Information zur Verarbeitung personenbezogener Daten in HAN

- Das Dokument beschreibt, welche personenbezogenen Daten im datenverarbeitenden Verfahren HAN verarbeitet werden und mit welchen Mechanismen diese Daten geschützt werden. -

Inhalt

Einleitung 1
Datenschutzmechanismen 2
HAN Rollen- und Benutzersystem 2
Anonymisierung/Pseudonymisierung 2
Regelmäßiges Löschen 2
Passwortschutz der Datenbank 2
Verarbeitete Daten 2
Active-Directory-Benutzerdaten 2
Konfiguration von Authentifizierungsdiensten 3
E-Mail-Daten für den Fehlerfall 3
HAN Protokolldaten 3
Webserver-Logs 3
Ereignisanzeige 3
Summiertes Protokoll 3
Detailliertes Protokoll 3
HAN Statistik 4
HAN Missbrauchsschutz (Datentransfer) 4
Lizenzmonitor 4
Benutzerverwaltung 4
E-Skripteigenschaften 4
Freigabe 4

Einleitung

HAN folgt den Grundsätzen der Datenvermeidung und Datensparsamkeit, d.h. es werden keine personenbezogenen Daten verarbeitet, die nicht für interne HAN Prozesse benötigt werden. Die Menge der verarbeitenden personenbezogenen Daten ist in HAN insgesamt gering. HAN unterstützt sowohl Anonymisierungs-, als auch Pseudonymisierungsmechanismen, um den Personenbezug aus

Daten zu entfernen. Lesen Sie in den folgenden Kapiteln, welche Daten HAN verarbeitet und wie diese Daten geschützt werden.

Datenschutzmechanismen

Die Grundlage aller Datensicherheit in HAN ist, dass Sie Ihr Windows-System entsprechend absichern und geeignete Zugriffsrechte definieren, da HAN sich in dieses System integriert. Definieren Sie den Kreis der zugriffsberechtigten Benutzer möglichst eng und vergeben Sie starke Passwörter.

HAN Rollen- und Benutzersystem

HAN verfügt über ein integriertes Rollenkonzept, mit dem Benutzern eine vordefinierte HAN Rolle zugwiesen wird. Mit den Rollen sind bestimmte Rechte verknüpft, so dass Mitglieder einer Rolle genau die Rechte in HAN erhalten, die sie zum Ausüben der Rolle benötigen. Nur HAN Administratoren erhalten Zugriff auf HAN Verwaltungsprogramme.

Anonymisierung/Pseudonymisierung

Standardmäßig werden in HAN Protokolldaten anonymisiert, d.h. jeglicher Personenbezug wird aus den Protokolldaten entfernt. Die Anonymisierungsfunktion ist über die HAN Einstellungen konfigurierbar. Statt einer Anonymisierung kann auf die Protokolldaten auch eine Pseudonymisierung angewendet werden, bei der der Personenbezug der Protokolldaten durch ein Pseudonym ersetzt wird (irreversibel). Diese Einstellungen sind nach dem Vier-Augen-Prinzip geschützt.

Regelmäßiges Löschen

Protokolldaten, die nicht zur statistischen Auswertung genutzt werden, werden in regelmäßigen (benutzerdefinierten) Abständen gelöscht.

Passwortschutz der Datenbank

Die HAN Datenbank ist, zusätzlich zur Windows-Authentifizierung, durch das HAN Rollensystem passwortgeschützt.

Hinweis: Das H+H Installationsteam wird vor der Abnahme die Datenschutzmechanismen mit Ihnen besprechen und den Datenschutz gemäß Ihren Vorgaben aktivieren.

Verarbeitete Daten

Lesen Sie im Folgenden, welche Daten HAN verarbeitet und welcher Schutzmechanismus verwendet wird. Das Dokument beschreibt alle Daten. Personenbezogene Daten, bzw. Daten, über die sich ein Personenbezug herstellen lässt, sind ***hervorgehoben***.

Active-Directory-Benutzerdaten

HAN greift auf Benutzerdaten der Active-Directory-Dienste von Microsoft zu. Folgende HAN Programme und Prozesse nutzen diese Daten:

- HAN Dateneditor > Berechtigungen > AD-Benutzer
- HAN Dateneditor > Datengruppen > Benutzer

Daten: Entsprechend der Konfiguration des Systemadministrators

Absicherung: Sicherung des Domänencontrollers, HAN Rollen- und Benutzersystem (Zugriff auf Verwaltungsprogramme nur mit administrativem HAN Benutzerkonto)

H+H Software GmbH | Maschmühlenweg 8-10 | 37073 Göttingen | Tel.: 0049 551 52208 0 |
Fax: 0049 551 52208 25 | E-Mail: hh@hh-software.com | Web: www.hh-software.com |

Konfiguration von Authentifizierungsdiensten

Bei der Konfiguration von Authentifizierungsdiensten wird über Schnittstellen auch auf Informationen in Datenbanken von Drittanbietern oder Verzeichnisdiensten (auch Microsoft ADS) zugegriffen. Die Daten der Datenbanken können dann zur Anmeldung an HAN verwendet werden. HAN fragt die Datenbanken in Echtzeit und nur bei Bedarf aus der jeweiligen Datenbank ab. Die Daten werden in HAN nicht gespeichert. Lediglich die Zugangsdaten zu der jeweiligen Datenbank werden in HAN hinterlegt:

- HAN Einstellungen > Anmeldung > Authentifizierung

Daten: Zugangsdaten zur jeweiligen Datenbank (***Benutzername*** und Passwort), ***IP-Listen***

Absicherung: HAN Rollen- und Benutzersystem

E-Mail-Daten für den Fehlerfall

- HAN Einstellungen > Global > Systemüberwachung

Daten: ***Absender***, ***Empfänger***, ***Benutzername***, Passwort, Domänenzugehörigkeit eines administrativen Accounts

Absicherung: HAN Rollen- und Benutzersystem (Zugriff auf Verwaltungsprogramme nur mit administrativem HAN Account)

HAN Protokolldaten

HAN erzeugt diverse Protokolldaten zur Fehleranalyse und statistischen Auswertung. Daten, die einen Rückschluss auf eine reale Person zulassen - Benutzername und Station – werden standardmäßig anonymisiert oder können alternativ pseudonymisiert werden. Folgende HAN Programme und Protokolle verarbeiten Protokolldaten:

Webserver-Logs

Zugriffs-Protokolldateien des HAN Webservers

Daten: ***Benutzer- und Stationskennung***

Absicherung: werden nach definiertem Intervall (wie Statistikdaten) gelöscht

Ereignisanzeige

Protokollierung von Ereignissen zur Fehleranalyse

Daten: ***Computername***, ***Benutzername***

Absicherung: Wird regelmäßig automatisch gelöscht

Summiertes Protokoll

Protokollierung der E-Skriptnutzung

Daten: ***Benutzername***, ***Computername***, verwendetes E-Skript (Protokoll-ID), Zeitstempel, Menge der übertragenen Bytes, Sitzungs-ID

Absicherung: HAN Rollen- und Benutzersystem, Anonymisierung/Pseudonymisierung

Detailliertes Protokoll

Protokollierung der E-Skriptnutzung

Daten: ***Benutzername***, ***Computername***, verwendetes E-Skript (Protokoll-ID), Zeitstempel, Menge der übertragenen Bytes, Sitzungs-ID

Absicherung: HAN Rollen- und Benutzersystem, Anonymisierung/Pseudonymisierung

HAN Statistik

Analyse der HAN Nutzung

Daten: ***Benutzername***, ***Computername***, verwendetes E-Skript

Absicherung: HAN Rollen- und Benutzersystem, Anonymisierung/Pseudonymisierung

HAN Missbrauchsschutz (Datentransfer)

Benachrichtigungssystem bei missbräuchlicher HAN Nutzung (erst ab HAN 5)

Daten: ***Benutzernamen*** aus Anmeldung, ***E-Mailadresse*** des Administrators, Webseite für Verwalter zum Nachsehen und Freigeben (nur für definierte Rolle)

Absicherung: Datenbankanmeldung, HAN Rollen- und Benutzersystem, regelmäßiges Löschen der Logdatei gemäß benutzerdefiniertem Intervall

Lizenzmonitor

Überwachung der Lizenzausnutzung unter Anzeige von Benutzername und IP-Adresse

Daten: ***Benutzername***, ***IP-Adresse***, verwendete Lizenz

Absicherung: HAN Rollen- und Benutzersystem (nur gemäß zugewiesener Rolle)

Benutzerverwaltung

Verwaltung der HAN Benutzer und Zuweisung von HAN Rollen

Daten: ***Benutzernamen*** (abgeleitet aus Windows System oder frei vergeben)

Absicherung: HAN Rollen- und Benutzersystem (Zugriff auf Verwaltungsprogramme nur mit administrativem HAN Benutzerkonto), Datenbankanmeldung

E-Skripteigenschaften

Konfiguration von E-Skripten

Daten: Protokollierung der letzten Änderung: ***Benutzername*** und Zeitpunkt

Absicherung: HAN Rollen- und Benutzersystem

Freigabe

Die Informationen wurden nach besten Wissen und Gewissen zusammengestellt. Wir hoffen, dass sie Ihnen beim Erstellen Ihrer Datenschutzdokumentation von Nutzen sind.

Markus Libiseller
Product Manager Hidden Automatic Navigator

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