COMPUTERWORLD Polska

Dlaczego open source nie jest tak bezpieczny, jak powinien?

Kwietniowa awaria OpenSSL, w wyniku której serwery dosłownie „krwawiły” poufnymi danymi (stąd w języku angielskim błąd ten nazwano „heartbleed”), jest niezaprzeczalnym dowodem na to, że otwarte kody źródłowe nie są ani analizowane ani testowane mimo wielu możliwości weryfikacji otwartego oprogramowania w celach bezpieczeństwa. Dlaczego tak się dzieje? Co można zrobić, aby to zmienić?

Computerworld/KB
14.07.2014, godz. 08:00

Przede wszystkim, należy pamiętać o tym, że bezpieczeństwo oprogramowania o otwartym dostępie do kodu źródłowego opiera się głównie na pracy dużych zespołów programistów, którzy dysponują specjalistyczną wiedzą umożliwiającą dokonanie prawidłowej analizy kodu, a następnie usunięcie lub naprawienie powstałych w nim błędów. Dlatego mówi się, zgodnie z Prawem Linusa, że „jeśli mamy wystarczająco dużo par oczu, wszystkie błędy są powierzchniowe”. Oznacza to, że posiadanie ogromnego zespołu testerów pozwala na dostrzeżenie i błyskawicznie rozwiązanie niemal każdego problemu.

Spójrzmy jednak na to, co przytrafiło się OpenSSL. Otóż, pewnego dnia niemiecki programista z Uniwersytetu w Münsterze, Robin Seggelemann, zaktualizował otwarty kod OpenSSL poprzez dodanie do niego nowej funkcji keep-alive o nazwie Heartbeat. Niestety, pominął ważny krok, jakim jest walidacja kodu. Gdyby nie to, z pewnością zauważyłby, że jedna zmienna miała wartość rzeczywistą. Pracownik zespołu ds. rozwoju kodu OpenSSL, który sprawdzał kod przed wypuszczeniem jego aktualizacji, również pominął ten etap. Nieuwaga, bądź zaniedbanie, po stronie dwóch osób niemal doprowadziło do „wykrwawienia”.

Zobacz również:

- **Apache Arrow ma zwiększyć wydajność przetwarzania Big Data**

Bardzo łatwo jest pominąć nieznaczny, wręcz trywialny błąd, niezależnie od tego, czy kod jest analizowany przed jednego czy więcej testerów. Najczęściej po prostu nie wie się, że jakiś błąd powstał, i że trzeba go koniecznie odszukać. Jednakże, w całej historii związanej z OpenSSL niepokojące jest to, że luka „heartbleed” straszyła w tym kodzie od dwóch lat, w przeglądarkach i

na serwerach sieciowych, a i tak nikt ze społeczności skupionej wokół idei otwartego kodu źródłowego nie zauważył, że coś jest nie tak. Wszystko wskazuje na to, że par oczu nie było dość dużo.

Sprzedawcy oprogramowania nie analizują kodu

Otwarty kod źródłowy OpenSSL był stosowany jako element oprogramowania sprzętu komputerowego oferowanego przez dostawców oprogramowania, takich jak m.in. F5 Networks, Citrix Systems, Riverbed Technology i Barracuda Networks. Żadna z tych firm nie przetestowała kodu przed jego wdrożeniem. Brak odpowiedzialności po stronie sprzedawców budzi obawy i kontrowersje, bo każdy kto opiera swoją działalność biznesową na elementach typu open source również powinien poczuwać się do zapewnienia odpowiedniego poziomu bezpieczeństwa.

Zdaniem Mamoona Yunusa, prezesa firmy Forum Systems dostarczającej rozwiązania bezpieczeństwa dla bram chmurowych, kod OpenSSL jest przydatny dla sprzedawców jako dodatek do standardowej oferty, ale nie analizują go pod kątem bezpieczeństwa, ponieważ jest otwarty. Po prostu zakładają, że musi zajmować się tym ktoś inny. A jeśli jest ktoś inny, kto to robi, to odpowiedzialność za kwestie bezpieczeństwa kodu nie spoczywa na nich. Niestety, właśnie z takiego podejścia rodzą się zaniedbania.

Jak sugeruje Yunus, potrzebne są skuteczne programy wzajemnej weryfikacji każdego otwartego kodu źródłowego, z jakiego korzystają sprzedawcy. Powinni oni samodzielnie przeprowadzać analizy statyczne i dynamiczne oraz testować odporność kodu na błędy, aby zapewnić jego możliwie największe bezpieczeństwo. To z kolei wymaga uważnego pochylenia się nad procesami kontroli i zapewnienia jakości w firmie.