

## Bezpieczeństwo Open Source

# Open Source – wodoszczelny?

Przeciwnicy oprogramowania Open Source twierdzą, że idea rozwoju tego typu oprogramowania jest źródłem wszystkich dziur w systemie bezpieczeństwa. Z kolei adwokaci Open Source twierdzą wręcz odwrotnie. Kto ma rację? Być może obie strony sporu, być może żadna... Postaramy się udzielić odpowiedzi na dręczące użytkowników pytania o Open Source i bezpieczeństwo naszych systemów.

OLAF KIRCH

Jednym z najstarszych banałów dotyczących prac nad systemem Linux jest koncepcja, że zarówno jądro systemu, jak i każdy pracujący pod kontrolą tego systemu program, powstał w mniej lub bardziej przypadkowy sposób. Mniej więcej tak, jakby to była filmowa scena eksplozji bomby puszczona od tyłu. Tysiące pojedynczych elementów porwanych przez wir i wrzuconych razem tworząc jedną, galaretowatą całość, wspartych armią efektów dźwiękowych, pojawiających się przy uruchamianiu systemu.

Wiele osób postronnych może postrzegać proces rozwoju oprogramowania Open Source



## Czy bezpieczeństwo jest policzalne?

Nie jest tajemnicą, że firma Microsoft boryka się cały czas z problemami wiarygodności dotyczącymi bezpieczeństwa jej oprogramowania. Mniej więcej, co sześć miesięcy jakieś dziecko znudzone lekcją informatyki paraliżuje połowę cywilizowanego świata przy pomocy mniej lub bardziej załozzonego robaka rozprzestrzeniającego się przez sieć. Każdy z nas powinien przyjąć te dane do wiadomości i zdać sobie sprawę z konsekwencji finansowych spowodowanych takim wirusem. Nawet jeżeli wyzerujemy ostatnie zero z kwoty pół miliarda dolarów (szacunkowo zniszczenia, jakie poczynił wirus ILoveYou), jest to nadal ogromna suma pieniędzy.

Naigrywanie się z koncernu Microsoft nie kosztuje. Co prawda, jak dotąd firma ta nie zajęła się problemem bezpieczeństwa wystarczająco poważnie, ale czyż nie powinniśmy najpierw sprawdzić, z czego jest zbudowany nasz dom? Nie zapominajmy, że do tej pory powstało już kilka wirusów działających w systemie Linux (np. Ramen), które wykorzystują lukę w zabezpieczeniach dystrybucji Apache. Każdy, kto usuał ze swojej maszyny zestaw eksploaty typu root kit wie, jak podstępne mogą być ataki w Linuksie.

Wiele takich luk jest jakby specjalnie przygotowanych dla początkujących programistów skryptowych. Wystarczy pobrać archiwum tar, rozpakować pliki i uruchomić skrypt. Potem należy tylko sprawdzić automatycznie całe zestawy adresów IP pod kątem podatnych na włamanie usług i zainstalować tylne wejście

właśnie w ten sposób. Ponadto, wielu programistów Linuksa nie sprzeciwia się tej opinii, przedstawiającej Open Source jako spontaniczną organizację wyznającą ideały zwykłych ludzi, które napędzają programistów do działania. A to wszystko wbrew oczywistemu trendowi w kierunku komercjalizacji każdej sfery życia człowieka. W niniejszym artykule nie chcielibyśmy przedstawiać kolejnego manifestu społeczności Open Source – jest już ich wystarczająco dużo. Skupimy się zatem na faktach, a naszym przyrządem pomiarowym będzie bezpieczeństwo oprogramowania.

## Gwarancja jakości a Open Source?

Osoby uważające powstanie ruchu Open Source za coś w rodzaju zjawiska hackerskiego, będą oczywiście poddawać w wątpliwość wszelkie gwarancje jakości, jakie ten proces może zapewnić, o kryteriach bezpieczeństwa nawet nie wspominając.

Oczywiście, że Linux jest bezpieczny! tak powie większość zwolenników tego systemu. Jakie jest jednak uzasadnienie takiego stwierdzenia? Innymi słowy, w jaki sposób można wycenić bezpieczeństwo systemu? Czy w ogóle w rozwoju Linuksa brane jest pod uwagę bezpieczeństwo? Jak można zapewnić wysokie standardy ochrony tego systemu w przyszłości?

AUTOR

Olaf Kirch jest od dziesięciu lat aktywnym użytkownikiem Linuksa. Obecnie pracuje dla SuSE, gdzie zajmuje się protokołami IPv6 i NFS oraz bezpieczeństwem systemu.



(backdoor) w systemach ofiar. Atakom tego typu towarzyszą coraz częściej występujące techniki szpiegowskie, dążące do ukrycia tylnego wejścia przed administratorami systemów: należą do nich np. specjalnie spreparowane wersje programów *ps*, *top* oraz *ls*, ale także ładowne moduły jądra, jak np. *adore*, który ukrywa całe procesy i pliki. Z tego miejsca jest już mały kroczek do stworzenia samorozpowszechniającego się wirusa.

Czy oznacza to, że Linux jest tak (nie)bezpieczny jak Windows? Kieruje to nas bezpośrednio do pytania, czy bezpieczeństwo jest wartością wymierną, a jeżeli tak, to w jaki sposób ją określać?

## Baza danych CERT

Baza danych CERT jest godna uwagi. Przede wszystkim CERT przechowuje wszelkie wydarzenia, które zapisywane są w repozytorium. Mogą to być luki w zabezpieczeniach systemów operacyjnych, raporty o wykryciu wirusów lub luki samego rutera.

W zależności od rodzaju i poziomu ważności CERT, może wydać notatki o podatności na atak, czy o wystąpieniu sytuacji nietypowych.

Baza danych (lub przynajmniej jej publicznie dostępna część) zapewnia także klasyfikację numeryczną każdej podatności na atak, jako ogólną wskazówkę jej poziomu ważności. Przy tworzeniu klasyfikacji wzięto pod uwagę wiele aspektów, np. jak rozległy jest dany problem, czy zagraża infrastrukturze sieci Internet oraz inne parametry. Informacje dotyczące podatności na atak (z kilku ostatnich lat) można ogólnie skatalogować według użytego systemu operacyjnego – rezultatem jest podsumowanie pokazane na Rysunku 1.

Nie wyciągamy jednak pochopnych wniosków z tego rysunku. Same cyferki nie są odpowiednio reprezentatywnym środkiem oceny bezpieczeństwa danego systemu operacyjnego. Wartości te mówią nam po prostu, ile odkryto już luk w bezpieczeństwie poszczególnych systemów oraz na ile poważne są to luki (według CERT). Słupki pokazują nam (mniej więcej dokładnie) jak bardzo zagrożone są poszczególne systemy.

Wykres pokazuje tylko podatność na ataki elementów spotykanych w systemie Li-

nux (pod etykietką Linux). Do tej kategorii należą zatem jądro systemu lub usługi niskiego poziomu obsługujące jądro. Pozostałe aplikacje, takie jak np. Apache czy OpenSSH, zostały umieszczone w grupie pod etykietką Open Source. Do kategorii Unix należą wyłącznie te wydarzenia, które ujrzały światło dzienne w systemie Unix (np. luki w różnych usługach CDE). Pod nazwą kategorii inni producenci umieściliśmy głównie aplikacje systemu Windows (np. serwery FTP i klienci poczty) nie stworzone przez Microsoft.

Wykres jasno pokazuje obecne trendy, zwłaszcza wzrost w tempie wykładniczym. Obecnie w zasadzie nie ma znaczenia, że do jednego systemu można włamać się 50 razy łatwiej niż do innego (w stosunku do 1996 roku), trend jest bardzo wyraźny. Nawet jeżeli zignorujemy konkretne liczby, jest to wystarczające wytłumaczenie, dlaczego bezpieczeństwo stało się tak istotnym problemem w ciągu kilku ostatnich lat. Kolejną rzeczą, na którą trzeba zwrócić uwagę jest fakt, że podatność na ataki rośnie w zasadzie w każdej z opisanych kategorii. Oczywiście niektóre z nich wykazują wyraźny wzrost (słupki Microsoftu podwaja swoją wielkość każdego roku), a inne spadek (np. słupki Linux i Open Source). Kategoria Unix wykazała nawet nieznaczne obniżenie w stosunku do wyjątkowo tłustego roku 2001, kiedy to odkryto całą gamę problemów z CDE.

Czy takie wyniki dają nam prawo do podsumowania, że Linux jest z natury systemem bezpieczniejszym niż Windows? Nie. Jak już pisaliśmy wcześniej, CERT uznaje systemy firmy Microsoft za systemy bardziej narażone na ataki niż systemy Linuksa. Bezpieczeństwo

systemu jako całości zależy zarówno od jakości oprogramowania, jak i od wielu innych aspektów, np. poziomu bezpieczeństwa zapewnianego przez domyślną konfigurację systemu czy też poziomu wiedzy przeciętnego użytkownika tegoż systemu.

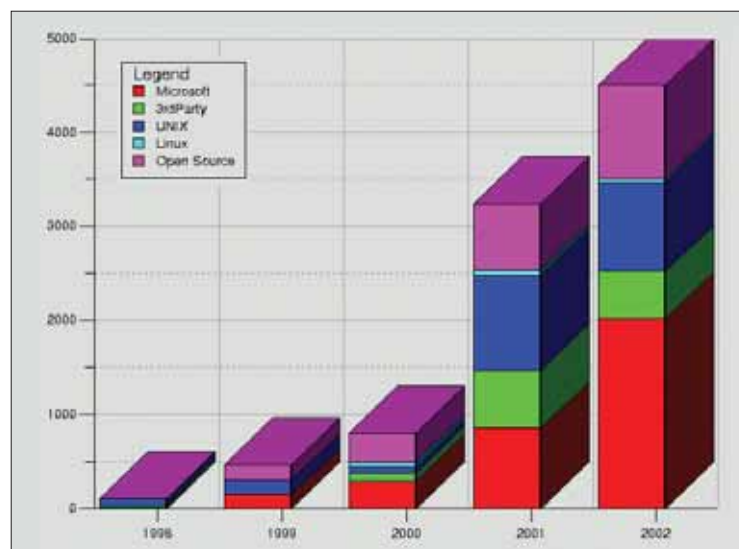
## Co czyni Linuksa systemem bezpiecznym?

Jeżeli podejmiemy się lektury szczegółów technicznych Microsoft Security Updates, znajdziemy tam wielu starych znajomych: błędy jądra, przepełnienie bufora w modułach serwera sieci Web, w serwerze SQL. Pamiętajmy, że Linux także boryka się z tymi problemami. Nie jest to zbyt zaskakujące, prawda? Pomimo wszystkich różnic w filozofii tych dwóch odmiennych systemów, możemy odnaleźć kilka istotnych podobieństw, np. jądro monolityczne, model uprawnień oparty na identyfikacji użytkownika, tzw. superużytkownik zarządzający pracą systemu i posiadający wszelkie przywileje.

Każdy może teraz powiedzieć, że wspomniane błędy występują dużo rzadziej pod Linuxem lub że są ogłaszane znacznie rzadziej. Przynajmniej tak mówią statystyki CERT.

Oczywiście model rozwoju oprogramowania Open Source ułatwia potencjalnym intruzom odkrywanie luk w systemach zabezpieczeń. Z jednej strony możemy samodzielnie przeszukiwać kod źródłowy przy pomocy różnego rodzaju narzędzi (od prostego *grep* do skomplikowanych narzędzi audytowych typu *line-by-line*). Jest to opcja, którą wybiera wielu użytkowników, nie tylko specjaliści, ale też osoby zainteresowane poprawieniem bezpieczeństwa i szczelności zabezpieczeń w Linuksie. Doradcy i agencje zajmujące się bezpieczeństwem, a także oczywiście dystrybutorzy Linuksa upodobałi sobie do badań szczególnie dystrybucje Red Hat i SuSE.

Z drugiej strony jest to normalny etap rozwoju, który (poza nielicznymi wyjątkami) jest procesem otwartym, zatem nie można schować ujawnionych błędów pod przysłowiowy dywan. W historii oprogramowania było już wielu programistów, którzy próbowali w tajemnicy rozwiązywać problemy związane z bezpieczeństwem ich oprogramowania.



Rysunek 1. Informacje statystyczne CERT umożliwiają nam przegląd systemów podatnych na ataki. Zauważmy wykładniczy wzrost ogólnego zagrożenia w tych systemach.

Nagle wydanie nowej wersji programu zmusza hackerów do skierowania swojej uwagi w tę stronę. Niektórzy monitorują nawet wydane poprawki i rozpoznają, czy usunięto właśnie błąd przepełnienia bufora, bez względu na to, jak uspokajające są informacje o wydaniu tej poprawki. Innymi słowy, Open Source posiada swoiste ubezpieczenie, czy też gwarancję jakości, która może być bolesna dla twórcy, ale w rezultacie dzięki niej użytkiwany jest końcowy produkt o wysokim standardzie jakości. Oczywiście nie oznacza to, że nie ma tu miejsca na jakieś ulepszenia, czego dowodem jest projekt OpenBSD. Inną sprawą godną uwagi jest zakres, w jakim ujawniona luka w bezpieczeństwie programu może zostać wykorzystana w typowym systemie. Wiele lat temu dystrybutorzy Linuksa rozpoczęli stopniowe ograniczanie liczby domyślnie włączonych usług.

## Bezpieczeństwo certyfikowane

Brzmi całkiem wyniośle i już samo to określenie przekonuje niektórych użytkowników, nękanych wirusami, do zmiany platformy systemowej na Linuksa. Nie jest to jednak przekonujący argument dla wszystkich – niektórzy użytkownicy potrzebują konkretnych dowodów.

I bardzo słusznie! Przyzwyczailiśmy się już wszyscy do wnikliwego rozważania niezależnych ekspertyz bezpieczeństwa i funkcjonalności naszego otoczenia. Czy wsiedlibyście do samochodu i wyjechali w długą podróż samochodem sklejonym naprędcie taśmą klejącą przez syna naszego sąsiada? Moi przyjaciele jeździli już nim i nic się nie stało – powie wtedy synek. No cóż... pewnie podziękujemy jednak za wrażenia z jazdy takim pojazdem.

Zastanówmy się jednak przez chwilę czy nie jest to sytuacja identyczna do tej, w jakiej stawiają nas producenci oprogramowania? Wypolerowana blacharka błyszczy się przepięknie, a pokrowce na fotele mają piękny kwiatowy wzorek, ale czy o to przede wszystkim chodzi? Linux doskonale pokazuje, że niekoniecznie tak jest.

Obecnie nie istnieje żaden obowiązkowy mechanizm kontroli bezpieczeństwa oprogramowania wprowadzanego na rynek, chociaż ostatnio poczyniono pewne kroki w celu wprowadzenia tego elementu w Stanach Zjednoczonych. W ciągu ostatnich dwóch lat producenci oprogramowania byli naciskani przez władze, aby systemy operacyjne spełniały ogólne wymogi bezpieczeństwa. W Europie także rozważa się wprowadzenie podobnych

wymogów. Również wiele dużych koncernów nalega na certyfikację systemów operacyjnych, z których zamierzają korzystać.

Jest to główny powód poddania dystrybutorów Linuksa ocenie pod kątem kontroli bezpieczeństwa oprogramowania (CC). W lutym ubiegłego roku Red Hat i Oracle wydały wspólne oświadczenie, mówiące o podjęciu prac nad certyfikacją EAL2. W sierpniu tego samego roku SuSE wraz z IBM przeszły pomyślnie proces certyfikacji EAL2, przygotowując się już do certyfikacji EAL3+.

Większości Czytelników nie zdziwi fakt, że cała ta certyfikacja jest głównie odpowiednim wykonaniem papierkowej roboty. Nie powinno jednak dochodzić do sytuacji, w której brak nowego kodu źródłowego będzie równoznaczny z brakiem nowych funkcji z zakresu ochrony systemu, przez co mogłoby dojść do odmowy certyfikacji danego systemu. Udokumentowanie procesów mających wpływ na poziom bezpieczeństwa systemu jest głównym elementem procesu certyfikacji. Przykładowo sprawdza się, w jaki sposób produkt jest testowany, jak obsługiwane są aktualizacje z zakresu bezpieczeństwa systemu, jak zapewnić integralność wersji traceroute, który ma działać nie tylko poprawnie, ale też chronić przed trojanami podrzuconymi na serwer CVS.

Dzięki takiej metodyce, certyfikacje mogą zapewnić pewien rodzaj przezroczystości w sprawach związanych z bezpieczeństwem.

## Trusted Computing?

Organizacja Trusted Computing Group jest oceniana ze skrajnych pozycji. Jedni twierdzą, że jest to największa rewolucja od wynalezienia koła, inni mówią, że jest to koniec oprogramowania Open Source.

Według nas oba twierdzenia są błędne. Chip TPM oraz każda technologia na nim oparta, np. intelowski LaGrande, może zwiększyć poziom bezpieczeństwa systemu operacyjnego. Technologia zabezpiecza nas przede wszystkim przez błędami przepełnienia bufora, czy innymi pomyłkami programistów. Możemy również dobrze całkowicie zignorować TPM. Można skompilować jądro Linuksa i uruchomić je na płycie głównej TPM/LaGrande bez korzystania z funkcji zabezpieczeń. Czy jednak powinniśmy ignorować tę technologię, jeśli daje nam ona coś, co zwiększy bezpieczeństwo Linuksa? Jest to główny powód do dyskusji, mimo że producenci sprzętu nie robią obecnie prawie nic w kierunku zachęcenia do tego rodzaju dyskusji.

Musimy przy tym pamiętać o istniejącym zagrożeniu, że TPM stanie się przeszkodą we

współdziałaniu różnych platform. Przykładowo, klienci CIFS mogą odmówić łączenia z kontrolerem domeny, który nie będzie posiadał certyfikacji Microsoft. Jest to oczywiście realne zagrożenie, ale tego typu problemy zdarzają się także przy okazji dowolnych innych technologii, nie zaś wyłącznie TPM.

## Nowe metody

Kiedy spojrzymy na tę sytuację pod innym kątem, dyskusja przybierze następujący obrót: w Linuksie mogą występować podobne problemy jak w Windows, ale Linux ma tę przewagę, że szybciej sobie z nimi daje radę. Dlatego można twierdzić, że jest bezpieczną alternatywą dla systemu Windows. Społeczność Open Source nie może pozwolić sobie jednak na to, żeby spocząć na laurach. Microsoft przygotował się już do walki, więc bezczynność może być zgubna.

Moim zdaniem musimy pomyśleć o nowych metodach rozwiązania tego problemu. Obecnie stosowana metoda ciągłego poszukiwania, poprawiania luk w systemie jest odpowiednia, ale wkrótce nie będzie już wystarczająca dla coraz większych wymagań bezpieczeństwa. Projekty typu SE-Linux wyglądają obiecująco, ale samo dodanie nowych narzędzi bezpieczeństwa do jądra systemu to za mało. Aplikacje powinny wykorzystywać te narzędzia, a to oznacza już dużo więcej pracy. Trudno jest przekonać twórców oprogramowania, że ich aplikacje, nie ważne jak wspaniałe i ekscytujące, stwarzają zagrożenie dla bezpieczeństwa całych systemów np. ze względu na instalację poprzez *setuid root*. Wielu autorów zripostuje twierdząc: „Pokażcie mi błąd przepełnienia bufora w moim programie, a przyznam wam rację”.

## INFO

- [1] CERT Vulnerability Database: <http://www.kb.cert.org/vuls>
- [2] Common Criteria Certification <http://www.commoncriteria.org/>
- [3] Red Hat/Oracle CC Certification: <http://www.redhat.com/solutions/industries/government/commoncriteria/>
- [4] Suse CC Certification: [http://www.suse.com/us/company/press/press\\_releases/archive03/security\\_certification.html](http://www.suse.com/us/company/press/press_releases/archive03/security_certification.html)
- [5] Trusted Computing: <https://www.trustedcomputinggroup.org>
- [6] Info on LaGrande: [http://www.extremetech.com/print\\_article/0,3998,a=107418,00.asp](http://www.extremetech.com/print_article/0,3998,a=107418,00.asp)

# Linux goes CeBIT!

**CeBIT**  
HANNOVER  
18. - 24. 3. 2004



Present yourself at the largest special exhibition of the CeBIT 2004 on the theme Linux:



**LINUXPARK**

This is where companies will be introducing their latest products and services.

An all-round perfect exhibition appearance:

- contact to thousands of Linux decision-makers
- address numerous new customers directly
- extensive advertising campaign in the run-up to the exhibition
- your own presentations in the LinuxForum
- selected keynote speakers
- renowned media partners/sponsors
- all-inclusive exhibition service

**Find out now!**

**Tel.: +49/2602-961314**

**[www.convigate.com](http://www.convigate.com)**

**CONVIGATE**

**linux**  
USER

**LINUX**  
MAGAZIN

**LINUX NEW MEDIA AG**  
The Pulse of Linux