WARSZTAT HAKERA

TESTY PENETRACYJNE I INNE TECHNIKI WYKRYWANIA PODATNOŚCI

MATTHEW HICKEY, JENNIFER ARCURI

WILEY

Helion

Tytuł oryginału: Hands on Hacking: Become an Expert at Next Gen Penetration Testing and Purple Teaming

Tłumaczenie: Wojciech Moch

ISBN: 978-83-283-7942-8

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *https://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
https://helion.pl/user/opinie/warhak
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

Spis treści

Rozdział

1

Hakowanie jako przypadek biznesowy

Koniecznie musisz przeczytać ten rozdział, jeżeli komunikujesz się z właścicielem firmy, jej *prezesem* (ang. *CEO — chief executive officer*), *dyrektorem ds. bezpieczeństwa informacji* (ang. *CISO — chief information security oficer*) albo po prostu z kimś, kto ma za zadanie poinformować zarząd firmy, dlaczego haking jest dla firm korzystnym zjawiskiem. W tym rozdziale nie znajdziesz praktycznych ćwiczeń związanych z hakowaniem, jakie umieściliśmy w pozostałych rozdziałach. Tutaj skupiamy się na rozważaniu, dlaczego firmy potrzebują hakerów. Wyjaśniamy nasze przekonanie, że najlepszą metodą poprawiania poziomu cyberbezpieczeństwa w organizacji jest przyjęcie przez poszczególne osoby, całe zespoły i ogólnie przez pracodawcę mentalności purpurowego zespołu i sposobu myślenia charakteryzującego złośliwych hakerów. Purpurowy sposób myślenia jest czymś pośrednim między tradycyjnym wyobrażeniem zespołów: niebieskiego i czerwonego, czyli obrońców i atakujących.

> **Jeżeli znasz swojego wroga i znasz siebie, to nie musisz się obawiać o wyniki stu bitew. Jeżeli znasz siebie, ale nie znasz swojego wroga, to każde zwycięstwo będzie okupione porażką. Jeżeli jednak znasz swojego wroga, ale nie znasz siebie, to w każdej walce poniesiesz porażkę.**
>
> ***Sun Tzu, Sztauka wojny***

Zajmowanie stanowiska dyrektora ds. bezpieczeństwa informacji jest podobne do prowadzenia armii. Aby działać efektywnie, armia musi znać siebie i znać swojego wroga. Innymi słowy, potrzebny jest nam zespół, który umie myśleć tak jak hakerzy. Potrzebny jest zespół aktywnie starający się wyszukiwać sposoby, którymi wróg mógłby przypuścić atak, a następnie budujący jeszcze silniejszą infrastrukturę przez łatanie podatności w oprogramowaniu albo tworzenie zasad i mechanizmów bezpieczeństwa. Firmy potrzebują hakerów. I właśnie tym zajmiemy się w niniejszym rozdziale.

Wszystkie komputery są zepsute

W firmie Hacker House mówimy, że „wszystkie komputery są zepsute". Haker nie musi „psuć" komputera, sieci albo oprogramowania, ponieważ każdy komputer od samego początku jest już zepsuty. Haker pokazuje nam jedynie, na czym polega to uszkodzenie. Nowoczesne systemy komputerowe zbudowane zostały na bazie zaufania i naiwności, która jest znacznie starsza od dzisiejszych firm. Po prostu na początku projektowania systemów nie zakładano potrzeby tworzenia zabezpieczeń, dlatego wszystko, co powstało później, stoi na dość chwiejnych fundamentach.

Przyjęcie odpowiedzialności za bezpieczeństwo informacji w dzisiejszych organizacjach to oznaka wielkiej odwagi. Taka odpowiedzialność zazwyczaj spada na barki dyrektora ds. bezpieczeństwa informacji (CISO). Osoba piastująca to stanowisko musi zapewnić odpowiedni poziom ochrony przed katastrofami (awariami systemu, siłami natury albo złośliwymi atakami) całej firmowej infrastrukturze oraz wszystkim danym. W mniejszych organizacjach może nie istnieć stanowisko CISO, a wtedy tę rolę pełni właściciel firmy albo jej prezes. Konieczność chronienia aktywów firmy przed niestrudzonymi, niewidzialnymi i częstymi atakami, które ogólnie nazywane są cyberprzestępczością, to wielka odpowiedzialność. Jeżeli coś pójdzie niezgodnie z planem (a to zdarza się bardzo często), to zwykle ma to fatalne skutki. Ujawnienie danych może pociągać za sobą ogromne straty finansowe, utratę reputacji firmy, a dla osoby piastującej stanowisko CISO może to oznaczać załamanie kariery albo utratę firmy. A to wszystko w wyniku kliknięcia myszą i naciśnięcia kilku klawiszy przez rozgarniętego włamywacza.

Osoby na stanowisku CISO muszą stosować się do reguł *bezpieczeństwa informacji* (ang. *information security*), które znane są też pod nazwą *infosec*. Jest to pojęcie używane jako opis całego sektora naszego przemysłu. *Infosec* oznacza ochronę danych i uniemożliwianie dostępu do systemów komputerowych osobom do tego niepowołanym. Infosec wymaga uzyskania równowagi między użytecznością systemów komputerowych i działającego w nich oprogramowania a bezpieczeństwem tych systemów. Gdyby mógł istnieć całkowicie bezpieczny system, to byłby on zapewne całkowicie nieużywalny z punktu widzenia użytkowników i firm. Na przykład można tu sobie wyobrazić komputer niepodłączony do internetu, zamknięty w bunkrze zakopanym głęboko pod ziemią i otoczony klatką Faradaya, tak aby uniemożliwić jakąkolwiek interakcję ze światem zewnętrznym.

Organizacje muszą jednak otwierać się na świat, aby umożliwić swoim klientom (i pracownikom) dostęp do swoich usług, dlatego całkowicie bezpieczny system nie jest dla nich praktycznym rozwiązaniem, z wyjątkiem ekstremalnych przypadków brzegowych. Przyjrzyjmy się zatem wyzwaniom, którym musi stawić czoła CISO.

W 2019 roku słyszeliśmy o wielu głośnych przypadkach, gdy zhakowane zostały naprawdę wielkie organizacje.

- WhatsApp, bardzo popularny komunikator, okazał się podatny na ataki, które pozwalały atakującemu na przejęcie kontroli nad smartfonem ofiary, co anulowało ochronę, jaką daje stosowane w tym komunikatorze szyfrowanie.
- Pracownik zajmującej się bezpieczeństwem firmy Trend Micro ukradł bazę danych klientów. Te informacje zostały wykorzystane do prób oszukiwania klientów przez kontakty telefoniczne. Ten przypadek pokazuje, jak ważne są wewnętrzne zasady bezpieczeństwa, uzupełniające ochronę usług skierowanych do klientów.
- Firmie Capital One, zajmującej się obsługą kart kredytowych, ukradziono dane ponad 100 milionów klientów. Dokonał tego haker, który podobno wykorzystał niepoprawnie skonfigurowaną zaporę sieciową aplikacji, czyli błąd w technologii, której zadaniem jest ochrona witryn WWW przed atakami! W ukradzionych danych znalazły się nazwiska, adresy, numery ubezpieczeń społecznych oraz dane kont bankowych. Gdy atak został ujawniony w czerwcu 2019 roku, firma Capital One oszacowała koszty związane z tym atakiem na 150 milionów dolarów.
- W grudniu 2019 roku brytyjska firma Travelex znalazła się w centrum zainteresowania, gdy okazało się, że stała się celem ataku typu ransomware. W atakach tego rodzaju atakujący kradną firmowe dane, a następnie żądają okupu w zamian za ich zwrot. W tym przypadku zażądano okupu w wysokości 6 milionów dolarów, choć firma Travelex podobno była w stanie odtworzyć swoje dane bez konieczności płacenia przestępcom. Nie można tego powiedzieć o wielu innych organizacjach i osobach prywatnych, które również stały się celem ataków ransomware.

To tylko niewielki wycinek listy wszystkich włamań, jakie nieustannie się pojawiają. Jeżeli sądzisz, że częstość i wielkość tych zdarzeń jest przerażająca, to przyjmij do wiadomości, że według prognoz w przyszłości będzie tylko gorzej. Cały czas wykładniczo rośnie liczba potencjalnych podatności w firmach oraz ilość gromadzonych danych, ale rośnie też nasza prawna i moralna odpowiedzialność za te dane.

Co więcej, te zagrożenia rosną znacznie szybciej niż tradycyjne możliwości reagowania na nie. Aktualnie polega się głównie na drogich, zewnętrznych usługach *testów penetracyjnych*, czyli takich, w których używane są szczególne umiejętności w celu wyszukania i zgłoszenia organizacji wszystkich wykrytych podatności w systemach komputerowych. W efekcie CISO znajduje się w sytuacji bez wyjścia. Musi próbować lepiej chronić te systemy, mając do dyspozycji zmniejszające się środki. Bez wątpienia coś musi się zmienić.

Na szczęście już teraz coś się zmienia. Dowiesz się tutaj, w jaki sposób można praktycznie, prosto i niedrogo wprowadzić ideę *purpurowych zespołów*, czyli specjalnie szkolonych zespołów bezpieczeństwa wewnętrznego połączonych z silną kulturą bezpieczeństwa panującą w firmie.

Purpurowe zespoły są nowoczesną i skuteczną metodą uzyskania cyberbezpieczeństwa w firmie. Jest to metoda bardzo potrzebna w wielu firmach, zarówno w małych korporacjach, jak i w wielkich, międzynarodowych konglomeratach. Innymi słowy, purpurowe zespoły są niezbędnym elementem w każdej firmie, ponieważ pozwalają uzyskać informacje o sposobach działania atakujących i zdefiniować wskazówki umożliwiające zapobieganie takim atakom.

Stawka

Zanim przejdziemy do opisu purpurowych zespołów i sposobów ich działania, musimy przyjrzeć się dokładniej kontekstowi, w którym musi działać CISO i niemal wszystkie dzisiejsze firmy.

Co jest kradzione i dlaczego jest to wartościowe?

Dane są wartościowe. Danych można użyć do manipulowania poglądami, przelewania gigantycznych ilości pieniędzy, wygrywania wyborów, eliminowania konkurencji, zatrudniania lub zwalniania kadry zarządzającej, szantażowania osób lub firm, a może nawet do wywoływania wojen. Ta lista ciągnie się w nieskończoność. W skrócie: dane są nowym rodzajem bogactwa gromadzonego przez firmy. Są naprawdę niezwykle wartościowe.

Niestety w wielu firmach mało kto (z wyłączeniem prezesów i dyrektorów ds. bezpieczeństwa) zdaje sobie sprawę z wartości tych danych. „Po co ktokolwiek miałby chcieć ukraść nasze zdjęcia albo dane logowania używane przez recepcjonistów?" Brzmi znajomo? Lepiej jest tutaj zadać sobie pytanie: „Dlaczego ktoś miałby *nie chcieć* ukraść tych informacji?". Dobrze jest nie robić rozgraniczeń, które dane są wartościowe, a które nie są. Dla atakującego wartość mają wszystkie dane. Dla złośliwych hakerów dane mają wartość, ponieważ można je sprzedać na czarnym rynku za konkretne pieniądze. Często jest to jedyna motywacja dla osób lub grup starających się ukraść dane.

Dane definiujemy jako informacje w surowej postaci, które można przekształcić w formę użytecznych informacji. Dane są wszędzie: lista płac, dane sprzedaży, szczegóły kont bankowych albo kart kredytowych, osobiste dane identyfikacyjne, e-maile, analizy, hasła, monitoring, statystyki, pliki rządowe, informacje medyczne, raporty naukowe, dokumenty prawne, informacje o subskrypcjach, witryny konkurencji, zapisy finansowe… można tak wymieniać jeszcze długo. Oczywiście im bardziej nasz świat staje się „smart" (używamy smartfonów, smartwatchy, wirtualnych asystentów, smart-wtyczek, smart-termostatów, smart-lodówek, dzwonków do drzwi z kamerą, elektrycznych samochodów, smart-zamków do drzwi… ta lista też nie ma końca), tym więcej generujemy danych, które jednocześnie są coraz słabiej zabezpieczone.

Internet rzeczy podatnych na ataki

Niestety, mimo że wiele domowych urządzeń stało się inteligentnych, to jednak w zakresie ich bezpieczeństwa ta inteligencja pozostawia wiele do życzenia. Powodem może być to, że producenci nie zdają sobie sprawy z istniejących zagrożeń albo te zagrożenia przerastają ich możliwości. Istnieje też możliwość, że producenci świadomie starają się ignorować te zagrożenia (w końcu prace nad zabezpieczeniami zmniejszają uzyskaną marżę), przez co miliony wytwarzanych codziennie inteligentnych produktów nie ma praktycznie żadnych funkcji zabezpieczających. Takie urządzenia (a są ich już miliardy) są używane powszechnie w firmach i prywatnych domach, a większość z nich stanowi poważne zagrożenie dla naszych cennych danych.

Każdy CISO musi zdawać sobie sprawę z faktu, że na świecie nie ma *internetu rzeczy* (*IoT — Internet of Things*), ale z całą pewnością istnieje „internet rzeczy podatnych na ataki" (ang. *Internet of Vulnerable Things*). Dyrektorzy ds. bezpieczeństwa danych muszą się poważnie zastanowić, czy mają zezwolić na zainstalowanie w firmowych budynkach inteligentnych termostatów albo czy

pozwolić członkom zarządu na korzystanie ze smartwatchy (oczywiście pod warunkiem, że ktokolwiek zdecyduje się w ogóle o to zapytać).

Na domiar złego firmy coraz częściej są pociągane do odpowiedzialności prawnej z powodu przechowywanych i przetwarzanych danych. Na przykład wprowadzona w Unii Europejskiej regulacja o nazwie *General Data Protection Regulation* (*GDPR*), która w Polsce znana jest jako RODO (rozporządzenie o ochronie danych osobowych), oznacza, że firmy muszą chronić takie dane jak adresy IP albo informacje z plików cookie, stosując te same zasady, jakie obowiązują w przypadku nazwisk i adresów. Wśród najważniejszych wymagań wynikających z zapisów RODO można wymienić konieczność uzyskania zgody użytkownika na przetwarzanie danych, stosowanie anonimizacji danych w celu ochrony prywatności, podawanie informacji o zauważonych włamaniach, bezpieczną obsługę i transfer danych ponad granicami krajów albo wymuszanie na wybranych firmach zatrudnienia dyrektora ds. ochrony danych, który będzie doglądał zgodności działań firmy z RODO.

Niebieskie, czerwone i purpurowe zespoły

Tradycyjne techniki bezpieczeństwa informacji zakładają istnienie niebieskiego zespołu i czerwonego zespołu (choć nie wszystkie firmy takie mają lub może nie potrzebują tworzyć tych zespołów w ich ścisłej formie). Spróbujmy tu w skrócie opowiedzieć, na czym polega rola każdego z tych zespołów.

Niebieskie zespoły

Niebieskie zespoły skupiają obrońców w „białych kapeluszach” — ludzi skoncentrowanych na swoich systemach, przeprowadzających analizy istniejących systemów w celu zapewnienia ich bezpieczeństwa. Poszukują oni różnych błędów w systemach bezpieczeństwa, kontrolują skuteczność wprowadzonych zabezpieczeń i ciągle sprawdzają, czy raz zaimplementowane zabezpieczenia zachowują swoją skuteczność. W składzie niebieskich zespołów zwykle znajdziemy ludzi świadczących pomoc zdalną, osoby łatające błędy systemów, zajmujące się tworzeniem i odtwarzaniem kopii zapasowych, zarządzające podstawowymi narzędziami zabezpieczającymi itd. Centra danych w większych firmach zatrudniają też administratorów sieci, którzy sprawują pieczę nad sieciami i reagują w przypadku wykrycia włamania. Dąży się do tego, żeby niebieski zespół był w stanie zauważyć przeprowadzany właśnie atak i podjąć kroki w celu zatrzymania go, zanim atakujący będzie w stanie wyrządzić jakiekolwiek szkody.

Czerwone zespoły

Jeżeli chodzi o dokładniejsze kontrole bezpieczeństwa, to większość dyrektorów ds. bezpieczeństwa danych nie będzie miała innego wyboru i będzie musiała utworzyć *czerwony zespół*, który jest niezależną grupą profesjonalistów starających się przełamać zabezpieczenia organizacji, stawiając się w roli atakującego. Czerwone zespoły używają tych samych narzędzi i technik, które są stosowane przez złośliwych hakerów. Ataki mogą być prowadzone przez całe tygodnie, a nawet miesiące.

Każda taka operacja ma zwykle wyznaczony określony cel, którym może być „kradzież" z firmy cennych danych. Po zakończeniu zadania czerwony zespół powinien współpracować z firmowym niebieskim zespołem w celu poprawienia zauważonych niedociągnięć i przygotowania działań naprawczych.

Nie należy mylić czerwonych zespołów z testerami penetracyjnymi. *Testerzy penetracyjni* przygotowują ocenę zabezpieczeń w firmowej sieci komputerowej, a to nie jest tematem tej książki. Przygotowanie takiej oceny bezpieczeństwa zazwyczaj trwa kilka dni. Na jej zakończenie przygotowywany jest raport wskazujący wykryte błędy i podatności. Tester penetracyjny zwykle pracuje samodzielnie i nie oczekuje się od niego przeprowadzania tak dogłębnych ataków, jakie może realizować czerwony zespół. Mimo tego testerzy penetracyjni powinni w swojej pracy stosować te same metody, których używają tradycyjne czerwone zespoły, i używać tych samych technik, którymi posługują się złośliwi hakerzy.

Uwaga **Nie każda firma może sobie pozwolić na zatrudnienie ludzi aktywnie poszukujących zagrożeń i sprawujących pieczę nad siecią (niebieski zespół). Nie każda firma wymaga też stosowania taktycznych, specjalizowanych czerwonych zespołów. Te ostatnie są jednak istotne dla firm przetwarzających wiele transakcji finansowych na sekundę, firm będących ciągłym celem ataków, w których nawet informacje znajdujące się w plikach protokołów mogą ujawniać różne przepływy pieniężne. Mowa tu oczywiście o bankach i firmach hazardowych. Niektóre z tych firm utrzymują własne czerwone zespoły lub testerów penetracyjnych, dzięki czemu nie muszą zlecać tych działań firmom zewnętrznych, chyba że w celu uzyskania dowodów na zgodność z normami.**

Wielkie firmy prywatne (szczególnie te często realizujące różne zlecenia rządowe lub wojskowe, takie jak IBM lub SAIC), jak również agencje rządu USA (takie jak CIA) już od dawna korzystają z czerwonych zespołów. Mniejsze organizacje korzystają z usług testerów penetracyjnych, zazwyczaj zatrudniając ich raz na rok, co daje im wgląd w jakość swoich zabezpieczeń.

Po zakończeniu kontroli zabezpieczeń firmowy niebieski zespół albo zatrudnieni konsultanci muszą podjąć działania na podstawie sugestii podanych przez czerwony zespół lub zapisanych w raporcie testera penetracyjnego. Na tym etapie mogą pojawiać się pierwsze problemy. Dawniej takie etapowe podejście do bezpieczeństwa informacji mogło się sprawdzać, choć też tylko do pewnego stopnia. Dzisiaj sprawdza się już tylko w nielicznych przypadkach.

Jednym z największych problemów jest samo podejmowanie działań na podstawie rekomendacji czerwonego zespołu lub raportu testera penetracyjnego. Ten etap bardzo często nie jest doprowadzany do końca (a czasem nie jest nawet zaczynany) z powodów, o których wspomnimy za chwilę. W efekcie tworzenie takich raportów staje się tylko próżnym zadaniem, które ma jedynie zadowolić udziałowców. Oto częste powody pojawiania się takiej sytuacji:

Niewystarczające przeszkolenie. Niebieskie zespoły często nie wiedzą, jakie działania mają podjąć, ponieważ brakuje im umiejętności wykraczających poza typowe zadania, takie jak zmiana konfiguracji zapory sieciowej, aktualizowanie oprogramowania albo zmiana haseł.

Brak zasobów. Wiele korporacji uważa, że zespoły cyberbezpieczeństwa mają zbyt mało ludzi, a jednocześnie ogromne pieniądze są wydawane na przeprowadzanie testów penetracyjnych, przez co nie ma już możliwości zatrudnienia dodatkowych pracowników.

Ograniczony czas. Firmom bardzo trudno jest nakazać swoim pracownikom, aby spędzali niemało czasu na czytaniu długich raportów technicznych i łataniu podatności, szczególnie wtedy, gdy niebieski zespół zmuszony jest gasić pożary na kilku frontach.

Brak zachęt. Zmotywowanie pracowników do przeczytania długiego raportu z testu penetracyjnego i załatania wskazanych podatności wcale nie jest proste, szczególnie że takie raporty tworzone są przez zewnętrzne osoby (które z pewnością zarobiły na tym sporo pieniędzy).

Czasami, gdy czerwony zespół lub tester penetracyjny (wewnętrzny lub zewnętrzny) wskazuje konkretne uchybienia, członkowie niebieskiego zespołu przechodzą do defensywy. Zaczyna się szukanie winnych, animozje, co prowadzi do chaosu. W efekcie dyrektor ds. bezpieczeństwa danych może być zmuszony nie tylko do zajmowania się technologią, ale i do współpracy z działem personalnym.

To wszystko oznacza, że rozbieżności między niebieskim a czerwonym zespołem, między atakującymi i obrońcami są po prostu zbyt wielkie. CISO musi mieć do dyspozycji ludzi, którzy będą rozumieć taktyki, techniki i procedury używane w cyberatakach i będą wiedzieć, jak najlepiej się przed nimi chronić. Organizacja potrzebuje wewnętrznego zespołu będącego w stanie doszukać się potencjalnych problemów i aktywnie zająć się ich usuwaniem niezależnie od tego, czy chodzi o aktualizację systemu operacyjnego na stacjach roboczych, czy wyłapanie w firmie pomysłu zainstalowania w budynkach firmowych inteligentnych termostatów z dostępem do internetu i podjęcie decyzji, czy to na pewno jest taki dobry pomysł.

Purpurowe zespoły

Rozpatrując bezpieczeństwo danych i systemów komputerowych, właściciele małych firm mogą stosować tę linię rozumowania:

„Potrzebuję skutecznego i niedrogiego rozwiązania dla cyberbezpieczeństwa, aby chronić firmowe dane tak, żeby możliwe było skierowanie wszystkich wysiłków na rozwój przedsiębiorstwa”.

To wszystko da się zrealizować, przyjmując mentalność purpurowego zespołu.

Purpurowy zespół jest prostym i dość oczywistym rozwiązaniem w razie gwałtownego wzrostu liczby włamań i przypadków utraty danych. Chodzi to u to, żeby zespół ekspertów realizował jednocześnie zadania czerwonego i niebieskiego zespołu, starając się przewidywać ewentualne ataki i reagować na pojawiające się podatności i słabości, jeszcze zanim ktokolwiek będzie w stanie je wykorzystać. Purpurowe zespoły są odpowiedzialne za całość systemu firmowych zabezpieczeń. Takie zespoły aktywnie starają się poznawać i oceniać ryzyko, stosując przy tym różne symulacje techniczne. Członkowie takich zespołów wiedzą, czym są cyfrowe aktywa przedsiębiorstwa (które w każdej organizacji stanowią ogromną wartość), gdzie są przechowywane i jak należy je chronić, projektując lepsze sieci i systemy.

To rozwiązanie umożliwia tradycyjnym niebieskim zespołom zrozumienie sposobów wykorzystywania istniejących podatności przez hakerów (albo przez czerwone zespoły). Purpurowe zespoły są lepiej przygotowane do „włączania ludzkiej zapory sieciowej”, co wynika z lepszej edukacji w zakresie typowych metod inżynierii społecznej stosowanych przez cyberprzestępców i pracowników firmy o złych zamiarach. Przykładem może być tutaj *phishing*, czyli technika polegająca

na wysyłaniu do pracowników e-maili próbujących zachęcić ich do kliknięcia łącza ze złośliwą zawartością. Istnieje wiele wariantów tego ataku, ale ataki wykorzystujące inżynierię społeczną generalnie starają się wykorzystać słabości ludzkie, a nie niedostatki systemów komputerowych.

Uwaga ***Phishing*** **(łowienie) jest procesem, który ma doprowadzić do ujawnienia przez ofiarę istotnych informacji, takich jak hasła lub dane karty kredytowej, wykorzystując do tego fałszywe strony WWW zaprojektowane tak, aby przypominały prawdziwe strony banków lub innych instytucji. Hakerzy często korzystają przy tym z e-maili lub komunikatorów, za pomocą których przesyłają swoim ofiarom linki do spreparowanych stron WWW. Istnieją też warianty phishingu, takie jak *spear phishing* (łowienie celowane), gdzie atakujący koncentruje się na określonej osobie, której zachowania są wcześniej analizowane, albo *whaling* (polowanie na grubą rybę), gdzie celem ataku stają się prezesi i dyrektorzy firm, którzy mają zwykle uprawnienia do zatwierdzania transakcji finansowych sprawiających wrażenie całkowicie poprawnych, choć w rzeczywistości będących oszustwami.**

Najlepszym sposobem na uzupełnienie brakujących umiejętności w dowolnym czerwonym lub niebieskim zespole jest połączenie ich w jeden purpurowy zespół, w którym wszyscy członkowie mogą uzyskać niezbędne umiejętności i poznawać zasady rządzące środowiskiem IT i cyklami życia rozwoju oprogramowania, inżynierię społeczną oraz standardy zabezpieczenia systemów, takie jak *STIGs* (*Security Technical Implementation Guides*) dostępne na stronie *www.nist.gov*. Purpurowy zespół cały czas musi działać w „stanie pełnej gotowości na odparcie ataku".

To absolutna konieczność. Jeżeli chcemy zaimplementować rzeczywiście skuteczne praktyki bezpieczeństwa, to firmy muszą zachęcać swoich pracowników do lepszego zrozumienia ryzyka wynikającego z cyberbezpieczeństwa. To naprawdę jest proste. Zmiana polegająca na umieszczeniu bezpieczeństwa w centrum działań firmy oznacza, że dyrektorzy ds. bezpieczeństwa danych nie muszą już wydawać pieniędzy poza własną firmą.

Po utworzeniu purpurowego zespołu nie istnieje już potrzeba opłacania zewnętrznych konsultantów, którzy mieliby prowadzić długotrwałe próby spenetrowania firmowej infrastruktury. Takie działania nierzadko kosztują dziesiątki, a nawet setki tysięcy dolarów. Firmy mogą uzyskać te same efekty dzięki utworzeniu purpurowych zespołów i to bez konieczności proszenia dyrektora finansowego o niezbędne środki. Nie będzie już opóźnień wynikających z oczekiwania na raport, który może zostać źle zrozumiany i nieprawidłowo zaimplementowany. Kariera CISO nie będzie zatem bezpośrednio zagrożona, a firma będzie mogła przeznaczyć czas, pieniądze i energię na właściwe jej innowacje i rozwój.

Purpurowy zespół będzie się sprawdzał wtedy, gdy wszyscy zrozumieją (i to rzeczywiście zrozumieją), jakich zniszczeń mogą dokonać hakerzy w firmowej sieci. Wszyscy muszą też doskonale wiedzieć, jak działają wewnętrzne systemy — sprzęt, systemy operacyjne, zakupione oprogramowanie i to tworzone na zamówienie — jak można je naprawiać i poprawiać, aby zminimalizować istniejące ryzyko. Nie twierdzimy, że każdy członek zespołu musi być ekspertem we wszystkich tych dziedzinach, ale każdy musi znać obszary wiedzy innych członków zespołu, dzięki czemu będą mogli skutecznie ze sobą współpracować, wspomagając się wzajemnie.

Uwaga **Czarny zespół jest rozbudowaną formą czerwonego zespołu, który może realizować ataki będące kombinacją ataków sieciowych oraz ataków osobistych. Czasami takie zespoły nazywane są zespołami bliskiego kontaktu. Czarne zespoły muszą zmagać się nie tylko z zabezpieczeniami cyfrowymi, takimi jak zapory sieciowe, systemy wykrywania włamań albo systemy antywirusowe, ale również muszą uzyskiwać dostęp do kamer monitoringu, systemów alarmowych, systemów kontroli drzwi lub do technologii bezprzewodowych wspomagających mechanizmy bezpieczeństwa w danym miejscu. Czarne zespoły są naprawdę rzadko wykorzystywane w większości organizacji komercyjnych (zwykle nie używa się ich jednak wcale), a z ich usług korzysta się niemal wyłącznie w przypadku krytycznej infrastruktury i zabezpieczanych budynków, gdy istnieje wysokie ryzyko włamania realizowanego przez połączone ataki cyfrowe i fizyczne.**

Hakowanie jako część systemu odpornościowego firmy

Aby skutecznie realizować politykę bezpieczeństwa informacji, trzeba przemyśleć swoje podejście do tematu bezpieczeństwa. Na początek należy odrzucić wszystkie wynikające z lęku uprzedzenia dotyczące hakowania, którymi karmione jest społeczeństwo: zakapturzone postaci, ciemne piwnice i powiązania kryminalne. Dlaczego to takie ważne? Po prostu najlepszym sposobem wprowadzania skutecznych zabezpieczeń jest nauka, aby móc *stać się* hakerem, czyli być w stanie zrobić to, co robią hakerzy.

I to ma sens! Aby zbudować doskonałe zabezpieczenia, trzeba wiedzieć, z czym przyjdzie się nam mierzyć. Nikt nie rusza na wojnę bez uprzedniego pozyskania informacji o przeciwnikach, przeanalizowania własnych słabości i przygotowania metod na ich poprawienie. Niestety właśnie tak zachowuje się większość firm. Nie wyszukują u siebie słabych punktów. Jeżeli organizacja ma zwiększyć swoją odporność na cyberataki, to musi zacząć myśleć tak jak hakerzy. Kropka.

Jednym ze sposobów na poruszenie tego tematu w rozmowach z uczniami i klientami jest zadawanie pytania: „Czy kiedykolwiek włamałeś się do swojego domu?”. Oczywiście większość osób musiała to zrobić (zwykle w wyniku zgubienia kluczy ktoś musiał przynajmniej raz wchodzić do domu przez okno w łazience). W ten sposób doskonale pokazujemy konieczność przyjęcia sposobu myślenia hakera. Skoro próbujesz się włamać do własnego domu, to dlaczego nie próbujesz włamać się do swoich systemów cyfrowych? Na początek można zacząć od wypisywania stanu posiadania, rozmyślania o możliwych punktach wejścia, tworzenia wizualizacji opisującej, kiedy i gdzie zatrzymują się ludzie, itd.

W ten sam sposób można myśleć o całych firmach. W końcu dokładnie tak myślą atakujący nas hakerzy. Zaletą rozbierania rzeczy na części pierwsze jest to, że w ten sposób możemy użyć procesu inżynierii wstecznej, aby przygotować zabezpieczenia i różne rodzaje ataków, które pomogą nam zrozumieć, jak należy chronić swoje systemy.

W związku z tym zachęcamy, żeby porzucić stare wyobrażenia na temat hakingu i zastąpić je takim: hakerzy są wytrwali, niewidoczni, skupieni na swoim celu i na posiadanych danych. *Haking to poszukiwanie wiedzy*.

Aby jeszcze lepiej zabezpieczyć swoją firmę, musimy utworzyć w całej organizacji zupełnie nowe nawyki związane z cyberbezpieczeństwem. To niezbędne, ponieważ większość małych i średnich przedsiębiorstw może nie przetrwać ataku hakerów, a wynikać to może z braku umiejętności szyfrowania oprogramowania albo aktualizowania plików, używania wspólnych danych uwierzytelniających albo nieuczenia pracowników, że nie wolno klikać podejrzanych linków. Innymi słowy, *to pracownicy stanowią jedną z największych podatności niemal każdej organizacji*.

Błędy pracowników często są wynikiem niestosowania się do procedur, braku wyszkolenia i codziennych interakcji z aplikacjami sieciowymi i stronami WWW. Wynika z tego, że zwiększenie poziomu bezpieczeństwa w organizacji powiązane jest z odpowiednią edukacją jej pracowników i ich zaangażowaniem w sprawy bezpieczeństwa. Potwierdza to raport firmy Protiviti z 2017 roku (*https://www.protiviti.com/US-en/insights/it-security-survey*). W tym raporcie wymieniane są cztery najważniejsze elementy:

- Zaangażowany zarząd i zdefiniowane zasady bezpieczeństwa (już tylko to daje wielką różnicę).
- Wprowadzenie klasyfikacji danych i systemu zarządzania nimi (mapowanie danych i wiedza o tym, gdzie znajdują się poszczególne elementy).
- Skuteczność zabezpieczeń zależna od wprowadzonych zasad i od stosujących je ludzi.
- Dojrzały system zarządzania ryzykiem związanym z dostawcami.

W przeszłości implementowanie tych praktyk sprawiało wielkie trudności. Dzięki zastosowaniu purpurowych zespołów staje się ono możliwe, ponieważ do dyspozycji CISO stoją teraz zaangażowani i wykształceni ludzie, niezbędni przy tworzeniu i wprowadzaniu skutecznych zasad bezpieczeństwa oraz odpowiedniej kultury w całej organizacji.

Purpurowe zespoły lepiej radzą sobie z minimalizowaniem ludzkich błędów w firmie przez aktywne definiowanie zasad bezpieczeństwa i informowanie o nich wszystkich pracowników. Dzięki temu pracownicy są świadomi zagrożeń i angażują się w stosowanie zasad bezpieczeństwa. Purpurowe zespoły wspomagają całą załogę firmy, od recepcji, po prezesa, w prawidłowym implementowaniu procesów bezpieczeństwa, ułatwiają rozpoznawanie *inżynierii społecznej*, phishingu i wykrywanie podejrzanych linków. W ten sposób cała firma staje się rozszerzeniem purpurowego zespołu.

INŻYNIERIA SPOŁECZNA

Inżynierię społeczną można postrzegać jak próbę hakowania ludzkiego mózgu, zwykle z zamiarem uzyskania dostępu do systemów komputerowych (przynajmniej w interesującym nas aktualnie kontekście). Inżynieria społeczna wykorzystuje ludzką psychologię w celu manipulowania ludźmi, aby wykonali oni pewne działania albo przekazali wybraną informację. Przykładem może tu być zadzwonienie do jednego z pracowników i przedstawienie się jako pracownik działu IT, a następnie poproszenie o otwarcie określonej strony WWW (którą całkowicie kontrolujemy), aby usunąć wykryty wcześniej problem. Za pomocą takiej strony można następnie uruchomić złośliwy kod na komputerze ofiary i w ten sposób uzyskać dostęp do ważnych danych.

Od strony praktycznej definiowane zasady mogą zawierać plany ochrony informacji (ważną częścią tych planów jest wyznaczenie osoby odpowiedzialnej za ochronę danych), procedury awaryjne (żeby każdy został przeszkolony w czynnościach, jakie trzeba wykonać w przypadku włamania, takich jak wykonywanie kopii zapasowych i automatyzowanie aktualizacji) oraz instrukcje podnoszące świadomość użytkowników.

Zaangażowanie zarządu w te działania będzie znacznie łatwiejsze, jeżeli bezpieczeństwo stanie się częścią firmowej kultury. Z drugiej strony zaangażowanie zarządu w sprawy bezpieczeństwa informacji jest też ważnym czynnikiem przy *tworzeniu* tej kultury. Ponownie musimy odwołać się do badania firmy Protiviti, które wykazało, że zaangażowanie zarządu sprawia, że menedżerowie znacznie lepiej rozumieją, czym są firmowe „klejnoty" (dane), stosują lepsze zasady klasyfikacji danych i potrafią lepiej przekazać pracownikom, czym dokładnie są firmowe dane i jak należy się z nimi obchodzić.

Jak można uzyskać zaangażowanie zarządu? Po pierwsze nie należy stosować zastraszania. W tym przypadku musimy raczej sprawić, żeby ludzie zaczęli poważnie traktować swoje dane i poznawać ich wartość. W wielu przypadkach okazywało się, że pomocne było zastosowanie języka normalnie używanego w rozmowach o bezpieczeństwie informacji. Na przykład członkowie zarządu doskonale znają się na takich tematach jak ryzyko finansowe, ryzyko rynkowe, ryzyko płynności itd. i oczekują, że będzie się o nich wspominać w naszych rozmowach. Mówiąc o cyberbezpieczeństwie, możemy zatem zastosować ich język i mówić o *ryzyku danych* lub o *ryzyku informacji*. W większości przypadków tak przedstawione wiadomości trafiają do celu. Dobrze jest też poszukać możliwości uproszczenia technicznego języka raportów o ryzyku informacji, dzięki czemu treść tych raportów będzie zrozumiała dla większej liczby ludzi. To naprawdę istotne, ponieważ 54% członków zarządów twierdzi, że raporty dotyczące cyberbezpieczeństwa zawierają zbyt wiele technicznych szczegółów (Bay Dynamics Osterman Research, 2016)[1].

Podsumowanie

Wszystkie komputery są zepsute. Nie istnieje coś takiego jak doskonale bezpieczny system. Małe i wielkie organizacje są regularnie atakowane, co często skutkuje kradzieżą znacznych ilości danych ich klientów. Ta sytuacja wcale się nie poprawia, a ciągle pojawiają się nowe urządzenia (zwykle podłączone do internetu) oraz aplikacje, sprawa bezpieczeństwa informacji nabiera więc niespotykanej dotąd wagi.

Aby chronić swoje dane, musimy poznać ich wartość i aktywnie przeciwdziałać próbom ich wykradzenia lub wymuszania okupu. Połączenie wiedzy cechującej atakujących i broniących danych, poznanie metod stosowanych przez przestępców oraz promowanie lepszej kultury bezpieczeństwa są sposobami lepszego chronienia swojej organizacji i jej danych.

Niezależnie od tego, czy pracujesz samodzielnie dla klienta, czy też jesteś częścią zespołu, który przyjął lub właśnie przyjmuje mentalność purpurowego zespołu, z pewnością zawartość tej książki będzie miała dla Ciebie dużą wartość. Być może dopiero zaczynasz pracę nad bezpieczeństwem informacji, a może już od lat pracujesz w dziale IT i chcesz zwiększyć zakres swoich umiejętności. Tę książkę napisaliśmy właśnie dla Ciebie.

[1] *https://www.hackerhousebook.com/.docs/how-board-of-directors-feel-about-cyber-security-reports-1.pdf.*

Przyjrzymy się tu różnym aspektom infrastruktury organizacji — technologiom, z których wszyscy dzisiaj korzystamy, ponieważ gdy chodzi o bezpieczeństwo, często są one błędnie postrzegane. Najpierw jednak w rozdziale 2. „Etyczne i legalne hakowanie" zajmiemy się ważnymi sprawami związanymi z hakowaniem w sposób etyczny i zgodny z prawem. Następnie w rozdziale 3. „Przygotowanie narzędzi do hakowania" przedstawimy techniczny pokaz sposobów konfigurowania własnego systemu na potrzeby etycznego hakowania lub testów penetracyjnych. W kolejnych rozdziałach omówimy różne techniki hakowania, przyjrzymy się bardzo widocznym podatnościom i opiszemy najważniejsze narzędzia. W przedostatnim rozdziale zastanowimy się nad istotą haseł i możliwościami wydobywania ich z plików, które uda się uzyskać w trakcie naszych ćwiczeń. Na zakończenie pokażemy, jak można umieścić znalezione nieścisłości w raporcie, który zostanie przekazany klientowi albo dyrektorowi firmy. Taki raport powinien wyjaśniać wykryte problemy i opisywać metody ich rozwiązania.

Przekonaj się, jak łatwo jest się włamać do Twojego systemu

Bezpieczeństwo systemów informatycznych niejednemu spędza sen z powiek, konsekwencje udanego włamania mogą bowiem oznaczać milionowe straty i zrujnowaną reputację. Przy czym odpowiednie zabezpieczenie systemu jest dla wielu podmiotów niezwykle trudne, gdyż w zespołach brakuje osób z odpowiednimi umiejętnościami. Nawet zatrudnienie zewnętrznego konsultanta nie daje gwarancji, że firmowy system informatyczny będzie bezpieczny i odpowiednio chroniony przed atakami. Okazuje się, że najpewniejszą metodą jest gruntowne przyswojenie wiedzy i umiejętności hakerskich.

Ta książka stanowi kurs praktycznych technik hakowania, dzięki którym dokładnie poznasz zasady i narzędzia używane do przełamywania zabezpieczeń i uzyskiwania dostępu do chronionych danych. Dowiesz się, w jaki sposób należy się przygotować do przeprowadzenia ataku, a także jakie aspekty infrastruktury sieciowej stanowią o jej niedoskonałości i podatności. Poznasz metody zbierania informacji z otwartych źródeł, systemu DNS, usług pocztowych, serwerów WWW, sieci VPN, serwerów plików lub baz danych i aplikacji sieciowych. Nauczysz się korzystać z narzędzi i exploitów do hakowania systemów: Linux, Unix i Microsoft Windows. Do praktycznych ćwiczeń posłużą Ci laboratoria — specjalne środowiska przygotowane do bezpiecznego hakowania, dzięki czemu łatwiej zdobędziesz potrzebne umiejętności.

W książce:

- teoretyczne, praktyczne, prawne i etyczne aspekty hakowania
- koncepcja purpurowych zespołów
- protokoły współczesnego internetu i ich problemy
- włamywanie się do maszyn pracujących pod kontrolą różnych systemów operacyjnych
- krytyczne podatności aplikacji sieciowych
- metody zawodowego hakera

MATTHEW HICKEY jest ekspertem w dziedzinie cyberbezpieczeństwa. Specjalizuje się w hakowaniu, tworzeniu testów penetracyjnych, exploitów i innych narzędzi do hakowania. Prowadzi badania nad zabezpieczeniami systemów osadzonych i nad kryptografią.

JENNIFER ARCURI jest założycielką i prezeską firmy Hacker House. Jest też organizatorką jednej z ważniejszych konferencji technicznych — Innotech. Od lat angażuje się w upowszechnianie wiedzy o cyberbezpieczeństwie.

Helion
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl
KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-283-7942-8
9 788328 379428
Cena: 99,00 zł
WILEY