

Krótki przewodnik etycznego hakowania



tl;dr

(too long, didn’t read)

W skrócie:

Nigdy nie testuj bezpieczeństwa systemów, jeżeli nie masz na to pisemnej zgody właściciela systemu.

Nigdy nie zgłaszaj (sic) luk bezpieczeństwa do banków, instytucji finansowych lub urzędów.

(Chcesz wiedzieć dlaczego? Czytaj dalej)

Krótka sesja Q&A

Q: Co mi grozi, jeżeli przełamuję zabezpieczenia elektroniczne systemu?

A: Zgodnie z polskim Kodeksem Karnym:

Art.267.§1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

(…)

§5.Ściganie przestępstwa określonego w§1–4 następuje na wniosek pokrzywdzonego.

Q: Co mi grozi, jeżeli naruszę spójność danych w systemie?

A: Zgodnie z polskim Kodeksem Karnym:

Art.268.§1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§2.Jeżeli czyn określony w §1dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.

Q: Co mi grozi, jeżeli przełamię zabezpieczenia, a następnie naruszę spójność danych w systemie?

A: Po prostu tego nie rób… :)

Q: A programy bug bounty?

A: Pamiętaj, że istnienie programów *bug bounty* nie sprawia, że Kodeks Karny przestaje obowiązywać. Nadal istnieje zagrożenie, że Twoje działanie przyniesie Ci więcej szkody niż pożytku. Życie. Choć z drugiej strony nie są nam znane przypadki, aby działanie ściśle w ramach programu *bug bounty* wiązało się z konsekwencjami prawnymi dla uczestnika.

Q: „Ale była taka nowelizacja w Kodeksie Karnym, że teraz to wolno hakować wszystkich i wszystko!”

A: Kodeks Karny mówi o tym w inny sposób:

Art.269c.Nie podlega karze za przestępstwo określone w art.267 §2 lub art.269a, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej albo opracowania metody takiego zabezpieczenia i niezwłocznie powiadomił dysponenta tego systemu lub sieci o ujawnionych zagrożeniach, a jego działanie nie naruszyło interesu publicznego lub prywatnego i nie wyrządziło szkody.

Czyli najpierw zarekwirują Twój sprzęt i wytoczą Ci proces, a później zostaniesz uniewinniony w sądzie. :)

Q: Czy to znaczy, że nie powinienem zapewniać bezpieczeństwa systemów?

A: Jesteś testerem lub programistą? Zostałeś zatrudniony do zapewnienia jakości systemu informatycznego? To jest cel Twoich testów. Bezpieczeństwo jest elementem jakości i nie istnieje jakość, jeżeli nie zapewnisz systemowi bezpieczeństwa. Poinformuj kierownika lub *product ownera* swojego projektu. Określ zakres testów. Uzyskaj od niego pisemną zgodę na aktywność (może być mailowa). Przygotuj backup i bierz się do dzieła. Potrafisz testować bezpieczeństwo systemów, prawda?

Q: Dlaczego nie powinienem zgłaszać błędów bezpieczeństwa do banków, instytucji finansowych i urzędów?

A: Czytaj dalej. :)

<http://niebezpiecznik.pl/post/glebokie-ukrycie-danych-w-pko-bp/>

5/5/2010 “Głębokie ukrycie” danych w PKO BP

Pan Waldemar wpisał w Google nazwisko jednego ze swoich dłużników. Wyskoczył mu plik, który zawierał pełne dane ponad 1 000 firm, jak się okazało też dłużników, ale PKO BP. Pan Waldemar zgłosił PKO BP ten fakt …i został przez bank oskarżony o złamanie zabezpieczeń bankowych i próbę szantażu.

“Haker” niewinny

Dziś jest już po śledztwie, na komputerach pana Waldemara biegli sądowi nie znaleźli żadnych śladów umyślnego przełamywania zabezpieczeń bankowych, oskarżenie było bezpodstawne. Pan Waldemar zamierza dochodzić odszkodowania, bo jak sam mówi w wypowiedzi dla TVN24:

*Nie miałem sprzętu. Prace, które miałem zlecone musiałem robić de facto dwa razy, bo sprzęt zabrano. Musiałem kupić na nowo sprzęt, nowe licencje na oprogramowanie*

…a więc jak wszyscy podejrzani o przestępstwa komputerowe, Pan Waldemar stał się ofiarą bezsensownego prawa, które w Polskich warunkach interpretowane jest nie jako zabezpieczenie dowodów elektronicznych, ale ich zarekwirowanie (bo tak jest, mówiąc w skrócie, taniej i wygodniej).

Dlaczego baza PKO była dostępna publicznie?

Przedstawiciel banku, Marek Ryczkowski w wypowiedzi dla TVN24, wyjaśnia:

*Ten plik został zabezpieczony w tak zwanym głębokim ukryciu, jak to mówią informatycy. Jak się okazało po czterech latach za pomocą wyszukiwarki można było do tego pliku dotrzeć. Udało się to jednej osobie*

Macie pomysł, co oznacza “głębokie ukrycie”? ;-)

<http://niebezpiecznik.pl/post/zatrzymala-go-policja-bo-zglosil-blad-na-stronie-urzedu-wojewodzkiego/>

19/5/2013 Zatrzymała go policja, bo zgłosił dziurę urzędnikowi

Jak informuje Echo Dnia, kielecka policja zatrzymała 28-latka, który zgłosił się do Urzędu Wojewódzkiego z informacją o dziurze w jednym z serwerów należących do urzędu…

Zhackował i się przyznał

Jak wynika z relacji rzecznika prasowego wojewody świętokrzystkiego, 28-latek powiadomił w czwartek urząd, że udało mu się włamać na jeden z należących do urzędu serwerów. Przedstawicielka urzędu zapewnia, że nie doszło do kradzieży żadnych ważnych baz danych urzędu, ale sprawę “na wszelki wypadek” badają biegli, którzy w trakcie przeszukania mieszkania 28-latka zajęli 100+ płyt CD/DVD, telefon komórkowy i 2 laptopy.

Ciekawa jest wypowiedź rzecznika prasowego Komendy Wojewódzkiej Policji w Kielcach, który podejrzewa, iż

*niewykluczone, że na nośnikach znajduje się między innymi oprogramowanie służące do łamania zabezpieczeń, czyli tak zwanego hackingu*

Abstrahując od niezbyt precyzyjnego paragrafu, na który zapewne powołuje się rzecznik prasowy KWP (na jego podstawie możnaby przecież postawić zarzuty prawie każdemu administratorowi sieci, albo każdemu użytkownikowi dystrybucji BackTrack; ba zwykła przeglądarka internetowa jest “przystosowana do popełnienia przestępstw” na które powołuje się ten artykuł KK), naszym zdaniem reakcja kieleckiego urzędu, choć całkowicie zgodna z prawem, jest dość surowa jak na okoliczności opisywane przez rzeczniczkę — z jej wypowiedzi wszakże wynika że 28-latek nie żądał pieniędzy za ujawnienie informacji o dziurze ani nie szantażował w żaden inny sposób urzędników — ba, rzeczniczka nawet zapewnia, że “włamywacz” nie uzyskał dostępu do żadnych wrażliwych danych.

Reakcja urzędu jest więc ostra, ale jak najbardziej zgodna z prawem i uzasadniona, jeśli Urząd nie ma pewności co do intencji włamywacza i skali/skutku włamania.

Na niezamówione pentesty jest paragraf

Niech to zdarzenie będzie przestrogą dla wszystkich miłośników “niezamówionych pentestów“. Tego typu czynności to łamanie prawa — wykonując testy bezpieczeństwa bez zgody właściciela infrastruktury, wykonujesz je na własną odpowiedzialność i ryzykujesz zatrzymanie przez policję nawet jeśli swoimi odkryciami za darmo i bezinteresownie podzielisz się z właścicielem. Prawda jest taka, że “po ujawnieniu” twój los jest całkowicie w rękach właściciela sieci, do której się włamałeś — a łatwo jest sobie wyobrazić, jaka jest pierwsza reakcja osoby, która dowiaduje się, że ktoś mógł np. czytać jej pocztę ;)

(…)

Ale ja lubię się włamywać…

Jak widać, czasem hobby pt. “chęć pomocy innym w byciu bardziej bezpiecznym” (jak często tłumaczą się włamywacze) może nas kosztować wiele stresu. Dlatego jeszcze raz przestrzegamy wszystkich przed wykonywaniem niezamówionych testów bezpieczeństwa. Jeśli koniecznie musicie coś “psuć”, celujcie w te firmy, które pozwalają się testować w ramach programów typu Bug Bounty. Nie dość, że za znalezione i zgłoszone firmie w odpowiedzialny sposób błędy nic wam nie grozi, to jeszcze możecie na tym zarobić!

<http://prawo.vagla.pl/node/8154>

2008-10-06 "Nie można przełamać czegoś, co nie istnieje" - polski wyrok w sprawie SQL Injection

Sąd Rejonowy w Głogowie VI Wydział Grodzki w dniu 11 sierpnia 2008 r. wydał ważny wyrok w sprawie mężczyzny oskarżonego o to, że używając komputerów nie będąc do tego uprawnionym, po przełamaniu elektronicznego zabezpieczenia, serwera pewnej firmy, uzyskał informacje - dane osobowe - dla niego nie przeznaczone, działając tym samym na szkodę tej firmy, a więc w sprawie oskarżonego o czyn z art. 267 §1 kodeksu karnego. Sąd wyrokiem (sygn. akt VI K 849/07) uniewinnił oskarżonego od zarzutu, nakazał zwrócić oskarżonemu dowody rzeczowe wymienione w wykazie dowodów, a na podstawie art. 632 pkt 2 KPK orzekł, że koszty procesu ma ponieść Skarb Państwa. Wyrok jest prawomocny. To bardzo ważne rozstrzygnięcie, a dotyczy m.in. granic możliwości przeprowadzania "audytu bezpieczeństwa" serwisów internetowych, a także spraw związanych z tzw. SQL Injection.

(…)

Co znajdziemy w uzasadnieniu wyroku Sądu Rejonowego w Głogowie w sprawie oskarżonego? W pierwszej kolejności opis podjętych przez niego działań. Odwiedził on stronę internetową i stwierdził, że serwis zawiera błędy. Następnie w formularz logowania wpisał ciąg znaków "' or 1=1" (powtarzając tą czynność również w polu hasła), co spowodowało, że został "zalogowany" na konto losowego użytkownika. To zaś spowodowało, że mężczyzna uzyskał dostęp do kilku kont użytkowników z jednoczesnym dostępem do ich danych osobowych. Mężczyzna postanowił wykorzystać ten fakt, a to w ten sposób, iż skontaktował się z przedstawicielami przedsiębiorstwa prowadzącego serwis internetowy i poinformował ich, że "wykrył lukę umożliwiającą wejście do bazy danych marketingowych firm należących lub związanych właścicielsko" z przedsiębiorstwem. W międzyczasie mężczyzna sprawdził również inne strony i serwisy internetowe stworzone przez autora witryny użytkowanej przez przedsiębiorstwo. Zauważył, że wszystkie te strony internetowe zawierały podobne błędy (zostały skonstruowane z wykorzystaniem tego samego systemu zarządzania treścią). Mężczyzna, by uwiarygodnić swoją propozycję, wysyłając list elektroniczny do przedsiębiorstwa umieścił tam dane jednego z pracowników, które uzyskał w wyniku opisywanych wyżej działań. Nie uzyskał żadnej odpowiedzi na propozycję współpracy postanowił wysłać listy bezpośrednio do zainteresowanych firm, których dane były w ramach serwisu przetwarzane.

Doszło do nawiązania kontaktu i mężczyzna został zaproszony do współpracy. W czasie spotkania, na które mężczyzna został zaproszony miała zostać podpisana umowa o dzieło, na podstawie której miał rozpocząć prace w celu usunięcia luk w zabezpieczeniach. Mężczyzna przyjechał na umówione spotkanie, tam podpisał przedstawione mu zobowiązanie do zachowania poufności (z datą sprzed wykrycia błędów), a następnie został zatrzymany przez współpracującą z przedsiębiorstwem Policję.

(…)