**From:** Grzegorz Pol - Superparkiet [mailto:g.pol@superparkiet.pl]
**Sent:** Monday, December 19, 2011 9:47 PM
**To:** 'aep@o2.pl'
**Subject:** I0G1S4 Pol Grzegorz, zadanie 2 - skanery bezpieczeństwa

Szanowny Panie!

Poniżej zamieszczam rozwiązania zadania nr 2. Skaner GFI niestety nie chciał mi prawidłowo funkcjonować na moim prawdziwym systemie, więc uruchomiłem go na systemie Windows XP SP2 za pomocą wirtualnej maszyny.

|  |
| --- |
| **Microsoft Baseline Security Analyzer** |
|  |  |   Windows 7 x64 |  |
|  |  |  |  |
| **Wykaz niedoskonałości** | **Ryzyko** | **Ocena** | **Postępowanie z ryzykiem** |
| Narzędzia deweloperskie | Duże | Dziurawe aplikacje podatne na ataki | Zainstalować 2 aktualizacje dla Visuala C++ |
| Pakiet Office | Duże  | Dziurawe aplikacje podatne na ataki | Zainstalować 12 aktualizacji dla pakietu Office |
| Wtyczka Silverlight | Duże | Dziurawa aplikacja podatna na ataki | Zainstalować aktualizację dla wtyczki |
| Wtyczka Bing | Średnie | Zmniejszona stabilność i niezawodność systemu Windows Live Toolbar  | Zaktualizować wtyczkę |
| Aplikacja Windows Update | Średnie | Problemy ze strefami czasowymi | Doinstalowąć aktualizację dla systemu x64 |
| Apliakcja SQL Security Update | Niskie | Dziurawa aplikacja Microsoft XML Core Services 6.0 podatna na ataki | Pobrać uaktualnienie aplikacji |
| Wygaśnięte hasła | Średnie | 4 z 5 użytkowników ma hasła, które nie wygasają - ułatwienie włamania | Ustawić maksymalną długość życia hasła |
| Krótkie lub puste hasła | Niskie | 2 z 5 użytkowników ma krótki hasła lub są puste - ułatwienie włamania | Zmienić hasła 2 użytkownikom |
| Aktualizacje automatyczne | Średnie | System jest odpowiednio chroniony zanim użytkownik manualnie zainstaluje aktualizację | Włączyć aktualizacje automatyczne |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **GFI Languard Network Security Scanner** |
|  |  |       Windows XP SP 2 x86 - wirtualna maszyna | **(aplikacja GFI błędnie działała na Win7 x64)** |
|  |  |  |  |
| **Wykaz niedoskonałości** | **Ryzyko** | **Ocena** | **Postępowanie z ryzykiem** |
| Service Pack | Duże | Bardzo duże prawdopodobieństwo ataku dzięki "dziurom" w systemie | Doinstalować dodatek Service Pack 3 |
| Internet Explorer 6 Gold SP 1 | Duże  | Bardzo duże prawdopodobieństwo ataku dzięki "dziurom" w aplikacji | Doinstalować nową wersję aplikacji |
| Outlook Express 6 Gold SP 1 | Duże | Bardzo duże prawdopodobieństwo ataku dzięki "dziurom" w aplikacji | Doinstalować nową wersję aplikacji |
| Dodatek MS01-059(315000) | Duże | Brak kontroli nad buforem w Universal Plug & Play co może doprowadzić do uszkodzenia OS | Zainstalować dodatek |
| Telnet | Niskie | Możliwość wyłudzenia informacji tj. nazwa użytkownika i hasło | Odinstalować telnet |
| Cached Logon Credentials | Niskie | Możliwość wyłudzenia niektórych informacji | Wyłączyć CLC |

Z poważaniem,

Grzegorz Pol