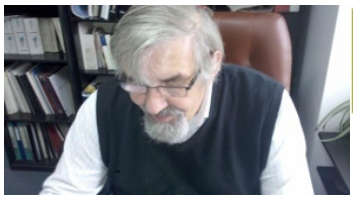

Old Man GURU Magazine

Wychodzi bardzo nieregularnie, kiedy wydaje mi się, że mam coś ciekawego lub pożytecznego do napisania...

Numer 16/2011 26 lipiec 2011

Znaczna większość współcześnie wykorzystywanych systemów informatycznych została zbudowana według następującej zasady:

Wykorzystujemy typowe urządzenia sprzętowe powszechnego użytku oraz wyposażamy je w typowe oprogramowanie. Następnie instalujemy szereg dodatkowych zabezpieczeń sprzętowych (np. popularne linki „Kensington Lock" zabezpieczające przed kradzieżą komputery przenośne) oraz programowych (oprogramowanie antywirusowe, programy Firewall, a nawet programy szyfrujące zapis na dyskach). Jednym słowem – najpierw budujemy sam system zwracając przede wszystkim uwagę na jego funkcjonalność, a dopiero potem wprowadzamy zabezpieczenia.

Ta metoda, choć powszechnie wykorzystywana nie wydaje się być jednak optymalna, ponieważ wiąże się z koniecznością poniesienia dodatkowych kosztów – i nie ma tu znaczenia, czy korzystamy z oprogramowania komercyjnego czy udostępnianego nieodpłatnie. O ile bowiem zabezpieczenia sprzętowe mogą być co prawda dość drogie w zakupie to ich eksploatacja nie generuje zazwyczaj znaczących wydatków, to z oprogramowaniem zabezpieczającym sprawa ma się zupełnie inaczej. Nawet jeśli zdecydujemy się na oprogramowanie nieodpłatne, to musimy wziąć pod uwagę, że wymaga ono ciągłego nadzoru, śledzenia pojawiających się poprawek i uzupełnień itp. Dostawcy oprogramowania komercyjnego zaproponują nam zapewne zawarcie tak zwanego „Maintenance Contract", który co prawda odciąży nas od poszukiwania (niestety nie od instalacji) aktualizacji, jednakże będzie nas kosztować przeciętnie około 20-30% ceny zakupu oprogramowania rocznie.

Warto sprawdzić u źródła – www.us-cert.gov w samym tylko 2011 roku zaleca instalację 9 ważnych ze względów bezpieczeństwa poprawek i uzupełnień dla oprogramowania firm Adobe, Microsoft oraz Oracle, przy czym uwzględnia jedynie poprawki usuwające krytyczne podatności programów, czyli takie, które mogą doprowadzić do uzyskania nieautoryzowanego dostępu do systemu, informacji w nim przechowywanych lub poważnych zakłóceń w jego pracy (np. Denial of Service).

19 lipca br. CERT w USA zdecydował się opublikować dokument o sygnaturze TA11-200A zatytułowany „Security Recommendations to Prevent Cyber Intrusions", który jest dostępny po adresem www.us-cert.gov/cas/techalerts/TA11-200A.html. Zawiera on zestaw zaleceń uzupełniających informacje zawarte w publikacjach NIST poświęconych bezpieczeństwu systemów komputerowych (seria 800).

Czy naprawdę nie można zbudować profesjonalnego systemu informatycznego, którego bezpieczeństwo nie będzie wynikać jedynie z mnogości wielu zastosowanych dodatkowych zabezpieczeń?
Odpowiedź brzmi – można, pod warunkiem, że wymagania bezpieczeństwa uwzględnimy już na etapie projektowania, budowy lub modernizacji systemu. I wcale nie musi to oznaczać ograniczenia funkcjonalności systemu i wygody jego użytkowania.

W poprzednim numerze „Guru" napisałem, że uczyć się należy nawet od diabła. Zacznę więc od początku, czyli od systemu BIOS.

Zapewne wiele osób będzie bardzo zdziwionych – bo co może mieć wspólnego BIOS komputera PC z bezpieczeństwem systemu informatycznego? A jednak tak poważna instytucja jak NIST opublikowała w kwietniu 2011 dość obszerny dokument zatytułowany „Basic Input/Output System (BIOS) Protection Guidelines" (SP800-147). Jest on dostępny pod adresem http://csrc.nist.gov/publications/PubsSPs.html#800-50. Poświęcono go przede wszystkim zagadnieniom bezpieczeństwa związanym z uaktualnieniami BIOS.

System BIOS ma zasadnicze znaczenie dla sprawnej pracy komputera. Błędy w tym oprogramowaniu (przypadkowe lub celowo wprowadzone), a nawet niepoprawna konfiguracja mogą skutkować brakiem możliwości korzystania z komputera. BIOS jest pierwszym programem uruchamianym przy uruchamianiu komputera i np. niepoprawna konfiguracja monitora może doprowadzić do tego, że nie będzie on w ogóle obsługiwany i stracimy możliwość komunikacji z komputerem. Doświadczyłem już w praktyce takich przypadków. BIOS jest także odpowiedzialny za załadowanie systemu operacyjnego oraz uruchomienie obsługi urządzeń peryferyjnych.

Dostęp do systemu BIOS powinien podlegać ochronie. Producenci sprzętu przewidują możliwość wprowadzenia hasła dostępu do interfejsu pozwalającego skonfigurować BIOS, jednakże w większości popularnych komputerów może być łatwo usunięte za pomocą odpowiedniej operacji sprzętowej. Ustanawiając SZBI (System Zarządzania Bezpieczeństwem Informacji) należy więc bezwzględnie opracować procedury związane z ochroną samego systemu BIOS, jak i jego konfiguracji oraz aktualizacji.

W tym miejscu warto przypomnieć po raz kolejny podstawową zasadę bezpieczeństwa: „Nie można zabezpieczyć skutecznie sprzętu za pomocą oprogramowania". Dlatego komputery PC wykorzystywane w systemach profesjonalnych powinny być bezwarunkowo zabezpieczone przed otwarciem obudowy lub przynajmniej w plomby, bez uszkodzenia których nie da się obudowy otworzyć. Obecnie komputery PC nie są na ogół plombowane przez producentów ze względu na ich otwartą architekturę, zabezpieczenie lub zaplombowanie obudowy powinno być więc wykonane przez dział IT organizacji przed przekazaniem komputera do eksploatacji. Procedury z tym związane powinny obejmować także wprowadzenie wymaganej konfiguracji systemu BIOS, zapisanie parametrów konfiguracyjnych w metryce komputera i zabezpieczenie programu konfiguracyjnego hasłem spełniającym wymagania Polityki Bezpieczeństwa.

W nowszych systemach klasyczny BIOS jest coraz częściej zastępowany przez nowsze rozwiązanie UEFI (Unified Extensible Firmware Interface) opracowane początkowo dla serwerów z procesorami Intel , którego najnowsza wersja (2.3.1) została zatwierdzona w kwietniu 2011 r. Szczegóły tego rozwiązania publikowane są na stronie UEFI Forum – www.uefi.org.

UEFI BIOS posiada budowę modularną, umożliwia start systemu operacyjnego z dysków o bardzo dużej pojemności oraz jest w dużej mierze niezależny od rodzaju wykorzystywanego przez system procesora (CPU Independent Architecture).

W niektórych systemach komputerowych dostarczanych przez producentów w komplecie z oprogramowaniem BIOS jest często w dużym stopniu zintegrowany z systemem operacyjnym, lecz wydaje się, że tego typu rozwiązania nie będą już powszechnie stosowane.

Procedury bezpieczeństwa związane z BIOS nie są jednak w dużej mierze niezależne od jego rodzaju i powinny być stosowane zarówno dla komputerów osobistych (biurkowych i przenośnych) jak i dla serwerów.

Powinny one obejmować co najmniej:

- zabezpieczenie fizycznego dostępu do wewnętrznych podzespołów komputera lub co najmniej skuteczne zaplombowanie jego obudowy,
- wprowadzenie silnego hasła dostępu do programów umożliwiających konfigurowanie systemu BIOS. Hasło to powinno być znane jedynie upoważnionym pracownikom działu IT oraz składowane w sposób bezpieczny (np. w zalakowanej kopercie przechowywanej w bezpiecznym miejscu) wraz z metryką zawierającą parametry konfiguracyjne BIOS. Dla komputerów PC można dopuścić stosowanie powtarzalnej konfiguracji i identycznego hasła. Dla serwerów hasła powinny być indywidualne,
- przed przekazaniem komputera do naprawy lub innych działań wymagających dostępu do systemu BIOS hasło powinno być zmienione na tymczasowe hasło serwisowe.

Osobnym problemem są uaktualnienia BIOS, którym poświęcony jest cytowany dokument NIST. Wyróżnia on kilka procedur związanych z przeprowadzaniem uaktualnienia BIOS stosowanych przez producentów oraz zwraca uwagę na związane z nimi podatności. Ze względu na brak miejsca nie będę ich tu wymieniał szczegółowo (polecam jak zwykle lekturę dokumentu źródłowego), lecz ograniczę się do kilku wniosków i „dobrych praktyk".

Dokument NIST stwierdza, że „BIOS is a critical component of a secure system". Często nie przywiązujemy wagi do tego oprogramowania, a przecież ze względu na to, że jest ono uruchamiane jako pierwsze nie dysponuje rozbudowanymi mechanizmami ochrony, a jest traktowane domyślne jako „godne zaufania" (Trusted). Modyfikacje i rozszerzenia systemu BIOS są od dawna wykorzystywane w celu obsługi dodatkowego sprzętu, lecz równie dobrze może wykorzystać je atakujący wprowadzając własne programy.

Bezwzględnie konieczna jest więc staranna kontrola integralności BIOS. NIST zaleca stosowanie rozbudowanych mechanizmów sprawdzania autentyczności oraz integralności BIOS z podpisem cyfrowym włącznie. Klucz publiczny powinien być również poddany weryfikacji. NIST podaje zestaw wymagań, jakie powinien spełniać obraz systemu BIOS przeznaczony do wykonania uaktualnienia. BIOS powinien być uaktualniany jedynie po sprawdzeniu danych uwierzytelniających.

W niektórych przypadkach może zajść potrzeba awaryjnej instalacji BIOS (np. jeśli zainstalowany fabrycznie BIOS uległ poważnej awarii). Dla tego typu przypadków są przewidziane procedury „Secure Local Update", które wymagają z zasady fizycznej obecności administratora systemu, a niekiedy nawet interwencji sprzętowej.

Na zakończenie NIST definiuje wymagania eksploatacyjne związane z systemem BIOS:

W fazie akwizycji systemu należy zwracać uwagę na procedury stosowane przez producenta/dostawcę określające sposób zarządzania programem BIOS, a w szczególności mechanizmów udostępniania i zabezpieczania uaktualnień. NIST zaleca posiadanie wzorcowycm wersji systemów BIOS („Golden Master Images").

Podczas uruchamiania systemu należy zwrócić uwagę na integralność systemu BIOS oraz wprowadzić przed przekazaniem systemu do eksploatacji odpowiednich zabezpieczeń fizycznych i programowych, o których była mowa powyżej.

W trakcie eksploatacji powinno się w sposób ciągły monitorować poprawność działania systemu BIOS.

Postępowanie w przypadku awarii BIOS powinno być opisane w odpowiednich procedurach oraz należy zabezpieczyć środki niezbędne do jak najszybszego usunięcia takich awarii (Master Image, dane konfiguracyjne itp.).

Zakończenie pracy i przekazanie komputera na zewnątrz organizacji może się odbyć dopiero po usunięciu wszelkich danych z systemu BIOS (hasła, klucze itp.). Należy przywrócić fabryczne ustawienia systemu BIOS. Jeśli organizacja korzystała z dodatkowych rozszerzeń BIOS konieczne jest ich usunięcie i zainstalowanie fabrycznego obrazu BIOS.

Cóż można stwierdzić na zakończenie tego krótkiego opisu? Przyzwyczailiśmy się traktować BIOS jako coś, co należy raz skonfigurować, a potem można o tym zapomnieć. Nic bardziej błędnego. W mojej praktyce spotkało mnie ze strony tego oprogramowania kilka przykrych niespodzianek i wcale nie uważam zaleceń NIST za przesadne „dmuchanie na zimne".

Więcej informacji o przygotowywaniu i wdrażaniu szczegółowych polityk i procedur bezpieczeństwa uzyskacie Państwo podczas naszych kursów i warsztatów, na które serdecznie zapraszam!

Tomasz Barbaszewski