TRANSKRYPCJA – Odcinek IX

Dzień z życia pentestera

[00:00:05]

Prowadzący: Cześć. Witam wszystkich słuchaczy w kolejnym odcinku naszego podcastu. Dzisiaj wraz z moim gościem powiemy wam, czy hacking może być legalny? Czy można na tym zarabiać mając to w pewnym sensie wpisane wprost w swoje CV? Przybliżymy wam pracę pentesterów, czym się zajmują, na czym tak naprawdę polega ich praca? Zaczynamy. Moim dzisiejszym gościem jest Magdalena Mielke, pentesterka w TestArmy CyberForces, pasjonatka cyberbezpieczeństwa, z zamiłowaniem do gastronomii. Chociaż zaczęła od Test QA, to testy penetracyjne są tym, co daje jej największą zawodową satysfakcję. Dzięki za Twoją obecność.

Magdalena Mielke: Cześć. Dzięki śliczne za zaproszenie.

Prowadzący: Magda, skąd u Ciebie zainteresowanie cyberbezpieczeństwem i dlaczego akurat pentesty? Dlaczego akurat ta strona zagadnień, związanych z cybersecurity?

Magdalena Mielke: Wiesz co, to jest dosyć śmieszna historia dlatego, że ja generalnie miałam podejście od czasu studiów, że zawsze będę robiła coś związanego z geologią, czyli tym, co studiowałam. Życie zweryfikowało inaczej i trafiłam do IT. Krótko moja przygoda trwała z testami manualnymi, ponieważ szybko się zaczęłam nudzić. Szukałam czegoś ciekawszego, wyzwań i w którymś tam momencie, na takich spotkaniach, meetupach usłyszałam o testach bezpieczeństwa, zaczęłam o tym czytać, robiłam rekonesans, uczestniczyłam w różnego rodzaju spotkaniach i mnie to uderzyło, że jest to – to, że to jest fajne. No i tak się zacięłam, żeby się jednak w to wgryźć, żeby coś zacząć z tym robić. No i w pewnym momencie mi się udało. Trafiłam do firmy, w której dostałam możliwość, żeby posmakować pentestów i się w tym odnalazłam. I teraz nie wyobrażam sobie robić czegoś innego.

Prowadzący: Hacking kontrolowany, praca pentestera. Pracujesz w zespole fachowców, którzy, no co tutaj dużo mówić, włamują się do systemów informatycznych czy aplikacji klientów i to w zupełności legalnie. Może nie w celu dobrania się do wrażliwych danych, ale w celu oceny bieżącego stanu systemu bezpieczeństwa czy prób przełamania zabezpieczeń. I zanim rozpoczniemy z kolejnymi aspektami Twojej pracy, przybliż proszę, czym na razie tak dosyć ogólnie oczywiście, są testy penetracyjne? Zdaję sobie sprawę, że jest to temat rzeka, ale jeżeli mogłabyś przybliżyć dosłownie w kilku zdaniach esencję pracy pentestera.

Magdalena Mielke: W takim najprostszym znaczeniu, testy bezpieczeństwa to są takie kontrolowane testy wykorzystania podatności i takich słabości w systemach informatycznych albo w aplikacjach, czy webowych, czy mobilnych, czy desktopowych w celu określenia, czy istnieją luki bezpieczeństwa i czy

jesteśmy w stanie je wyeksploitować, a następnie w zarekomendowaniu klientowi, który nam zlecił te testy, w jaki sposób te luki naprawić.

Prowadzący: Wiesz co, na jakich typach testów najczęściej właśnie zależy klientom? Oczywiście dalej pozostając w temacie testów penetracyjnych, tak. Co jesteśmy w stanie osiągnąć przez tego typu testy? Czy jest to, biorąc pod uwagę zlecenia, częściej takie całościowe podejście do infrastruktury IT, czy raczej takie kluczowe elementy składające się na perimeter security lub pojedyncze aplikacje, ważne z punktu biznesowego dla klienta?

Magdalena Mielke: Znaczy wiesz co, tutaj ja bym zaczęła od tego, dlaczego w ogóle przeprowadzamy te testy penetracyjne. I tutaj skupiłabym się na tym, że bardzo często działania hakerów, czyli takich złośliwych atakujących mają na celu, jakby wyciągnięcie danych, zablokowanie czy utworzenie jakiejś przerwy w działaniu aplikacji czy serwisów różnych organizacji. I naszym zadaniem jest to, żebyśmy my, zanim taki haker zewnętrzny, taka złośliwa osoba, atakujący znajdzie taką podatność i ją wykorzysta, żebyśmy my ją zlokalizowali, najczęściej na środowisku jakimś testowym odpowiednio do tego przygotowanym, udokumentowali to, wyjaśnili, w jaki sposób to działa i do czego może taka podatność doprowadzić. A następnie pokazali, w jaki sposób to naprawić i jak się przed tym uchronić. Po czym po, już po takim pierwszym teście przeprowadzili retest i zweryfikowali, czy te nasze sugestie, które gdzieś tam zawarliśmy w raportach, zostały poprawnie zaimplementowane i, czy mechanizmy naprawcze, które oni zastosowali są wystarczające, żeby tych zabezpieczeń już nie przełamywać.

Prowadzący: Jasne. Ale biorąc pod uwagę teraz dalej. Czyli częściej spotykasz się z jakimiś pojedynczymi elementami, które powinny podlegać pentestom ze strony klientów? Czy również takie podejście całościowe do sieci takiej ogólnej?

[00:05:01]

Magdalena Mielke: To bardzo zależy od tego, z jakiego typu klientami mamy do czynienia. My, jako firma świadczymy usługi i takiego typowego red teamingu, czyli takich szerokich testów, gdzie przeprowadzamy i testy aplikacji webowych, i testy aplikacji mobilnych, aplikacji desktopowych, sieci wewnętrznych, zewnętrznych, czy socjotechnikę. Więc to jest taki bardzo szeroki wachlarz. I w zależności od tego, jakiego mamy klienta, z jakim typem danych pracuje, jakie usługi świadczy, względem tego jesteśmy w stanie mu doradzić, jakie testy potrzebuje. Bo niejednokrotnie się zdarza, że przychodzą do nas klienci, którzy przychodzą i mówią – chcę test penetracyjny. Tylko, że trudno im wtedy zdefiniować, czego dokładnie oczekują od takiego testu. I naszym zadaniem jest to, żeby wybadać czy porozmawiać z klientem, określić właśnie, czego dokładnie względem tego, jakich technologii używa, jakich testów potrzebuje. Takim standardem, który zalecamy, to poza testami aplikacji i ich systemów, są testy też infrastruktury zewnętrznej tak, aby nie tylko zweryfikować samą aplikację webową czy tę usługą www, którą gdzieś tam hostuje, jest gdzieś tam hostowana, ale także

zweryfikować czy na tych serwerach, które są wykorzystywane przez klienta są hostowane inne aplikacje, które nie są na takich standardowych portach, czy 80, czy 443, tylko gdzieś tam są dodatkowo poukrywane. Tak, żeby sprawdzić czy na przykład nie są gdzieś, jakieś panele logowania do jakichś innych serwisów dostępne, czy nie są używane domyślne dane logowania, czy systemy, które są wykorzystywane, czy oprogramowania są aktualne. To też jest element, który jesteśmy w stanie testować z zewnątrz, w jakiś sposób. I zawsze rekomendujemy klientowi, żeby łączyć właśnie infrastrukturę zewnętrzną razem z testami aplikacji.

Prowadzący: Wiesz co, to pytanie, które od razu mi się też nasuwa, biorąc pod uwagę Twoją odpowiedź. Kiedy najczęściej, w jakich momentach warto decydować się na pentesty? I pomińmy może fakt organizacji, które no po prostu regularnie muszą wykonywać działanie tego typu. Czy jest to po prostu świeże spojrzenie na bezpieczeństwo swoje i swoich pracowników czy raczej na przykład właśnie takie przypieczętowanie pewnych zmian w infrastrukturze? Czyli to, o czym wspominałaś dwie klatki filmu, przed i po jakichś zmianach?

Magdalena Mielke: Znaczy, jak najbardziej cykliczne przeprowadzanie testów bezpieczeństwa jest istotne. Ale musimy pamiętać o tym, że po każdych większych zmianach, które są wprowadzane w systemie, czy jest to rozbudowa sieci, czy jest to dodawanie nowych funkcjonalności do aplikacji, wprowadzanie aktualizacji systemów. Przy każdych takich zmianach większych, przepisywaniu kodu aplikacji, zalecane są na nowo testy bezpieczeństwa, ponieważ podczas wprowadzania zmian, funkcjonalności, które wcześniej były bezpieczne mogły zostać zmodyfikowane w ten sposób, że gdzieś tam pojawiły się drobne luki.

Prowadzący: To teraz jeszcze kolejne pytanie. White box vs grey box vs black box, czyli ile informacji uzyskujemy od klienta na wstępie i jak bardzo nasza praca ma przypominać, no w pewnym sensie realny atak tak, biorąc pod uwagę informacje, którymi dysponujemy? Czym się różnią między sobą właśnie te podejścia i na którym najczęściej zależy klientom? W jakich przypadkach, sytuacjach?

Magdalena Mielke: Znaczy, standardowo klienci przychodzą i ustalamy testy grey boxowe. Może zacznijmy od tego, czym się w ogóle te testy różnią. Testy black boxowe, są to testy, podczas których my, jako pentesterzy mamy najmniejszą wiedzę o systemie. Czyli mamy na przykład tylko nazwę firmy, mamy adres strony, mamy aplikację, ale nie wiemy nic o środowisku, nie wiemy o tym, jakie są role, jakie są funkcjonalności aplikacji, nie mamy dostarczonej architektury tej aplikacji i nie mamy dostarczonego kodu źródłowego. Więc działamy tak po omacku i jest to tak naprawdę najbardziej, taka praca najbardziej odzwierciedla działania prawdziwego hakera i takiego złośliwego ataku. W przypadku testów white boxowych, znaczy dobra, przejdźmy do grey boxowych, tak po kolei. W przypadku testów grey boxowych jesteśmy bardziej uświadomieni z tym, co testujemy. Czyli na przykład dostajemy konta do aplikacji, które nie posiadają takiego najniższego stopnia z poziomu użytkownika, który jest w stanie

sam się zarejestrować, ale dostajemy także konta administracyjne, z większą ilością funkcjonalności, dostajemy listę od klientów [niepewne] apki. Dostajemy architekturę tej aplikacji, co pozwala nam weryfikować więcej elementów, takich jak uprawnienia na poziomie wertykalnym, czyli tych uprawnień między administratorem, a użytkownikiem niskiego szczebla.

[00:10:15]

Magdalena Mielke: Co standardowo z poziomu testów black boxowych jest praktycznie niemożliwe. Więc tutaj mamy taki podział, że w przypadku testów black boxowych plusem jest to, że one są najbardziej odzwierciedlające realny atak, czy taki najbardziej prawdopodobny scenariusz. Ale z drugiej strony one są bardzo powierzchowne i wiele elementów może zostać niedotestowanych. Mówiąc o testach white boxowych, w tym przypadku mamy już taką pełną wiedzę o aplikacji, którą testujemy, czy o systemie. Mamy dostęp do kodów źródłowych, jesteśmy w stanie przeanalizować każdą funkcjonalność od strony implementacyjnej. Tylko, że white box wiąże się z tym, że te testy są najbardziej czasochłonne, ponieważ musimy przebrnąć przez tysiące linii kodu, żeby znaleźć potencjalne luki czy błędy w kodzie aplikacji, które mogą być z pozoru ukryte w samym funkcjonowaniu aplikacji czy to webowej, czy desktopowej.

Prowadzący: No i zostaje grey box, który jak stwierdziłaś najczęściej pojawia się w waszej pracy.

Magdalena Mielke: Tak, tak. W mojej ocenie, przynajmniej z tego, co my się spotykamy, najczęściej zalecamy grey boxowe testy.

Prowadzący: Czyli, jeżeli mogłabyś rozwinąć? Teraz połączenie grey boxy, jako no częściowo hybrydy tych dwóch.

Magdalena Mielke: Czyli dostajemy taką, to znaczy dostajemy dużo informacji na temat aplikacji. Dostajemy informacje na temat jej architektury, tego, w jakich językach jest pisana, jakie ma dostępne funkcjonalności, dostajemy konta testowe na poziomie administracyjnym, kierowniczym i użytkowników najniższego stopnia. Wiadomo, że przy okazji testowania grey box wykonywane są także testy black boxowe domyślnie dlatego, że zawsze w momencie, kiedy spotykamy się z aplikacją przeprowadzamy najpierw takie testy z poziomu użytkownika niezalogowanego, czyli takiego, tych właśnie testów black boxowych, żeby sprawdzić jak daleko jesteśmy w stanie zajść i co jesteśmy w stanie znaleźć. I dopiero w tym momencie po takich testach przechodzimy do etapu grey boxowego, czyli już z poziomu użytkownika, będącego wewnątrz aplikacji.

Prowadzący: Okej. Magda, kolejna sprawa. Test penetracyjny vs audyt bezpieczeństwa. Czym tak naprawdę się różnią te dwie usługi? Czy to kwestia usystematyzowanej metodologii czy celu, na przykład stwierdzenie zgodności z konkretnymi normami, czy to [niepewne] i tak dalej?

Magdalena Mielke: Znaczy, tutaj od razu powiedzmy – audyt nie jest testem penetracyjnym. I to trzeba mocno podkreślić, bo często jest to mylone. Tak, najprostszym rozróżnieniem jest, znaczy

zobrazowaniem audytów w porównaniu do pentestów jest to, że audyt jest tak jakby check listą dla regulacji związanych z przestrzeganiem przepisów na przykład czy takich standardów bezpieczeństwa, zaś pentest jest taką techniczną, praktyczną formą sprawdzenia, czy te zabezpieczenia, które są, są zaimplementowane, czy skonfigurowane poprawnie. Więc to jest taka główna zasada, główna różnica między audytem, a testem penetracyjnym.

Prowadzący: Do raportów na pewno bym jeszcze za chwileczkę do Ciebie wrócił. Natomiast poruszyłaś też kwestię związaną ze skanerami, z automatami. I to też chciałbym poruszyć. Testy automatyczne czy praca manualna? I różnice płynące z podejścia względem osiąganych rezultatów. Oczywiście jedno i drugie jest wykorzystywane, tak jak wspominałaś, ale czego możemy się spodziewać po każdym z nich? Jakie jest jego przeznaczenie? Zmierzam do porównania na przykład wiesz, pracy skanera podatności czy narzędzi do automatycznego powiedzmy nie wiem, mapowania sieci do takiej manualnej pracy pentestera.

[00:20:05]

Magdalena Mielke: To znaczy, testy automatyczne są na pewno przydatne i w jakiś sposób dla mnie nieodłączne, jeśli chodzi o testy bezpieczeństwa, testy penetracyjne. Dlatego, że dają nam taki ogólny pogląd i lokalizują w dosyć szybki sposób potencjalne miejsca ataku, czy zlokalizują podatności, czy błędy w konfiguracji. Jednak sam test automatyczny nie potwierdza nam tego, czy ta podatność jest możliwa do eksploitacji. Dlatego tak ważne jest przeprowadzanie testów manualnych, ponieważ automat działa schematycznie, on ma jakieś skrypty względem, których działa, sprawdza konkretne elementy. Jednak każdy system, który jest testowany, jest trochę inny i dlatego ważne jest to, żeby siadając do aplikacji móc dostosować odpowiednie scenariusze testowe, odpowiednie metodyki testowe do tego, z jakim typem aplikacji pracujemy. Co same automaty pomijają, bo mają po prostu takie uszeregowane, stałe elementy, które sprawdzają w aplikacjach, stałe skrypty, które wykonują. I mniej więcej w ten sposób to wszystko wygląda. Dlatego praca manualna jest bardzo istotna, ale w szczególności wtedy, kiedy mamy do czynienia z doświadczonym pentesterem, ponieważ umiejętności pentestera odzwierciedlają to, jak skutecznie podatności mogą być wyeksploitowane.

Prowadzący: Czyli pozostaje kwestia rzemiosła?

Magdalena Mielke: Jak najbardziej. Ale to jest kwestia praktyki. Im więcej, z im większą ilością projektów się pracuje, tym łatwiej się odnaleźć w różnego typu aplikacjach, ponieważ spotyka się wiele technologii. My świadczymy usługi testów penetracyjnych w szerokim zakresie, dlatego i testujemy aplikacje, które są bardzo duże, bardzo złożone, skomplikowane, składające się z wielu modułów, a czasami testujemy proste aplikacje, które mają tylko interfejs webowy. Więc mamy tak jakby styczność z bardzo dużą ilością technologii, co pozwala nam dosyć szybko odnajdować się w różnego typu aplikacjach, jeśli chodzi o testy bezpieczeństwa, i dobierać odpowiednie techniki testów.

Prowadzący: Wiesz co, wspominałaś również o raportach, które generujecie po testach. Więc częściowo już poruszyłaś ten temat i jakie elementy tam mogą się znajdować, jeżeli mogłabyś jeszcze to bardziej rozwinąć, to byłbym oczywiście bardzo wdzięczny.

Magdalena Mielke: Jasne.

Prowadzący: A z drugiej strony to, co mnie jeszcze też interesuje to, jaką wartość tak naprawdę dla firm zlecających takie testy mają później te raporty? I czy to często jest, tak brzydko mówiąc, podkładka tak, biorąc pod uwagę infrastrukturę? Czy również często masz do czynienia z przykładami, że te testy tak naprawdę rzeczywiście służą poprawie stanu systemów bezpieczeństwa, czy jakichś procedur związanych z bezpieczeństwem w danej organizacji?

Magdalena Mielke: Jeśli chodzi o raporty, to głównym celem raportów jest właśnie przedstawienie testu, w jaki sposób przebiegł, od początku do końca. Czyli taki standardowy raport, który dostarczamy klientowi zawiera metodyki prac, które wykorzystujemy, obszary, które zostały objęte audytem, obszary, które zostały wykluczone tym testem, są też bardzo istotne. Zawsze zawierają takie streszczenie dla kierownictwa, które jest bardziej ogólne i część techniczną. Ta część techniczna zawiera przede wszystkim klasyfikację zgłoszenia ze względu na jego krytyczność. Zawiera wskazanie adresu, czy to jest adres url, czy jest to jakaś ścieżka do konkretnego pliku, jeśli jest to analiza kodu źródłowego, wskazanie miejsca wystąpienia tej podatności, klasyfikację, jakiego typu jest to podatność. I tutaj zazwyczaj wspieramy się taką listą najczęściej spotykanych podatności z OWASP. Następnym krokiem jest opis tej podatności, czyli mamy miejsce, mamy opis, w jaki sposób tę podatność zlokalizowaliśmy, w jaki sposób ją wykorzystaliśmy, czyli cały ten proces eksploitacji. I w tym miejscu udokumentujemy, jeśli używaliśmy jakiegoś konkretnego payloadu, przedstawiamy, co to był za payload, wrzucamy dokumentację i graficzną, w postaci czy screenów, czy takich fragmentów kodu, czy zachowań aplikacji i dokumentację taką opisową, która wyjaśnia, na czym polega podatność, jakie konsekwencje za sobą niesie wykorzystanie takiej podatności, a na samym końcu rekomendacje, które mówią, w jaki sposób naprawić te błędy, które gdzieś tam występują.

[00:25:00]

Prowadzący: Dobra, wiesz co, jeszcze kolejna kwestia, którą też poruszałaś wcześniej – red team vs blue team. Czyli tak naprawdę starcie dwóch drużyn. Jedna ma za zadanie przedrzeć się przez zabezpieczenia, a druga skutecznie się bronić i sprawdzać swoje wewnętrzne procedury. Jak często występujecie w roli właśnie czerwonych? I jaki jest, oczywiście też mi się wydaje, to wydaje mi się interesujące, odbiór tego typu ćwiczeń przez stronę niebieską, którą może być na przykład nie wiem, właśnie dział IT bądź dział security w danej firmie i która, ta właśnie niebieska strona musi się po prostu wykazać przed swoim pracodawcą? Jak wyglądają realia i odbiór tego typu ćwiczeń?

Magdalena Mielke: No to my przede wszystkim działamy red teamingowo. I nasza praca polega na tym, żeby zweryfikować, jeśli chodzi o ocenę reakcji zespołu blue teamingowego, bo takie testy też przeprowadzamy. Nasza praca polega na tym, żeby odzwierciedlić możliwie realny atak na daną organizację, czy to z poziomu zewnętrznego, czy wewnętrznego, czyli na przykład złośliwego pracownika, który ma standardowe dostępy, jego uwierzytelnienia już w środowisku wewnętrznym. Czy jest to pracownik biura, czy jest to osoba, która gdzieś tam nie wiem, przynosi pocztę, w zależności od tego, czy jest to socjotechnika, czy jest to test infrastruktury, tutaj mamy taki podział, że właśnie naszym zadaniem jest to, żeby zweryfikować, w jaki sposób.

Prowadzący: Wiesz co, jako red team, to jest sprawa jasna. Natomiast, no często przypuszczam, że masz taką sytuację, że po prostu, jako blue team występuje, no po prostu organizacja, tak i członkowie, którzy wchodzą w skład tak naprawdę kadry danej organizacji. Pytam się o odbiór celu takich ćwiczeń, czyli wy jesteście tą stroną atakującą, a tutaj blue team od strony tak naprawdę zleceniodawcy musi się bronić.

Magdalena Mielke: To znaczy, to jeszcze rozgraniczmy, bo nie zawsze każde testy red teamingowe mają odzwierciedlać to czy, jak, w jaki sposób reaguje blue team. Bo testy mogą polegać na tym, że my oceniamy, w jaki sposób aplikacje zostały zabezpieczone, czy sieć została zabezpieczona i serwery, ale możemy też weryfikować to, w jaki sposób strona blue teamingowa od strony klienta reaguje na incydenty, w przypadku próby przełamania zabezpieczeń, w przypadku dostania się do zasobów, do których z pozoru nie powinniśmy mieć dostępu. Więc to są różne aspekty tego, w jaki sposób te testy są przeprowadzane. Jeśli chodzi o odbiór od strony klienta to wiadomo, że w przypadku, gdy weryfikujemy działania zespołu niebieskiego, także wskazujemy to, jak szybko te reakcje zostały podjęte, jakie czynności zostały podjęte, w jakim czasie i czy zostały podjęte skutecznie. I nie ma to na celu wytykania błędów – sorry, ale sknociliście albo – nie zauważyliście, że tutaj się włamaliśmy albo tutaj otrzymaliśmy do czegoś dostęp. Raczej wskazanie błędów typu – ten element jest źle skonfigurowany, tutaj należy poprawić to albo – tutaj zajęła wam za dużo reakcja na, za dużo czasu zajęło wam zauważenie, że udało nam się, jako nieautoryzowany użytkownik wykonać jakieś rzeczy albo ominąć zapory. Więc tu nie chodzi o wytykanie błędów, a uświadamianie, co jeszcze zostało do poprawy. I wydaje mi się, że jest to bardzo istotne dla klienta, że ma świadomość tego, że po takich testach i po takim raporcie, który od nas otrzyma ma świadomość tego, gdzie jeszcze ma braki i co należy poprawić, żeby jak najbardziej podnieść jakość bezpieczeństwa swojej firmy.

Prowadzący: Wiesz co, to coś, co mnie jeszcze też bardzo interesuje, to aspekty prawne związane z testami. I tutaj wracając do samego początku, bo to już też było częściowo poruszone. Często różnica w Twojej pracy, a działaniami potencjalnego włamywacza, no polega na tym, że Ty masz po prostu zgodę klienta na takie działanie. Więc kwestię związaną z procedurą już też omówiłaś, czyli na samym

początku oczywiście ugadujecie się z klientem, na jakie działania, jakie działania wam wolno podjąć, jakich nie. Ale tutaj jeszcze oczywiście pozostaje kwestia na przykład, no niepożądanych efektów, które tego typu testy mogą mieć dla infrastruktury klienta. Począwszy tak naprawdę, no często mówimy po prostu o pracy na środowisku produkcyjnym, tak, więc no pewne niespodziewane efekty zawsze mogą się tutaj wydarzyć. I to też mnie bardzo interesuje. Pytam, bo sam tak naprawdę nieraz miałem podniesione ciśnienie, w przypadku na przykład nie wiem, majstrowania przy produkcyjnym Firewallu. Zresztą pamiętam jak jakiś czas siedziałem, jakiś czas temu siedziałem powiedzmy nad managementem Firewalla w jednej instytucji, zdalna sesja, do tego sesja video i nagle rozumiesz, że po drugiej stronie słyszę telefon – Jak to nie działa, co nie działa?

[00:30:00]

Prowadzący: Mimo tego, że nic nie robiłem, co mogłoby spowodować przestój, ale tak naprawdę wiesz, cała zasłyszana rozmowa dotyczyła całkiem innej sprawy, to moje myśli jednak poleciały w wiadomym kierunku, powodując palpitację serca. Więc, czy często tego typu sytuacje gdzieś tam się również w Twojej pracy zdarzają? I jak wygląda właśnie kwestia związana z odpowiedzialnością za jakieś efekty niepożądane tego typu testów?

Magdalena Mielke: Znaczy, my z zasady odradzamy przeprowadzanie testów na środowiskach produkcyjnych. Wiadomo, że czasami przychodzi klient, gdzie tak naprawdę nie mamy możliwości przygotowania odpowiedniego środowiska i pracujemy na tym, co zostało nam dostarczone, czyli produkcji.

Prowadzący: Czyli ze stanem.

Magdalena Mielke: Tak. Tylko, że wtedy podkreślamy to, jak te testy, które przeprowadzamy, jakie ryzyko ze sobą niosą i, że może wystąpić ryzyko odmowy dostępu do pewnych usług, które będziemy testować. Istotne w testach penetracyjnych, jako pentestera, jest to, czy w ogóle firmy, która świadczy takie usługi jest to, żeby sporządzać bardzo konkretne umowy, które zawierają zakres wykonywanych prac, które zawierają, które dokładnie elementy mogą zostać przebadane, w jaki sposób te testy mają być przeprowadzane, co pentesterowi jest wolno, czego nie wolno. Więc nawet, jeśli pentester ma nadane uprawnienia administracyjne w organizacji to to, że ma te uprawnienia administracyjne to, że ma dostęp do bazy danych, że ma dostęp do poczty pracowników nie znaczy, że może te dane odczytywać sobie, kopiować, przeglądać. Więc to wszystko jest bardzo ważne, żeby ustalać w umowie, którą sporządzamy z klientem, którą podpisujemy. Bo musimy pamiętać o tym, że każde działanie, które my wykonujemy, jako pentesterzy, które nie zostało zawarte w umowie, na które nasz zamawiający nie przydzielił zgody, jest tak naprawdę działaniem hakerskim, tym działaniem złośliwym, które w przypadku wyrządzenia szkody może nieść za sobą odpowiedzialność.

Prowadzący: Wiesz co, kolejne w takim razie pytanie. Zalety outsourcingu testów. Dlaczego warto zlecać testy firmom trzecim, a nie polegać jedynie na swoich działach IT lub security? Nie mówię tutaj wiesz, o bardzo zaawansowane testy penetracyjne tylko na przykład nie wiem, wykorzystanie rzeczywiście jakichś automatów, skanerów podatności i tak dalej.

Magdalena Mielke: Firmy, które tworzą oprogramowanie i jednocześnie testuje to oprogramowanie ma w pewien sposób takie podejście, że zna produkt i testuje to, co uważa, że może być gdzieś tam niebezpieczne. Za każdym razem, kiedy wykonywane są testy bezpieczeństwa warto jest wziąć osobę z zewnątrz, która zweryfikuje to, co zaimplementowaliśmy. To, co po pierwsze, co zaimplementował klient to, co wydaje mu się, że jest bezpieczne, czy w rzeczywistości jest bezpieczne. Bo to bardzo zależy od umiejętności osoby, która to testuje. Deweloper ma inne podejście, jeśli chodzi o weryfikowanie bezpieczeństwa, do pentestera, który nie tyle skupia się na tym czy jakaś funkcjonalność została poprawnie zaimplementowana, co czy jest w stanie obejść to zabezpieczenie, które zostało zaimplementowane i znaleźć jakąś lukę, którą może wykorzystać, z której może wyciągnąć jakieś dane albo zaszkodzić, czy przerwać działanie tej aplikacji. Więc takie testy zewnętrzne są potrzebne. Są potrzebne, bo są takim świeżym spojrzeniem. My też, jak wykonujemy testy staramy się zawsze, żeby przynajmniej dwie osoby z naszego zespołu pracowały nad jednym projektem, żeby mieć taki świeży punkt widzenia czy dwa punkty widzenia, czy dwa podejścia do testów danego systemu. Bo zawsze jedna osoba może mieć doświadczenie lepsze w analizie kodu albo w atakach typu injection, a druga osoba czuć się lepiej w atakach typu weryfikacje uprawnień czy testach sieci na przykład. Więc tutaj jest to istotne, żeby jednak weryfikować to zawsze gdzieś tam z zewnętrznego źródła osoby obiektywnej, która nie tworzyła tego oprogramowania.

Prowadzący: Czyli z jednej strony obiektywnie, z drugiej strony świeże spojrzenie tak naprawdę na temat i na produkt.

Magdalena Mielke: Tak, jak najbardziej.

Prowadzący: Słuchaj, OSINT, biały wywiad. Jakie informacje są dla Ciebie, jako dla pentestera najciekawsze? I z jakich narzędzi najczęściej korzystasz, jeżeli chodzi o OSINT?

Magdalena Mielke: Znaczy, OSINT to jest w ogóle taka…

Prowadzący: Narzędzi to może za dużo powiedziane.

Magdalena Mielke: Tak.

Prowadzący: No ale z jakich źródeł, z jakich źródeł, o tak bym to nazwał, teraz lepiej. Z jakich źródeł korzystasz, aby wygrzebać jakieś ciekawe informacje, które później mogą zostać wykorzystane?

Magdalena Mielke: OSINT jest taką fazą tego początkowego, początkowych faz testów, czyli tego rekonesansu. OSINT to jest tak zwany ten biały wywiad, podczas którego gromadzimy informacje na temat aplikacji czy klienta, firmy, która nam zleca testy, żeby sobie zbudować tak jakby mapę tego, jak

aplikacja może funkcjonować, co może być dostępne, jakie subdomeny mogą występować, czy są jakieś aplikacje, które mogą być ze sobą powiązane, kto pracuje.

[00:35:21]

Magdalena Mielke: OSINT bardzo często jest wykorzystywany w przypadku na przykład testów socjotechnicznych, co pozwala nam zlokalizować osoby, które pracują w danych firmach. To pozwala nam tworzyć ukierunkowane scenariusze ataku na takie firmy i bezpośrednie jednostki. I w przypadku takich, takiego rekonesansu, czy zbierania informacji najczęściej wykorzystuje się w jakiś sposób to, co jest dostępne w Internecie, czyli media społecznościowe, czyli to są jakieś strony o jakichś publicznych rejestrach, czy sprawozdania finansowe, jeśli mamy stricte jakiegoś klienta związanego z finansami, czy informacje o spółkach akcyjnych, czy kontaktach między klientami, jeśli mamy klienta, który jest dostawcą to, z kim współpracuje. To zawsze pozwala nam stworzyć mapę i dobrać bardziej ukierunkowane metody ataku na taką firmę.

Prowadzący: Wiesz co, to skoro już jesteśmy właśnie przy OSINT to nie mogę się powstrzymać, aby nie poruszyć po raz właśnie kolejny stref związanych z social engineeringiem. Przykłady wykorzystania, w celu dostania się do wnętrza infrastruktury, jakieś ciekawe przypadki. Często korzystacie z narzędzi, czy raczej z tak naprawdę kampanii, powiedzmy phishing spear phishing, czy nawet jakichś działań w terenie, bezpośrednio w placówce klienta? Bo pytam się nie przypadkowo, bo w jednym z wcześniejszych odcinków Paweł Maziarz bardzo fajnie na przykład pokazywał, jak wielką moc ma social engineering i jak można to przekuć, tak naprawdę świetne rezultaty dobrania się do infrastruktury.

Magdalena Mielke: Nie bez powodu mówi się, że człowiek jest najsłabszym ogniwem. Więc tak, social engineering jest bardzo istotny, jeśli chodzi o to, jakie informacje możemy pozyskać z danej firmy. I czy jesteśmy w stanie, jak bardzo jesteśmy w stanie zaszkodzić danej organizacji. I tutaj mamy różne metody przeprowadzania takich ataków. Bo mamy taki standardowy phishing, gdzie wysyłamy masowo wiadomości sugerujące kliknięcie w link, informujące o tym, że jest jakaś zniżka albo trzeba coś zresetować, jakieś hasło, bo było nieprawidłowe logowanie, przeróżnego rodzaju scenariusze. Ale są też ataki bardziej ukierunkowane, tak zwane spear phishing i właśnie w tym przypadku wykorzystywany bardzo często jest OSINT, żeby dobrać odpowiednią tematykę i grupę, do której będzie kierunkowany atak phishingowy, w celu podniesienia skuteczności takiego ataku. My dosyć, to znaczy my przeprowadzamy takie ataki, jak najbardziej. I bardzo często sugerujemy też testy socjotechniczne połączone z posteksploitacją, czyli jeśli uda nam się dostać, czy uzyskać jakieś dane, czy to są dane logowania, to sprawdzamy gdzie te dane logowania możemy wykorzystać i jakie informacje jeszcze jesteśmy w stanie dzięki tym danym pozyskać. Oczywiście to też wszystko dokumentujemy. I oferujemy szkolenia z zakresu socjotechniki, czy uświadamiania raczej pracowników

na temat zagrożeń związanych z cyberbezpieczeństwem i socjotechniką, phishingiem. A jeśli chodzi o testy takie typowe terenowe, tak to chyba nazwałeś?

Prowadzący: Tak, tak. No ja tak to nazwałem, dokładnie. Testy w terenie.

Magdalena Mielke: To jest bardzo zależne wiesz dlatego, że to zależy od tego, z jak dużą organizacją mamy do czynienia. Wiadomo, że w przypadku testów małych organizacji, powiedzmy jest to firma, która ma 30-50 osób, testy w terenie są dużo trudniejsze do zrealizowania niż testy w dużych firmach, korporacjach.

Prowadzący: Wiesz, no każdy każdego zna, nie. Więc to jest…

Magdalena Mielke: No właśnie o to chodzi, że tutaj dużo trudniej dostać się do takiego budynku, do takiego biura. W przypadku dużych firm jest to dużo łatwiejsze i nie powiem, że jest to bardzo często wysokoprocentowa skuteczność, powiedzmy 80% skuteczności w takich przypadkach, żeby dostać się do biura, jako osoba podająca się za kogoś, kto ma spotkanie albo pracuje w danej firmie. I tak naprawdę tutaj są różne metody osiągania takich celi. To jest kwestia na pewno wywierania wpływu na innych, kwestia prezencji człowieka.

[00:40:06]

Magdalena Mielke: I do takich testów terenowych wiadomo, że potrzebny jest ktoś, kto jest pewny siebie, ma dobre gadane, tak to powiedzmy, nie jest osobą skrępowaną, łatwo się denerwującą. To musi być osoba bardzo swobodna. W przypadku testów takich typowych phishingowych, na zasadzie kampanii organizowanych w postaci mailowej czy testów socjotechnicznych, polegających na wysyłaniu smsów czy rozmowach telefonicznych, no tutaj jest to troszeczkę inne. Dlatego, że my tutaj przygotowujemy odpowiednio doprecyzowane kampanie pod danego klienta i zbieramy te informacje, mamy narzędzia do tworzenia takich kampanii i automatyzujemy to. Więc to też troszeczkę inaczej wygląda.

Prowadzący: Magda, tak na zakończenie. Czy z Twojego punktu widzenia testy penetracyjne stały się swojego rodzaju normą dla polskich przedsiębiorstw, w odniesieniu do sprawdzenia czy to infrastruktury, czy to aplikacji? Czy ciągle dla niektórych są to elementy egzotyczne i tak mówiąc brzydko, szukanie dziury w całym?

Magdalena Mielke: Wiesz co, wydaje mi się, że to w dużej mierze zależne od tego, z jaką grupą mamy do czynienia, a raczej z jaką branżą. Jeśli chodzi o branżę medyczną, finansową e-commerce mam wrażenie, że ta świadomość cyberzagrożeń znacznie wzrosła, a w szczególności w ostatnich 2 latach, nie oszukujmy się. Bardzo, jeśli chodzi o siłę, wzrost ataków w branży e-commerce wzrosły one prawie o 40% na przestrzeni ostatnich, ostatniego roku czy dwóch lat. Więc tak, świadomość u takich organizacji wzrosła i oni oczekują tych testów. Tylko bardzo często klient chce testów, które zostaną przeprowadzone szybko, zostaną przeprowadzone w taki sposób, że. Inaczej, standardowo klient

zakłada, że w tych testach nic nie wyjdzie, bo jest bezpieczny. Więc tak, podejście wielu klientów jest takie, że chcemy tanie testy i chcemy szybkie testy, w których nic nie wychodzi. No niestety rzeczywistość jest bardzo odwrotna. I bardzo często jest tak, że właśnie u klientów, którzy przychodzą z takim podejściem, że – robimy testy, bo musimy, bo wymaga od nas to jakaś regulacja prawna czy jakieś standardy, ale nic nie znajdziecie. Kończy się tym, że znajdujemy bardzo poważne podatności.

Prowadzący: I z reguły wtedy odbiór, odbiór w sensie, jaka jest reakcja wtedy, że mimo tego, że [niepewne]?

Magdalena Mielke: Znaczy, na pewno zaskoczenie. Ale też bardzo dużo klientów podchodzi do tego z pokorą i nawiązuje dłuższą współpracę z nami, ponieważ jeśli my jesteśmy w stanie pokazać klientowi, że mimo takich zapewnień czy jego przekonania, że jego aplikacja jest bezpieczna czy rozwiązanie, które dostarcza jest bezpieczne, my jesteśmy w stanie pokazać mu, że nie do końca, że są pewne luki, które da się wykorzystać i co się z tym wiąże, ale też pomagamy mu to naprawić. Wspieramy go podczas implementacji, standardowo też podczas naszych, dla naszych klientów oferujemy jakiś tam pakiet konsultacji, które są już po wykonaniu testów w ramach wyjaśnienia, gdyby były problemy z implementacją tych naszych zaleceń. Wyjaśnienia, w jaki sposób to zrobić, żeby było, żeby następnym razem, już podczas retestów te podatności nie zaistniały.

[00:50:06]

Magdalena Mielke: No tutaj mieliśmy właśnie przykład ransomware, więc. Czy wyciek danych z Morele. Kolejna rzecz jest taka, że musimy pamiętać, że jak już przeprowadzane są takie testy i wskazywane są te błędy, to one nie są wskazywane tylko po to, żeby po prostu odbębnić raport i odhaczyć – tak, test został wykonany, ale żeby wprowadzić te zmiany dlatego, że podchodzenie do tematu podatności typu – akceptujemy ryzyko, w jakiś sposób naraża dalej firmę na straty i to straty nie tylko finansowe, ale reputacyjne. Ponieważ firma, która nie przeprowadza testów albo mając świadomość tego, że aplikacja jest w jakiś sposób niebezpieczna, wypuszcza ją na produkcję, nie tylko naraża dane klientów, ale także w pewien sposób sama siebie spisuje na straty. Większość małych firm czy takich typu właśnie e-commerce, typu sklepów internetowych, które pada ofiarami ataków czy wycieku danych, znika z rynku, jeśli są to małe firmy. A duże firmy tracą setki, tysiące klientów i ponoszą gigantyczne straty finansowe, w związku z przełamaniem zabezpieczeń.

Prowadzący: Moim i Państwa gościem była Magdalena Mielke z TestArmy CyberForces. Magda, wielkie dzięki za Twoją obecność i za rozmowę.

Magdalena Mielke: Dzięki śliczne jeszcze raz za zaproszenie i mam nadzieję, że chociaż w niewielkim stopniu udało mi się odpowiedzieć na te pytania i przekazać to, jak istotne są testy bezpieczeństwa, i dlaczego warto je robić.

Prowadzący: Dzięki Magda, jeszcze raz. Do usłyszenia w następnym odcinku.