Informacje na temat przetwarzania danych osobowych w HAN-ie

- Dokument ten opisuje, jakie dane osobowe są w HAN-ie przetwarzane w ramach procedury przetwarzania danych oraz za pomocą jakich mechanizmów dane te są chronione. -

Treść

Przedmowa

HAN przestrzega zasad minimalizacji konieczności gromadzenia danych oraz zasad oszczędności danych, tj. nie przetwarza żadnych danych osobowych, które nie są wymagane do wewnętrznych procesów HAN-a. Całkowita ilość danych osobowych przetwarzanych w HAN-ie jest niewielka. W celu usunięcia z danych odnośników osobowych, HAN wspiera zarówno mechanizmy anonimizacji, jak i

pseudonimizacji. W kolejnych rozdziałach mogą Państwo zapoznać się z tym, jakie dane HAN przetwarza oraz w jaki sposób dane te są chronione.

Mechanizmy ochrony danych

Podstawą bezpieczeństwa danych w HAN-ie jest odpowiednie zabezpieczenie systemu Windows i zdefiniowanie odpowiednich praw dostępu, co wynika z faktu, że HAN integruje się z systemem operacyjnym Windows. Proszę zdefiniować krąg uprawnionych użytkowników tak wąsko, jak to tylko możliwe i proszę przydzielić im silne hasła.

Użytkownicy i role użytkowników w HAN-ie

HAN posiada zintegrowaną koncepcję ról, za pomocą której użytkownikom przydzielane są odpowiednie role HAN-a. Z rolami powiązane są odpowiednie uprawnienia, tak aby członkowie danej roli otrzymali dokładnie te prawa w HAN-ie, które są im potrzebne do pełnienia tej roli. Tylko administratorzy HAN-a mają dostęp do programów administracyjnych HAN-em.

Anonimizacja/pseudonimizacja

Domyślnie dane protokołu są w HAN-ie anonimizowane, tzn. z danych protokołu usuwane są wszelkie odniesienia do danej osoby. Funkcję anonimizacji można skonfigurować za pomocą programu HAN Settings (Ustawienia HAN-a). Zamiast anonimizacji, dane protokołu mogą być poddane pseudonimizacji, w której odniesienie osobowe do danych protokołu zostaje zastąpione nieodwracalnym pseudonimem. Ustawienia te są chronione zgodnie z zasadą reguły „dwóch par oczu”.

Regularne usuwanie danych

Dane protokołu, które nie są wykorzystywane do analizy statystycznej, są usuwane w regularnych (zdefiniowanych przez użytkownika) odstępach czasu.

Ochrona bazy danych za pomocą haseł

Oprócz uwierzytelniania Windows‘owego, baza danych HAN-a jest chroniona hasłem przez system ról HAN-a.

Przetwarzane dane

Poniżej znajduje sie opis danych, które HAN przetwarza oraz opis stosowanego tu mechanizmu zabezpieczającego. Dokument opisuje wszystkie dane. Dane osobowe lub dane poprzez które można dotrzeć do danych osobowych podane są tu ***tłustym*** drukiem.

Dane użytkowników Active Directory

HAN ma dostęp do danych użytkowników usług Active Directory firmy Microsoft. Dane te są wykorzystywane przez następujące programy i procesy HAN-a:

- Data Editor (Edytor Danych HAN-a) > Uprawnienia > Użytkownicy AD
- Data Editor (Edytor Danych HAN-a) > Grupy danych > Użytkownicy

Dane: Zgodnie z konfiguracją wykonaną przez administratora systemu

Mechanizm zabezpieczający: Kopia zapasowa kontrolera domeny, role HAN-a i system użytkowników HAN-a (dostęp do programów administracyjnych tylko z administracyjnym kontem użytkownika HAN-a).

Konfiguracja usług uwierzytelniania

Podczas konfigurowania usług autentykacji HAN otrzymuje poprzez odpowiednie interfejsy dostęp do informacji w obcych bazach danych lub w usługach katalogowych (w tym także Microsoft ADS). Dane z takich baz danych mogą być następnie wykorzystane do zalogowania się do HAN-a. HAN zapytuje te

H+H Software GmbH | Maschmuehlenweg 8-10 | 37073 Goettingen | Tel. 0049 551 52208 0 | Fax: 0049 551 52208 25 | E-mail: hh@hh-software.com | Web: www.hh-software.com | © 2018

bazy danych w czasie rzeczywistym i tylko wtedy, gdy jest to konieczne. Takie dane osobowe nie są w HAN-ie zapisywane. Zapisywane są natomiast dane dostępu do samej bazy danych:

- Program HAN Settings (Ustawienia HAN-a) > Logowanie > Uwierzytelnianie

Dane: Dane dostępu do bazy danych (***nazwa użytkownika*** jego hasło), ***listy adresów IP***.

Mechanizm zabezpieczający: Role HAN-a i system użytkowników HAN-a

Dane poczty mailowej w przypadku wystąpienia błędu

- Program HAN Settings (Ustawienia HAN-a) > Global > System monitoring

Dane: ***Nadawca***, ***odbiorca***, ***nazwa użytkownika***, hasło, przynależność konta adminstracyjnego do domeny

Mechanizm zabezpieczający: Role HAN-a i system użytkowników HAN-a (dostęp do programów administracyjnych tylko z administracyjnym kontem HAN-a)

Protokół HAN-a

HAN generuje różnorodne dane protokołu w celu analizy błędów oraz dla analizy statystycznej użytkowania. Dane, poprzez które można dotrzeć do danych konkretnej osoby, a mianowicie nazwa użytkownika oraz nazwa jego stacji roboczej, są domyślnie anonimizowane lub – alternatywnie – mogą być pseudonimizowane. Następujące programy i protokoły HAN-a przetwarzają dane protokołu:

Logi serwera webowego

Protokół usługi HAN WebService

Dane: ***Identyfikator użytkownika i stacji roboczej***

Mechanizm zabezpieczający: Dane usuwane są po upływie określonego czasu (ten sam interwał czasowy jak dla anonimizacji danych statystycznych).

Event Viewer (protokół zdarzeń)

Rejestrowanie zdarzeń w celu analizy błędów

Dane: ***Nazwa komputera***, ***nazwa użytkownika***

Mechanizm zabezpieczający: Protokól ten jest regularnie i automatycznie usuwany

Protokół Summarized (protokół sumujący)

Protokołowanie użytkowania e-skryptów HAN-a

Dane: ***Nazwa użytkownika***, ***nazwa komputera***, nazwa e-skryptu (jego identyfikator), znacznik czasu, ilość przesłanych bajtów, identyfikator sesji przeglądarki

Mechanizm zabezpieczający: Role HAN-a i system użytkowników HAN-a, anonimizacja/pseudonimizacja

Protokół Detailed (protokół szczegółowy)

Protokołowanie użytkowania e-skryptów HAN-a

Dane: ***Nazwa użytkownika***, ***nazwa komputera***, nazwa e-skryptu (jego identyfikator), znacznik czasu, ilość przesłanych bajtów, identyfikator sesji przeglądarki

Mechanizm zabezpieczający: Role HAN-a i system użytkowników HAN-a, anonimizacja/pseudonimizacja

Statystyka HAN-a

Statystyka użytkowania źródeł elektronicznych udostępnianych za pomocą HAN-a.

Dane: ***Nazwa użytkownika***, ***nazwa komputera***, nazwa używanego e-skryptu

Mechanizm zabezpieczający: Role HAN-a i system użytkowników HAN-a, anonimizacja/pseudonimizacja

Ochrona przed niewłaściwym wykorzystaniem HAN-a (nadmierne ściąganie źródeł elektronicznych przez użytkowników)

System powiadamiania o nadużyciach w korzystaniu z HAN-a (od wersji HAN 5)

Dane: ***Nazwa użytkownika*** z loginu, ***adres mailowy*** administratora, strona internetowa administratora HAN-a służąca do kontroli oraz odblokowywania dostępu (obsługa możliwa tylko dla odpowiednich ról HAN-a)

Mechanizm zabezpieczający: Logowanie do bazy danych, role HAN-a i system użytkowników HAN-a, regularne usuwanie pliku protokołu zgodnie ze zdefiniowanymi interwałami czasowymi

Monitor licencji

Monitorowanie wykorzystania licencji z wyświetleniem nazwy użytkownika i jego adresu IP

Dane: ***Nazwa użytkownika***, ***adres IP***, nazwa (znacznik) licencji

Mechanizm zabezpieczający: Role HAN-a i system użytkowników HAN-a (tylko zgodnie z przypisaną rolą)

Zarządzanie użytkownikami

Zarządzanie użytkownikami HAN-a i przypisywanie im ról

Dane: ***Nazwa użytkownika*** (wywodząca się z systemu Windows lub dowolnie przypisana)

Mechanizm zabezpieczający: Role HAN-a i system użytkowników HAN-a (dostęp do programów zarządzania tylko z administracyjnym kontem użytkownika HAN-a), logowanie do bazy danych.

Właściwości e-skryptu

Konfiguracja e-skryptów

Dane: Rejestrowanie ostatniej zmiany właściwości e-skryptu: ***Nazwa użytkownika*** oraz czas zmiany

Mechanizm zabezpieczający: Role HAN-a i system użytkowników HAN-a

Udostępnianie niniejszego tekstu

Powyższe informacje zostały przez nas zebrane zgodnie z naszą najlepszą wiedzą. Mamy nadzieję, że będę one Państwu pomocne w przygotowaniu dokumentacji dotyczącej ochrony danych.

Markus Libiseller
Product Manager Hidden Automatic Navigator

H+H Software GmbH | Maschmuehlenweg 8-10 | 37073 Goettingen | Tel. 0049 551 52208 0 | Fax: 0049 551 52208 25 | E-mail: hh@hh-software.com | Web: www.hh-software.com | © 2018