

Framework MITRE Attack

[00:00:07]

Prowadzący: Cześć. Witam wszystkich słuchaczy w kolejnym odcinku naszego podcastu. W tej audycji z moim gościem przeniesiemy się na plan filmu albo jak ktoś woli, do dobrego kryminału. Wyobraźmy sobie detektywów na miejscu zbrodni. Macie to przed oczami, to teraz patrzcie jak ci detektywi szukają śladów, a następnie je analizują. Ich praca poparta doświadczeniem i narzędziami, którymi dysponują pomaga im z tą analizą. To z kolei powoduje, że przestępca może być szybko rozpracowany, a jednocześnie techniki przestępcze mogą zostać udaremnione, dzięki pewnym wzorcom. I właśnie o tym dzisiaj będziemy rozmawiali. Przedstawiam bohatera dzisiejszego odcinka – Framework MITRE Attack, model, który nawiązuje i bada najbardziej zaawansowane przypadki ataków sieciowych, które mają krytyczne znaczenie z punktu widzenia bezpieczeństwa geopolitycznego, gdyż są wynikiem aktywności ośrodków państwowych cybermocarstw. Wracając do mojego dzisiejszego gościa – Mirosław Maj, osoba niezwykle zasłużona dla cyberbezpieczeństwa w naszym kraju, ale nie tylko w naszym kraju, wieloletni kierownik CERT Polska, prezes Fundacji Bezpieczna Cyberprzestrzeń, współzałożyciel i wiceprezes ComCERT SA, wykładowca na wielu uczelniach, ekspert Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA). Aktywnie uczestniczył w powstawaniu CERT-ów w Polsce i za granicą. Ale to tak naprawdę tylko część jego aktywności. Mirku, bardzo miło mi Cię dzisiaj gościć.

Mirosław Maj: Cześć. Dziękuję za zaproszenie.

Prowadzący: Mirku, zanim przejdziemy do tematu, który nam dzisiaj przyświeca, chciałbym trochę rozwinąć, czym tak naprawdę zajmuje się MITRE. Bo z mojej perspektywy to organizacja taki totalny kombajn, tak, począwszy od cve, czyli opisu podatności, wielu narzędzi, które mają dać w ręce oręż przed cyberprzestępcami, najróżniejszymi badaniami, do tego organizacja non-profit. Co jeszcze warto dodać w tym temacie?

Mirosław Maj: Ja myślę, że to już wystarczy, ale rzeczywiście MITRE to jest taki kombajn, który akurat w obszarze, o którym dzisiaj rozmawiamy, w cyberbezpieczeństwie ma bardzo duże dokonania. Historycznie też ma duże doświadczenia, no bo MITRE, no to pamiętajmy o tym, że powinniśmy też kojarzyć z samym MITem, czyli zdaje się, że chyba najstynniejszą historycznie uczelnią zajmującą się technologiami informatycznymi, z którą ja zawsze kojarzę też taką, już do oporu ten przykład przywołuję z 1988 roku, takiego robaka – Morris Worm, który dla mnie osobiście o tyle jest ważny w tej historii cyberbezpieczeństwa, że był powiązany z powstaniem pierwszego CERT-u na świecie. A CERT-y to jest taka rzecz, która jest mi bardzo bliska, w czym się zawodowo specjalizuję. No i właśnie ten Morris Worm miał miejsce swoje, swoje źródło, właśnie na MIT. A dzisiaj MITRE w obszarze, w

którym najczęściej jest kojarzony właśnie, może nie wszyscy nawet kojarzą, że chodzi tutaj o ośrodek badawczy z MITu. To jest matryca MITRE Attack, tak. I to jest bardzo ciekawy projekt, który moim zdaniem, warto o nim rozmawiać, warto się nim zajmować i go wykorzystywać, bo w bardzo praktyczny sposób zaimplementował badania, tak. Czyli mamy tutaj jakby początek i źródła, fundamenty z uczelni, z ośrodka researchowego, a to co wytworzyło się, to jest bardzo, bardzo praktyczna rzecz. I to jest o tyle ważne, że no generalnie jest problem znany taki, prawda, czy wszystkie badania, które są robione w różnych miejscach później się zamieniają w coś praktycznego. Ci, którzy obserwują na przykład, nie wiem, projekty europejskie też mogą mieć swoje zdanie na temat tego, na ile te wszystkie euro wydane w tych projektach rzeczywiście później kończą się praktycznymi implementacjami, z których możemy korzystać i pewnie te statystyki nie wyglądają najlepiej. Natomiast, no tutaj bardzo fajnie to wygląda i zdaje się, że doczekaliśmy się takiego standardu, który, no jest już powszechnie używany i dużo wskazuje na to, że na wiele, wiele następnych lat będzie powszechnie używany w odróżnieniu do wielu innych standardów. Ci, którzy na przykład interesują się Intrusion Detection, to może pamiętają takie standardy jak IDDOF i ITF. To są standardy, które no jakby się nie sprawdziły, mimo, że miały bardzo fajne założenia, ale po prostu w praktyce nie zaistniały. A tutaj jest coś, z czego możemy korzystać.

[00:05:01]

Prowadzący: No właśnie, bezpośredni temat naszego dzisiejszego podcastu – MITRE Attack Framework. Co to tak naprawdę jest? I dlaczego warto go używać? I tutaj też no też ważny element – z jakich elementów się składa tak naprawdę?

Mirosław Maj: MITRE Attack jest zestawem takiej uporządkowanej wiedzy na temat zagrożeń, które w sieci się pojawiają i takich zagrożeń, które są najbardziej niebezpieczne. One bardzo często, zresztą pewnie dzisiaj będziemy mieli okazję jeszcze parę razy wspominać o tak zwanych grupach APT, to wyjaśnijmy sobie od razu ten skrót – Advanced Persistent Threat, czyli grupy, które w sposób bardzo systematyczny, z dużą determinacją, w sposób bardzo zaawansowany technologicznie często przez bardzo długi czas, potrafią dążyć do celu i w związku z tym, mają bardzo duże dossier swoich działań i arsenał swoich działań. Nawet moglibyśmy powiedzieć, tu wspominałeś o wątku geopolitycznym i o tym, że za takimi grupami też czynniki państwowe się kryją, więc słowo arsenał też chyba będzie na miejscu. I no MITRE attack próbuje to wszystko uporządkować, czyli powiedzieć sobie, czym tak naprawdę jest, jak zapanować nad tym wszystkim. Dlatego w związku z tym, no pojawiają się takie charakterystyczne, najważniejsze elementy z tego modelu, takie jak taktyki, techniki, czy nawet subtechniki, procedury, czy też bardzo ważne może, nieczęsto przywoływane tak zwane źródła danych - data sources. Każda z tych rzeczy, możemy sobie krótko, może nawet warto je zdefiniować, no opisuje pewne bardzo ważne rzeczy. Więc taktyki to byśmy mogli sobie jakby określić, jak próbujemy odpowiedzieć na pytanie-dlaczego ktoś coś robi? No to gdzieś powinniśmy to wiązać z taktyką, czyli jakie cele ktoś chce zrealizować, tak bo sobie założy, że ma jakiś określony cel w infrastrukturze, swoje

ofiary, no i gdzieś do tego dąży. Techniki, no to są znowu rzeczy, to są konkretne czynności techniczne właśnie, trochę masło maślane, no ale tak to jest, które są wykonywane już w infrastrukturze atakowanego, które mają doprowadzić do zrealizowania tej taktyki, tak, do osiągnięcia pewnych celów. Subtechniki, no to, to są jeszcze bardziej jakby wyspecjalizowane ujęcie tych technik, no ale generalnie to te techniki, to jest coś, co nam odpowie na pytanie – jak to zrobić, jak osiągnąć, dlaczego coś osiągamy, dlaczego próbujemy osiągnąć, to są te właśnie taktyki, później techniki – jak my chcemy to zrobić? No procedury to jest to, co kojarzymy, tak, najczęściej z procedurami. Nie ma tu co wymyślać zbyt skomplikowanych definicji, jest to zestaw po prostu czynności, które muszą być wykonywane po to, żeby w szczególności zrealizować te nasze, te czyjeś działania, tak. Ktoś realizuje te działania poprzez wykorzystywanie odpowiednich technik, w jakimś ujęciu, w jakiejś sekwencji, i to są procedury. Natomiast, myślę, że bardzo ważne, tak sobie myślę, zastanawiając się, o czym pewnie dzisiaj warto by było najbardziej porozmawiać, to są właśnie jeszcze te źródła danych. No, bo to z punktu widzenia naszego, bo zakładam, że tutaj większość słuchaczy naszego podcastu tego odcinka to jednak reprezentuje tych, którzy będą musieli się bronić przed tym wszystkim, o czym opowiadamy. No to źródła danych, no to to są te miejsca, które warto w swojej infrastrukturze posiadać, które będą naszymi takimi oczami, prawdą, i uszami na to wszystko co się dzieje. Czyli jeżeli będziemy chcieli wykryć jakąś technikę, no to będziemy musieli się zastanowić, jakie źródło danych pozwoli nam wykryć tę technikę. Więc no te kilka pojęć, jeszcze raz, taktyki, techniki, czy subtechniki, procedury i źródła danych, to są jakby najważniejsze elementy całego modelu i tymi elementami próbujemy opisać wszystko, co w modelu jest dostępne.

Prowadzący: Czyli mamy techniki, mamy taktyki. Ale cały Framework to tak naprawdę trzy macierze. To jest enterprise, to jest mobile i od jakiegoś czasu ICS, tak, jeżeli dobrze pamiętam. Czy te techniki i taktyki pomiędzy tymi macierzami tak mocno się różnią?

Mirosław Maj: No one się różnią, jeszcze tutaj do tego zestawu można dołożyć jeszcze zestaw chmurowy, tak. Jeszcze jest zestaw cloudowy, oprócz enterprise, mobile, ICS, czyli automatyka przemysłowa.

[00:10:07]

Mirosław Maj: To jeszcze zestaw jest chmurowy. No one się różnią, tak jak się różnią jakby te środowiska, prawda. Czyli jeżeli mamy na przykład środowisko mobilne, no to po prostu pewne techniki mogą być tylko tam użyte, dlatego one się pojawiają, no bo akurat ta matryca dla mobilnego środowiska, no to ona zawiera jakby różne techniki, które mogą być wykorzystywane w środowisku Android czy iOS. Znowuż jak mamy enterprise, to jest Windows, Linux i MacOS. Jak mamy chmurę, no to mamy te najbardziej popularne platformy chmurowe. No i ICS, to jest cały jakby system automatyki przemysłowej. Więc krótko mówiąc stąd te rozróżnienie, dlatego że no właśnie te elementy, w szczególności techniki używane są jakby ściśle skoordynowane, no z systemami operacyjnymi. Tak

byśmy mogli sobie chyba najogólniej powiedzieć, bo to jest chyba takie pojęcie, które będzie najbardziej, możemy je przypisać do każdego z tych środowisk. I tyle. No wiadomo, że Android jest poniekąd Linuxem, no ale jest Linuxem specyficznym, prawda. No dlatego też powstają jakby specjalne modele do zastosowania.

Prowadzący: A czy występuje jakieś połączenie pomiędzy Attack, a innymi modelami na przykład cyber kill chain Lockheed martin, czy podobnymi?

Mirosław Maj: No właściwie to fajnie, że o to pytasz, bo to historycznie myślę, że warto też sobie zdać sprawę i w ogóle jakby sobie powiedzieć o tej idei, dlaczego coś tutaj staje się popularne i od strony atakujących, i od strony broniących się, no. No więc może Ci, którzy dłużej się zajmują trochę cyberbezpieczeństwem pamiętają taki jeden ze słynniejszych chyba cyberataków historycznie, gdzieś z połowy maj/czerwiec 2011 roku, kiedy no jeden z gigantów na rynku cyberbezpieczeństwa, czyli firma RSA Security została zaatakowana. I to był atak, który ją bardzo, bardzo dużo kosztował. Tak wymiennie dużo kosztował, tak, pieniędzy. W tamtych czasach, dzisiaj to już coraz rzadziej chyba są używane, dlatego, że wszyscy głównie przeszliśmy do warstwy software'owej, prawie ze wszystkimi rozwiązaniami cyberbezpieczeństwa również. No ale, może nie tylko, tak, wiadomo, że są popularne też jakieś rozwiązania devicowe, tak i na poziomie użytkownika indywidualnego. No ale tamten czas to ja go dobrze pamiętam, bo sam korzystałem przez lata z takiego rozwiązania SecureID, takiego tokena, tak, który generował hasła jednorazowe, ważne przez, no zazwyczaj przez minutę tam można było to zmieniać, też na 30 sekund, czy wydłużać, skracać, ale to chyba zdaje się minuta była najbardziej popularna. W wyniku takiego zaawansowanego ataku na RSA Security, zaawansowanego, chociaż zaczął się bardzo banalnie i to historia też pokazuje, że pewne rzeczy się nie zmieniają. No bo on zaczął się od tego, że pracownik RSA Security dostał Excela, o nazwie zdaje się lista płac. Możemy się domyślić dalej, co nastąpiło, po otwarciu tego Excela. Ale to był tylko początek, prawda.

Prowadzący: Taka socjotechnika.

Mirosław Maj: Tak, no typowa socjotechnika, ale z zastosowaniem już elementu technicznego, tak. No bo gdzieś makro jakieś zadziałało, ale to był tylko początek, tak. I to jest ciekawe właśnie w tych ujęciach modeli zaawansowanych ataków, że no te ataki mogą długo trwać i one potrzebują czegoś właśnie, co się kojarzy z łańcuchem, z sekwencją, prawda. No jakby zdobywamy tego użytkownika pierwszego, później musimy zdobyć drugiego, czy zasób, komputer drugiego użytkownika. I tak dalej, i tak dalej. I nieraz kilka albo kilkanaście różnych przeskoków już w infrastrukturze ofiary trzeba wykonać, żeby dojść do tego ostatecznego celu. Coś, na czym atakującemu najbardziej zależy to może być baza danych, ale to niekoniecznie. To może być wykonanie jakiejś komendy, która doprowadzi do tego, że wirówki w irańskim programie atomowym zostaną jakby uszkodzone, tak.

Prowadzący: Stuxnet?

Miroslaw Maj: Tak, mówimy tutaj o Stuxnet, prawda. I tak dalej, i tak dalej. Te cele mogą być różne, natomiast ważne jest to, że są dosyć skomplikowane sekwencje ataków i stąd też to, o czym Ty wspomniałeś jest to pojęcie kill chain, czyli to, że ten łańcuch tego ataku można powstrzymać poprzez skuteczne zaatakowanie którejs z fazy tych ataków.

[00:15:14]

Miroslaw Maj: W klasycznym takim APT kill chain to mamy zazwyczaj podawanych 7 faz takiego ataku, od rekonesansu do osiągnięcia właśnie tego ostatecznego celu. Natomiast tutaj matryca MITRE ma jeszcze bardziej rozbudowane, bo zdaje się, że tam jest 12 faz różnych. Ale tak naprawdę, jak na nie popatrzymy, no to one też układają się w pewien ciąg. Być może jest pewna kumulacja niektórych faz, że gdzieś tam jakby z punktu widzenia takiego modelu prostego, to gdzieś drepczemy w miejscu, ale tak naprawdę to jest krok po kroku. I właśnie te sekwencje, wykonanie po kolei wszystkich rzeczy, sprawiają, że coś się udaje albo się nie udaje, tak. Czyli, to jest ważne, że atakujący ma jakąś procedurę, ma jakąś sekwencję i ją próbuje realizować. Ale z punktu widzenia naszego, broniących się, my też mamy pewne podpowiedzi, pod warunkiem, że poznamy te sekwencje, prawda. To próbują robić researcherzy, którzy się angażują właśnie w projekt MITRE Attack, że my próbujemy, no jakby przewidzieć te sekwencje i krótko mówiąc, doprowadzić do przerwania tego łańcucha, tak. Jeżeli uda nam się przerwać ten łańcuch to z dużym prawdopodobieństwem, no jakby nie dojdzie do najgorszych rzeczy, tak. To nie znaczy, że nie ma włamania. Zresztą, ja podaję często taki przykład, że jak gdzieś tam medialnie się dowiadujemy o tym, że ktoś się do kogoś włamał, to tak naprawdę w większości przypadków to jest dopiero początek problemu, tak. Jeżeli nie ma dobrego systemu reakcji, opartego o kompetencje, no to dopiero ten problem okazuje się, że za chwilę może urosnąć do jeszcze większej skali, takiej skali katastroficznej dla ofiar. Więc jak najbardziej jest to, wracając do tej historii, o której wspominałem, czyli ataku na RSA, no to wtedy podaje się, że jednym z celów tego ataku nie było dokładnie nawet samo RSA, tylko możliwość wykradzenia takich tych ziaren algorytmu do tych tokenów, a w rezultacie do zaatakowania bardzo poważnych instytucji, na przykład w systemie obronnym USA, takich jak na przykład Lockheed Martin, czyli dostawcy uzbrojenia. No i wtedy też pojawił się, myślę, że z mojego punktu widzenia, ja bym go nazwał nawet – kultowy artykuł na ten temat, napisany przez specjalistów z Lockheed Martin, który... Pewnie masz tam jakieś opisy do podcastu, więc będziemy mogli go wrzucić. On jest bardzo inspirujący, on dzisiaj być może jest postrzegany, jako taki bardzo teoretyczny, ale ja bym bardzo zachęcał do tego, żeby sobie, jak ktoś się zainteresuje MITRE Attack, żeby sięgnął do tych źródeł. Żeby zrozumiał czym jest tak naprawdę ten kill chain i w rezultacie gdzieś matryca MITRE Attack, jak należy na nią patrzeć, jak należy rozumować i ją wykorzystywać potencjalnie do tego, żeby radzić sobie z atakami. Bo tam na przykład jest taki bardzo fajny fragment tego artykułu, gdzie się pokazuje, że jest wiele, wiele, zdaje się tam jest wymienionych aż 7 najróżniejszych sposobów reakcji, w stosunku do zaobserwowanych zjawisk, tak. To oczywiście

tam też zahacza o teorię militarną, bo jedną z reakcji to jest zniszczenie, unicestwienie tej próby ataku, co może się wiązać jakby z kontratakiem nawet, prawda, na tego, który ten atak przeprowadzałby. Więc możemy sobie wyobrazić, że pewne z tych sposobów zachowania są jednak zarezerwowane dla na przykład czynników państwowych, które mogą według swojej doktryny na przykład przeprowadzić takie obronne działania. Wiadomo, że Amerykanie mają swoją doktrynę, określają w tym obszarze cyber, jako defence forward. No to możemy się domyślać, co oznacza forward w tym ujęciu. Więc ten związek w mojej opinii jest bardzo, bardzo bliski i on ukształtował jak widać, no bo mówimy tutaj o sytuacji sprzed mniej więcej 10 lat, ale w mojej ocenie on ukształtował, kształtował przez następne lata, a dzisiaj już chyba ukształtował i to się mocno rozwija – sposób myślenia o tym, czym są najbardziej niebezpieczne i najbardziej zaawansowane ataki, jak powinniśmy je badać i w rezultacie jak im przeciwdziałać, jak zarządzać incydentami związanymi z takimi atakami.

[00:20:09]

Prowadzący: Jednym z elementów, który bardzo często się przewija, czy to przykład atak czy różnych innych opracowań, a nawet tych opracowań tworzonych przez producentów na poczet powiedzmy, jakichś swoich produktów, szczególnie gdy mówimy tutaj o kwestiach związanych z threat huntingiem, to piramida bólu, tak zwana piramida bólu opracowana przez Davida Bianco. Piramida mająca obrazować jakby, jak dużo wysiłku atakujący musi włożyć, aby zmienić wskaźnik ataku. Jeżeli mógłbyś powiedzieć kilka słów na temat tejże piramidy, a także tego czy dotyczy ona jedynie atakujących, czy właśnie również drugiej strony barykady, aby obrazować, na czym tak naprawdę najlepiej czy najskuteczniej się skupić w przypadku obrony.

Mirosław Maj: No tak, piramida bólu to jest rzeczywiście kolejny, taki bardzo praktyczny aspekt, który w obrazowej, no bo nie ma nieobrazowej piramidy, tak, jest narysowana, można sobie ją znaleźć – piramida bólu i zobaczyć, co jest u jej podstawy i co jest na jej wierzchołku. Znowuż, to jest taki bardzo praktyczny element, który uzmysławia, co tak naprawdę jest najtrudniejsze w atakach, a jednocześnie powinno kształtować sposób obrony. No bo, jeżeli sobie spojrzymy na tę piramidę bólu, to patrząc od dołu, to u jej podstaw leżą takie elementy techniczne, tak, elementy techniczne ataku, które no są powszechnie znane. Często nawet kojarzone z czymś takim, jak mówimy sobie I was indicator of compromise, takie wskaźniki ataku, takie jak, nie wiem, wartości hash, czy adresy IP powiązane z atakiem czy nazwy domenowe. I one rzeczywiście przez wielu są używane w tym, żeby sobie kształtować swój system obronny. Ale z drugiej strony, no życie pokazuje, że sposób obrony w oparciu o takie elementy, właśnie te najbardziej podstawowe, takie elementarne, właśnie jeszcze raz te hashe, adresy IP czy domeny, jest dalece nieskuteczny. Dlatego, że to z drugiej strony są elementy, które w piramidzie bólu są na samym dole i z punktu widzenia atakującego, są najprostsze do modyfikacji, tak. Ci, którzy się interesują, nie wiem na przykład tym, jak działają botnety, tak. No to wiedzą na przykład, że bardzo często popularnymi protokołami zarządzania botnetów, to są algorytmy, które służą do

automatycznej, częstej, skutecznej zmiany adresacji domenowej, na przykład jak taki DGA Domain Generation Algorithms czy adresacji IP Fast, gdzie w zależności od ustawień, pewnie w ekstremalnej wersji można nawet liczyć to w sekundach, a już na pewno w minutach. Atakujący obiekt jest identyfikowany poprzez kompletnie inny adres IP na przykład. No i teraz sobie wyobraźmy, że próbujemy nasz system obronny ustawić w oparciu o filtrację IP, no i co się dzieje? Oczywiście no ten adres IP, który właśnie po zmaganiach z naszymi administratorami, udało nam się zaimplementować w naszej infrastrukturze, no w momencie implementacji jest już zupełnie nieważny, dlatego, że atak jest zupełnie z innego adresu IP. Więc ważne jest to, o czym wspominałeś, tak, że ta piramida bólu pokazuje, co jest proste, ale również z punktu widzenia atakującego, ale poprzez to również podpowiada, jak próbować zorganizować swój system obronny, tak. Czyli, być może nie wyrzucać kompletnie, chociaż no to zawsze trzeba przeanalizować, tych najprostszych wskaźników ataku, ale absolutnie nie można na tym spocząć, tak. To znaczy one są niewystarczające. Nieraz są konieczne, a nieraz są niekonieczne. To trudno, trzeba by było jakby dyskutować case by case. Natomiast na pewno są niewystarczające w większości, jeśli nie we wszystkich przypadkach. Na pewno we wszystkich w momencie, kiedy mówimy o zaawansowanych atakach, dlatego że, to co później, na tej piramidzie, na górze tej piramidy bólu się pojawia, to są już bardziej skomplikowane rzeczy, związane z takimi artefaktami na systemach operacyjnych, na hostach, tak, czy sieciowymi, czy narzędziami, które są wykorzystywane, czy wręcz to co też jest bardzo często kojarzone z MITRE znowu, czyli te TTP, czyli Tactics, Techniques and Procedures. To, o czym sobie wspominaliśmy, prawda. Te techniki, taktyki i procedury.

[00:25:05]

Mirosław Maj: No i okazuje się, że tutaj, znowuż powrócę jakby do tych definicji, do tych terminów takich jak sekwencja zdarzenia, gdzieś tam ten chain, czy później w rezultacie kill chain. Okazuje się, że później zamiana takiego całego sposobu działania, na przykład jakieś procedury, no to już rzecz nie jest trywialna. Dlatego, że ona jest związana z tym, że ktoś długo pracował, jakaś grupa APT długo pracowała nad tym, żeby wymyślić jakiś scenariusz. Raz, związany bardzo ściśle z infrastrukturą atakowanego, no bo nie zastosujemy techniki związanej z danym systemem operacyjnym jeśli tego systemu operacyjnego tam nie ma, prawda. No więc jeżeli my zaczniemy budować swój system obrony, który, pewnie tę budowę warto rozpocząć od systemu monitoringu, tak, czyli znowuż sięgamy do źródeł danych, tak, data sources. W oparciu o właśnie te rzeczy z górnej części piramidy bólu, no to okaże się, że jeżeli nam się uda coś zaimplementować, na przykład wyeliminować jakąś podatność, założyć dobry system monitoringu, gdyby jednak ktoś tam, coś grzebał, czy w rezultacie napisać reguły SIEMowe tak, do naszego systemu SIEM, które wykryją coś. No to okazuje się, że w tej warstwie zaczynamy być skuteczni, te ataki są dla nas mniej groźne i atakujący, żeby nam się dobrać do skóry, no muszą kompletnie, jakby od początku rozpocząć swoje dzieło, tak, to wymyślanie tego wszystkiego.

Dlatego ta piramida bólu znówuż, mimo tego, że przedstawia bardzo proste ujęcie, bardzo prosty model, ale właśnie jest bardzo, bardzo skuteczna, a może właśnie dlatego, że przedstawia prosty, tak, jak zazwyczaj mówimy, że najprostsze rzeczy są najbardziej skuteczne. No więc kolejny element, do którego warto zajrzeć i budować swoje myślenie o tym, jak organizować swój system cyberbezpieczeństwa w oparciu właśnie o to ujęcie, żeby nie spocząć na czymś, co się wydaje takie bardzo kuszące – a, będę znał adresy IP atakujących, będę znał domeny, które wykorzystują w swojej infrastrukturze albo hashe malwaru, tak. Tylko no wiemy, że to już jest historia chyba nastoletnia, że algorytmy też, które zmieniają w locie po prostu hashe poprzez obfuskację. Techniki obfuskacji malwaru sprawiają, że w ogóle malware, jeżeli byśmy tak na niego patrzyli, na przykład jako hashe, no to w większości przypadków pojawia się w sieci tylko raz. A prawda jest taka, że ten sam malware pojawia się tysiące albo setki tysięcy razy w zupełnie innej postaci z punktu widzenia jego wartości hashy.

Prowadzący: Wiesz co, tutaj właśnie poruszyłeś już powolutku ten temat, do którego ja też zmierzam, czyli właśnie jak Framework atak można wykorzystać w praktyce? I tutaj bardzo chętnie również wróciłbym do wprowadzenia i tej tezy, że model bada najbardziej zaawansowane przypadki ataków sieciowych, które mają tu krytyczne znaczenie z punktu widzenia bezpieczeństwa. Co dzięki niemu można tak naprawdę dla siebie wyciągnąć? I w jaki sposób zmapować w jakiś sposób na swoją organizację, tak żeby zobrazować potrzeby przedsiębiorstwa, biorąc pod uwagę właśnie no kwestie cyberbezpieczeństwa, biorąc pod uwagę techniki i taktyki, które tam są opisane? W jaki sposób właśnie ta organizacji może wypełnić powiedzmy swoje luki mapując na dane rozwiązania, czy na dane procedury, czy powiedzmy na dane polityki, które mogą być zaimplementowane u siebie w sieci, u siebie w organizacji?

Mirosław Maj: No i to jest właśnie bardzo ciekawa rzecz, którą można wykorzystać bardzo, bardzo praktycznie. Jak z tego skorzystać? No, spróbujmy podpowiedzieć. Pewnie, może będzie jeszcze chwila na to, żeby wspomnieć o pewnym projekcie, który my realizujemy w ComCERT, projekt badawczo-rozwojowy, ale wspominam o tym w tej chwili już dlatego, że właściwie to, co teraz będę mówił, no to jest bardzo ściśle związane z tym projektem. No otóż cała rzecz w organizowaniu tego systemu bezpieczeństwa, no to to jest zmaganie się ze znanymi historiami, typu po prostu brak zasobów. Jakkolwiek na nie nie spojrzymy, czy to są finansowe, dzisiaj bardzo często również związane z kompetencjami, w ogóle no jakby z tym, czy mamy odpowiednie kadry, czy mamy odpowiednie narzędzia, ten budżet oczywiście się przenosi na to, jaki sprzęt możemy kupić i tak dalej. Czyli krótko mówiąc, jeżeli zaczniemy korzystać w sposób taki efektywny z tego modelu, to może się okazać, że mamy fajny sposób na zoptymalizowanie naszych działań. Tak, że no zrobimy najlepsze co się da. Czyli nie będziemy, że tak powiem działali na oślep w budowaniu tego systemu cyberbezpieczeństwa. Bo teraz sobie wyobraźmy, no nawet weźmy z naszego podwórka, tak, żeby nie iść daleko. No jeżeli

jesteśmy firmą, powiedzmy z branży energetycznej w Polsce, tak, to czym my powinniśmy się zainteresować?

[00:30:07]

Mirośław Maj: No powinniśmy się zainteresować, no na przykład matrycą ICS, prawda, bo ona dotyczy automatyki przemysłowej. To jest jedno, tak. Powinniśmy się dobrze poznać, a mówię specjalnie to, bo to się okazuje, że to nie jest zadanie, że nie dlatego, że ktoś jest leniwy, ale to nie jest zadanie trywialne, poznanie, dobre poznanie swojej własnej infrastruktury. Bo to często, przy bardzo dużych strukturach IT w wielu systemach, rozległych sieciach jest bardzo, bardzo skomplikowane. I dobra ich wiedza na ten temat jest bardzo, bardzo ważna. Dlaczego musimy to poznać? No dlatego, że jeżeli będziemy to dobrze znali, no to będziemy mogli z tej matrycy wyciągnąć te techniki, które dotyczą naszej infrastruktury, żebyśmy my się nie zaczęli zajmować czymś, co no u nas się nie może zdarzyć, tak. A my będziemy nie wiem, na przykład zakupimy rozwiązania albo będziemy poświęcali czas na implementację jakichś reguł, czegośkolwiek, co w ogóle nas nie dotyczy, tak. Więc mamy kolejną odpowiedź. Jeżeli znamy dobrze środowisko swoje IT, czym my tak naprawdę powinniśmy się zająć? Co jeszcze może być odpowiedzią? No może być odpowiedzią, o tej specyfice branży już powiedziałem, tak, że na przykład, że konkretnie to jest z obszaru ICS. Chociaż no uczciwie tu musimy od razu wspomnieć, że taka branża, jak branża energetyczna, to niestety musi od razu sobie wziąć załadować obydwie matryce do roboty, tak, przynajmniej tę jeszcze matrycę enterprise. To środowisko OT nie istnieje przecież w zawieszeniu i ono w oparciu o systemy, które są w enterprise, też jest ściśle powiązanie. No ale jeszcze jest jedna, bardzo ważna rzecz, że no działamy w pewnym obszarze ryzyka i tutaj przechodzimy też do bardzo ciekawej rzeczy, która bardzo wzbudza emocje, kto to tak naprawdę robi. No to możemy sobie wyobrazić, bo to nie jest żadną tajemnicą, że są takie państwa, które szczególnie są zainteresowane innymi państwami. No i jeżeli sobie historycznie popatrzymy na to co się działo czy dzieje w Polsce, no to na pewno z matrycy MITRE od razu bym wziął na warsztat wszystkie grupy APT, gdzie są, w opisie pojawia się angielskie słowo russia albo russian, tak. I wiemy już, że grupy APT z tego obszaru state-sponsored przez Federację Rosyjską to jest coś, co jeżeli mamy ograniczone zasoby, bo najlepiej się pewnie uchronić przed wszystkimi, bo różnie to bywa, zresztą zaraz powiem o ciekawym przypadku grup z jednego państwa, które właśnie mówi o tym, że pewnie warto się zainteresować wszystkimi, no ale wróćmy do tego przykładu. No to najlepiej sobie wziąć właśnie te techniki, które są używane przez rosyjskie grupy APT i nimi na dobry początek zacząć, no i tak zapewniam, że jest dużo roboty, tak. To nie jest projekt na tydzień. Jeżeli będziemy znali swoje środowisko IT, swoją branżę, tak i zastosujemy odpowiednie matryce i sprawdzimy, kto potencjalnie ma największy interes, żeby nas zaatakować, no to już mamy tyle danych, że czeka nas dużo, dużo roboty, żeby zakończyć dobrymi regułami, z dobrym uruchomieniem monitoringu czyli źródeł danych, które są nam potrzebne, żeby mieć te oczy i uszy, a w rezultacie być może napisać też poprawne

playbooki dla naszych operatorów z SOCA albo procedury dla ludzi, którzy są na drugich i trzecich liniach w tych organizacjach. Więc znowuż widzimy jak w bardzo praktyczny sposób możemy tego użyć. No mówię też o historiach z życia wziętych, że w ten sposób no już my osobiście mieliśmy nie jeden dowód na to, że jest to fajny sposób na zoptymalizowanie różnych działań.

Prowadzący: No właśnie, do jakich zespołów najczęściej adresowany jest ten Framework? Czy korzystają z niego właśnie głównie zespoły SOC czy sytuacja wygląda inaczej? Czy jest to narzędzie, które może być stosowane i ma rację bytu również na przykład w mniejszych organizacjach, które powiedzmy nie mają tego typu jednostek bądź czasami nawet nie mają oddzielnych działów security, tylko tak naprawdę tymi kwestiami również zajmuje się szeroko pojęte IT?

Mirosław Maj: No ja jednak wiem jak wygląda realne życie, tak, w polskim środowisku, w polskich firmach. Zresztą, nie tylko polskich, żebyśmy tutaj nie stygmatyzowali w jakiś negatywny sposób. No często jest tak, że nadal IT jest pomieszane z cyberbezpieczeństwem.

[00:35:06]

Mirosław Maj: Tak specjalnie użyłem takiego pewnie o bardziej pejoratywnym, lekkim zabarwieniu słowa – pomieszane, no bo w mojej ocenie powinno być to oddzielone, bo no jakby są potencjalne, duże obszary konfliktogenne, tak. Tak jakby mamy potencjalny konflikt interesów, gdzie IT musi zapewnić głównie dostępność i działanie jakichś systemów. Natomiast security, jako priorytet stawia sobie, że one spełniają trzy podstawowe cechy bezpieczeństwa, czyli nie tylko dostępność, ale również integralność i poufność. Więc ja jestem zwolennikiem tego, żeby tym głównie zajęły się Departamenty Cyberbezpieczeństwa. Nie schodzę specjalnie do dyskusji, bo byśmy chyba musieli mieć inny odcinek. To nie jest żaden podstęp, nie namawiam, ale to jest zagadnienie samo w sobie, co to jest SOC, co to jest CERT, czym jest Departament Cyberbezpieczeństwa, z czego powinien się składać i tak dalej. Więc nie chciałbym może tutaj jakby dotykać tego tematu, no on jest ciekawy, ale decydować, że to SOC ma się tym zająć, no na pewno dzisiaj SOC jest tym elementem systemu cyberbezpieczeństwa organizacji, na który mocno się stawia i ci, którzy decydują się na posiadanie SOCa dużo sobie po nim obiecują, ale to jest jakby inny temat. Natomiast na pewno cyberbezpieczeństwo, czyli struktury odpowiedzialne za cyberbezpieczeństwo powinny z tego korzystać. Natomiast od razu dodam, nie da się tego zrobić bez współpracy z zespołem IT, z działem IT, dlatego, że no jak sobie mówimy o tym na przykład, źródła danych, tak, wielokrotnie już wspominałem. Uruchomienie ich, no to to jest uruchomienie na poziomie najróżniejszych systemów, nie tylko systemów związanych z cyberbezpieczeństwem, ale systemów po prostu, które pełnią najróżniejsze funkcje w tej infrastrukturze, no i bez działu IT po prostu tego się nie da zrobić. Więc dobrze jest jak ta wiedza też jest w zespole IT. Zresztą, no dzisiaj IT bez świadomości, wiedzy, sporej wiedzy nawet o tym jak robić security w IT, no to trudno powiedzieć, że ktoś jest specjalistą IT, jeśli po prostu nie zna podstaw i nie zajmuje się bezpieczeństwem swoich systemów.

Natomiast, no dedykowane zespoły, no muszą zrobić to w sposób specjalistyczny, jakby poprowadzić taki projekt, zdecydowanie.

Prowadzący: Ja chciałbym zapytać i wrócić z powrotem do grup APT, tajemniczo brzmiących elementów. Jakie organizacje właśnie się za nimi kryją? I czy są rzeczywiście tak w pewnym sensie przewidywalne, tak, że MITRE jest w stanie zmapować pewne techniki i taktyki dla danej grupy? Szczególnie, jeżeli właśnie mówimy wiadomo o takich atakach, jak APT. Skąd się biorą nazwy, numery APT, jakieś informacje o danych grupach, jakie informacje o danych grupach możemy wyciągnąć i jak to też może pomóc naszym organizacjom? To już też częściowo stwierdziłeś, na które grupy warto żebyśmy się czasami, żebyśmy czasami spojrzeli, ale jeżeli możesz coś więcej na temat samych grup powiedzieć.

Mirosław Maj: To może zacznijmy od najprostszego, skąd się biorą nazwy. Bo to są nazwy, które są, w niektórych przypadkach wręcz randomowe, no bo jak mamy w ogóle APT z numerkiem, prawda, to co kiedyś wprowadził Mandiant, czyli dzisiaj czytaj FireEye, no to to są po prostu kolejne numerki, które gdzieś tam w dokumencie specjaliści z tych organizacji sobie przypisywali te działania, a później się bardziej sexy pojawiły też takie nazwy typu Dragonfly, czy Charming Kitten, czy różne inne odmiany, prawda. I teraz no nawet gdzieś, kiedyś znalazłem i to jest pewnie do tworzenia w ogóle, taką matrycę, jak ta sama grupa jest, ile ma nazw, prawda. W zależności od tego po prostu, kto ją nazywa, bo to też sobie powiedzmy. To jeszcze na chwilę wrócę do tej historii RSA. RSA kiedyś, jak właśnie zostało zaatakowane i mocno poległo, no, czyli straszne pieniądze po prostu zapłacili, liczone w milionach dolarów za tę wymianę tokenów na całym świecie. No to jednocześnie zastosowało taki bardzo fajny manewr, oskrzydlający, bym to nazwał, w którym generalnie narracja tego manewru wyglądała tak – no słuchajcie, my, no nie ma co ukrywać zostaliśmy zaatakowani, takiego ataku doświadczyliśmy i co w związku z tym? No w związku z tym jesteśmy najlepszymi specjalistami na świecie od radzenia sobie z takimi atakami, tak, bo my już wszystko wiemy, po prostu, jak to zrobiliśmy analizy, teraz nasze urządzenia są tak netwitne do RSA security, tak, że były wykorzystywane przy analizie tego ataku. No i później się stało głównym narzędziem, reklamowanym jako tym, które ma sobie z atakami APT radzić.

[00:40:19]

Mirosław Maj: Dzisiaj wiadomo, że ta obrona jest znacznie bardziej trudna. Ale jak dobrze wiemy, też powstają narzędzia, które wprost w swoich nazwach mają anty APT, prawda. No i teraz, dlaczego o tym wspominam? No dlatego, że te analizy, znaczy te wszystkie ataki i bardzo dobrze, że od razu zaznaczam, stały się podstawą najróżniejszych badań, tak, takich analiz. A jednocześnie promocji najróżniejszych ośrodków związanych z vendorami, z cybersecurity, ale w ogóle też z firmami jakimiś callingsowymi i tak dalej, które poprzez publikację swoich raportów na temat działania różnych grup APT, no próbowały się. No i to zaczął się taki wyścig, tak. Ten, który niestety też, trochę mówię niestety no, bo on w którymś momencie zaczął przybierać też taki wymiar mocno marketingowy. No i w tym

marketingu, co jest ważne? No jeżeli ja badam, a nie można nikomu odebrać i rzeczywiście tak było, nie można nikomu odebrać tego, że kolejni specjaliści, kolejni researcherzy z różnych, nowych organizacji wynajdowali nowe elementy działania na przykład tej samej grupy, no wcześniej nieznanne. No ale teraz mamy taki efekt marketingowy, że nawet jak coś znalazłem nowego, no to właściwie jeżeli bym chciał znowu napisać, nie wiem, na przykład APT 28, no to wszyscy wiedzą, że ktoś inny pierwszy o tym napisał. Więc no co zrobię, no to nazwę ich inaczej, dlatego, że oni tam gdzieś w kodzie napisali sobie, że są jakimś misiaczkami albo kimkolwiek innym, prawda. I tak zaczęły się mnożyć, pączkować te różne nazwy. Dzisiaj jest tak, że niektóre grupy mają wiele, wiele różnych nazw. To jest taki efekt uboczny, powiedziałem, że proste, a zacząłem się, ale myślę, że...

Prowadzący: Może po prostu efekt zmylenia przeciwnika i oni sami nie wiedzą, że to o nich piszą.

Mirosław Maj: Nie, myślę, że to, to akurat nie następuje. Raczej zmylenia być może w ogóle całego środowiska, dlatego, że dzisiaj to pewnie jest kawałek odrębnej wiedzy, jakby ktoś chciał się popisać tym, że potrafi dobrze przepisać, znaczy się skojarzyć nazwy. Właściwie to bardzo fajny może materiał na jakąś grę, taką karcianą może, prawda. Dopasuj, taki Piotruś trochę, tak, prawda. O właśnie, musimy zrobić Piotrusia cybersecurity APT group i trzeba będzie jakby dwie takie same karty zebrać, żeby zebrać w pary.

Prowadzący: Zebrać w pary.

Mirosław Maj: Proszę?

Prowadzący: Zbierać w pary, tak?

Mirosław Maj: Tak, zbierać w pary. Więc to pewnie jest kawałek wiedzy. Natomiast, jak wygląda w ogóle ten i dlaczego tutaj bardzo często z czynnikiem państwowym wiążemy? No dlatego to wiążemy z czynnikiem państwowym, że no taka, tak opisywana tutaj w trakcie naszej rozmowy działalność zaawansowana, skomplikowana, wymagająca dużych środków i determinacji, no to bardzo często powiązana jest właśnie z tym, że jest no, występuje ten element, co już raz to określenie padło state-sponsored, tak, czyli poważnych czynników na poziomie państwowym, mniej lub bardziej oficjalnych, bo niektórzy się bardziej do tego przyznają, a niektórzy nie chcą się przyznawać, które no są w stanie zainwestować w takie działania. No i teraz mamy, i dlatego często się, no właściwie takim wręcz niemal, że związkiem frazeologicznym jest dodawanie pewnej narodowości do grup APT, czyli się mówi rosyjska grupa APT, czy północnokoreańska grupa APT prawda, czy irańska, czy chińska, tak i tak dalej. Akurat nie mówi się amerykańska grupa APT czy brytyjska grupa APT, ale możemy sobie jasno powiedzieć, że takie grupy APT również istnieją w tych państwach, które, we wszystkich państwach, które poważnie jakby traktują rozwój swoich zdolności w cyberprzestrzeni, tak. Na przykład swego czasu i to jest znany przypadek, Wietnamczycy bardzo dużo zainwestowali w to i no jakby specjaliści wskazywali na to, że to taki jakby niepozorny kraj na arenie, że tak powiem mocarstw między, globalnych mocarstw, tak, nagle pojawia się jako dosyć istotny gracz w obszarze APT.

[00:45:02]

Mirosław Maj: Więc, no te grupy są związane z działalnością różnych państw. W zależności od tego jak przebiega analiza, no one na przykład nieraz się pojawiają, później znikają, później tak naprawdę często jest tak, że co analizy pewne mogą wykazać, że specjaliści gdzieś tam przechodzą do nowych grup, tak. Dlatego, że inna była, inna została skompromitowana, więc ktoś to zamyka, prawda i tak dalej, i tak dalej. Więc jest duży ruch w interesie, ale na poziomie poszczególnych państw i później to też zresztą doprowadza do pączkowania, do tych różnych nazw. Więc mamy te kilka państw na tej mapie grup APT. Obiecałem powiedzieć o ciekawym przypadku. No dla mnie takim ciekawym przypadkiem, nie mówię, że ulubionym, bo tutaj chyba nie warto mieć ulubionych grup APT, prawda, ale bardzo ciekawym przypadkiem, który...

Prowadzący: Taki, który zrobił jakieś wrażenie, tak, takie czy inne.

Mirosław Maj: Tak. Znaczący, może wrażenie nie tyle sama grupa, co pewien sposób działania. To jest, w ogóle to często podaję ten przykład Iranu, tak. Czyli państwa, które zostało, no powszechnie jest kojarzone, jeżeli chodzi o jakby te różne zjawiska cyberbezpieczeństwa, ze wspomnianym przez Ciebie Stuxnetem. Czyli mamy tutaj historię z 2010 roku, jeśli dobrze pamiętam datę. I to jest o tyle ciekawy przypadek, że to, co się wtedy stało, zdecydowało, że Irańczycy w bardzo systematyczny sposób podeszli do budowania swoich własnych zdolności w obszarze cyber. No i jednym z elementów tych zdolności, no to jasno trzeba postawić, że to jest również posiadanie takich zespołów, które są w stanie przeprowadzać, no bo jak to się nazywa, jak to zjawisko o którym mówimy się nazywa, że tak powiem w doktrynach, oficjalnych doktrynach mocarstw globalnych. No to się nazywa operacje w cyberprzestrzeni, tak, to jest operacja w cyberprzestrzeni. Więc Iran też postanowił, że będzie miał zdolność do przeprowadzania operacji w cyberprzestrzeni, no i mamy APT 33, APT 39, Charming Kitten czy Kitten. Wspominamy o kotkach, bo chyba wczoraj czy przedwczoraj był dzień kota podobno. Ja nie mam kota, ale to tak popularne zwierzę, że i tak o tym słyszałem. Więc po prostu jest ileś takich grup i ciekawe jest też to, że im się udało, no w mojej ocenie bardzo szybko osiągnąć te zdolności. Również dlatego, że zastosowali taki dosyć efektywny, sprytny zabieg, że dużo poświęcili czasu na analizy działania innych i widać w ich działaniach, że wykorzystywali wiele technik czy nawet całych TTP wspomnianych już, czyli taktyk, technik i procedur, stosowanych przez inne grupy, z innych państw, prawda. Więc, po prostu sobie taką przyjęli strategię, po prostu rozbudowywania swoich zdolności. Dlatego często, znaczący też rodzi pewne takie zamieszanie dotyczące czegoś, co i tak jest trudne. Chociaż niektórzy twierdzą, że dzisiaj to jest w wielu przypadkach i tak rzeczywiście jest, nikt się już nie kryje z tym, że jakieś tam ataki przeprowadził i się nikt nie przejmuje tym, że go wykryli. Ale generalnie no, znany jest tak zwany problem atrybucji, tak, żebyśmy ustalili, kto to zrobił. No to możemy sobie wyobrazić, że w momencie, kiedy ktoś zaczyna stosować, zresztą nieraz to się intencjonalnie robi, żeby

zmylić, ale jeżeli nawet nie, no to, jeżeli ktoś zaczyna stosować coś, co jest charakterystyczne dla kogoś innego, no to zaczynamy mieć zamieszanie i dodatkowe kłopoty.

Prowadzący: No właśnie, to jest właśnie ciekawa kwestia, którą teraz poruszyłeś. Czyli jak często można ustalić pochodzenie i autora takiego ataku APT? Szczególnie, jeżeli mówimy, czy to tak jak w tym momencie stwierdziłeś o metodach wykorzystywanych powiedzmy przez inne grupy, ale również, jeżeli mówimy o swojego rodzaju, ja to tak nazwę, takiego łańcuchu dostaw, tak, czyli opracowane oprogramowanie przez jedną stronę, narzędzia jakieś deweloperskie, jeszcze coś innego, hosting jeszcze w innym miejscu. Jak często tak naprawdę rzeczywiście udaje się dociec, kto stoi za tego typu, zaawansowanymi atakami?

Mirosław Maj: Wiesz, to jakiś czas temu, no to jest bardzo częsty przykład, który był podawany to jak ktoś tam gdzieś wykrył, że jakiej na przykład klawiatury używano przy pisaniu jakiegoś kodu prawda, no i pisane cyrylicą, to jest znane określenie zresztą w Polsce. Albo na przykład, w jakiej strefie czasowej był kompilowany kod prawda, i tak dalej, i tak dalej, i tak dalej.

[00:50:00]

Mirosław Maj: Ale te techniki ustalania atrybucji, no to znowuż jest historia, nie wiem, pewnie z okolic 10 lat temu, prawda. I one no pewnie nadal gdzieś są wykorzystywane, ale dzisiaj, no jakby druga strona też to wie, tak i bardzo łatwo może po prostu, to zmienia tak, żeby była utrudniona ta, to ustalanie atrybucji. Więc, no dzisiaj w mojej opinii ustalanie atrybucji to jest takie działanie, które łączy ze sobą kilka różnych obszarów, tak. Oprócz tego, że analizujemy bardzo szczegółowo kod, nie wiem, jakiegoś malwaru prawda i potrafimy to wykryć, to zaczynamy po prostu wszystkie rzeczy, które tam znajdujemy w przypadku takiego ataku, no jak to się popularnie mówi, próbować łączyć kropki, tak. Czy ten element gdzieś nie wystąpił, tak. No okazuje się, że ktoś tam gdzieś w jakimś raporcie o tym napisał albo ktoś podejrzewa po prostu, że u nich był podobny atak i oni mają jakieś ślady, bo coś tam jeszcze dokładnie ustalili, że to jest takiego, a nie innego państwa. To jest też bardzo często powiązane z dołożeniem prawdopodobieństwa, które wynika no z jakiejś przesłanki, tak, z motywacji, której, co zostało na przykład, co się stało w wyniku tego ataku. Wiadomo, że przez lata jednym z głównym działań chińskich grup APT to były działania cyberszpiegowskie, związane na przykład z wykradaniem tajemnic przemysłowych, tak, związanych z patentami i tak dalej. No i jeżeli takie coś znajdujemy, no to gdzieś tam możemy podbić po prostu ten słupek, związany z prawdopodobieństwem, że to jest grupa chińska i tak dalej, i tak dalej. Więc myślę, że dzisiaj to jest połączenie wielu różnych elementów, zarówno takich stricte technicznych, tak, analiz tych artefaktów, które znajdujemy w sieci, znajdujemy na hostach, tak, czy narzędzi, które używamy, przeanalizujemy kod tych narzędzi, znajdziemy podobieństwa do innego kodu, który już wiemy, że zrobiła taka i taka grupa albo grupa z tego kraju i tak dalej, i tak dalej. Więc to są takie techniczne, ale również gdzieś tam takie bardziej miękkie,

związane na przykład z tymi motywacjami czy nie wiem, na przykład jakimś napięciem geopolitycznym, tak, związanym z jakąś tam sprawą.

Prowadzący: I jeszcze chciałem wrócić, czy cały Framework bazuje w głównej mierze na danych, jeżeli chodzi tu o źródła, danych pochodzących z rozwiązań końcowych? Czy również z danych sieciowych? Na przykład wiele elementów skorelowanych jest z danymi rejestrowymi, monitorowaniem procesu, sprawami związanymi z commandline.

Mirosław Maj: Jak najbardziej. To nawet, tak, tak, tak, jak najbardziej. Nawet jeżeli sobie weźmiemy przeanalizujemy sobie na przykład te źródła danych, no to możemy sobie powiedzieć, no jakbym miał kogoś zachęcać, znaczy zachęcamy cały czas jak rozumiem, w tym wszystkim co mówimy, że to jest i ciekawe, i warte zainteresowania również, z punktu widzenia tego sposobu zabezpieczania się, ale jeżeli już bym miał bardziej konkretnie zachęcać do tego, co warto zaimplementować, jeżeli chodzi na przykład o źródła danych, no to jak sobie popatrzymy na statystyki użycia technik pewnych, to okazuje się, że gdybyśmy zaimplementowali możliwość monitoringu procesów, czy związanych z plikami czy procesów z commandline, no to byśmy osiągnęli tak zwane Pareto najprawdopodobniej, tak. To znaczy z tych trzech rzeczy, o których wspominałem, no to większość rzeczy jesteśmy w stanie identyfikować, jeżeli chodzi o użycie jakichś technik. Natomiast tak naprawdę to i tak powinno być elementem dosyć szczegółowego procesu, jakim jest modelowanie zagrożeń, tak. No znowuż powróćmy sobie do tego przykładu i do tego pomysłu, który tu podpowiadałem, że bierzemy sobie po prostu to nasze środowisko, bierzemy sobie to miejsce geopolityczne, w którym się znajdujemy i ryzyko z tym związane, czy sektor, w którym funkcjonujemy. I wtedy w ten sposób dopasowujemy matrycę, prawda i tak dalej. Ale również na przykład dopasujemy to, które grupy APT na przykład działają w obszarze, na przykład tej automatyki przemysłowej, tak. No bo są też takie grupy APT, które się specjalizują w tej automatyce przemysłowej. No to mamy taki zestaw, z którym rozpoczynamy no coś, co ja wspominałem o tym, ale nie nazywając tego wprost, a może warto to nazwać też bardzo tak konkretnie – modelowaniem zagrożeń, tak.

[00:55:05]

Mirosław Maj: Czyli zaczynamy przechodzić proces dosyć szczegółowy, który się już odnosi do konkretnych elementów naszej infrastruktury, gdzie krok po kroku te źródła danych analizujemy, analizujemy jakby te też obszary, które musimy zabezpieczyć, decydujemy jaki monitoring uruchamiamy, jakim procesom pozwalamy na działanie. Może przy takim modelowaniu zagrożeń zaraz się okazać, że jest pełno zupełnie niepotrzebnych, działających na jakichś serwerach i tak dalej, i tak dalej. Więc to jest takie konkretne modelowanie zagrożeń, coś co metodycznie jest do ogarnięcia, my takie rzeczy wykonujemy i są metodyki, mówiące o tym, jak warto to robić. A to daje no niezwykle precyzyjne szanse na osiągnięcie niezwykle precyzyjnego zoptymalizowania po prostu swoich wysiłków, tak bym to powiedział, tak. No bo, bo to jest też takie poczucie, no wyobraźmy sobie, że

nagle, no troszeczkę takiego tego złotego Graala naszego odkrywamy, że wiemy wreszcie po prostu, co my mamy zrobić, tak. No bo, no bo to cyberbezpieczeństwo dzisiaj jest już tak szerokie, tak wiele elementów dotyczy, że ludzie, którzy się tym zajmują no albo mogą pójść ścieżką takich zawsze ważnych tak, ale jednak takiego bardzo banalnego, defaultowego podejścia typu – no to tak, musimy mieć ICS, musimy mieć Firewall, musimy mieć antywirusa, musimy mieć SIEMa i tak dalej. I to wszystko jest prawda, tylko, że no dzisiaj specjalistyczna implementacja tych wszystkich narzędzi plus oczywiście jeszcze procedur z tym związanych i ludzi, którzy mają to obsługiwać, no to to jest niewystarczające, to jest zagadnienie znacznie bardziej skomplikowane. Takie proste jakby stwierdzenie, że postawić sobie Firewalla, no to jest dopiero początek drogi, a co my tam zrobimy dokładnie, tak. I to, i oczywiście możemy znowuż powiedzieć, że znaleźć sobie, wygoogłać sobie najważniejsze reguły na Firewalla, no i też coś znajdziemy, tak. Tylko, co to znaczy najważniejsze? No najważniejsze statystycznie, tak. Może się okazać, że my jesteśmy przykładem absolutnie niestatystycznym i dla nas bardzo ważne jest, no bardzo specjalistyczne zamodelowanie zagrożeń, które nas dotyczy i podjęcie decyzji, wykonanie już jakby kroków w budowaniu tego systemu bezpieczeństwa, które jest związane jakby z wynikiem takiego modelowania.

Prowadzący: Tak jest w praktyce z wykorzystaniem Firewalla i w postaci opracowania.

Mirosław Maj: Tak, na pewno są. Ja kiedyś na konferencji, którą współorganizowałem był bardzo ciekawy wykład, który miał tytuł – Fire your Firewall, tak. Jakby człowiek, który przyszedł i tłumaczył, przekonywał do tego, że właśnie jakby takie wstawianie Firewalla dla wstawienia Firewalla to jest proszenie się o kłopoty, tak. Bo to do niczego nie prowadzi, a tylko może mylnie wrażenie wywołać, że jesteśmy bezpieczni.

Prowadzący: Podczas naszej rozmowy wspominałeś jeszcze o pracy badawczej, dotyczącej właśnie MITRE Attack, jaką razem z zespołem z Fundacji prowadzisz. Czy możemy się dowiedzieć jeszcze czegoś więcej na ten temat?

Mirosław Maj: Zespół osobowy to pewnie też można powiedzieć, że Fundacja, ale prawda jest taka, że jest to konsorcjum, które składa się z trzech organizacji Politechniki Warszawskiej, firmy i naszej firmy ComCERT, w której również pracuję. I to jest projekt, który nam się udało w ramach takiego konkursu CyberSecIdent, takiej linii, to była czwarta edycja tego konkursu, który jest przez Narodowe Centrum Badań i Rozwoju ogłaszane. Więc my zaproponowaliśmy projekt, który roboczo się nazywa, a właściwie się nazywa, roboczo z punktu widzenia tego wszystkiego, co ma zrobić tak, bo to jest bardziej zaawansowane niż sama nazwa, bo się po prostu nazywa – Detektor APT. Więc można sobie po tej nazwie – Detektor APT wyobrazić, co on ma robić, ale to oczywiście trochę tak jak z całym, z tym wszystkim, o czym mówiłem, to tylko wstęp jest do tego, jakie zadania są w tym projekcie. My sobie tutaj postawiliśmy taki cel, żebyśmy potrafili maksymalnie dużo, w sposób zautomatyzowany próbować ustalać i identyfikować różne operacje w cyberprzestrzeni, które są takimi atakami APT. Po

to właśnie, żeby prowadzić, żeby mieć narzędzie do bardzo fajnego i skutecznego modelowania zagrożeń. Ale po to również, żeby mieć właśnie bardzo dobry przegląd sytuacyjny tego wszystkiego, co się dzieje, co jest niezwykle ważne w procesie zarządzania incydentami.

[01:00:07]

Mirosław Maj: I w ogóle w samym też zareagowaniu na incydent. No bo jak sobie przeanalizujemy znowuż modele te kill chain prawda i w ogóle takiego sekwencyjnego ujęcia danych, to jest bardzo ważne to, o czym tak troszeczkę wspominałem, że niezwykle ważne jest, sposób w jaki my zareagujemy na rozpoznane nie tyle prawdopodobieństwo jakiegoś zagrożenia, tylko zmaterializowane zagrożenie. Na przykład to takie kolokwialne stwierdzenie – ktoś się włamał. I to, co mówiłem wcześniej, co zazwyczaj oznacza, że dopiero rozpoczął swoją prawdziwą operację, w naszej infrastrukturze. I takie narzędzie, o którym my myślimy w ramach tego projektu, to jest narzędzie, które będzie dostarczało bardzo pożytecznej i efektywnej takiej wiedzy na temat tego wszystkiego, co jest obserwowane po to, żeby jak najszybciej reagować w związku z taką sytuacją i mówiąc kolokwialnie, obrazowo – wykurzyć takiego atakującego z tego, z naszego środowiska. No i projekt również ma elementy bardzo, jeszcze bardziej ambitne, związane z pewną predykcją, predykcją takich ataków, też powiązanych z zarządzaniem incydentami. No wyobrażamy sobie, że w oparciu o dane ustrukturyzowane pochodzące na przykład ze źródeł danych, ale też mniej ustrukturyzowane, wynikające z analiz eksperckich na temat działania najróżniejszych grup APT, będziemy w stanie, w momencie, kiedy coś wykryjemy, z dużym prawdopodobieństwem przewidywać kolejne, bardzo specyficzne na poziomie technicznym, tak, działania w sieci, w systemach operacyjnych. Będziemy w stanie identyfikować z dużym prawdopodobieństwem kolejne potencjalne kroki atakującego, tak żeby znowuż po prostu, nie wiem, rzucić wszystkie siły do tego, że – no wynika nam tutaj z tej analizy i nasza predykcja mówi o tym, że następnym krokiem w ramach tego ataku, to z 70% prawdopodobieństwa jest takie, że weźmie się za ten system operacyjny i zaatakuje ten proces na tym systemie operacyjnym, a 30%, że tamtego. No i w tym momencie, no jakby możemy wręcz nawet dokładnie z takimi proporcjami gdzieś tam przyłożyć nasze siły do zareagowania. Więc zakładamy, że powstanie narzędzie, które będzie bardzo, bardzo pomocne, no jakby w kształtowaniu całego systemu obrony, ale również tak operacyjnie, w momencie, kiedy będziemy musieli się bronić. Takie są założenia tego projektu. Projekt właściwie się zaczyna, bo to jest dosłownie historia ostatnich tygodni, więc jeszcze dużo przed nami. Trzyletni projekt, więc pewnie jeszcze dużo się zdarzy, ale jest niezwykle interesujący, dotyczy materii, która tak jak już sobie od samego początku mówimy, jest też bardzo dynamiczna i rozwija się mocno. Mamy już przecież ósmą wersję matrycy MITRE Attack, a pewnie powstaną kolejne i kolejne obszary, będzie co chwilę tam coś się pojawiało. Ale z drugiej strony też dotyczy materii, która nawet w perspektywie dosyć długiej jak na 3 lata, no bo w tej dziedzinie cybersecurity, to jest sporo. No mamy także, będziemy zajmowali się czymś, co w mojej ocenie jest pewnikiem, że za te 3 lata to już będziemy się zajmowali, tak, być może

w bardziej nowoczesny sposób i tak dalej, ale jest to, no ten MITRE Attack przełamał pewną barierę i stał się realnym, operacyjnym standardem. Tak jak nie wiem, na przykład w dziedzinie wymiany informacji na temat zagrożeń, takim standardem stał się MISP na przykład prawda, czyli platforma do wymiany informacji o zagrożeniach, które właściwie no wszyscy praktycznie w tym świecie reagowania na incydenty korzystają. Tak samo w mojej ocenie jest tutaj, z tym modelem i czujemy się bezpiecznie. No i trochę jakby podekscytowani tym, że będziemy mogli jakby tutaj tę dynamikę, spróbować przenieść ruch bezpośrednio na nasz projekt.

Prowadzący: Mirku, na zakończenie pytanie mocno podchwytliwe i troszeczkę oderwane od tematu dzisiejszego odcinka, troszeczkę. Ransomware czy APT, co straszniejsze z Twojego punktu widzenia dla organizacji?

Mirosław Maj: Znaczący jedno nie wyklucza drugiego prawda, bo pewnie się nie obrazisz, że z reklamuje również nasz fundacyjny podcast Cyber Cyber, chociażby dlatego, że mamy tę przyjemność być tym pierwszym polskim podcastem o cyberbezpieczeństwie. Ale dlaczego o tym mówię? Nie dla samej reklamy, tylko dlatego, że no w ostatnim odcinku był bardzo ciekawy przypadek, który no śledzą wszyscy w naszym świecie, czyli ataku na CD projekt, tak.

[01:05:08]

Mirosław Maj: I też tamransomware. I teraz to, że tam jest ransomware, no to nie oznacza, że ransomware nie jest sposobem zaimplementowania pewnej techniki w postaci narzędzia, które jest, było zrealizowaniem pewnej taktyki, prawda, że jeśli ktoś, dla czegoś coś chciał zrobić, no i zrobił to w ten sposób. To jedno nie wyklucza drugiego. I myślę, że warto też zapamiętać z tej naszej rozmowy to, żeby słuchacze sobie zapamiętali, że ten APT, no to to jest kolejny jakby synonim pewnego takiego ujęcia, takiego bardzo szerokiego, tak. Na dzień dzisiejszy chyba jednego z najbardziej kompletnego dzisiaj w cyberbezpieczeństwie, który jest dosyć pojemny, tak. I hasła, które my słyszymy dotyczące ataków, takie jak właśnie phishing, no to wspominałem, że RSA zostało zaatakowane z phishingiem, tak. To o co Ty pytasz, ransomware, to no to ktoś został zaatakowany. I nieraz to jest taki rzeczywiście, taki pojedynczy strzał, tylko że ja bym go wtedy kojarzył bardziej z takimi sytuacjami niemal, że wręcz ataków takich półautomatycznych. Tak jak nagle mieliśmy też takie ataki w Polsce, gdzie ileś stron naraz się zmienia, tak, no dlatego, że nie ktoś tam szukał specjalnie jakiejś lokalnej gazety, gdzieś tam w jakimś województwie chce koniecznie zdobyć witrynę, tylko po prostu przeleciał się po skanowaniu, znalazł podatność i wszystko z automatu podmienił. I tyle, prawda. I wtedy to jest atak, który trudno nazwać atakiem APT prawda, no to jest po prostu atak na coś podatnego, łatwego i wtedy może to się to skończyć ransomwarem, ddosem, i phishingiem i wszystkim, co sobie wyobrażamy. Natomiast każdy z tych elementów jakiegoś typu ataku może być elementem znowuż operacji APT, bo tak byśmy to ujęli.

Prowadzący: Czyli tak po prostu trafiło się?

Mirosław Maj: Nieraz się trafiło, nikomu nie życzymy, a nieraz, no i dlatego efektem takiego działania bardziej zaawansowanego jest to, że lista tych, którzy no jeszcze nie zostali skutecznie zaatakowani, a są ważni, to jest chyba pusta. Taka jest prawda. Nie o wszystkich pewnie przypadkach wiemy, ale z dużym prawdopodobieństwem możemy taką tezę postawić.

Prowadzący: Moim i Państwa gościem był Mirosław Maj. Mirku, bardzo serdecznie Ci dziękuję za Twoją obecność. A dla naszych słuchaczy hasło dzisiejszego podcastu to Do usłyszenia w kolejnym odcinku. Dzięki jeszcze raz.

Mirosław Maj: Bardzo dziękuję za zaproszenie i możliwość porozmawiania o tym ciekawym temacie. Dzięki. Cześć.