Be sure. testo


# testo Saveris 2
# Security Dossier

# Twoje bezpieczeństwo jest dla nas ważne

## Ochrona danych i prywatności w testo Saveris 2

W celu zapewnienia spójności i nienaruszalności danych osobowych i odczytów pomiarowych podczas użytkowania rejestratorów testo Saveris 2, Testo AG, jak i jej usługodawcy IT zobowiązani są do spełnienia najwyższych standardów bezpieczeństwa, przepisów i dyrektyw.

W poniższym dokumencie zabraliśmy wszystkie najważniejsze informacje dotyczące ochrony danych i prywatności użytkownika. Skontaktuj się z nami, jeśli masz dodatkowe pytania.

**1. Jakie dane przechowujemy?**
Oprócz podanego przez użytkownika imienia/ nazwy użytkownika, adresu poczty elektronicznej i numerów telefonów komórkowych, wykorzystywanych do przesyłania komunikatów ostrzegawczych o przekroczeniu pomiarowych wartości granicznych, operator nie zapisuje żadnych innych danych osobowych. Podane przez użytkownika dane służą tylko i wyłącznie do przesyłania komunikatów ostrzegawczych o przekroczeniu alarmowych wartości granicznych.

Aktualne, zapisywane wartości pomiarowe nie zastępują poprzednich, już zapamiętanych wartości pomiarowych. Wszystkie dane zapisywane i dokumentowane są chronologicznie. Dzięki temu użytkownik może śledzić historię danych pomiarowych w każdym dowolnym momencie. Z drugiej strony, system taki umożliwia sprawdzanie danych pomiarowych z przeszłych okresów pomiarowych. Rozwiązanie takie umożliwia śledzenie historii w razie takiej potrzeby.

**2. Gdzie zapisywane są moje dane?**
Wszystkie dane pomiarowe gromadzone są w centrum hostingowym, ulokowanym w Niemczech , certyfikowanym zgodnie z normą ISO/IEC 27001:2005, prowadzonym przez renomowanego operatora - firmę - Host Europe. Centrum to podlega surowym niemieckim przepisom o ochronie danych osobowych.

Operator Host Europe posiada certyfikat TÜV Süd na zgodność z normą ISO/IEC 27001:2005 w zakresie „udostępniania powierzchni serwerowej o dużej pojemności , w tym połączeń sieciowych i ich eksploatacji". Dzięki wdrożonemu certyfikowanego przez TÜV Systemu Zarządzania Bezpieczeństwem Informacji (ISMS) Host Europe gwarantuje najwyższe bezpieczeństwo danych oraz spełnienie wszystkich wymagań w zakresie ochrony danych.

Oznacza to: Zapewnienie optymalnej ochrony danych w odniesieniu do ich dostępności, zachowania poufności, nienaruszalności i autentyczności.
Certyfikacja obowiązuje nie tylko dla istniejących procesów operatora Host Europe, ale również dla wszelkich wymagań w przyszłości, koniecznych do spełnienia standardów bezpieczeństwa. Ochrona bezpieczeństwa danych obejmuje, w zależności od produktu, następujące aspekty:

<u>Dostepność</u>
Operator Host Europe zapewnia pełną dostępność i użyteczność danych i informacji dzięki:
- codziennym kopiom bezpieczeństwa
- zewnętrznym kopiom bezpieczeństwa offsite
- skanowaniu antywirusowemu
- regularnym aktualizacjom funkcji bezpieczeństwa i użytkowych

<u>Poufność</u>
Odpowiednie procedury Host Europe zapewniają wykorzystywanie danych i i informacji jedynie przez autoryzowany personel:
- ochrona dostępu
- różne strefy bezpieczeństwa
- bezpieczna utylizacja danych i ich nośników
- wewnętrzne szkolenia bezpieczeństwa

<u>Integralność</u>
Operator Host Europe zapewnia pełną ochronę danych i informacji przed wprowadzaniem nieautoryzowanych zmian poprzez:
- ochronę dostępu
- zabezpieczenie przed nieautoryzowanym zapisywaniem, przetwarzaniem, wykorzystywaniem i rozpowszechnianiem danych
- szyfrowana transmisja danych
- ochrona przed atakami hakerów

Autentyczność
Operator Host Europe zapewnia bezpieczeństwo realizowanych transakcji i wymiany informacji z podmiotami zewnętrznymi przy pomocy:
- kilkuetapowego procesu uwierzytelniania
- bezpiecznej identyfikacji użytkownika
- proaktywnego wypełniania luk bezpieczeństwa

Ochrona fizyczna
Operator Host Europe realizuje szeroko zakrojony program ochrony serwerów, poprzez np.:
- regularne testy wytrzymałości i odporności infrastruktury oraz zapewnie odpowiednich rozwiązań redundancyjnych
- ochrona przeciwpożarowa, ochrona przed zalaniem wodą
- plan postępowania w przypadku katastrof naturalnych
- zarządzanie sytuacjami awaryjnymi
- ochrona przed zagrożeniami zewnętrznymi

Chmura „Trusted Cloud”
W celu wyeliminowania istniejących zagrożeń organizacyjnych, prawnych i technicznych, z którymi wiąże się realizacja idei chmury danych (cloud computing) operator Host Europe zdecydował się na potwierdzenie bezpieczeństwa usług świadczonych „w chmurze” przy pomocy certyfikatu TÜV TRUST IT. Na podstawie szczegółowego katalogu wymagań certyfikacji TÜV TRUST IT dla usług świadczonych w chmurze (cloud services) przez operatora Host Europe, wykonano kontrole na poziomie infrastrukturalnym (IaaS) odnośnie bezpieczeństwa danych, ochrony danych i zgodności z przepisami. Host Europe otrzymał w listopadzie 2011 - jako pierwszy dostawca usług hostingowych - certyfikat Trusted Cloud Service. Bezpieczeństwo usług w chmurze, potwierdzone certyfikatem Trusted Cloud oznacza optymalną dostępność, zachowanie poufności oraz integralność danych i systemów.

**3. Czy moje dane są rzeczywiście bezpieczne?**
Ochrona prywatności
Wszelkie dane transmitowane są do przeglądarki internetowej użytkownika wyłącznie szyfrem SSL. Serwery, na których zapisywane są dane pomiarowe, zainstalowane są w Niemczech i podlegają niemieckim przepisom ochrony danych, które są jednymi z najbardziej rygorystycznych na świecie.
Cały transfer danych w sieci protokołowany jest okresowo na serwerze sieciowym przez okres jednego miesiąca. Rozwiązanie takie ma na celu wyłącznie umożliwienie wykonywania prac serwisowych lub zapewnienie prawidłowej eksploatacji systemu. Dane te są usuwane lub anonimizowane po upływie tego okresu. W przypadku ataków z sieci na infrastrukturę istnieje możliwość okresowego przekierowania strumieni danych do sieci usługodawców zewnętrznych, którzy analizują zagrożenia na bieżąco i usuwają elementy niebezpieczne.

Ochrona przed utratą danych
Serwery, na których zapisane są wszystkie dane, dysponują dwoma przestrzennie rozdzielonymi od siebie strefami pożarowymi. Pojęcie „strefy pożarowej" można w tym przypadku rozumieć całkiem dosłownie: jeśli rzeczywiście dojdzie do przypadku, w którym wyniku działania np. pożaru dojdzie do uszkodzenia bazy danych, to jej funkcje przejęte zostaną przez drugą strefę. Oczywiście w sytuacji takiej przekazujemy naszym użytkownikom natychmiast wszystkie szczegółowe informacje.
Baza danych z wartościami pomiarowymi stanowi wielowarstwowy klaster o wysokiej dostępności (high availability cluster). Klaster ten dzieli się na nadrzędną i podrzędną bazę danych (master i slave), które znajdują się zawsze w oddzielnych strefach pożarowych. Codzienne kopie zapasowe zapewniają aktualność obydwu baz danych i umożliwiają kompletne i szybkie odzyskiwanie danych w przypadku awarii jednej z nich. Dodatkowo wszystkie dane zapisywane są na drugim serwerze w innej lokalizacji.
W każdej strefie pożarowej, oprócz baz danych znajduje się klaster aplikacyjny obejmujący między innymi tak zwany „broker", czyli interfejs zapewniający komunikację pomiędzy nadajnikami radiowymi a bazą danych. Każdy klaster aplikacyjny obciążony może być maksymalnie do poziomu 50 %. Dzięki temu można zapewnić bezpieczną transmisję danych pomiarowych przez nadajnik radiowy do bazy danych, nawet w przypadku usterki brokera.

**4. Kto ma dostęp do moich danych?**
• tylko i wyłącznie osoby, które posiadają upoważnienie do dostępu do konta
• pracownicy spółki Testo AG w Niemczech w celu wykonywania prac konserwacyjnych na testo Saveris 2 i zapewnienia sprawnego funkcjonowania systemu. Dane pomiarowe nie są ani modyfikowane ani usuwane

**5. Jakie przepisy zapewniają bezpieczeństwo i ochronę moich danych?**
Serwery, na których zapisywane są dane, zlokalizowane są w Niemczech i podlegają niemieckim przepisom ochrony danych.

**6. Jakie certyfikaty zapewnia operator?**
Host Europe posiada certyfikat ISO/IEC 27001:2005.

ISO/IEC 27001:2005 to wiodąca międzynarodowa norma dla systemów zarządzania bezpieczeństwem informacji (ISMS). Norma obowiązuje dla przedsiębiorstw prywatnych, jednostek publicznych i organizacji non-profit i określa wymagania dotyczące wdrażania, realizacji, kontroli i optymalizacji systemów zarządzania bezpieczeństwem informacji.

Norma określa wymagania dotyczące wdrażania odpowiednich mechanizmów bezpieczeństwa dla różnych branż, które powinny być dopasowane do indywidualnych wymagań poszczególnych organizacji. ISO/IEC 27001:2005 została stworzona w celu zapewnienia i umożliwienia odpowiedniego wyboru mechanizmów zabezpieczających do ochrony wszelkich informacji przedsiębiorstwa.

**7. Co muszą wiedzieć informatycy użytkownika?**
• radiowe nadajniki danych testo Saveris 2 komunikują z brokerem przez port 1883 i standardowy protokół MQTT
• synchronizacja czasu rejestratorów z SNTP przez port 123
• rozpoznawanie nazw DNS przez port 53
• wszystkie trzy porty (1883, 123, 53) muszą być otwarte tylko na zewnątrz. Nie ma potrzeby stosowania dwukierunkowych ustawień dla portów
• bramka sieciowa domyślna przekazywana do czujnika przez DHCP lub ręcznie musi odpowiadać na zapytanie PING nadajnika radiowego. Wskazówka: podczas pierwszej konfiguracji należy wybrać odpowiednią opcję: DHCP lub statyczny numer IP. W celu wprowadzenia odpowiednich konfiguracji należy wybrać moduł ustawień zaawansowanych
• każdy rejestrator testo Saveris 2 posiada przypisany unikalny adres MAC
• adres IP każdego rejestratora testo Saveris 2 jest dynamiczny, ale można go indywidualnie zmienić na statyczny
• testo Saveris 2 obsługuje 2.4 GHz-WLAN (IEEE 802.11 b/g/n)
• stosowana metoda szyfrowania komunikacji pomiędzy radiowym rejestratorem testoSaveris2 i routerem to WPA2
• aplikacja testo Saveris 2 obsługiwana jest przez przeglądarkę internetową. Wykorzystywane są w ty celu porty standardowe TCP http (80) i https (443)