ROZBUDOWA I KONSERWACJA

Podczas tworzenia naszych produktów opieramy się wyłącznie na bezpiecznych zasadach i procesach programowania, które gwarantują sprawną eksploatację.

Okres eksploatacji i rozbudowy bezpiecznego oprogramowania obejmuje:

- Weryfikację projektu
- Określenie kierunku rozwoju
- Ocena jakości oraz testowanie funkcji
- Zarządzanie wersjami i zmianami
- Analizy statyczne kodu (OWASP Top 10 / SANS Top 25)

Dodatkowo pracujemy nad wewnętrznymi programami mającymi na celu zabezpieczenie naszego obszaru technicznego:

- Edukacja pracowników w zakresie bezpieczeństwa
- Testowanie i weryfikacja systemów bezpieczeństwa na etapie wdrażania
- Wzmacnianie systemu
- Zarządzanie poprawkami i lukami w zabezpieczeniach
- Testowanie bezpieczeństwa aplikacji internetowej

Prace inżynieryjne	Całościowy rozwój	Kontrola jakości	Wdrożenie
Analiza architektury oprogramowania	Analiza statyczna kodu oprogramowania	Dynamiczna analiza aplikacji	Wdrożenie i stabilizacja aplikacji

RELACJE Z DOSTAWCĄ

Dzięki ciągłej analizie zewnętrznych zagrożeń zapewniamy bezpieczeństwo organizacji i współpracujących z nami partnerami, którzy stosują międzynarodowe standardy bezpieczeństwa informacji, a także kierują się podobnymi wartościami, co firma TomTom w kwestii ochrony informacji i danych.

Zarządzanie zdarzeniami naruszającymi bezpieczeństwo informacji

W przypadku, gdy ma miejsce naruszenie bezpieczeństwa, istotne jest, aby dysponować skutecznym podejściem do zarządzania takim zdarzeniem. Obejmuje to szybką komunikację ze wszystkimi stronami, jak również odpowiednią weryfikacją słabych stron zabezpieczeń, które wpłyną na dalsze ulepszenie obszaru zabezpieczeń.

Aspekty bezpieczeństwa informacji w zakresie zarządzania ciągłością działania

Zarządzamy programem ciągłości działania i bezpieczeństwa informacji, który ma na celu zapewnienie naszym klientom bezproblemowego dostępu do platformy TomTom Telematics, nawet podczas awarii. Dzięki odpowiedniej konfiguracji w naszych centrach danych prawdopodobieństwo wystąpienia poważnej awarii w obu centrach jest nieznaczne, ponieważ każde centrum może samodzielnie prowadzić całe nasze działania. Oznacza to, że Klienci mogą korzystać z naszej platformy, kiedy jej tylko potrzebują.

ZGODNOŚĆ Z PRZEPISAMI

W firmie TomTom Telematics stosujemy najwyższe standardy dotyczące ochrony danych zgodnie z rozporządzeniem (GDPR) Unii Europejskiej oraz lokalnymi przepisami dotyczącymi ochrony prywatności.

Nasz zespół do spraw bezpieczeństwa SZBI regularnie weryfikuje wymagania w zakresie prawa i bezpieczeństwa, które mogą mieć wpływ na platformę telematyczną lub zasoby informacyjne objęte systemem zarządzania informacjami.

NAJWAŻNIEJSZE CECHY

- **INTEGRALNOŚĆ I MAKSYMALNE BEZPIECZEŃSTWO**
  Twoje dane są w bezpiecznych rękach dzięki naszemu systemowi z certyfikatem ISO 27001.
- **OCHRONA PRYWATNOŚCI PRACOWNIKÓW**
  Zapewniamy najwyższą ochronę danych naszych pracowników i współpracujących z nami podmiotami.
- **USUWANIE DANYCH**
  Aby uniemożliwić dostęp do danych nieupoważnionym stronom dane w systemie oznaczane są jako niewymienione i nadpisywane w przypadku ich usunięcia.
- **PRZECHOWYWANIE DANYCH**
  Dane systemowe przechowujemy przez dziewięćdziesiąt (90) dni, natomiast karty drogowe, wykresy i raporty przez bieżący rok a dane historyczne przez dwa (2) lata. Wymagania te mogą się różnić w związku ze specyficznymi przepisami obowiązującymi w danym kraju.
- **WYBIERZ INTEGRALNOŚĆ I CHROŃ ŚRODOWISKO**
  Zapewniamy bezpieczną platformę, która pozwala oszczędzać pieniądze, a jednocześnie dbać o środowisko naturalne.

Let's drive business

www.tomtom.com/telematics

TOMTOM TELEMATICS

Czy chcesz uzyskać szczegółowe informacje na temat bezpieczeństwa usług telematycznych?

Wejdź na **https://telematics.tomtom.com/isms** Ci odbierz certyfikowany poradnik dotyczący bezpieczeństwa informacji i ochrony danych.

Skontaktuj się z nami:
privacy@telematics.tomtom.com

CERTYFIKOWANE BEZPIECZEŃSTWO INFORMACJI I DANYCH TELEMATYCZNYCH

TOMTOM TELEMATICS

W TOMTOM TELEMATICS ZOBOWIĄZUJEMY SIĘ DO PRZESTRZEGANIA **ZASAD BEZPIECZEŃSTWA INFORMACJI I OCHRONY DANYCH.**

Nieustannie inwestujemy w technologie, dział inżynieryjny oraz pracujących w nim pracowników zapewniając naszym klientom najbardziej niezawodną platformę usług telematycznych, jaka jest dostępna na rynku.

WYDAJNOŚĆ PLATFORMY USŁUGOWEJ TOMTOM TELEMATICS

CERTYFIKAT BEZPIECZEŃSTWA DANYCH ISO/IEC 27001:2013
Posiadamy certyfikację naszej platformy i naszych procesów wewnętrznych, aby zagwarantować, że nasi klienci korzystają z najwyższego poziomu ochrony pod kątem bezpieczeństwa informacji i ochrony danych.

NAJWYŻSZY STANDARD SZYFROWANIA EV SSL
Zapewniamy szyfrowane logowanie do naszej platformy dzięki czemu Klienci mogą mieć pewność, że ich dane są bezpieczne.

LOKALNA INSTALACJA
Posiaday autoryzowaną sieć instalatorów

NAJWYŻSZEJ JAKOŚCI OBSŁUGA
Świadczona przez lokalnych sprzedawców i integratorów systemów

APP CENTER
Sprawdzone rozwiązania i aplikacje dostępne w App Center

Jesteśmy światowym liderem w dziedzinie telematyki i zarządzania flotą pojazdów.

Ponieważ jesteśmy jednym z największych dostawców usług telematycznych na świecie, stałe ulepszanie oferowanych przez nas usługi jest dla nas najważniejsze, ponieważ chcemy mieć pewność, że jesteśmy i będziemy najlepszym partnerem dla Twojej firmy.

Zgodność z normą ISO 27001

Nasz System Zarządzania Bezpieczeństwem Informacji (SZBI) obejmuje wszystkie najważniejsze procesy biznesowe konieczne do zabezpieczenia zasobów informacyjnych związanych z platformą usługową TomTom Telematics. Obejmuje to usługi związane z architekturą systemów, inżynierią, zapewnieniem jakości i informatyką dostarczaną przez firmę TomTom Telematics w naszym centrum technologicznym w centra danych znajdujące się na terenie Unii Europejskiej. Działania te przeprowadzanie są w zgodnie ze normą ISO/IEC 27001:2013 i realizowane zgodnie z oświadczeniem o stosowalności w wersji z listopada 2016 r.

„Certyfikat ISO 27001 gwarantuje pełną kontrolę nad naszymi procesami, a dane naszych klientów są w bezpiecznych rękach. Jest to dla nas wyjątkowo istotne, ponieważ dostarczamy rozwiązania z zakresu zarządzania flotą pojazdów typu „Software as a Service" (oprogramowanie jako usługa).

Thomas Schmidt, dyrektor zarządzający, TomTom Telematics

System zarządzania bezpieczeństwem informacji

Podstawą działań TomTom Telematics na rzecz bezpieczeństwa informacji jest zestaw kluczowych zasad i programów bezpieczeństwa, które obowiązują w organizacji. W oparciu o program zarządzania ryzykiem zgodny z celami firmy strefa bezpieczeństwa działa w zakresie systemu SZBI, który obejmuje między innymi następujące dziedziny:

ZASADY BEZPIECZEŃSTWA INFORMACJI
Szczegółowy zestaw zasad bezpieczeństwa stworzony po to, aby ukierunkowywać i wspierać system zarządzania informacjami oraz wszystkie działania operacyjne związane z platformą TomTom Telematics.

ORGANIZACJA BEZPIECZEŃSTWA INFORMACJI
Role i obowiązki wszystkich pracowników określone są na podstawie procedur bezpieczeństwa informacji. Za kontrolę, przestrzeganie powyższych czynności, jak również za stosowanie się do ogólnego rozporządzenia o ochronie danych (GDPR) Unii Europejskiej oraz stosownych lokalnych przepisów dotyczących ochrony prywatności odpowiedzialny jest dedykowany zespół działający zgodnie z certyfikatem ISO 27001.

BEZPIECZEŃSTWO DANYCH W DZIALE KADR
Bezpieczeństwo informacji ma zasadnicze znaczenie przed zatrudnieniem, w jego trakcie i po ustaniu stosunku pracy. Dotyczy to również wyboru właściwych pracowników i zapewnienia im stałych oraz indywidualnie dopasowanych szkoleń.

ZARZĄDZANIE ZASOBAMI
Inwentaryzacja, posiadanie oraz konserwacja zasobów przez cały okres eksploatacji gwarantuje właściwą kategoryzację, oznaczanie oraz przypisanie właściciela ryzyka. Obejmuje to bezpieczne obchodzenie się z własnością intelektualną firmy i danymi klientów.

KONTROLA DOSTĘPU
Dzięki narzędziom do zarządzania tożsamością wszelki dostęp do danych jest ograniczony i udzielany na zasadzie „ścisłej potrzeby". Dodatkowe kontrole pomagają zapobiegać nieuprawnionemu dostępowi. Na przykład logowanie do systemu i monitoring pozwalają w czasie rzeczywistym wykrywać zagrożenia w obrębie naszej strefy bezpieczeństwa.

KRYPTOGRAFIA
Inwestujemy w najnowocześniejszy sprzęt i oprogramowanie. Sprawdzone technologie kryptograficzne chronią prywatność, integralność danych naszych klientów oraz naszych systemów operacyjnych.

BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE
Zgodnie z obowiązującymi w Unii Europejskiej przepisami dotyczącymi ochrony danych posiadamy dwa niezależne centra danych Tier3+ na terenie Unii Europejskiej. Konfiguracja typu „aktywne-aktywne" zapewnia funkcje przywracania pracy po awarii oraz największą dostępność, które są regularnie sprawdzane.

BEZPIECZEŃSTWO OPERACYJNE
Dokładamy wszelkich starań, aby stosować w naszych działaniach operacyjnych ścisłe i powtarzalne procesy, którymi można zarządzać. Określenie podstaw bezpieczeństwa pozwala zarządzać poziomami ryzyka i pozwala podejmować skuteczne decyzje operacyjne.

Najważniejsze cechy bezpieczeństwa operacyjnego:

- **Procedury operacyjne i dokumentacja**
- **Testy kopii zapasowych i przywracania ważnych systemów**
- **Monitorowanie środowisk operacyjnych**
- **Zarządzanie zdarzeniami, problemami i zmianami w oparciu o dobre praktyki**
- **Zarządzanie wydajnością z testami obciążeniowymi**
- **Podział obowiązków**
- **Wzmacnianie systemu**
- **Podział środowisk na rozwój, testowanie i produkcję**
- **Skanowanie słabych punktów**
- **Testy penetracyjne**
- **Zarządzanie poprawkami**

BEZPIECZEŃSTWO KOMUNIKACJI
Bezpieczeństwo danych podczas ich przesyłania wymaga bezpiecznej sieci, którą one podróżują. Stosujemy bezpieczne metody komunikacji, takie jak:

- **Podział sieci**
- **Rozdział sieci VLAN i stref DMZ z wielopoziomowymi zaporami**
- **Narzędzia kontroli dostępu do sieci (NAC)**
- **Domyślne szyfrowanie przy użyciu najnowszych standardów branżowych**

Let's drive business

www.tomtom.com/telematics

TOMTOM TELEMATICS