekie od rozpoznania w cyberprzestrzeni.-Paul Cornish, Chatham House

Wprowadzenie

Cyberprzestrzeń to wyjątkowa instytucja, która wspiera wszystkie aspekty i sektory społeczeństwa, w związku z czym bezpieczeństwo tej przestrzeni ma absolutne znaczenie dla wszystkich rządów dla ich społeczeństw. Kraje, jeden po drugim, tworzą agencje rządowe zajmujące się bezpieczeństwem tej przestrzeni. Podobnie w Stanach Zjednoczonych Departament Bezpieczeństwa Wewnętrznego (DHS), obok wielu innych obowiązków i we współpracy z innymi agencjami rządowymi, otrzymał zadanie cyberbezpieczeństwa. DHS uznał, że istnieje potrzeba stworzenia „odpornego ekosystemu cybernetycznego", co oznacza, że cyberprzestrzeń nie jest izolowanym systemem wsparcia, ale wielowymiarowym ekosystemem, który musi działać w sposób ciągły i odporny, wolny od zagrożeń i możliwości załamania. Ponadto obrona tego ekosystemu musi być dokładna i „zautomatyzowanych działań zbiorowych". Oznacza to, że bezpieczeństwo cyberprzestrzeni musi zostać zautomatyzowane, ponieważ nie może być to proces do zatrzymania, zbadania i podjęcia decyzji z interwencją człowieka - jest po prostu zbyt wolny. System obrony w cyberprzestrzeni musi realizować swoją decyzję działania z prędkością elektroniczną, jeżeli działania te mają charakter zbiorowy są wdrażane w rozproszonych lokalizacjach centrów informacyjnych.

W tym przypadku „sztuczna inteligencja na poziomie węzła sieci rozpoznaje i zapobiega zagrożeniom w czasie rzeczywistym". Cyberprzestrzeń z dnia na dzień staje się coraz ważniejsza w każdym aspekcie życia. Oferuje bezprecedensową i niezastąpioną wygodę, dzięki której społeczeństwo staje się zakładnikiem. Mamy dwie możliwości. Albo odmawiamy użycia cyberprzestrzeni i ponosimy konsekwencje, takie jak izolacja i nieefektywność, lub w pełni cieszymy się z jej nieograniczonych korzyści, wiedząc dobrze, że jej awaria może być katastrofalna, chyba że podejmiemy wszystkie niezbędne środki ostrożności. DHS pojawił się na scenie z pełnym uznaniem tego dylematu i stale zwiększa swoje doświadczenie i wiedzę, starając się dotrzeć do asymptoty - bezpiecznej cyberprzestrzeni.

Cyber Warfare

Cybernetyczna wojna jest spodziewaną wrogą działalnością, którą zrobią przeciwnicy będą próbować wykorzystać, jeśli postrzega się przewagę. „Mówiąc najprościej, wojna cybernetyczna jest nowym, ale nie do końca odrębnym elementem wieloaspektowego środowiska konfliktu". „Dzisiaj w cyberprzestrzeni inteligentni przeciwnicy wykorzystują luki i tworzą incydenty, które rozprzestrzeniają się z prędkością [elektroniczną]… w celu kradzieży tożsamości, zasobów i [tworzenia] przewagi" . W cyberobronie trudno powiedzieć, kto ma przewagę, ponieważ nikt nie wie dokładnie, ile „dziur" znajduje się w cyberprzestrzeni. W kontekście działań wojennych cyberprzestrzeń to przestrzeń elektroniczna, w tym Internet, a także fale radiowe niezależnie od częstotliwości. Miały miejsce liczne cyberataki, ale żadnego z nich nie przypisano wyraźnie przeciwnikowi politycznemu lub wojskowemu. Wszystkie główne mocarstwa - Wielka Brytania, Francja, Niemcy, Rosja i Chiny - na różne sposoby potwierdziły, że włączyły „cyberwarfare jako nową część swojej doktryny militarnej…. Francuzi mogą widzieć uzasadnioną rolę cyberprzestępczości gospodarczej w dążeniu do celów krajowych. " Rosjanie postrzegają „cyberwarfare jako akt wojny, na który każda reakcja… jest uważana za uzasadnioną". Ponadto uważa się, że „Rosja zachowuje prawo do użycia broni jądrowej najpierw przeciwko środkom i siłom wojny informacyjnej, a następnie przeciwko samemu państwu-agresorowi" [6]. Chińczycy postrzegają to jako kolejną wojnę i stworzyli Niebieską Armię [7]. Wydarzenie, które miało miejsce na Syberii, eksplozja gazociągu w 1982 r., jest uważane za pierwszy znany akt cyberbroni. Według zachodnich publikacji wydarzenie było wynikiem sabotażu, w ramach którego system nadzoru i

akwizycji danych (SCADA) systemu rurociągów został źle zaprogramowany w celu spowodowania wybuchu. Jest to skomputeryzowany system, który nadzoruje i kontroluje proces przemysłowy. Jedna strona mówi, że „był to trojan wstawiony [przez CIA] do oprogramowania systemu SCADA, który spowodował masową eksplozję gazu ziemnego wzdłuż rurociągu transsyberyjskiego w 1982 r." Program „resetuje prędkości pompy i ustawienia zaworów, aby wytworzyć ciśnienia znacznie przekraczające wartości dopuszczalne dla połączeń i spoin rurociągów". Druga strona twierdzi, że „było to spowodowane raczej słabą konstrukcją niż sabotażem". Gdyby rzeczywiście był to wrogi akt przypisywany pochodzeniu, jak na przykład bombardowanie, Stany Zjednoczone byłyby winne aktu wojny, ze wszystkimi konsekwencjami prawnymi i moralnymi, jakie Związek Radziecki mógłby ponieść. Ponieważ ofiara wojny cybernetycznej ma trudny przypadek, jeśli nie niemożliwy, do udowodnienia tożsamości cyberatakującego, przyszłość będzie pełna cyberataków. Jeśli w powyższym przypadku rurociągu syberyjskiego urzędnicy byłego lub byłego napastnika twierdzą o odpowiedzialności, kraj będący ofiarą cybernetyczną ma wszelkie prawo do odszkodowania. Dlatego jeśli w momencie wojny cybernetycznej solidne dowody nie wskazują na winnych, nic nie stoi na przeszkodzie prawu do odszkodowania po przyznaniu się do winy lub udowodnieniu pochodzenia czynu przed sądem międzynarodowym. Oznacza to, że po zidentyfikowaniu sprawcy umyślnego szkodliwego działania cybernetycznego ofiara cybernetyczna, zarówno osoba fizyczna, jak i całe państwo, ma prawo do odszkodowania. Uznając ważną rolę, jaką cyberprzestrzeń będzie odgrywać w przyszłości, wszystkie główne potęgi opracowały polecenia cyberprzestrzeni, chcąc stworzyć cyber wojowników gotowych do ataku lub obrony, gdy nadejdzie odpowiedni moment. Mówi się, że cyberprzestrzeń jest korektorem, w tym sensie, że każdy może założyć potężną stronę internetową bez odwiedzającego znającego pełną organizację za fasadą strony. Podobnie wojna w cyberprzestrzeni jest korektorem w tym sensie, że siła militarna, ekonomiczna lub polityczna nie odgrywa żadnej roli, a umiejętności złośliwego oprogramowania są jedynym arsenałem. Jest całkiem możliwe, że dzięki cyberwojnie można osiągnąć niewielkie cele geopolityczne bez konfrontacji militarnej. We wszystkich przypadkach nie ma niepodważalnych dowodów na to, że za suwerenami stoją poszczególne suwerenne państwa. Należy uznać, że ani pochodzenie ataków przez IP, ani osiągnięty cel, jeśli w ogóle, nie mogą absolutnie powiązać ataków z rządami. Większość oskarżeń to uzasadnione spekulacje. Słabym ogniwem w scenariuszu cyberwojny jest telekomunikacja zapadni tworzonej dla organów ścigania, aby ułatwić im misję w walce z przestępczością. Trapdoor jest terminem w kontekście bezpieczeństwa odnoszącym się do mechanizmu, który omija procedury uwierzytelniania i / lub autoryzacji bezpieczeństwa w celu uzyskania nieograniczonego dostępu do zasobów. Jest to odpowiednik klucza głównego w zamkach fizycznych. Biorąc pod uwagę, że żadna informacja o wartości nie może być utrzymywana w tajemnicy, kody zapadni lub inne informacje mogą wyciekać w ręce wroga.

Konwencja o broni cybernetycznej

Około sto lat temu mocarstwa światowe zdały sobie sprawę, że energia atomowa może być również użyta do celów destrukcyjnych. Trzydzieści lat później eksplozja dwóch głowic atomowych udowodniła światu możliwy poziom zniszczenia. Podobnie dzisiaj światowe mocarstwa - widoczne i niewidzialne - rozwijają defensywne i ofensywne cyber arsenały broni cybernetycznej (CW), nieustannie testując je pod kątem ewentualności. Ponownie, podobnie jak w przypadku broni atomowej, niektóre „chłodne głowy" wskazują na potrzebę Konwencji o broni cybernetycznej (CWC) [13]; konwencja - międzynarodowy traktat o kontroli zbrojeń dla cyberprzestrzeni - do którego sygnatariusze zgodzą się nie wykorzystywać swoich broni w scenariuszach zabronionych [13]. Mówi się, że w otwartych działaniach wojennych pierwsza ofiara jest prawdą. Niewątpliwie drugą ofiarą będzie cyberprzestrzeń. Jednak w przeciwieństwie do wszystkich innych broni, w których początkowy punkt początkowy nie może być ukryty ani zakwestionowany, początkowy punkt początkowy CW może pozostać nieznany na

zawsze. Ostatecznie CWC zostanie sporządzony i podpisany, ale będzie to trudne do wyegzekwowania, podczas gdy wiele pytań pozostaje bez odpowiedzi, takich jak,

• Jak można sprawdzić obecność CW?

• Czy powinna istnieć minimalna liczba CW?

• Jakie udogodnienia należy wykluczyć z takich ataków?

• Czy prawdziwe źródło ataku można zlokalizować bez najmniejszego problemu?

Wojna cybernetyczna ma zaledwie dziesięć lat, w porównaniu do wszystkich innych rodzajów wojny, i nie ma formalnej ani nieformalnej „etyki, norm i wartości".

Cyberterroryzm

Terroryzm jest innym rodzajem wrogiej konfrontacji, często pomiędzy suwerennymi mocarstwami, które anonimowo atakują swoje interesy. Zazwyczaj terroryzm obejmuje bezpośrednie lub pośrednie akty przemocy skierowane przeciwko określonym celom lub przeciwko pewnej niewinnej populacji przez grupy, które nie mają formalnego związku z żadną suwerenną mocą, to znaczy z żadnym krajem.

Terroryści wykorzystali szeroką gamę broni jako środka do osiągnięcia swoich celów, a cyberprzestrzeń nie została pominięta. Jeśli chodzi o definicję, można śmiało powiedzieć, że cyberterroryzm to wykorzystanie cyberprzestrzeni do popełniania przemocy lub grożenia jej popełnieniem. Korzystanie z cyberprzestrzeni może być dodatkiem do przestępstwa. Na przykład organizacja terrorystyczna utrzymuje stronę internetową, aby „zabiegać o pieniądze dla nich z różnych przyczyn lub rozpowszechniać zakodowane wiadomości, jawnie lub steganograficznie ". Stenografia to praktyka ukrywania wiadomości w niepowiązanych plikach. Na przykład wiadomości tekstowe można ukryć w plikach obrazu bez widocznego wpływu na wyświetlany obraz. W przypadku terroryzmu cyberprzestrzeń jest najbardziej opłacalną bronią, a także najbezpieczniejszą z punktu widzenia terrorystów. Cyberterroryzm można określić jako

• Sponsorowane przez państwo. W chwili obecnej żaden kraj nie zaakceptował przeprowadzania wrogich działań wobec kogokolwiek. Tacy aktorzy są zwykle wysoko wykwalifikowani, koncentrując się na konkretnych celach wroga.

• Grupy ekstremistyczne. Takie grupy używają cyberprzestrzeni do promocji, rekrutacji i zbierania funduszy, a także do cyberataków na cele, które uważają za wrogie. Takie grupy należą do następujących ogólnych kategorii:

• polityczny

• religijne

• Etniczne

• ideologiczny

• Przestępczość zorganizowana. Są to grupy, które mają pewną wiedzę specjalistyczną w danym sektorze i popełniają wymuszenia na podstawie zagrożeń szkodą - ekonomiczną lub fizyczną. Ich motywami są zawsze korzyści finansowe.

• Przestępstwa indywidualne. Są to izolowane osoby, które popełniają cyberprzestępstwa lub grożą im. W takim przypadku motywy mogą, ale nie muszą, być zyskami finansowymi.

Jeśli chodzi o narzędzia, minimalne badania w Internecie mogą stworzyć skuteczne narzędzia hackerskie. Specjaliści od zwalczania cyberterroryzmu dokumentują incydenty terrorystyczne poprzez identyfikację sześciu głównych parametrów, które wspólnie definiują incydent. To są

• Sprawca. Osoba lub grupa, która popełniła akt cyberterroryzmu.

• Akcja. Cyberprzestępczość terrorystyczna, która została popełniona lub grożono jej popełnieniem.

• Zasób cybernetyczny. Zwykle składa się z trzech części.

• Wirtualna lokalizacja cybernetyczna zdefiniowana przez adres URL.

• Logiczna lokalizacja zdefiniowana przez tożsamość serwera lub bazy danych.

• Fizyczna lokalizacja, w której znajdują się dane. W przypadku przetwarzania w chmurze określenie tej lokalizacji może być trudne.

• Znaczy. Technika złośliwego oprogramowania lub włamania zastosowana w ataku.

• Luka w cyberprzestrzeni. Słaby punkt cyberbezpieczeństwa atakowanego zasobu.

• Motywacja. Zwykle ma to dwa widoki.

• Upubliczniona „szlachetna" motywacja

• Ukryty motyw ukryty

• Przynależność. Zwykle ma to dwie tożsamości.

• Podmiot powołujący się na odpowiedzialność za działanie

• Podmiot podejrzewany o beneficjenta działania

Powyższe stanowią punkt wyjścia w klasyfikacji incydentu. Takie incydenty obejmują szereg przypadków - od unieważnienia lub tymczasowego rozproszonego ataku typu „odmowa usługi" (DDoS) na oficjalnej stronie internetowej po zniszczenie dostępnych publicznych rejestrów lub ingerencję w sterowanie siecią energetyczną. W przeciwieństwie do ostrzeżeń specjalistów ds. Cyberbezpieczeństwa, wiele infrastruktur krytycznych wykorzystuje Internet jako operacyjny intranet ze względu na wynikające z niego korzyści finansowe, zamiast budować i utrzymywać własną sieć fizycznie i logicznie odizolowaną od Internetu. Obecnie kilka sektorów wytwarzania energii jest narażonych na działanie Internetu, a „Dzięki najnowszym osiągnięciom w dziedzinie inteligentnych systemów sieciowych i coraz większemu wykorzystaniu technologii informatycznych w infrastrukturze elektroenergetycznej takie ataki mogą mieć miejsce, szczególnie na dużą skalę przy użyciu wyrafinowanych technik wtargnięcia". Atak na pokolenie może doprowadzić do zniszczenia dużych turbin, odcięcia zasilania i spowodowania ofiar wśród ludzi. Atak na dystrybucję i kontrolę mocy może pozostawić duże obszary bez usługi zasilania; podczas gdy atak na przetwarzanie danych może zniszczyć ważne, być może niezastąpione zapisy. Eksperci twierdzą, że „kliknięcie myszą może pogrążyć miasto w ciemności" i wezwał przedsiębiorstwa energetyczne do „Odłączenia sieci elektrycznej od Internetu" , stwierdzając, że „infrastruktura krytyczna każdego kraju - komunikacja, sieci energetyczne, zasoby wodne, linie gazowe , wojsko i tym podobne - a ich sieci nie mogą mieć nic wspólnego z Internetem. Taka infrastruktura musi mieć własny intranet, dostępny tylko z wybranych lokalizacji oraz fizycznie i praktycznie bezpieczny ". Co więcej, dowódca amerykańskiego Cyber Command, odnosząc się do słabości cybernetycznych w sieciach elektroenergetycznych, stwierdził, że „cyberataki przez Internet przechodzą z kradzieży danych na ataki fizyczne". Możliwość destrukcyjnego ataku cyberterrorystycznego mieści się w sferze rzeczywistości i należy podjąć wszelkie środki, aby temu

zapobiec. Biorąc pod uwagę, że terroryzm jest zwykle „lewą ręką" suwerennych mocarstw, cyberterroryści są wirtualnymi urzędnikami służby cywilnej, którzy są tak wyszkoleni i równie dobrze wykwalifikowani, jeśli nie więcej, niż uprawnieni agenci ścigania, którzy ich ścigają. Terroryzm w cyberprzestrzeni jest w powijakach, a jego działania w końcu przyćmią działania fizyczne.

Cyberszpiegostwo

Dzięki cyberprzestrzeni szpiegostwo stało się mniej niebezpieczne i bardziej satysfakcjonujące w wielu przypadkach jest to „jedna z najbardziej rozpowszechnionych aktywności cybernetycznych". Organizacje ze względu na wygodę dostępu i pozorną opłacalność bardzo często korzystają z Internetu jako intranetu. W związku z tym dane są narażone na nielegalny dostęp i często są narażone na szwank. Organizacje czasami ustawiają doniczki z miodem, aby zwabić cyberprzestępców i ujawnić ich cyberpochodzenie. Honey pot to termin określający bezpieczeństwo sieci używany w odniesieniu do plików zawierających fałszywe informacje , umieszczone na stronie internetowej w celu wprowadzenia w błąd szpiegów i ujawnienia ich adresu IP. Takie szpiegostwo może mieć charakter polityczny, wojskowy, przemysłowy, handlowy lub osobisty w celu uzyskania informacji w sposób nielegalny lub nieupoważniony. Upubliczniono, że szpiegostwo cybernetyczne po cichu szpiegowało oficjalne zapisy kilkudziesięciu krajów i organizacji, a ingerencje miały miejsce w latach 2006–2011. Kraje rozciągały się od Stanów Zjednoczonych po Wietnam, a wśród organizacji były komitety igrzysk olimpijskich. Zaskakujące było to, że cyber szpiegostwo było dziełem jednego komputera. Zostało to potwierdzone, gdy wszystkie adresy IP ofiar cyberprzestępców zostały przeciwdziałane. Szpiegostwo gospodarcze rośnie, ponieważ wykorzystanie takich informacji może przynieść duże zyski prawne. Zazwyczaj cyberszpiegostwo nie używa haseł, ponieważ takie informacje są trudne do uzyskania, jeśli w ogóle. Cyber-szpiegostwo zaczyna się od wysłania e-maila do powiernika poufnych informacji, takiego jak dyrektor generalny firmy, od nadawcy, który podszywa się pod renomowaną i zaufaną organizację. Wiadomość e-mail zawiera załącznik. Odbiorca, nie podejrzewając oszustwa, wykonuje załącznik, który wyświetla raczej przydatną lub interesującą informację. Podczas wykonywania załącznika na komputerze odbiorcy instalowane jest złośliwe oprogramowanie, które zapewnia nadawcy pełny dostęp do komputera odbiorcy. Mając takie przywileje, nadawca nie tylko przeszukuje komputer, ale również uzyskuje dostęp do stron internetowych, które wymagają nazw użytkowników i haseł, które zwykle pozostawiają cyberprzestępcom dla wygody, zamiast wpisywać je za każdym razem, gdy potrzebują dostępu do poczty e-mail lub innych usług. Szpiegostwo uznano za akt nieprzyjazny, ale nie za akt wojny, podobnie cyberszpiegostwo będzie „tolerowane", co będzie miało konsekwencje dyplomatyczne, a nie działania wojenne. Jednak po rozpoczęciu otwartych działań wojennych między dwoma przeciwnikami cybernetyczne działania wojenne i szpiegostwo cybernetyczne z pewnością nadejdą, jeśli jeszcze nie zostaną wprowadzone.

Bezpieczeństwo wewnętrzne

W Stanach Zjednoczonych, aby zająć się kwestiami bezpieczeństwa innymi niż obrona wojskowa, powołano rządowy departament, 25 listopada 2002 r. Ustawą o bezpieczeństwie wewnętrznym z 2002 r. „Departament Bezpieczeństwa Wewnętrznego [DHS] ma ważną misję: zabezpieczyć naród przed wieloma zagrożeniami… [w tym] cyberbezpieczeństwem…. [Obowiązki] są szerokie, ale nasz cel jest jasny - zapewnienie Ameryce bezpieczeństwa ". DHS został początkowo utworzony przez przeniesienie, z innych departamentów rządowych, różnych agencji, które były bezpośrednio lub pośrednio odpowiedzialne za bezpieczeństwo wewnętrzne kraju

National Cyber Security Division

W ramach DHS działa National Cyber Security Division (NCSD), którego misją jest współpraca „z podmiotami publicznymi, prywatnymi i międzynarodowymi w celu zabezpieczenia cyberprzestrzeni i amerykańskich zasobów cybernetycznych” . Strategią jest

• Zbudowanie i utrzymanie skutecznego krajowego systemu reagowania w cyberprzestrzeni

• Wdrożenie programu zarządzania ryzykiem cybernetycznym w celu ochrony infrastruktury krytycznej

DHS-NCSD jest gospodarzem Zespołu ds. Gotowości na wypadek awarii komputera w Stanach Zjednoczonych (US-CERT), który dostarcza biuletynów bezpieczeństwa związanych z cybernetycznymi, alertów bezpieczeństwa technicznego oraz wskazówek bezpieczeństwa, a także cennych informacji o wydaniach dotyczących luk w zabezpieczeniach dużego oprogramowania. US-CERT jest także miejscem zgłaszania incydentów związanych z cybernetycznymi [28]. Uznając, że nie ma czasu do stracenia, NCSD „agresywnie dąży do zbudowania światowej klasy zespołu ds. Bezpieczeństwa cybernetycznego, a my koncentrujemy się na kluczowych priorytetach, które dotyczą ludzi, procesów i technologii” . Jedną z dyrekcji DHS jest Dyrekcja ds. Nauki i Technologii, która wspiera programy promujące świadomość w zakresie bezpieczeństwa cybernetycznego i zwiększone możliwości zarówno w sektorze publicznym, jak i prywatnym. W ramach tej dyrekcji działa Centrum Badań i Rozwoju w zakresie bezpieczeństwa cybernetycznego, które zapewnia kierunek przyszłych badań i rozwoju w zakresie bezpieczeństwa cybernetycznego. Działalność centrum obejmuje również zapobieganie cyberprzestępczości, bezpieczeństwo sieci bezprzewodowej, niezawodność i integralność systemu nazw domen (DNS) oraz współpracę z innymi zainteresowanymi agencjami rządowymi agencjami. DNS to tablica serwerów rozproszonych na całym świecie z bazami danych, które przekształcają nazwy domen, takie jak www.xyz.com, na adresy IP, takie jak 34.167.86.94. W przypadku zaatakowania tych serwerów cyberprzestrzeń oparta na www upadnie. Utrzymywanie pamięci podręcznej DNS na komputerze może sprawić, że surfowanie będzie szybsze i mniej zależne od serwerów DNS. Pamięć podręczna DNS to dwupolowa baza danych obsługiwana na komputerze PC, która ma nazwy domen i odpowiednie adresy IP odwiedzanych stron internetowych.

Gotowość do cyberbezpieczeństwa

NCSD sponsoruje różne działania i inicjatywy mające na celu poprawę umiejętności i możliwości cyberobrony. Dwie główne to

• Cyber Storm. Jest to odbywające się co dwa lata ćwiczenie w zakresie cyberobrony, które przyciąga międzynarodowy udział i gdzie testowane są nowe umiejętności w zakresie cyberobrony. Pierwsze ćwiczenie Cyber Storm miało miejsce w 2006 r. Dzięki tym ćwiczeniom ocenia się gotowość do reagowania na incydenty cybernetyczne, a także wymianę informacji i koordynację między partnerami. Uczestnikami Cyber Storm w 2010 r. Były inne agencje rządowe USA, stany w ramach związku, liczne kraje i wiele organizacji sektora prywatnego. Cyber Storm IV ma się odbyć w 2012 roku.

• Krajowy system ostrzegania cybernetycznego. Ten program zwiększa świadomość zaniepokojonych mieszkańców cyberprzestrzeni na temat aktualnych zagrożeń i słabości w cyberprzestrzeni. Zainteresowane osoby mogą się zarejestrować [30], aby otrzymywać comiesięczne aktualizacje, a także biuletyny, dotyczące stanu bezpieczeństwa cybernetycznego. Główne inicjatywy są następujące:

• Alerty bezpieczeństwa cybernetycznego - techniczne

• Alerty bezpieczeństwa cybernetycznego - nietechniczne

• Biuletyny bezpieczeństwa cybernetycznego

• Wskazówki dotyczące bezpieczeństwa cybernetycznego

• Uwagi o luce w zabezpieczeniach

• Aktualna działalność

Subskrypcja systemu powiadomień jest bezpłatną usługą publiczną świadczoną przez DHS, a kilka tysięcy subskrybentów korzysta z tych miesięcznych powiadomień.

Wyzwania związane z bezpieczeństwem w cyberprzestrzeni

Każda agencja rządowa odpowiedzialna za bezpieczeństwo cyberprzestrzeni stoi przed licznymi wyzwaniami, które można podzielić na społeczne, gospodarcze, technologiczne i polityczne. Społeczeństwo oczekuje, że władze zapewnią bezpieczeństwo w sposób przejrzysty, skuteczny, skuteczny i w żaden sposób nie narusza wolności obywatelskich, zwłaszcza prawa do prywatności i prawa do wyrażania własnej opinii.

Bardzo ważnym czynnikiem w walce z przestępczością jest możliwość spojrzenia w przeszłość. Zdolność do wyszukiwania danych i wydobywania cennych informacji dotyczących kryminalnych nie może zostać zastąpiona informacjami z okresu po popełnieniu przestępstwa. Jednak przechowywanie zapisów cybernetycznych we wszystkich obszarach, na wypadek gdyby cyberprzestępca mógł popełnić przestępstwo w ciągu najbliższych pięciu lat, nie powinno być dopuszczalne w wolnym społeczeństwie. Socjologowie i prawodawcy zawsze będą mieli wyzwanie w dążeniu do znalezienia właściwej równowagi między prawami obywatelskimi a bezpieczeństwem, równowagi, która podlega normom społecznym, które ewoluują wraz z technologią. W związku z tym polityka bezpieczeństwa cybernetycznego może być kompletna tylko wtedy, gdy ma odpowiednią „ocenę wpływu na prywatność". Nie ma przedsięwzięcia, które nie byłoby ekonomicznie trudne. Fundusze trafiające do dowolnego sektora, czy to cyberbezpieczeństwa, czy upiększania ulic, muszą konkurować z wymaganiami innych sektorów. Chociaż więcej zasobów spowoduje lepsze bezpieczeństwo cybernetyczne, odpowiedzialni menedżerowie będą musieli przeprowadzić własną akcję równoważenia, rozkładając dostępne zasoby między różne podsektory bezpieczeństwa cybernetycznego, mając nadzieję na maksymalizację ogólnego bezpieczeństwa. Dzięki „kwantyfikacji wartości ekonomicznej bezpieczeństwa i pewności" menedżer może najlepiej obliczyć zwrot z inwestycji w bezpieczeństwo cybernetyczne. Biorąc pod uwagę, że cyberbezpieczeństwo wymaga wysoko wykwalifikowanych cyber wojowników lub cyberobrońców, dostępne fundusze mogą odegrać zasadniczą rolę w programach edukacyjnych i specjalistycznych szkoleniach, a ciągłe kształcenie jest kamieniem węgielnym sukcesu. Ważnym wyzwaniem w ramach cyberekonomii są wskaźniki bezpieczeństwa cybernetycznego. Metryki są wynikiem uzyskanym po przetworzeniu powiązanych pomiarów. Wyzwanie polega na tym, jakie powinny być pomiary i jak należy przetwarzać wyniki. Zarządzanie przedsiębiorstwem i administracja rządowa nie wahają się zatwierdzać środków na bezpieczeństwo cybernetyczne, ale ponieważ same nie są technikami, szukają namacalnego, choć parametrycznego sposobu pomiaru zwrotu z inwestycji. Pomiar skuteczności lub skuteczności środka bezpieczeństwa, który stał na straży, ale nigdy nie został skonfrontowany, jest wyzwaniem samym w sobie. W kontekście cyberprzestrzeni odpowiedź na pytanie: czy jesteśmy wystarczająco bezpieczni? zawsze jest nie. Wynika to z faktu, że sieć jest nie tylko narażona na znane i nieznane zagrożenia cybernetyczne, ale każdy członek organizacji poprzez surfowanie, wysyłanie e-maili i tworzenie sieci społecznościowych stwarza dodatkowe podatności, przed którymi środki bezpieczeństwa cybernetycznego przedsiębiorstwa nie muszą koniecznie chronić. Oznacza to, że „stopień zrozumienia problemów bezpieczeństwa wśród użytkowników komputerów" w organizacji jest głównym czynnikiem w ocenie poziomu cyberbezpieczeństwa w systemie. Efektywne wykorzystanie technologii jest najważniejszym czynnikiem w praktycznie każdym sektorze, zwłaszcza w cyberbezpieczeństwie. Internet jest bardzo złożonym systemem, a identyfikacja źródła cyberataku może nie zawierać

marginesu błędu. Wyzwanie polega na opracowaniu ergonomicznego bezpieczeństwa cybernetycznego; oznacza to, że wykorzystuje zautomatyzowane procesy i procedury, które najlepiej wspierają specjalistów w ich misji. Po absolutnym zidentyfikowaniu źródła cyberataku wyzwaniem politycznym jest jego sklasyfikowanie. Taka klasyfikacja może wahać się od uciążliwych do cyberwarfare, ze wszystkimi powiązanymi konsekwencjami. W większości przypadków odwet będzie dokonywany raczej w naturze niż w innym trybie.

Rozproszona obrona

Ponieważ cyberprzestrzeń staje się integralną częścią praktycznie każdego aspektu współczesnego życia, zagrożenia dla jej bezpiecznego i niezawodnego działania rosną. Dzięki kryptografii zawartość komunikacyjna jest stosunkowo bezpieczna, a szybkie dostarczanie komunikacji może być utrudnione przez ataki typu „odmowa usługi" (DoS). Cyber-antimalware skutecznie chroni przed wirusami. Jednak ataki DDoS wydają się pozostawać poza kontrolą. Takie ataki przychodzą w dużych seriach tysięcy żądań, które przytłaczają możliwości obliczeniowe hostów internetowych. Zazwyczaj tak się dzieje

• Poprzez powtarzające się żądania, które obezwładniają zasoby serwera, atakują serwery, sieć lub urządzenia końcowe

• Poprzez wstrzyknięcie fałszywych komunikatów, takich jak komunikaty o połączeniach, rozłączeniach lub błędach, które dezorientują operacje serwera.

Internet nie został zaprojektowany z myślą o cyberprzestępcach i jest całkowicie podatny na wyrafinowane ataki DDoS, które stały się główną troską wszystkich funkcjonariuszy ds. Bezpieczeństwa cybernetycznego. Bardzo zaniepokojeni są także opiekunowie serwerów DNS. Nasycenie lub nieprawidłowe działanie takich serwerów spowoduje niedostępność tysięcy stron internetowych. Ataki DDoS zwiększały częstotliwość i siłę, osiągając poziom blisko 50 Gb / s w jednym ataku.

Środki zaradcze w zakresie cyberbezpieczeństwa

Środki zaradcze DDoS rozpoczynają się od wykrycia potencjalnego ataku, następnie oceniają potencjał ataku, a kończą koniecznymi działaniami, które należy podjąć. Takie działania obejmują opóźnienie lub odrzucenie podejrzanych pakietów oraz, jeśli to możliwe, powiadomienia węzłów internetowych do przodu i do tyłu o podejrzeniu ataku DDoS. Zwiększona prędkość sieci w połączeniu z równie zwiększonym rozmiarem pamięci i pamięci komputera pozwala teraz na włączenie zaawansowanych algorytmów w węzłach sieci, w których można monitorować, oceniać i kontrolować ruch. W ten sposób „funkcje bezpieczeństwa są wbudowane w urządzenia cybernetyczne w sposób, który pozwala na koordynację działań zapobiegawczych i obronnych w obrębie społeczności urządzeń i pomiędzy nimi". Wdrożenie takich algorytmów w węzłach internetowych może wspólnie stworzyć system prognozowania ruchu, w którym serwery docelowe będą informowane o zbliżającym się ruchu, jego natężeniu i, co równie ważne, jego pochodzeniu. Obecnie nie ma takiego systemu. Trwają jednak znaczące badania, które wskazują na potrzebę opracowania SCADA przez Internet. Każdy internetowy system SCADA musi mieć ściśle określony zakres, mierzalną skuteczność, możliwą do kontrolowania złożoność oraz praktyczną skalowalność, koncentrując się na wczesnym ostrzeganiu typu wykrywania DoS

Ekosystem Cyberobrony

Liczne działania badawcze w zakresie cyberobrony wskazują na jeden konkretny kierunek, to znaczy stworzenie specjalnego oprogramowania sztucznej inteligencji , które zostaną osadzone w każdym węźle internetowym, gdzie będą zbierać informacje o ruchu. Wspólnie i we współpracy ze sobą, takie

oprogramowanie będzie służyć jako SCADA internetowa, która będzie w stanie wykrywać potencjalne ataki DoS i zapobiegać im.

Obecnie Internet jest jedynie globalną siecią połączonych routerów, które ułatwiają kompleksową komunikację między klientami internetowymi a serwerami internetowymi, bez żadnego potencjału cyberbezpieczeństwa. Zarządzając tym ruchem, węzły internetowe uzyskują dostęp do danych, które łącznie mogą dać najbardziej cenne informacje. Na podstawie ocen statystycznych i innych obserwacji pakietów, internetowy SCADA - ekosystem cyberobrony - będzie w stanie monitorować powiązany ruch i dynamicznie ustalać kryteria, które będą w stanie rozpoznać podejrzane ataki DDoS. Wszystkie usługi wspierane technologią mają minimalny rozmiar i funkcjonalność i stopniowo stają się potężnymi i użytecznymi zasobami społecznościowymi. Podobnie Internet zaczął się jako platforma do wysyłania wiadomości tekstowych i stał się integralną częścią życia każdego. Obecnie poziom funkcjonalności węzłów internetowych można porównać do poziomu telefonów komórkowych z lat 90. - minimalnego i inteligentnego. W przypadku węzłów internetowych następnym krokiem jest wyjście poza etap przekazywania pakietów i wspólne stworzenie infrastruktury, która wspiera bezpieczeństwo serwera i ładuje projekcje, przynajmniej na początek. Jako system, węzły internetowe są niewykorzystanym zasobem. Po wprowadzeniu do nich danych wywiadowczych dotyczących bezpieczeństwa powstanie ekosystem cyberobrony.

Szkolenie w zakresie cyberbezpieczeństwa

Szkolenie w zakresie bezpieczeństwa cybernetycznego jest obowiązkiem wszystkich osób, które je ujawniają, ich komputery do cyberprzestrzeni. Stopień szkolenia będzie się różnić w zależności od zaangażowania. Jeśli spojrzymy na dwa końce spektrum, widzimy użytkowników cyberprzestrzeni z jednej strony i specjalistów ds. Cyberbezpieczeństwa na drugim końcu. Użytkownicy cyberprzestrzeni ponoszą odpowiedzialność za siebie i społeczność cyberprzestrzeni za utrzymanie zdrowego komputera, wolnego od złośliwego oprogramowania, które może infekować innych za pośrednictwem cyberprzestrzeni. Co najmniej komputer musi mieć aktywne oprogramowanie antywirusowe, które sprawdza każdy plik przed jego otwarciem lub zainstalowaniem na komputerze. Użytkownicy cyberbezpieczeństwa muszą mieć świadomość bezpieczeństwa, zwłaszcza, że dotyczy to akceptacji plików i aplikacji z nieznanych źródeł, ponieważ akceptacja użytkownika może zastąpić zaporę ogniową lub program antywirusowy w celu ochrony komputera. Tę świadomość należy wzmocnić poprzez częste seminaria - seminaria internetowe, jeszcze lepsze - oraz wiedzę na temat ryzyka związanego z sieciami społecznościowymi. Specjaliści ds. Cyberbezpieczeństwa muszą mieć szerokie spektrum umiejętności i wiedzy specjalistycznej, koncentrując się na co najmniej jednej specjalizacji. Specjaliści od cyberbezpieczeństwa wybrali karierę, która charakteryzuje się intensywnym uczeniem się przez całe życie i monitorowaniem prawodawstwa technologicznego.

Cyber-symulacja i ćwiczenia

Duża ilość zasobów jest stale przeznaczana na cyberbezpieczeństwo i potężne twierdzenia co do poziomu gotowości. Nie ma jednak wiarygodnych danych pozwalających ocenić i skalibrować siłę cyberobrony. Nie było prawdziwej cyber wojny, która przetestowałaby możliwości obronne i ofensywne potencjalnych przeciwników. Zamiast tego istnieje możliwość symulacji cyber wojny. Przez lata przeprowadzano symulacje przy użyciu dużych tablic cyber hostów - komputerów - i serwerów. Botnetowanie dużej liczby hostów w celu bombardowania określonego serwera i utworzenia DoS nie jest łatwym atakiem. Na szczęście było oprogramowanie do symulacji cyberwojennego opracowania, które mogą naśladować ataki w milionach. Biorąc pod uwagę zależność nowoczesnego społeczeństwa od Internetu,i jak „cyberwojna jest subtelna i dewastująca” , rządy były bardzo zaniepokojeni lukami w sieci. W rezultacie cyberćwiczenia są ważnymi mechanizmami przeprowadzanymi w celu]

• Oceń środki gotowości w stosunku do

• Cyber-zagrożenia

• Klęski żywiołowe

• Awarie technologii

• Umożliwić organom zaradzenie określonym słabościom

• Zwiększenie współpracy między odpowiednimi zainteresowanymi stronami

• Zidentyfikuj współzależności

• Stymuluj planowanie ciągłości

• Trenuj i edukuj ludzi

• Stwórz poziom pewności co do cyberbezpieczeństwa

Cyber ćwiczenia wymagają obszernych

• Planowanie ataków i kontrataków, fałszowania i włamań, zakłóceń i degradacji

• Testowanie [oceny] różnych strategii i taktyk ograniczania szkód, identyfikowania słabych punktów i tworzenia redundancji

• Szkolenie personelu w zakresie rozpoznawania problemów oraz skutecznego dostosowywania się i reagowania

• Cyber Endeavour, rząd USA, przemysł i środowisko akademickie

• Cyber Storm, międzynarodowe ćwiczenie zorganizowane przez Stany Zjednoczone

• Cyber Europe, ćwiczenie regionalne zorganizowane przez Unię Europejską

Cyber Endeavour to coroczne wydarzenie organizowane przez podmioty wojskowe rządu Stanów Zjednoczonych, które „zapewnia oddolną, poziom pracy i środowisko dla operatorów, myślicieli i praktyków, aby wspólnie dyskutować i identyfikować potencjalne rozwiązania najbardziej krytycznych, palących wyzwań cybernetycznych oraz zestawy problemów stojące przed… ”cyberbezpieczeństwem. Wydarzenie obejmuje Sympozjum Cyber, Cyber Gry i Konkursy oraz Cyber Wystawy. Cyber Storm jest ćwiczeniem cybernetycznym, które odbywa się co dwa lata od 2006 roku. Jest organizowane przez National Cyber Security Division Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych i zapewnia ocenę gotowości Stanów Zjednoczonych na wypadek wojny cybernetycznej. Uczestniczą w nim organizacje sektora publicznego i prywatnego, a także podmioty międzynarodowe [39]. Cyber Europe to pierwsze europejskie ćwiczenie cyberbezpieczeństwa, którego celem było stworzenie społeczności cyberobrony wśród członków państwa. Uczestniczyło w nim siedemdziesiąt organizacji sektora publicznego z dwudziestu dwóch krajów, a niektóre dodatkowe uczestniczyły jako obserwatorzy. Ćwiczenie zostało zorganizowane przez Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA), agencję Unii Europejskiej. Jednym z zaleceń było, aby takie ćwiczenia odbywały się również na poziomie krajowym w celu zdobycia doświadczenia i wiedzy specjalistycznej [40]. Wspólne cele ćwiczeń były następujące

• Twórz, testuj i ulepszaj zasady i procedury komunikacyjne dla różnych scenariuszy cyberataków

• Zidentyfikuj obszary wymagające poprawy i oceń wartość polityki zagadnienia

• Oceń mechanizmy wymiany informacji

• Zidentyfikuj krytyczne współzależności między infrastrukturą cybernetyczną a fizyczną

• Zwiększenie świadomości roli cyberbezpieczeństwa w bezpieczeństwie narodowym i gospodarce

• Rozwijanie znajomości dostępnych narzędzi i technologii dla cyberbezpieczeństwa

Informacje o działaniach wojennych w obszarze informacji o działaniach wojennych W wojnie informacyjnej najcenniejszą informacją o działaniach wojennych jest wiedza o istnieniu luk w zabezpieczeniach zero-day. To znaczy, wiedząc, jakie dziury istnieją w cyberprzestrzeni przeciwnika i jak zadać maksymalne obrażenia poprzez ich wykorzystanie. Jest już stara wiadomość, że każde ministerstwo obrony narodowej ma dział walki cybernetycznej, a każde ministerstwo spraw zagranicznych ma dział cyberinformacji. Obecnie jest otwarte, że cyberwojna wojna jest rzeczywistością. 20 stycznia 2017 r. Strona internetowa Białego Domu opublikowała: „Cyberwarfare to nowe pole bitwy i musimy podjąć wszelkie środki, aby zabezpieczyć nasze tajemnice i systemy bezpieczeństwa narodowego. Priorytetem dla nas będzie rozwój defensywnych i ofensywnych zdolności cybernetycznych w naszym amerykańskim Cyber Command oraz rekrutacja najlepszych i najbystrzejszych Amerykanów, którzy będą służyć w tym kluczowym obszarze.

Ta publikacja w witrynie mówi światu, aby zrobiła to samo. Różnica między umowami o wojnie konwencjonalnej a umowami o nierozprzestrzenianiu polega na tym, że rozmiary sił zbrojnych i zdolności są dobrze znane lub można je rozsądnie oszacować. Dokładniej mówiąc, nie można poznać wielkości siły cybernetycznej w kraju lub siły informacyjnej, ponieważ cyberwojna jest ograniczona do cyberprzestrzeni, czyli przestrzeni internetowej, natomiast w wojnie informacyjnej cała przestrzeń elektroniczna jest uwzględniona.

Fałszowanie sygnałów GPS, które może wprowadzać w błąd działania wspierane przez GPS, takie jak nawigacja, jest potężnym środkiem obronnym przeciwko dronom wroga. Doskonałym przykładem jest to, że „[rząd] Iranu ogłosił, że amerykański bezzałogowy samolot, wykryty w irańskiej przestrzeni powietrznej, został zestrzelony przez jednostkę cyberwojną stacjonującą w pobliżu Kaszmaru i sprowadzony z minimalnymi uszkodzeniami". Na poziomie stanu cyberbezpieczeństwo nie jest tak bardzo zagrożone przez samouków cyberprzestępców i cyberterrorystów, ale przez dobrze finansowanych, dobrze wykształconych i dobrze wykwalifikowanych sponsorowanych przez państwo cyber-aktorów. W rezultacie „… istnieje pilna potrzeba, aby wszystkie sektory i rządy (w celu stworzenia państwowego podmiotu cyberobrony / przestępstwa) zapobiegały cyberatakom, wykrywały je, odzyskiwały i broniły się przed nimi. Przy tworzeniu państwowego podmiotu cyberobrony / przestępstwa istnieją cztery główne wyzwania, a mianowicie:

• Jak odróżnić misję nominalną od prawdziwej misji przedsięwzięcia.

• Jak określić najbardziej efektywny jakościowo i ilościowo rozmiar i struktura.

• Jak przyznać mu autonomiczny, ale uzasadniony autorytet

• Jak wybrać agencję rządową, w której ma być, bez naruszania istniejącej wewnętrznej równowagi politycznej władzy w kraju. Główną różnicą między wojną konwencjonalną a cyberwoją jest to, że w wojnie konwencjonalnej napastnicy i ich lokalizacje są dobrze identyfikowalne, podczas gdy w wojnie cybernetycznej praktycznie niemożliwe jest ustalenie lokalizacji lub tożsamości atakującego.

Opracowanie krajowej strategii na rzecz bezpieczeństwa cybernetycznego

Gdy cyberprzestrzeń narzuciła się światu, rządy uznały jej nieunikniona dominacja i jedna po drugiej uświadomiły sobie potrzebę opracowania krajowej strategii bezpieczeństwa cybernetycznego. To musi być strategia, która się równoważy na potrzeby ochrony krajowej i ochrony praw obywatelskich. Mianowicie prawa obywateli do wypowiedzi i prawa obywateli do prywatności. Ponadto należy przyjąć, że nie będzie absolutnej ochrony i że strategia ta będzie musiała zostać zaktualizowana w miarę ewolucji społeczeństwa i technologii. Ogólnie rzecz biorąc, taka strategia powinna obejmować:

* Stwórz grupę roboczą ds. Bezpieczeństwa cybernetycznego ze scentralizowanym zespołem wsparcia w sytuacjach kryzysowych, służącym jako zaufany punkt kontaktowy i jako krajowy koordynator ds. Cyberprzestrzeni.

* Ustanowienie programu edukacyjnego dotyczącego świadomości w zakresie bezpieczeństwa cybernetycznego, rozpowszechnianie najlepszych praktyk w zakresie bezpieczeństwa cybernetycznego i budowanie kultury bezpieczeństwa cybernetycznego

* Zbuduj bezpieczną i niezawodną agencję rządową udostępniającą informacje w cyberprzestrzeni.

* Daj obywatelom i organizacjom możliwość wniesienia wkładu w dialog krajowy.

* Wyszczególnij narodowe priorytety, zasady, polityki i programy.

* Określ role i misje każdej zaangażowanej agencji rządowej i organizacji pozarządowej.

* Określ cele, kamienie milowe i wskaźniki, aby mierzyć i komunikować zakres postępów w rozwiązywaniu problemów.

* Wspieranie międzynarodowej współpracy w zakresie bezpieczeństwa cybernetycznego.

Podobnie jak w przypadku każdej współczesnej strategii, każda krajowa strategia bezpieczeństwa cybernetycznego musi rozpoznać odpowiednie potrzeby i wskazać drogę ,że należy się tym zająć. W takim przypadku strategia musi spełniać następujące zasady:

* Oparte na ryzyku. Cyberprzestrzeń jest pełna różnych rodzajów ryzyka.

* Modelowanie zagrożeń. Zajmij się wszystkimi możliwymi zagrożeniami, niech to będzie cyberprzestępczość lub szpiegostwo.

* Zorientowany na wyniki. Wyartykułuj i skup się na pożądanym wyniku końcowym.

* Priorytetowo. Ustal jasne priorytety wśród celów strategii.

*Pełen szacunku. Obejmują ochronę prywatności i swobód obywatelskich.

Chociaż w wielu krajach przyjęto narodową strategię bezpieczeństwa cybernetycznego, Austria przyjęła „samoregulację" w celu zachęcania sektora prywatnego do ustanowienia własnych standardów w zakresie bezpieczeństwa cybernetycznego, a państwo tworzy niezbędne ramy regulacyjne. Podsumowując, celem krajowej strategii bezpieczeństwa cybernetycznego jest służyć jako centralny punkt obrony narodu przed tym niewidzialnym, choć realnym zagrożeniem dla interesów narodowych kraju.