

## Zabezpieczanie Linuksa w firmach

# Aspekt bezpieczeństwa

Linux już dawno przestał być narzędziem tylko dla naukowców. Odpowiada za wiele ważnych elementów infrastruktury informatycznej przedsiębiorstw, kluczowych dla ich działania. Ale czy jest już wystarczająco bezpieczny?

CEZARY PIEKARSKI



www.photocase.de

**Z**arządzający infrastrukturą informatyczną przedsiębiorstw stają dziś przed trudnym zadaniem – jak zapewnić wysoką wydajność i dostępność systemu, generując jak najmniejsze koszty, jednocześnie gwarantując najwyższe bezpieczeństwo przesyłanych danych? Niemal idealnym rozwiązaniem okazują się systemy bazujące na jądrze Linux, a wśród nich wyróżnia się RedHat Enterprise Linux [2].

System ten w doskonały sposób łączy zalety oprogramowania rozpowszechnianego zgodnie z modelem Open Source (szybkie nanoszenie poprawek, duża dostępność oprogramowania) oraz systemów komercyjnych (dostępność dla wielu platform sprzętowych, wsparcie produktu, ciągłość rozwo-

ju systemu). Przed dystrybucją RedHat Enterprise Linux, produktem dedykowanym dla biznesu, postawiono dużo większe wymagania dotyczące bezpieczeństwa systemu operacyjnego oraz usług niż przed zwykłymi, „akademickimi” dystrybucjami Linuksa. RHEL w aktualnej wersji 3 spełnia te wymagania i oferuje jeszcze więcej.

## Bezpieczeństwo lokalne w RHEL

RHEL3 bazuje na jądrze serii 2.4. To mądry wybór – jądra tej gałęzi są stabilne, wydajne i sprawdzone, jednocześnie zachowują nowoczesny charakter i nie odcinają się od nowych technologii. Model ten udało się uzyskać dzięki włączaniu do jądra serii 2.4 dobrze przetestowanych fragmentów kodu

z jąder gałęzi 2.6. Zaoferowano również szereg poprawek zwiększających bezpieczeństwo systemu właśnie w jego najbardziej kluczowym obszarze – w jądrze. Doskonałym przykładem może być włączony do jądra RHEL3 moduł obsługujący niskopoziomowy fragment warstwy kryptograficznej protokołu IPSEC.

Kolejnym systemem bezpieczeństwa, dołączonym do jądra RedHat Enterprise Linux, jest Exec Shield. Jest to mechanizm utrudniający wykonanie kodu dołączonego przez atakującego do programu. Dodatkowo PIE (Position Independent Executable) dba o zwiększenie pseudolosowego rozrzutu danych zapisywanych przez program w segmentach pamięci.

Dodanie mechanizmu ACL (Access Con-

trol List) dla systemów plików Ext2/Ext3 zwiększyło elastyczność i bezpieczeństwo obiektów. Standardowym dla Linuksa modelem opisującym prawa dostępu do obiektów jest *r-w-x* wraz z podziałem ze względu na UID/GID. ACL'e są idealne w sytuacjach, w których ten model przestaje wystarczać. Przy użyciu mechanizmu ACL pliki oraz użytkownicy proszący o dostęp do tych plików mogą być efektywnie i elastycznie zarządzani oraz grupowani. Na przykład: plik może być dostępny zgodnie z odpowiednimi zasadami dla różnych użytkowników oraz grup na podstawie indywidualnych reguł.

## Bezpieczeństwo usług

Dzięki odpowiedniej konstrukcji systemu udało się uzyskać bezpieczne i stabilne środowisko dla aplikacji uruchamianych w przestrzeni użytkownika. Lecz one także wymagają zwiększonych środków bezpieczeństwa, takich jak możliwość szyfrowania połączeń sieciowych. Jednym z elementów kompleksowego rozwiązania firmy RedHat, mającego zapewnić wysoki poziom bezpieczeństwa aplikacji, są odpowiednie moduły autoryzacji. Za podstawową autoryzację w systemie odpowiada mechanizm PAM. Jego możliwości są naprawdę ogromne. Aplikacja ta potrafi przeprowadzić autoryzację w praktycznie każdym dostępnym systemie udostępniania informacji o użytkownikach.

Dodatkowo jego elastyczna konstrukcja pozwala trochę bardziej zaawansowanym inżynierom systemowym stworzyć własne moduły autentykacji dla jeszcze nie obsługiwanych protokołów. Dla mniej skomplikowanych zastosowań z pewnością wystarczy obsługa LibWrap, zaimplementowana w większości programów dostępnych w dystrybucji RHEL3. LibWrap jest nowym wcieleniem mechanizmu TCP wrappers.

Należy także wspomnieć o dobrze znanym z innych dystrybucji systemu Linux oprogramowaniu NetFilter, realizowanym przez aplikacje iptables, które w RedHat

## Atak typu Man in the middle

Ataki tego typu możliwe są wówczas, gdy napastnik ma dostęp do warstwy pakietów transmitowanych poprzez sieć. Zgodnie z terminologią, atak ten ma miejsce, gdy napastnik jest umieszczony między nadawcą a odbiorcą informacji. Ataki na sesję SSL w większości przypadków rozpoczynają się od sfalszowania odpowiedzi serwera DNS, która powinna wskazywać na komputer atakującego. Następnie intruz przedstawia fałszywy certyfikat w celu nawiązania sesji z klientem, jednocześnie symulując połączenie z rzeczywistym celem atakowanego. W ten sposób może podsłuchiwać lub fałszować dane przesyłane przez klienta.

Enterprise Linux pełni rolę firewalla systemowego oraz umożliwia tworzenie odpowiednich reguł pozwalających na dostęp do serwisów sieciowych tylko z wybranych miejsc. Dla bardziej wymagających użytkowników dostępne są zaawansowane modele autentykacji, takie jak Kerberos, LDAP, RADIUS/TATACS oraz bardzo ciekawy moduł obsługi haseł jednorazowych OPIE/Skey. Systemy te czynią RHEL3 niezależnym od środowiska autentykacji, w którym pracuje.

Kolejnym ważnym modułem kompleksowego zabezpieczenia infrastruktury informatycznej jest dostarczenie oprogramowania pozwalającego na stworzenie odpowiednich kanałów dostępowych do systemu, zarówno w warstwie sieci jak i aplikacji. Zadanie to realizowane jest poprzez udostępnienie narzędzi wspierających standardy IPsec oraz openvpn. Implementacje te pozwalają tworzyć bezpieczne kanały przesyłania danych w niezauważanych sieciach.

Cechą środowiska klasy enterprise powinno być zapewnienie spójności oraz bezpieczeństwa danych przesyłanych przez sieć. Musimy mieć pewność, iż dane dostarczane końcowemu użytkownikowi nie zo-

stały w żaden sposób zmodyfikowane. Cel możemy osiągnąć poprzez mechanizmy kryptograficzne zaimplementowane w aplikacjach oraz oprogramowanie dostarczające takie możliwości programom, które same protokołów szyfrowanych nie obsługują. Poprzez dostarczenie odpowiednich alternatyw dla aplikacji sieciowych nieudostępniających szyfrowania możemy stworzyć środowisko zapewniające wyższy poziom bezpieczeństwa, jednocześnie nie tracąc funkcjonalności normalnych aplikacji. W Tabeli 1 znajduje się wykaz najpopularniejszych usług, wraz z ich bezpiecznymi odpowiednikami, numerami portów oraz aplikacjami realizującymi te usługi.

RedHat Enterprise Linux 3 dostarcza wszystkie aplikacje oraz biblioteki potrzebne do uruchomienia wymienionych usług w środowisku produkcyjnym. Oprócz tego mamy do dyspozycji aplikację, dzięki której sami decydujemy, gdzie i kiedy użyć szyfrowania strumieni sieciowych: stunnel. Jest to doskonałe oprogramowanie stworzone przez Michała Trojnarę (w Linux Magazine 7/2004 opublikowaliśmy artykuł o Stunnel – przypis Redakcji), dostarczające możliwość nawiązywania szyfrowanych połączeń sieciowych tam, gdzie takie połączenia nie zostały przewidziane przez autora aplikacji.

Dodatkowo Stunnel częściowo zdejmuje z programistów obowiązek implementacji protokołów szyfrowanych w ich aplikacjach – to bardzo przyspiesza tworzenie oprogramowania. Sam Stunnel bazuje na bibliotekach projektu OpenSSL [1], dostarczając 128-bitowe algorytmy kryptograficzne. Jego przykładowym zastosowaniem jest zestawienie połączenia pomiędzy klientem pocztowym nie wspierającym protokołu szyfrowanego POP3S a serwerem pocztowym, który obsługuje tylko ten protokół. Stunnel to doskonałe rozwiązanie i oczywiście posiada swój port dla dystrybucji RedHat Enterprise Linux.

Zabezpieczenia oparte o biblioteki OpenSSL są oczywiście możliwe do złamania. Ataki typu Man in the middle (patrz

### Tabela 1: Bezpieczne usługi

Nieszyfrowany (port)	Szyfrowany (port)	Aplikacja
HTTP (80/8080)	HTTPS (413)	Apache + mod_ssl
SMTP (25)	ESMTP/SMTPS (465)	Postfix/Sendmail
POP3 (110)	POP3S (995)	Dovecot
IMAP (143)	IMAPS (993)	Dovecot
FTP (21)	Scp/sftp (22)	OpenSSH
Telnet (23)	SSH (22)	OpenSSH

### Tabela 2: Ilość błędów w różnych systemach operacyjnych

Producent oprogramowania	Liczba błędów	Zakres dni testu	Średnia liczba dni „od błędu do poprawki”
Microsoft	61	982	16.1
SUN	8	716	89.5
RedHat	31	348	11.23

Źródło: Security Portal [4]

ramka obok) są jednak mniej częste i trudniejsze do przeprowadzenia niż zwykłe podsłuchiwanie (sniffing), które grozi nam, gdy używamy protokołów nieszyfrowanych.

### Polityka przygotowywania poprawek

Wybierając oprogramowanie dla systemów kluczowych z punktu widzenia bezpieczeństwa musimy pamiętać o tym, iż żaden z nich nie da nam 100% pewności. System informatyczny nie będzie bezpieczny, jeżeli nie zapewnimy mu możliwości szybkiego dostępu do poprawek oraz opieki odpowiednio przygotowanych administratorów. RedHat rozwiązał ten problem poprzez udostępnienie produktu o nazwie RHN (RedHat Network).

Umożliwia on użytkownikom szybki dostęp do nowych wersji oprogramowania (RedHat nie udostępnia poprawek rozumianych jako moduły do istniejącego oprogramowania – poprawiona wersja jest oddzielnym pakietem typu RPM zawierającym cały program) oraz ułatwia zarządzanie systemem. RHN pozwala łączyć wiele maszyn w grupy, dokonywać automatycznej instalacji nowego oprogramowania i nie tylko. Cały mechanizm zarządzany jest przez interfejs webowy. Dodatkowo RedHat dostarcza cały zestaw aplikacji pozwalających przyspieszyć proces nanoszenia poprawek w wypadku instalacji składających się z wielu systemów (np. RedHat Satellite).

Oprócz dostępności poprawek, ważny jest także czas, jaki upływa od odnalezienia błędu do udostępnienia poprawki. Niezależni specjaliści z firmy Security Portal przeprowadzili porównanie czasu odpowiedzi na wykryty błąd pomiędzy systemami o otwartych źródłach a produktami komercyjnymi, których kody źródłowe nie są udostępniane. Analizie poddano ponad 2000 błędów w różnych systemach operacyjnych. Wyniki (Tabela 2) są zdecydowanie korzystniejsze dla produktów zgodnych z ideą Open Source. Co ciekawe, poprawki dla większości krytycznych błędów w systemie RHEL3 są dostępne dużo szybciej – nawet po kilku godzinach od momentu powiadomienia o błędzie.

W ciągu dwóch lat od udostępnienia Re-

dHat Enterprise Linux pokonał dużą odległość na drodze przystosowania oprogramowania typu Open Source do komercyjnych zastosowań w instalacjach o podwyższonych wymaganiach dotyczących bezpieczeństwa. W 2003 roku RHEL, jako pierwszy z dystrybucji systemu Linux, otrzymał certyfikat zgodności z wymaganiami Departamentu Obrony USA dotyczącymi systemów operacyjnych do podstawowych zastosowań (DoD DISA/COE Certificate). W lutym 2004 roku RedHat Enterprise Linux otrzymał prestiżowy certyfikat EAL2, przeznaczony dla systemów zapewniających wysoki poziom bezpieczeństwa. System ten został także nagrodzony certyfikatem Mitre CVE za pracę nad zwiększeniem bezpieczeństwa systemów operacyjnych. Już wiadomo, że następne wersje dystrybucji RHEL będą starały się o uzyskanie tytułów EAL3 oraz 4. Dzięki planowanemu włączeniu do projektu oprogramowania SE-Linux (początkowo rozwijanego przez Narodową Agencję Bezpieczeństwa USA i przeznaczonego dla systemów krytycznego znaczenia [3]) RedHat Enterprise Linux ma bardzo dużą szansę te tytuły uzyskać.

Z pewnością jest wiele dystrybucji bazujących na jądrze Linux, które przy odpowiednim nakładzie pracy będą bardziej bezpieczne niż RHEL3. Potęgą RedHat Enterprise to jednak nie tylko dobrze przygotowane środowisko, lecz rozsądnie prowadzona polityka przygotowania dystrybucji, ciągłość udostępniania poprawek i doskonałe wsparcie, tak ważny w wypadku rozwiązań przeznaczonych dla biznesu. W najbliższym czasie możemy spodziewać się rewolucyjnych zmian w dystrybucji RedHat Enterprise Linux. Jedną z nich będzie mechanizm SE-Linux, który zupełnie zmieni sposób tworzenia bezpiecznych systemów operacyjnych. Ale to materiał na zupełnie inny artykuł...

### INFO

- [1] Projekt OpenSSL:  
<http://www.openssl.org>
- [2] Informacje o RHEL:  
<http://www.redhat.com/software/rhel/>
- [3] Informacje o SELinux:  
<http://www.nsa.gov/selinux/index.cfm>
- [4] Security Portal:  
<http://odl.lwn.net/2000/0120/security.php3>



Johann Gutenberg, wbrew potocznemu przekonaniu, nie wynalazł wcale druku jako takiego, a drukowania za pomocą pojedynczych, ruchomych czcionek odpowiadających literom w szczególności – idea ta, jeżeli nawet nie przywędrowała bezpośrednio z Chin, to była z całą pewnością znana i wykorzystywana w Europie przed Gutenbergiem. Najważniejszą innowacją Gutenberga było natomiast zastosowanie odpowiedniego stopu cyny, cynku



Rysunek 1: Pierwsza strona (Genesis) Biblii Gutenberga (około 1454 r).

AUTOR

Cezary Piekarski – inżynier systemowy w firmie Altkom Akademia S.A., autoryzowany instruktor RedHat.



www.photocase.de

O wykorzystywaniu dorobku intelektualnego

# Nie tylko Gutenberg

W dyskusji na temat swobody wykorzystywania dorobku intelektualnego dwie historie wydają się bardzo pouczające.

JAROSŁAW UBYSZ

i ołowiu, umożliwiającego skuteczne odlewanie i w rezultacie stosowanie w praktyce czcionek wykonanych z metalu. Drugie usprawnienie polegało na zaadaptowaniu tłoczni do wina i sporządzeniu na tej podstawie prasy drukarskiej.

Ciekawe, co by było, gdyby poszczególne idee i rozwiązania, połączone tak skutecznie przez Gutenberga w jedną całość, podlegały ochronie jako dorobek intelektualny – czy rozwój europejskiej kultury musiałby poczekać na wygaśnięcie odpowiednich praw patentowych? W 30 lat po wynalazku Gutenberga funkcjonowały w Europie 382 prasy drukarskie, przy pomocy których wydano więcej książek niż przez poprzednie tysiąc lat.

Dla sukcesu i rozwoju drukarstwa w Europie nie bez znaczenia był także wybór tytułu pierwszego wydanego przez Gutenberga nakładu. Nie można przy tym nie zauważyć, że wybrał on tytuł chroniony bardzo specyficzną licencją – tekst Biblii mógł być przecież dowolnie powielany, byle by niczego przy tym nie zmieniać.

Podobnie jak wszyscy wielcy uczeni i wynalazcy, Gutenberg skorzystał dowolnie z dorobku intelektualnego swoich poprzedników, dokładając własne idee i tworząc nową jakość, która przy okazji stała się symbolem i którą w historii Europy trudno przecenić.

Drugi przykład dotyczy najważniejszego wynalazku rewolucji naukowo-technicznej. Tłokowa maszyna parowa, skonstruowana przez Thomasa Newcomena, funkcjonowała z powodzeniem w górnictwie angielskim od ponad pięćdziesięciu lat, kiedy James Watt otrzymał zlecenie na wyremontowanie jej modelu należącego do uniwersytetu w Glasgow. Następnie na przestrzeni 20 lat Watt wprowadził do niej wiele rewolucyjnych innowacji, także dzięki temu, że pierwotna konstrukcja nie była chroniona żadnymi licencjami ani patentami.

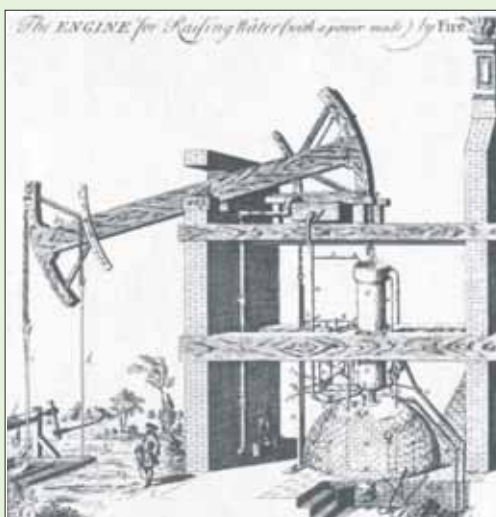
Natomiast zastosowanie przez Watta do zamiany ruchu posuwistego na obrotowy

przekładni planetarnej zamiast korbowodu było spowodowane prozaicznym faktem opatentowania wcześniej przez kogoś rzutkiego i sprytnego zasady działania zwykłej korby. Całkowicie genialnym pomysłem był natomiast odśrodkowy regulator prędkości obrotowej. I w tym przypadku twórcze wykorzystanie powszechnie dostępnego dorobku intelektualnego swoich poprzedników złożyło się na nową jakość i postęp, z niewątpliwym pożytkiem dla wszystkich.

Obie historie, które przytaczam za nieźmiernie ciekawymi opracowaniami na temat historii techniki Bolesława Orłowskiego, mogą służyć jako jedno z wielu, choć na pewno znakomite i bardzo dobitne argumenty na rzecz udziału Wolnego Oprogramowania w rozwoju informatyki.

Tyle tylko, że obie historie wcale się na tym nie kończą. Gutenberg nie zapewnił sobie żadnej skutecznej ochrony własności swojego wynalazku i po wieloletnich procesach zmarł w nędzy, pozbawiony prawa do używania prasy drukarskiej. Natomiast James Watt opatentował swoją maszynę parową i został dzięki temu dobrze prosperującym przedsiębiorcą.

Jaki jest ostateczny morał – zależy po prostu od punktu „siedzenia” i pewnie dlatego wszelkie dyskusje o roli Wolnego Oprogramowania są tak trudne i wydają się z góry pozbawione jakichkol-



Rysunek 2: Maszyna parowa Newcomena.