



Cena 28 zł

M I E S I Ę C Z N I K M E N E D Ż E R A

INFOMAN

S Y S T E M Y I N F O R M A C Y J N E Z A R Z Ą D Z A N I A

INDEKS 345229

ISSN 1505-3245



3/2000

**Zarządzanie
bezpieczeństwem
systemów
informatycznych str. 40**

**Kradzież informacji
jest bardzo powszechna str. 42**

**Ochrona danych
w środowisku bankowym str. 46**

**Model sieci
bezpiecznej str. 50**

Jacek KURAS

Hakerzy

Omawiając zagadnienia bezpieczeństwa systemów komputerowych nie sposób pominąć bardzo istotnego problemu osobników, którzy wykorzystują Internet do niszczenia pracy innych osób.

W ubiegłym roku opublikowałem w CHIPie felieton piętnujący praktyki stosowane przez hackerów. Chciałem w nim zwrócić uwagę na niebezpieczną działalność tych osób i równocześnie szkodliwą rolę mediów, które częściej gloryfikują niż piętnują praktyki hakerskie.

Po felietonie otrzymałem pocztą internetową obelżewę listy. Na liście dyskusyjnej przeczytałem pod swoim adresem wiele niestosownych komentarzy. Co zatem powoduje, że ponownie postanowiłem włożyć kij w mrowisko? W ostatnich miesiącach spotkałem się z kolejnymi niszczycielskimi wyczynami hackerów, a w mediach przeczytałem i zobaczyłem wiele informacji, które przedstawiają środowisko włamywaczy komputerowych w nazbyt pozytywnym świetle. Spowodowało to, iż ponownie zdecydowałem się zająć tym tematem.

W sylwestrowy wieczór pierwszy program telewizyjny publicznej zaszerwował nam film „Hakerzy”. Gromadka dzielnych młodzieńców o dźwięcznie brzmiących pseudonimach: *Dopalacz, Szpaner, Świrus, Brzytwa, Kosa* ratują świat przed ekologiczną katastrofą. Można byłoby potraktować ten film jako nieszkodliwą bajkę, gdyby nie poglądy młodej widowni. W rozmowie z uczniami stwierdziłem, że ich reakcja na wspomniany film była podobna jak na filmy o Janosiku lub Robin Hoodzie. Nic więc dziwnego, że niejeden ze wspomnianych uczniów chętnie posmakowałby hakerskiego chleba. Oczywiście jestem całkowicie przeciwny wszelkim zakazom wyświetlania lub próbom cenzurowania podobnych filmów. Wydaje się jednak, iż bardzo pożyteczną byłaby, przeprowadzona bezpośrednio po takim filmie, krótka i rzetelna dyskusja specjalistów którzy wyjaśniliby wątpliwości związane z filmem i objaśnili widzom co w filmie jest prawdą, a co wyłącznie ubarwiającą akcją fikcją.

Mam przed sobą czasopismo o ogólnopolskim zasięgu. Po raz kolejny przeglądam artykuł, w którym autor zastanawia się czy warto być hackerem. Czytam, czytam i nadal nie mogę zrozumieć jaki cel przyświecał autorowi? Hacker w tym artykule to postać sympatyczna, a niektóre zdania to po prostu krótki instruktaż dla laików jak zostać hackerem. Nie mam wątpliwości, że wielu początkujących młodych internautów, którzy przeczytali wspomniany artykuł, wykorzysta zaczerpnięte z niego informacje i spróbuje włamać się do cudzego komputera. Z początku mogą być to tylko niewinne próby, które z czasem przerodzą się w niebezpieczną manię nocnych włamań do systemów komputerowych. Niestety, takie publikacje nie należą do rzadkości. Pełne infor-

macje o szkodliwości działań hackerów i ich niebezpiecznych wyczynach praktycznie nie pojawiają się w prasie. Szkoda, bo może pomogłyby one uniknąć wielu użytkownikom komputerów pracujących w sieci przykrych niespodzianek

W ostatnich dniach stycznia 2000 r. mury więzienne opuścił Kevin Mitnick. Artykuły na temat tego najsłynniejszego hakera, które czytałem w minionych latach, przypominały bardziej scenariusze do filmu o Arsenie Lupin niż rzetelną informację o najniebezpieczniejszym włamywaczu komputerowym. Tutaj milionowe straty poniosły wielkie firmy, w filmie cenną kolekcję brylantów zabrano obrzydliwie bogatemu człowiekowi. Ciężka praca FBI wykonywana w celu ujęcia przestępcy prezentowana była zazwyczaj jako seria pasjonujących potyczek samuraja (Tsutomu Shimomura) z legendą Internetu (Mitnick). Brak rzetelnego opisu strat uczynionych przez chorobliwego maniaka sugerował czyn o niewielkiej szkodliwości. Nikt nie próbował uświadomić czytelnika jakie nieobliczalne skutki mogło mieć włamanie Mitnicka do systemu NSCS (Narodowe Centrum Bezpieczeństwa Komputerowego). Nie spotkałem nigdzie informacji o szacunkowym bilansie strat poniesionych w wyniku przestępczych działań. Warto byłoby przedstawić młodym czytelnikom informację, z której dowiedzieliby się ile operacji przeszczepu szpiku kostnego można byłoby wykonać za te pieniądze.

7 lutego 2000 r. w programach informacyjnych telewizji publicznej „reklamowano” ogólnopolski zjazd





hakerów. Telewizja pokazywała jak hakerzy włamali się do serwera i przejęli kontrolę nad kawiarenką internetową. O stratach jej właściciela nikt nie wspominał. Po raz kolejny usłyszałem informację, że prawdziwi hakerzy mają swój kodeks honorowy. Czy ktoś, kto włamuje się bezprawnie do mojego komputera, może być człowiekiem honoru? Przecież ten osobnik różni się od tego, który włamuje się do naszego domu lub auta tylko tym, że robi to siedząc w miękkim fotelu z poczuciem pełnej bezkarności! Z wiadomości telewizyjnych dowiedziałem się jeszcze, iż według polskiego prawa szkodliwe jest tylko takie włamanie, które zagraża obronności państwa. I tutaj jest prawdopodobnie pies pogrzebany. Prawo nie dostosowane do współczesnych realiów, uzupełnione inercją polskiego wymiaru sprawiedliwości, będzie zachęcać hakerów do kolejnych włamań.

Przeglądałem w ostatnich miesiącach listy dyskusyjne dotyczące działań hakerów. Refleksje są bardzo ponure. Znakomita większość osób z list dyskusyjnych traktuje hakerów jako „pożyteczne stworzenia”. Pogląd, że dzięki hakerom wzrasta poziom bezpieczeństwa komputerowego, jest nagminny. Winą za utratę danych w wyniku włamania młodzi entuzjaści komputerów zazwyczaj obarczają osoby, które nie potrafiły zabezpieczyć przed hakerem swoich danych, a nie faktycznego sprawcę.

Nie mam wątpliwości, że żaden z dyskutantów nie doświadczył na własnej skórze efektów włamań hakerów. Taka mentalność, w pewnym stopniu, może być efektem publikacji i filmów przedstawiających komputerowych piratów jako nieszkodliwych maniaków. Nikt nie odważyłby się nakręcić filmu, w którym amator poprawia spartaczoną przez wybitnego chirurga operację na otwartym sercu, bo każdy widz uznałby to za idiotyzm absurd. Filmów o genialnych hakerach poprawiających błędy wybitnych inżynierów oprogramowania nakręcono już sporo.

„Dzień dobry! Wasz serwer ma dziury jak ser szwajcarski. Daję wam czas do przyszłej soboty, jeżeli nie wykorzystacie tego, to trudno. Do widzenia”. „Jaki z ciebie informatyk, że tak łatwo można dostać się

do twoich danych. Do końca tygodnia musisz zapłacić 500 zł, jak nie to usunę wszystkie dane z dysku”. Takie lub podobne informacje przesłane pocztą elektroniczną lub wpisane do plików systemowych spędzają często sen z oczu wielu użytkownikom komputerów.

Tych, którzy osobiście doświadczyli na własnej skórze wandalizmu nocnego gościa, jest coraz więcej. Prostota i niewielkie koszty podłączenia komputera do globalnej sieci powodują lawinowy wzrost liczby komputerów zagrożonych włamaniami. Często zdąza się, że instalując na swoim komputerze system Linux i podłączając go do Internetu nie zdajemy sobie sprawy, iż w wyniku nocnego włamania hakerów możemy utracić wszystkie dane (nawet te, które nie znajdują się na partycjach Linuxa).

Coraz więcej szkół podłączanych jest w naszym kraju do Internetu. Szkoły nie mają funduszy, żeby zatrudniać wykwalifikowanych specjalistów na stanowiskach administratorów sieci. Nic więc dziwnego, że szkolne serwery bardzo często padają ofiarami niszczycielskich zabaw hakerów. Gdy silniejszy bije słabszego trudno mówić o hakerskim kodeksie honorowym...

Do niedawna informacje o niszczycielskich działaniach hakerów były przez wiele osób odbierane jak bajki, które nas nie dotyczą, a więc nie trzeba się ich obawiać. Obecnie takie poglądy należą już do przeszłości.

Największe polskie banki coraz częściej zaczynają udostępniać swoim klientom nowe usługi przy pomocy Internetu. Każdy klient banku wielokrotnie upewni się, czy jego hasło dostępu do własnych oszczędności jest wystarczająco zabezpieczone przed hakerami, nim zdecyduje się poprosić bank o udostępnienie mu usług pozwalających wykonywać dyspozycje finansowe przy pomocy komputera.

W pierwszej dekadzie lutego 2000 r. pierwsze strony gazet relacjonowały przeprowadzoną na niespotykaną dotąd skalę inwazję hakerów. Najpopularniejsze serwisy internetowe zostały całkowicie sparaliżowane. Akcja została zaplanowana bardzo precyzyjnie. Kolejne serwisy trzeba było odłączać w wyniku przeciążenia serwerów gigantyczną liczbą zgłoszeń nadsyłanych z różnych stron USA.

Po atakach na najpopularniejsze serwisy, hakerzy obrali sobie za cel firmy brokerskie, pośredniczące w transakcjach giełdowych. Grupa dochodzeniowa FBI nie wyklucza, że w trakcie tych ataków hakerzy przejęli informacje o numerach kart kredytowych. Jakie będą skutki tej wielkiej akcji przestępczej, dzisiaj jeszcze nie wiadomo...

Czy grozi nam nowy rodzaj zorganizowanej przestępczości? Obecnie prawdopodobnie nikt nie jest w stanie odpowiedzieć na to pytanie. Musimy być jednak przygotowani na to, że nasze ważne dane przechowywane na komputerowym dysku mogą pewnego dnia przestać istnieć. Pamiętajmy więc o odpowiednim ich zabezpieczeniu. Nie tylko haker może usunąć te dane. Dyski czasami ulegają awariom, o czym nie wszyscy pamiętają.