

1 Wstęp

Na początku 2005 roku opublikowaliśmy pierwszy raport na temat bezpieczeństwa najbardziej popularnych przeglądarek internetowych <http://www.cert.pl/PDF/Raport_CP_przegladarki.pdf>. Naszą główną motywacją do przygotowania tego raportu był fakt, że poziom bezpieczeństwa poszczególnych przeglądarek stał się jednym z najważniejszych elementów wpływających także na bezpieczeństwo użytkownika Internetu. Od tego czasu w tej kwestii nic się nie zmieniło, a jeśli już, to możemy mówić o jeszcze większej korelacji.

Główne cele tegorocznej edycji raportu o bezpieczeństwie przeglądarek to dalsze zwrócenie uwagi użytkownika sieci na wagę wyboru przeglądarki oraz dalsza próba odpowiedzi na postawione już rok temu pytanie – czy popularność przeglądarki internetowej ma wpływ na wzrost liczby wykrywanych w niej luk?

W raporcie przedstawiamy również ranking bezpieczeństwa przeglądarek, który użytkownik może wykorzystać w procesie wyboru najlepszego rozwiązania dla siebie. Mamy nadzieję, że takie zestawienie będzie pomocne, niemniej jednak już na początku raportu chcemy podkreślić, że taki wybór nie tylko nie gwarantuje pełnego bezpieczeństwa korzystania z sieci, nie zapewnia nawet wyższego poziomu bezpieczeństwa w stosunku do tych osób, które wybrały teoretycznie „gorszą” przeglądarkę, ale o nią bardziej dbają, czyli przede wszystkim stale uaktualniają.

2 Dane statystyczne

Podobnie jak przed rokiem, dane o lukach oparte są o raporty firmy Secunia (<http://www.secunia.org/>). Luki podzielone zostały ze względu na stopień załatania oraz ważność.

Podział luk pod względem stopnia załatania:

- *zalatana calkowicie* – producent udostępnił poprawkę dotyczącą luki, która całkowicie likwiduje problem lub nową wersję aplikacji, w której problem nie występuje
- *zalatana czesciowo* – np. luka została poprawiona w niektórych liniach aplikacji lub została zmieniona konfiguracja domyślna aplikacji, lecz problem nadal może występować w szczególnych warunkach
- *niezalatana* – nie istnieje żadne rozwiązanie problemu ze strony producenta

Podział luk ze względu na ważność

- *krytyczna* – luka umożliwia zdalne i anonimowe przejęcie kontroli nad systemem, bez określonych działań ze strony użytkownika
- *inna*

Uwzględniając udział w rynku poszczególnych przeglądarek¹, zdecydowaliśmy się na porównanie trzech produktów: Microsoft Internet Explorer, Mozilla Firefox oraz Opera. Ponieważ w trakcie roku pojawiały się nowe wersje dwóch ostatnich przeglądarek, liczba wykrytych luk dotyczy również poprzednich wersji (o ile najnowsza stabilna wersja była podatna na lukę). Jako luki niezalatane braliśmy pod uwagę jedynie te, które dotyczą najnowszych stabilnych wersji w momencie zamknięcia raportu.

Raport obejmuje czas od maja 2004 do końca 2005 roku. Okres ten rozpoczyna się wraz z osiągnięciem „dojrzałości” przez przeglądarkę Firefox 0.8 i rozpoczęcie śledzenia jej błędów przez Secunię. Uwzględnione zostały także wszystkie niezalatane luki, bez względu na czas ich wykrycia. W niektórych miejscach umieszczamy dodatkowo statystyki obejmujące wyłącznie cały rok 2005, co pozwala na odniesienie ich do dłuższego okresu i obserwację konsekwencji wzrostu zmiany popularności przeglądarek.

Brane były pod uwagę wszystkie luki dotyczące danej przeglądarki, niezależnie od platformy, której dotyczą.

3 Wskaźniki dotyczące bezpieczeństwa

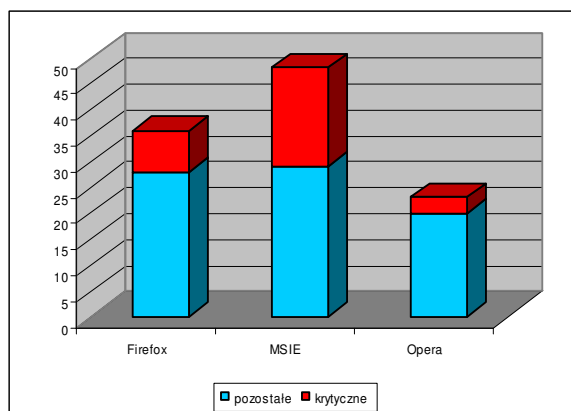
Próbując ocenić bezpieczeństwo przeglądarek na podstawie informacji o lukach, bierzemy pod uwagę dwa podstawowe wskaźniki. Pierwszym z nich jest liczba wykrytych luk w danym okresie ze szczególnym uwzględnieniem luk krytycznych. Drugi, nazwany

¹ Wszelkie statystyki dotyczące udziału poszczególnych przeglądarek pochodzą z badań GemiusTraffic przygotowywanego przez [Gemius S.A.](http://www.gemius.com.pl) i publikowanego na stronach serwisu <http://www ranking.pl/>.

przez nas „poziomem załatania przeglądarki” to liczba oraz procent luk, które zostały przez producenta załatane.

3.1 **Bezwzględna liczba luk, udział luk krytycznych**

Pierwszym kryterium branym przez nas pod uwagę przy ocenie bezpieczeństwa jest ogólna ilość wykrytych luk.



Wykres 1: Bezwzględna liczba luk, w tym luk krytycznych

Tabela 1: Bezwzględna liczba luk, udział luk krytycznych

Przełęczarka	Liczba luk (I.03-XII.04)	Liczba luk	Liczba luk krytycznych (I.03-XII.04)	Liczba luk krytycznych	Procent luk krytycznych
<i>Firefox</i>	18	36	2	8	22%
<i>MSIE</i>	58	48	24	19	40%
<i>Opera</i>	31	23	4	3	13%

Pomimo tego, że okres objęty raportem jest krótszy niż w poprzedniej edycji,, w przypadku przeglądarki Firefox nastąpił wyraźny wzrost zarówno ogólnej liczby luk, jak też luk krytycznych. Widać to jeszcze wyraźniej, gdy spojrzeć się na dane dotyczące jedynie ostatniego roku:

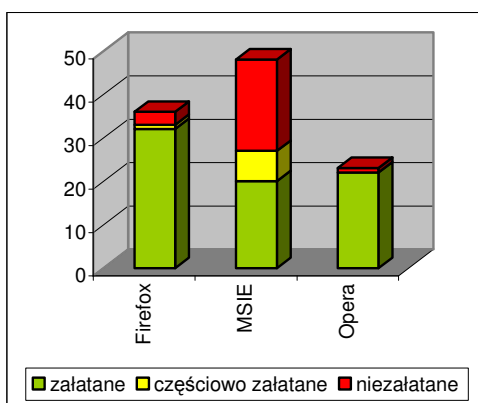
Tabela 2: Liczba wszystkich luk oraz luk krytycznych w 2005 r.

Przeglądarka	Liczba luk (2005)	Liczba luk krytycznych (2005)
<i>Firefox</i>	22	7
<i>MSIE</i>	17	7
<i>Opera</i>	9	3

Jeżeli wziąć pod uwagę wyłącznie bezwzględną liczbę luk wykrytych w przeglądarce, najłabiej wypadł w zeszłym roku Firefox. Wykryto w nim o 1/3 więcej luk niż w MSIE i tyle samo co w MSIE luk krytycznych. Nadal zdecydowanie najmniej luk wykrywanych jest w przeglądarce Opera.

3.2 Poziom załatania przeglądarki

Wskaźnik ten opisany został jako procent udziału luk załatanych we wszystkich lukach dotyczących danej przeglądarki (podajemy również liczbę niezalatanych luk). Obliczyliśmy również poziom załatania przeglądarki dla luk krytycznych.



Wykres 2: Bezwzględna liczba luk w rozbięciu na załatane, częściowo załatane i niezalatane

Tabela 3: Poziom załatania

Przeglądarka	Liczba luk niezalatanych (koniec 2004)	Liczba luk niezalatanych	Procent luk załatanych	Liczba luk krytycznych niezalatanych (koniec 2004)	Liczba luk krytycznych niezalatanych	Procent luk krytycznych załatanych
<i>Firefox</i>	3	3	89%	0	0	100%
<i>MSIE</i>	20	21	42%	4	1	89%
<i>Opera</i>	3	1	98%	0	0	100%

Zdecydowanie najlepszą wartość wskaźnika osiąga Opera – zaledwie jedna luka niezałatana i brak luk częściowo załatanych dają łączny wynik 98%. Tylko nieco słabiej wypada Firefox (89%), który, podobnie jak rok wcześniej, ma 3 niezałatane luki i 1 częściowo niezałatana. MSIE wyjątkowo niski wynik (42%) zawdzięcza aż 28 niezałatanych lub częściowo załatanych lukom. Większość z nich jest co prawda małej wagi (w metodologii Secunia są to zazwyczaj luki *less critical* oraz *not critical*), lecz są wśród nich także luki krytyczne (1 niezałatana oraz 1 częściowo załatana). Wśród pozostałych przeglądarek poziom załatania luk krytycznych wynosi 100%, co wydaje się jedyną akceptowalną wartością.

Liczba załatanych czy niezałatanych luk dotyczy oczywiście konkretnego momentu (w naszym przypadku końca roku). Lepszym wskaźnikiem byłaby informacja, jak dużo czasu zajmuje średnio danemu producentowi przygotowanie poprawki na ujawnioną lukę. Ze względu na trudności w uzyskaniu danych historycznych o dokładnych datach publikowania informacji o lukach i poprawkach, przedstawimy w zastępstwie dane o tym, jak długo znane są najstarsze niezałatane luki w poszczególnych przeglądarkach.

Tabela 4: Najstarsze niezałatane luki

Przeglądarka	Najstarsza niezałatana luka	Najstarsza niezałatana luka krytyczna
Firefox	30.08.2004	-
MSIE	13.03.2003	14.08.2003
Opera	16.11.2005	-

Jak widać, ponownie najlepiej wypada Opera, w której podobnie jak przed rokiem najstarsza luka ma niecałe 2 miesiące. W przypadku Firefoxa najstarsza luka jest z sierpnia 2004 r. Najgorzej wypada MSIE, w którym do tej pory nie załatano luk znanych już od blisko 3 lat, w tym luki krytycznej, którą wykryto w sierpniu 2003 r.

4 Wnioski i rekomendacje

Faktem ciekawym, aczkolwiek nie bezpośrednio związanym z bezpieczeństwem przeglądarek, jest to, że nastąpiła konsolidacja rynku przeglądarek i obecnie wszystkie trzy, omawiane w tym raporcie, posiadają ponad 94% udziałów w rynku. Co ciekawe wzrost popularności Firefoxa nie odbył się kosztem Internet Explorera, jak dość często zakładano w prognozach dotyczących zmian na rynku. Ponad pięciokrotny wzrost popularności Firefoxa nastąpił kosztem wielu innych, mało popularnych przeglądarek, które praktycznie zniknęły z rynku.

Wraz ze wspomnianym wzrostem popularności Firefoxa nastąpił wzrost liczby wykrytych luk w tym programie. W ciągu ostatniego roku luk tych wykryto więcej niż w MSIE, podobna natomiast była liczba wykrytych luk krytycznych.

Nastąpiła pewna polaryzacja, w porównaniu z rokiem ubiegłym, wskaźników poziomu załatania przeglądarek, które dla Firefoxa i Opery układają się na poziomie przynajmniej 90% (odpowiednio – 89% i 98%, niewielki wzrost w stosunku do roku ubiegłego odpowiednio o 6 p.p. i 8 p.p.), zaś dla MSIE wskaźnik ten wynosi zaledwie 42% (spadek aż o 24 p.p.). Warto zwrócić uwagę, że duża liczba luk niezalotanych w długim okresie, nawet jeśli nie są one krytyczne, również jest zjawiskiem niebezpiecznym, gdyż daje intruzom możliwość łączenia efektów wykorzystania kilku z nich i w ten sposób osiągnięcia sukcesu (np.: osiągnięcie wzrostu uprawnień w systemie poprzez atak zdalny w połączeniu z uzyskaniem uprawnień administracyjnych poprzez atak lokalny). Niemniej jednak, tak jak pisaliśmy w roku ubiegłym, jeszcze bardziej istotnym wskaźnikiem jest procent załatania luk krytycznych. Tak jak w ubiegłym roku jedyną przeglądarką, dla której ten wskaźnik nie wynosi 100%, jest MSIE, choć należy zwrócić uwagę na poprawę sytuacji, czyli wzrost z poziomu 83% do 95%.

Już w pierwszej edycji raportu o bezpieczeństwie przeglądarek zwracaliśmy uwagę na to, że największy wpływ na ocenę bezpieczeństwa ma zasada „najsłabszego ogniwa”. W przypadku luk systemowych „najsłabszym ogniwem” są niezalotane luki krytyczne. Biorąc zatem pod uwagę wskaźnik określający procent luk krytycznych załotanych, ocena bezpieczeństwa przeglądarek poddanych analizie jest właściwie taka sama, jak w roku ubiegłym (z uwzględnieniem faktu usunięcia z zestawienia Mozilli). Przeglądarkami rekomendowanymi, które wypadają najlepiej pozostają Firefox i Opera.

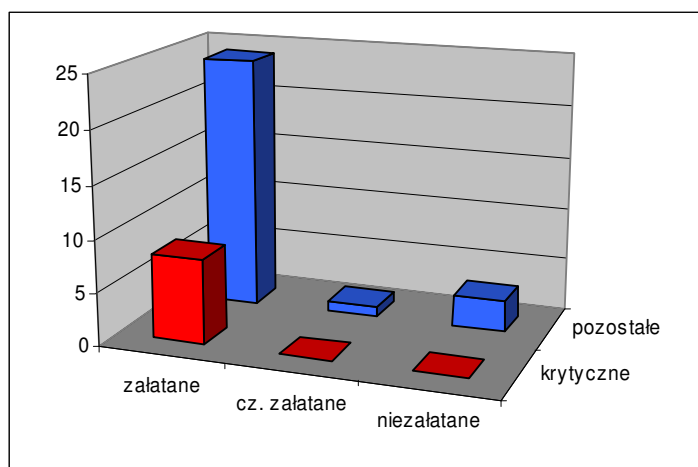
W zeszłym roku próbowaliśmy odnieść się do problemu, jak popularność danego oprogramowania wpływa na liczbę odkrywanych w nim luk, co mogłoby stanowić uzupełnienie wskaźników. Najlepiej jest oczywiście ocenić tę sytuację obserwując proces wzrostu lub słabnięcia popularności przeglądarki. Co prawda okres dwóch lat nie uprawnia do wysuwania zbyt daleko idących wniosków, niemniej jednak pewna prawidłowość została zauważona. W roku 2006 wraz ze wzrostem popularności Firefoxa wzrosła również liczba wykrytych luk w tym oprogramowaniu. Można więc założyć, że wzrost liczby wykrytych luk jest wprost proporcjonalny do wzrostu poziomu popularności przeglądarki. Wynika to przede wszystkim z większych możliwości wykorzystania potencjalnej luki, a więc większej efektywności pracy nad znalezieniem takiej luki. Należy jednak zauważyć, że zwiększona liczba luk w przeglądarce Firefox nie wpłynęła na obniżenie wartości wskaźnika poziomu jej załotania – wartość ta nawet wzrosła. Wskazuje to na duże znaczenie prawidłowego procesu obsługi luk systemowych przez

producenta. Niezależnie od faktu skutecznego załatwienia wszelkich nowych luk jest niestety również efekt ujemny zwiększonej liczby tych luk, wynikający z tego, że nie można liczyć na to, że wszyscy użytkownicy skorzystają z istniejących łat.

5 Dodatkowe informacje dotyczące bezpieczeństwa przeglądarek

W tym rozdziale umieściliśmy kilka zbiorczych informacji o lukach dotyczących poszczególnych przeglądarek oraz adresy stron producentów przeglądarek, na których znajdują się informacje na temat ich bezpieczeństwa.

5.1 Firefox

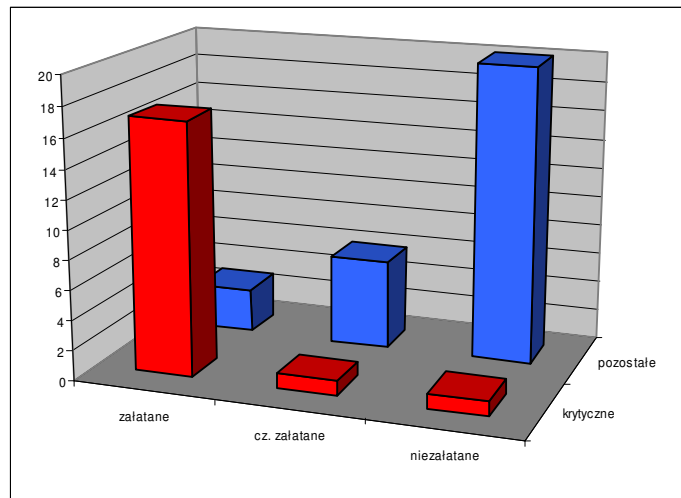


Wykres 3: Rozkład luk w przeglądarce Firefox

Raporty Secunia dotyczące przeglądarki Firefox: <http://secunia.com/product/4227/>

Strona producenta dotycząca bezpieczeństwa: <http://www.mozilla.org/security/>

5.2 MS Internet Explorer

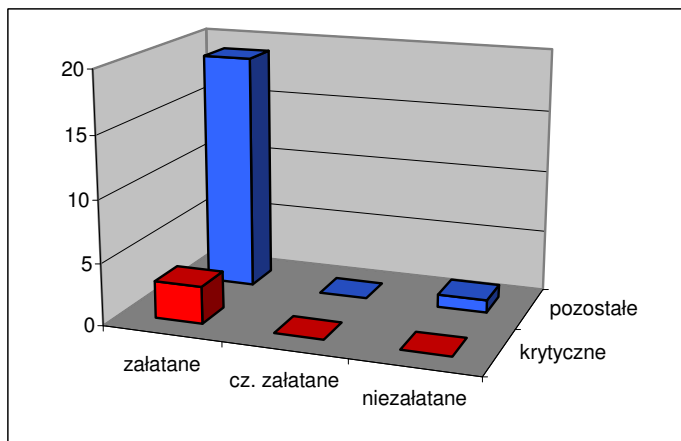


Wykres 4: Rozkład luk w przeglądarce MSIE

Raporty Secunia dotyczące przeglądarki MSIE: <http://secunia.com/product/11/>

Strona producenta dotycząca bezpieczeństwa: <http://www.microsoft.com/security/>

5.3 Opera



Wykres 5: Rozkład luk w przeglądarce Opera

Raporty Secunia dotyczące przeglądarki Opera: <http://secunia.com/advisories/12713/>

Strona producenta dotycząca bezpieczeństwa: <http://www.opera.com/support/service/security/>

6 Informacja o CERT Polska

CERT Polska (Computer Emergency Response Team Polska – <http://www.cert.pl/>) jest zespołem działającym w ramach Naukowej i Akademickiej Sieci Komputerowej (<http://www.nask.pl/>), zajmującym się reagowaniem na zdarzenia naruszające bezpieczeństwo w Internecie. CERT Polska powstał w 1996 roku, a od 1997 jest członkiem FIRST (Forum of Incidents Response and Security Teams - <http://www.first.org/>) - największej na świecie organizacji zrzeszającej zespoły reagujące i zespoły bezpieczeństwa z całego świata. Od roku 2000 jest także członkiem inicjatywy zrzeszającej europejskie zespoły reagujące – TERENA TF-CSIRT (<http://www.terena.nl/tech/task-forces/tf-csirt/>) i działającej przy tej inicjatywie organizacji Trusted Introducer² (<http://www.ti.terena.nl/>). W ramach tych organizacji współpracuje z podobnymi zespołami na całym świecie zarówno w działalności operacyjnej jak też badawczo wdrożeniowej..

Do głównych zadań zespołu CERT Polska należy:

- rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci;
- alarmowanie użytkowników o wystąpieniu bezpośrednich dla nich zagrożeń;
- współpraca z innymi zespołami IRT (Incidents Response Team) – m.in. w ramach FIRST i TERENA TF-CSIRT;
- prowadzenie działań informacyjno-edukacyjnych, zmierzających do wzrostu świadomości na temat bezpieczeństwa teleinformatycznego (zamieszczanie aktualnych informacji na stronie <http://www.cert.pl/>, organizacja cyklicznej konferencji SECURE);
- prowadzenie badań i przygotowanie raportów dotyczących bezpieczeństwa polskich zasobów Internetu;
- niezależne testowanie produktów i rozwiązań z dziedziny bezpieczeństwa teleinformatycznego;
- prace w dziedzinie tworzenia wzorców obsługi i rejestracji incydentów, a także klasyfikacji i tworzenia statystyk;
- udział w krajowych i międzynarodowych projektach związanych z tematyką bezpieczeństwa teleinformatycznego;

² Od 2001 r. zespół CERT Polska posiada najwyższy poziom zaufania Trusted Introducer Accredited Team.