Raport Administratora WWW

16.06.2023

Siedziba:
50668 Köln
Domstr. 58

Tel: +49 221 25079477 www. aaniemcy.de
e-mail: pomoc@aaniemcy.de

16.06.2023

Do wszystkich zainteresowanych

W ostatnich dniach doświadczylismy ataku hakerskiego na naszą stronę internetową.

Opis ataku:

Poza tym, że tekst naszych wyników w wyszukiwarkach został zamieniony na chińskie znaki, strona aaniemcy.de wyglądała całkiem normalnie.

Byłto to działanie zamierzone.

Po zainfekowaniu strony, w jej kodzie wprowadzane są zmiany, które nie są od razu widoczne. Dopiero po pewnym czasie, szkodliwy (z naszego punktu widzenia) kod uaktywnia się, a efekty jego działania są zauważalne.
Ma to na celu doprowadzenie do sytuacji, w której nie można już odzyskać strony z kopii zapasowej, gwarantowanej standardowo w usłudze hostingu przez firmy hostingowe (w naszym przypadku backup bazy danych z przed maksymalnie 8 tygodni, backup plików z przed maksymalnie 2 tygodni). Celem ataku były nasze wysoko pozycjonowane wyniki w wyszukiwarkach oraz wykorzystanie ich do linkowania do innych stron internetowych (np. wyłudzających dane). Brak możliwości odzyskania „czystego" backupu, zmusza właściciela do tworzenia strony od nowa. Skutkuje to często, pozostawiem zainfekownej i niebezpiecznej strony przez dłuższy czas w internecie „bo przecież strona działa".

Możliwe Przyczyny Ataku:

- nieodpowiednie zapezpieczenia komputerów administratora/webmastera - np brak programu antywirusowego
- zbyt słabe zabezpieczenia antywirusowe strony internetowej - w tej chwili, zmieniłem system zabezpieczeń na innym niestety również darmowy ale obecnie lepiej oceniany przez społeczności IT
- brak możliwości aktualizowania przestarzałych wtyczek (pluginów) - o tym już mówiłem na jednym ze spotkań PIK. Jak nie wykupimy licencji, nie mamy również aktualizacji tzn. nie łatamy dziur/błędów w kodzie. Takie błedy znalezione i wykorzystane przez hakerów do ataków są później poprawiane przez programistów w taki sposób aby uniemożliwić ponowny atak.

Podjęte działania:

12.06.2023

- *Pozostawienie jednego konta administracyjnego*
- *Analiza i ocena wprowadzonych zmian w zainfekowanych plikach oraz możliwości naprawy tych plików*
- *Użycie podstawowych narzędzi do naprawy plików oraz ich kodu źródłowego*

13.06.2023

- *Szczegółowa analiza i ocena wybranych zainfekowanych plików i rekordów w bazie danych.*
- *Odzyskanie najstarszej możliwej kopii zapasowej tj. z dnia 29.05.2023 z hostingu*
- *Porównanie stanu zainfekowanych plików i rekordów w bazie danych z ich odpowiednikami z kopii zapasowej.*
- *Wyłączenie strony internetowej*

14.06–16.06.2023

- *Zaimplementowanie kopii zapasowej wykonanej przez administratora,*
- *Przeprowadzanie niezbędnych prac serwisowych na plikach, w kodzie źródłowym strony i we wpisach w bazie danych,*
- *Przeprowadzenie testów funkcjonalnych,*
- *Ocena zagrożeń i wdrożenie środków mających na celu uniknięcia tych zagrożeń w przyszłości,*
- *Przygotowanie raportu administratora.*

Powyższe czynności zostały przeprowadzone z zachowaniem szczególnej ostrożności, ze względu na podatność odbudowywanej strony na podobne lub te same mechanizmy ataku.

Stan na dzień 16.06.2023:
Strona działa, została oczyszczona ze szkodliwego kodu, jest dostępna online niestety w ograniczonej formie i wymaga niezwłocznej aktulizacji

- *Stan serwera - prawidłowy*
- *Zmiany w plikach - nie wykryto*
- *Obecność złośliwego oprogramowania - nie wykryto*
- *Bezpieczeństwo zawartości - ustawienie prawidłowe*
- *Pliki publiczne - ustawienia prawidłowe*
- *Siła haseł - wysoka*
- *Test podatności na skuteczny atak - nie są wymagane dodatkowe zmiany - strona skonfigurowana poprawnie*
- *Kontrola kont użytkowników - nie są wymagane dodatkowe zmiany konta skonfigurowane poprawnie*
- *Niestety mamy nieaktualną listę mityngów co trzeba będzie w pierwszej kolejności zaktualizować.*
- *Na chwilę obecną konto webmastera Krzysztofa jest usunięte, do czasu aż wprowadzę wszystkie zmiany, podejmiemy decyzję dotyczącą aktywacji pluginu. Opisano w części „Podsumowanie".*

Podsumowanie:

Zwracam się z prośbą do Służebnych PIK o zgodę na **niezwłoczny** zakup pluginu (koszt około 55,00 EUR) aby można go było zaktualizować lub na nowo zaimplementować i przywrócić funkcjonalność strony do stanu z przed ataku.

Jeżeli nie ma zgody na zakup, również proszę o taką informację. W takiej sytuacji postaramy się z Krzysztofem odbudować/przebudować gruntownie stronę ale to może zająć znacznie więcej czasu.

O sukcesie wszystkich opisanych działań naprawczych, świadczy fakt, że po wyszukaniu strony w wyszukiwarce i kliknięciu w wynik wskazujący właśnie naszą stronę (na chwile obecną wyniki widoczne jeszcze z chińskimi znakami) zostajemy przekirwani właściwie do aaniemcy.de, a nie do strony obcej. Chińskie teksty i linki w wynikach wyszukiwarek powinny zmienić się po pewnym czasie automatycznie .

W Duchu Jedności
Administrator
Marcin

pomoc@aaniemcy.de www.aaniemcy.de Domstraße 58
tel. +49 221 25079477 50668 Köln