webfleet

Telematik-Lösung mit Zertifizierung für Informationssicherheit und Datenschutz

ISO 27001
Certified Information Security Management System
www.tuv-sud.com/ms-cert

BRIDGESTONE
Solutions for your journey

Der Zweck dieses Whitepapers besteht darin, Geschäftspartner, Interessenten und Kunden umfassend über die nach ISO/IEC 27001 zertifizierte Webfleet Telematics Service Platform zu informieren. Die darin enthaltenen Informationen genügen, um alle Interessenten bei Due-Diligence-Prüfung und Risikoanalyse sowie die Datenschutzbeauftragten und Betriebsräte bei ihren Datenschutzinitiativen zu unterstützen.

Webfleet bekennt sich zu Informationssicherheit und Datenschutz

Wir investieren fortlaufend in unsere Technik, Technologien, Prozesse und Mitarbeiter, damit wir unseren Kunden stets den zuverlässigsten Telematik-Dienst anbieten können, den es auf dem Markt gibt.

Die Leistungsfähigkeit der Webfleet Telematics Service Plattform

INFORMATIONSSICHERHEIT NACH ISO 27001
Unsere Service-Plattform und unsere ausgereiften Prozesse sind nach ISO 27011 zertifiziert, so dass unsere Kunden von einem Höchstmaß an Informationssicherheit und Datenschutz profitieren.

EV SSL-VERSCHLÜSSELUNG NACH HÖCHSTEN STANDARDS
Sichere, verschlüsselte Anmeldung bei der Service-Plattform und sichere Datenübertragung. Bei uns sind Ihre Daten in guten Händen.

LOKALE INSTALLATION
Installationsbetriebe im In- und Ausland.

ERSTKLASSIGE UNTERSTÜTZUNG
von inländischen Händlern und Systemintegratoren.

APP CENTER
Bewährte Integrationen und Zusatzanwendungen aus unserem App Center.

Es ist kein Zufall, dass wir ein weltweit führender Anbieter von Flottenmanagement- und Telematik-Lösungen sind.

Als einer der weltweit größten Anbieter von Telematik-Diensten investieren wir kontinuierlich in unsere Services. Wir entwickeln uns ständig weiter, weil wir der beste Partner für Ihr Unternehmen sein wollen – jetzt und in Zukunft.

Inhalt

1 MANAGEMENTSYSTEM FÜR INFORMATIONSSICHERHEIT

Was ist die ISO/IEC 27001?

Die internationale Norm ISO/IEC 27001 bietet einen Standard für den Schutz von Informationswerten. Als Informationen gelten alle physischen oder virtuellen Vermögenswerte, die für ein Unternehmen einen Wert haben. Unsere Strategie zum kontinuierlichen Schutz dieser Vermögenswerte sowie der Daten unserer Kunden wird durch unser Managementsystem für Informationssicherheit (ISMS) umgesetzt.

Das ISMS gewährleistet, dass alle im Unternehmen genutzten Prozesse und Informationswerte regelmäßig vollständig überprüft und auf die Webfleet-Baseline für akzeptable Risiken abgestimmt werden.

"Die ISO 27001 bietet eine der renommiertesten Managementzertifizierungen und belegt, dass wir die uneingeschränkte Kontrolle über unsere Prozesse und Informationswerte haben. Vor allem aber zeigt sie, dass unsere Kundendaten bei uns in sicheren Händen sind, was für uns als Anbieter einer geschäftskritischen SaaS-Lösung für das Flottenmanagement entscheidend ist."

Jan-Maarten de Vries,
President von Fleet Management Solutions,
Bridgestone Mobility Solutions

ISMS-zertifizierter Geltungsbereich

Unser ISMS umfasst alle unsere kritischen Geschäftsprozesse, die zur Sicherung der Informationswerte im Zusammenhang mit der Webfleet Telematics Service Platform erforderlich sind. Dazu zählen die Architektur, das Engineering, die Qualitätssicherung und die IT-Dienstleistungen, die in unserem Technikzentrum in Deutschland sowie in unseren sicheren Rechenzentren in der Europäischen Union für die Webfleet B.V. erbracht werden. Diese Struktur entspricht den Anforderungen der ISO/IEC 27001 und wird gemäß unserer Erklärung zur Anwendbarkeit umgesetzt.

Wir haben 2012 ein ISO/IEC 27001-konformes Managementsystem eingeführt und halten diese Zertifizierung durch jährliche interne und externe Bewertungen aufrecht, wodurch die Konformität unserer Prozesse mit der internationalen Norm gewährleistet ist.

Diese Zertifizierung zählt zu den anerkanntesten im Bereich des Informationssicherheitsmanagements, denn sie umfasst die meisten der von PCI oder ISAE 3402 empfohlenen Kontrollmechanismen bzw. übertrifft deren Anforderungen sogar. Dadurch ist Webfleet ein erstklassiger Anbieter von Software as a Service (SaaS)-Lösungen für das Flottenmanagement.

Die Zertifizierung kann im Zertifikats-/Auftraggeberverzeichnis der Zertifizierungsstelle TÜV SÜD eingesehen werden.

2 INFORMATIONSSICHERHEITSRICHTLINIEN

Webfleet legt größten Wert auf die Sicherheit der Webfleet Telematics Service Platform sowie die Sicherheit der Webfleet-Betriebsorganisation. Dazu zählen sämtliche Informationswerte, die gemäß den Angaben zum Geltungsbereich unseres ISMS im Zusammenhang mit der Entwicklung, dem Testen und dem Betrieb eine Rolle spielen.

Diese Selbstverpflichtung ist im Verhaltenskodex der Bridgestone Group festgelegt:

Zur Webfleet Corporate Ethics Policy

Siehe Bridgestone Verhaltenskodex und unsere Datenschutzrichtlinie:

Zur Webfleet-Datenschutzrichtlinie

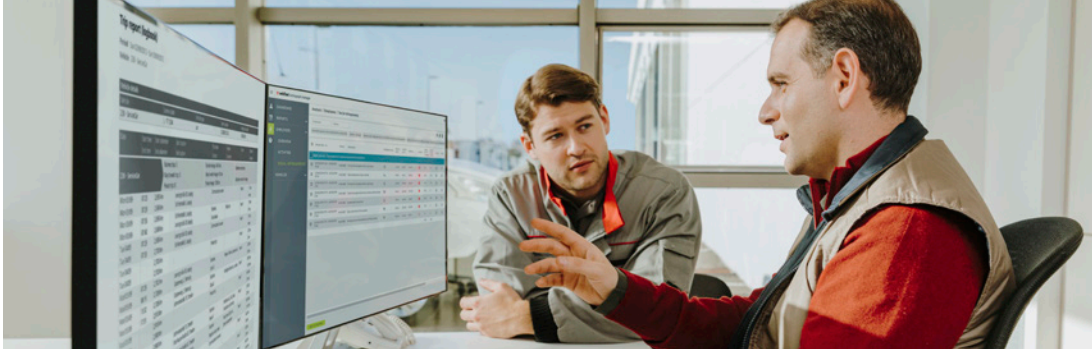
Die Grundlage für die Informationssicherheit bei Webfleet sind unsere Sicherheitsrichtlinien und -programme. Darin werden Festlegungen für die Informationssicherheit sowie für folgende Bereiche und Themen getroffen:

- **Sicherheit des Personals**
- **Asset Management**
- **Zutrittskontrolle**
- **Verschlüsselung**
- **Physische und ökologische Sicherheit**
- **Sicherheit im Betrieb**
- **Sicherheit der Kommunikation**
- **Erwerb, Entwicklung und Wartung von Systemen**
- **Lieferantenbeziehungen**
- **Umgang mit Informationssicherheitsvorfällen**
- **Bedeutung der Informationssicherheit für das Betriebskontinuitätsmanagement**
- **Compliance und Datenschutz**

Diese Richtlinien werden sowohl intern als auch extern regelmäßig von neutralen Stellen überprüft, um die Einhaltung der ISO/IEC 27001-Norm sowie aller einschlägigen Rechtsvorschriften zu gewährleisten und ihre fortgesetzte Rechtswirksamkeit und Rechtskonformität sicherzustellen.

Alle Mitarbeiter und Lieferanten der Webfleet Development Germany GmbH sind gehalten, die Sicherheitsrichtlinien oder vertraglich festgelegten Anforderungen zu beachten. Unsere Mitarbeiter werden regelmäßig zum Thema Informationssicherheit geschult, und es werden Unterlagen zur Verfügung gestellt, damit das Bewusstsein für die Bedeutung der Informationssicherheit im gesamten Unternehmen hoch bleibt. In den Unterlagen und Schulungen werden alle Sicherheitsaspekte abgedeckt, z. B. ein aufgeräumter Desktop, die sichere Nutzung des Internets, sichere Kodierungen, sicheres Arbeiten von entfernten Standorten aus sowie das richtige Verfahren für die Kennzeichnung und den Umgang mit sensiblen Daten.

Darüber hinaus werden durch Ad-hoc-Schulungen weitere Informationen und Kenntnisse vermittelt, damit sich alle Mitarbeiter ihrer Verantwortung für die Informationssicherheit bewusst sind und über die neuesten Technologien sowie die Schwachstellen im Zusammenhang mit dem Betrieb der Webfleet Telematics Service Platform und der Betriebsorganisation, für die sie verantwortlich sind, informiert sind. Die gesamte Dokumentation ist leicht verständlich gestaltet, damit die darin beschriebenen Maßnahmen auch gelesen und umgesetzt werden.



3 ORGANISATION DER INFORMATIONSSICHERHEIT

Informationssicherheit geht uns alle an

Webfleet beschäftigt ein Vollzeit-Informationssicherheitsteam, das in unsere Technik- und IT-Abteilungen integriert ist und von einigen der besten und klügsten Köpfe der Branche in den Bereichen Informations-, Anwendungs- und Netzwerksicherheit unterstützt wird. Das Team ist für die Aufrechterhaltung der Informationssicherheit im Unternehmen sowie die Entwicklung und Überprüfung der verschiedenen Sicherheitsrichtlinien und -maßnahmen verantwortlich und sorgt dafür, dass alle denkbaren Risiken gesteuert und auf die Strategien und die Risikobereitschaft des Unternehmens abgestimmt werden. Bei datenschutzrelevanten Themen stimmt sich unser externer Datenschutzbeauftragter mit dem Informationssicherheitsteam ab, um die Compliance sowie die Kommunikation mit Stakeholdern und internen Teams zu gewährleisten.

Zur Gewährleistung von Informationssicherheit und Datenschutz setzt Webfleet standardmäßig folgende Maßnahmen um:

- **Kontinuierliche Überprüfung und Verbesserung der Sicherheitsrichtlinien und -verfahren im Zusammenhang mit unserem hochverfügbaren Netzwerk, den redundanten Systemen und den erstklassigen Diensten auf der Grundlage von international anerkannten best practices und Standards; Integration von speziellen Kontrollmechanismen durch einen Multi-Layer-Ansatz**
- **Regelmäßige Überprüfung des technischen Sicherheitsdesigns und des Stands der Umsetzung auf allen Ebenen des Unternehmens im Rahmen des ISMS**
- **Kontinuierliche Rückmeldung an die Geschäftsleitung zum Status des ISMS und zu etwaigen Risiken, die ggf. eine Überprüfung durch die Geschäftsleitung erfordern**
- **Überwachung aller technischen Systeme, so dass auf alle sicherheits- oder informationsbezogenen Vorfälle in Echtzeit reagiert werden kann**
- **Incident Management Services, um einen taktischen Überblick und eine Analyse der Informationssicherheitsressourcen und der gegen diese gerichteten Bedrohungen zu erhalten**
- **Aufrechterhaltung konsequenter Kontrollen unserer getrennten Entwicklungs-, Test- und Produktionsumgebungen durch Maßnahmen wie Schwachstellenmanagement, Kapazitätsmanagement, Patch-Management, statische Code-Analyse und -Überprüfung, die sich an den best practices von Standards wie ITIL und ISO 20000 für das Service-Management orientieren**
- **Pflege von Kontakten zu Sicherheitsexperten, den örtlichen Strafverfolgungsbehörden sowie den Rechts- und Personalabteilungen der Webfleet Group, um die Einhaltung von Rechtsvorschriften sowie die Innenrevision zu gewährleisten**
- **Überprüfung und Sensibilisierung für die physische Sicherheit in unseren Büros und Rechenzentren**

4 SICHERHEIT DES PERSONALS

Die Informationssicherheit ist vor, während und nach der Beendigung des Arbeitsverhältnisses von entscheidender Bedeutung. So müssen geeignete Mitarbeiter oder Auftragnehmer ausgewählt und anschließend fortlaufend individuell geschult werden.

Die Personalabteilung sorgt dafür, dass unser wichtigstes Kapital, unsere Mitarbeiter, im Einklang mit den jeweils geltenden arbeitsrechtlichen Vorschriften geschützt werden, und dass ihre Aufgaben bei der Unterstützung und Aufrechterhaltung der Informationssicherheit innerhalb des Unternehmens vertraglich festgelegt sind, um so die Daten unserer Kunden und unser geistiges Eigentum effektiv zu schützen.

Die Mitarbeiter sind verpflichtet, die Richtlinien des Unternehmens in Bezug auf Vertraulichkeit, ethisch einwandfreies Geschäftsgebaren, die angemessene Nutzung von Vermögenswerten und professionelle Standards einzuhalten. Im Einstellungsverfahren überprüft Webfleet die Ausbildung, die früheren Beschäftigungsverhältnisse sowie die internen und externen Referenzen des Bewerbers. Soweit die jeweils geltenden arbeitsrechtlichen Vorschriften dies zulassen, kann Webfleet auch Führungszeugnisse anfordern, die Bonität und den Einwanderungsstatus prüfen und eine Sicherheitsüberprüfung durchführen, sofern dies für die jeweilige Stelle geboten ist. Der Umfang dieser Prüfungen hängt von den Merkmalen der zu besetzenden Position ab.

Mit der Aufnahme des Arbeitsverhältnisses bei Webfleet müssen alle Mitarbeiter eine Vertraulichkeitserklärung unterzeichnen. Ferner müssen sie bestätigen, dass sie die Richtlinien des Webfleet IT-Benutzerhandbuchs einhalten, und sich dazu verpflichten, diese sowie alle sonstigen in ihrem Arbeitsbereich geltenden Richtlinien und Verfahren zu beachten.

Zur Einhaltung der geltenden Rechtsvorschriften sind unsere Mitarbeiter in ihren Arbeitsverträgen auf das Datengeheimnis verpflichtet, das mit der Datenschutz-Grundverordnung (DSGVO) der EU und anderen einschlägigen Datenschutzvorschriften im Einklang steht. Darüber hinaus werden alle Mitarbeiter regelmäßig in den sie betreffenden Sicherheits- und Datenschutzbestimmungen geschult, um das Betriebsrisiko des Unternehmens insgesamt zu verringern. Der Einsatz von Subunternehmern in unseren Entwicklungs- und operativen Abteilungen wird auf ein Minimum beschränkt, und es werden zusätzliche Kontrollmechanismen durchgeführt, um ein hohes Maß an Sicherheit zu gewährleisten.

Die Vertraulichkeit und der Schutz von Kundeninformationen und -daten stehen in unseren Richtlinien und bei der Einarbeitung neuer Mitarbeiter im Mittelpunkt. Neue Mitarbeiter erhalten im Rahmen der Einarbeitung eine Sicherheitsschulung. Darüber hinaus ist jeder Webfleet-Mitarbeiter zur Einhaltung des Verhaltenskodex des Unternehmens verpflichtet. In dem Verhaltenskodex werden die Erwartungen von Webfleet festgelegt. So wird verlangt, dass jeder Mitarbeiter seine Aufgaben rechtskonform, ethisch einwandfrei und integer erledigt. Dabei sind nicht nur andere Mitarbeiter, sondern auch Kunden, Partner und sogar die Wettbewerber des Unternehmens zu achten. Je nach Aufgabenbereich eines Mitarbeiters sind ggf. zusätzliche Sicherheitsschulungen und -richtlinien relevant.

Webfleet-Mitarbeiter, die mit Kundendaten arbeiten, sind zur Erfüllung zusätzlicher Anforderungen gemäß diesen Richtlinien verpflichtet. In Schulungen zu Kundendaten werden die angemessene Verwendung von Daten im Zusammenhang mit Geschäftsprozessen sowie die Folgen von Datenschutzverletzungen erläutert. Jeder Webfleet-Mitarbeiter hat Fragen bzw. Probleme im Zusammenhang mit den Themen Informationssicherheit und Datenschutz den für Sicherheitsfragen zuständigen Mitarbeitern von Webfleet mitzuteilen. Das Unternehmen verfügt über vertrauliche Meldewege, damit die Mitarbeiter jeden von ihnen bemerkten Verstoß gegen ethische Grundsätze anonym melden können.

5 ASSET MANAGEMENT

Verantwortung und Klassifizierung von Informationen

Bei Webfleet werden alle Informationswerte einem Informationsverantwortlichen und einem Risikoverantwortlichen zugeordnet.

Die Aufgabe dieser Personen besteht darin, dafür zu sorgen, dass die Telematik-Assets unter Einhaltung der für die Informationssicherheit geltenden Richtlinien und Verfahren ordnungsgemäß verwaltet und klassifiziert werden. Außerdem müssen sie den Status der Telematik-Assets regelmäßig überprüfen. Bei der regelmäßigen Überprüfung unserer Informationssysteme stimmt sich das Informationssicherheitsteam mit allen Informations- und Risikoverantwortlichen ab, um sich zu vergewissern, dass die einschlägigen Vorschriften eingehalten werden.

Handhabung und Entsorgung von Medien

Alle Medien bei Webfleet unterliegen Sicherheitsrichtlinien und -verfahren, die den ordnungsgemäßen Umgang mit Medien regeln. Medien sind alle Formate, in denen Informationen enthalten sein können. Dazu zählen insbesondere physische Festplatten, USB-Sticks, Compact Discs, Papier, elektronische Dokumente und Nachrichten. Bei Webfleet gilt ein Lebenszyklus für Medien, der die sichere Handhabung und Entsorgung aller relevanten Medien in diesem Bereich umfasst.

Sobald ein Medium aus den Webfleet-Systemen entfernt wird, werden die Daten auf physischen Datenträgern, die Kundeninformationen enthalten, vernichtet, bevor die physischen Datenträger die Betriebsräume von Webfleet verlassen. Erstens sieht die Richtlinie vor, dass die Festplatte von autorisierten Personen gelöscht

wird. Der Löschvorgang besteht darin, das Laufwerk vollständig mit allen Nullen (0x00) zu überschreiben, gefolgt von einem vollständigen Lesen des Laufwerks, um festzustellen, ob das Laufwerk leer ist, sowie einer anschließenden Überprüfung, um Gewissheit zu haben, dass die Festplatte erfolgreich gelöscht wurde. Die Löschergebnisse werden zusammen mit der Seriennummer des Laufwerks protokolliert und bleiben so nachvollziehbar. Anschließend wird das gelöschte Laufwerk für die Wiederverwendung und den erneuten Einsatz im Unternehmen freigegeben.

Wenn das Laufwerk aufgrund eines Hardwarefehlers nicht gelöscht werden kann, muss es so lange sicher aufbewahrt werden, bis es sicher vernichtet werden kann. Die sichere Vernichtung erfolgt durch unsere nach ISO 27001 zertifizierten Medienvernichter, die auch die Protokolle für alle das Unternehmen verlassenden Medien überprüfen. Webfleet führt regelmäßig interne Audits durch, um die Einhaltung der Medienentsorgungsrichtlinien zu überprüfen.

6 ZUGANGSSTEUERUNG

Steuerung von Nutzerzugang und Zuständigkeiten

Webfleet verfügt über umfangreiche Kontrollmechanismen und Praktiken, um Kundendaten zu schützen. Unsere Plattform läuft in einer sicheren, verteilten Umgebung mit mehreren Tenants. Anstatt die Daten jedes Kunden auf einem einzelnen Rechner oder mehreren Rechnern vorzuhalten, werden die Daten aller Plattformkunden (Daten von Privat- und Firmenkunden und sogar unsere eigenen Daten) in einer gemeinsamen Infrastruktur verteilt, die aus vielen homogenen Rechnern von Webfleet besteht und sich in den Active/Active ISO/IEC 27001-konformen Rechenzentren von Webfleet in Deutschland befindet.

Die Webfleet Telematics Service Platform arbeitet mit einem System aus verteilten Dateien, das für die Speicherung großer Datenmengen auf einer Vielzahl von Computern ausgelegt ist. Die strukturierten Daten werden dann in einer großen verteilten Datenbank gespeichert, die auf dem Dateisystem aufbaut. Die Daten werden auf mehrere Systeme verteilt und repliziert, so dass kein einziges System einen Single Point of Failure (SPOF) darstellt. Die Datenpakete erhalten zufällige Dateinamen und werden nicht im Klartext gespeichert, so dass sie für Menschen nicht lesbar sind. Die Layer unserer Plattform sehen vor, dass die von anderen Komponenten kommenden Anfragen authentifiziert und autorisiert werden. Die Dienst-zu-Dienst-Authentifizierung beruht auf einem Sicherheitsprotokoll, bei dem ein Plattformsystem authentifizierte Kanäle zwischen Anwendungsdiensten vermittelt.

Das Vertrauen zwischen den Instanzen dieses Authentifizierungsbrokers wird wiederum von x509-Host-Zertifikaten abgeleitet, die von einer Webfleet-internen Zertifizierungsstelle für jeden Plattform-Produktionshost ausgestellt werden.

Der Zugang der Administratoren von Produktionsanwendungen zu den Produktionsumgebungen wird in ähnlicher Weise gesteuert. Ein zentrales Gruppen- und Rollenmanagementsystem legt fest, welche Zugangsrechte die Techniker in Bezug auf die Produktionsdienste haben, und überwacht den Zugang. Dabei wird eine Erweiterung des oben genannten Sicherheitsprotokolls verwendet, mit dem die Techniker durch ein für sie persönlich ausgestelltes x509-Zertifikat authentifiziert werden. Die Richtlinie schreibt vor, dass der administrative Zugang zur Produktionsumgebung zu Debugging- und Wartungszwecken über sichere, mit einem öffentlichen Schlüssel authentifizierte Shell-Verbindungen (SSH) erfolgen muss. In beiden Szenarien werden Gruppenmitgliedschaften, die Zugang zu Produktionsdiensten oder -konten gewähren, nach Bedarf eingerichtet.

Die oben beschriebenen Sicherheitskontrollen beruhen auf der Integrität der Produktionsplattform. Die Plattform wiederum stützt sich auf:

- **den physischen Schutz der Umgebung des Rechenzentrums**
- **die Integrität der Umgebung des Produktionsbetriebssystems**
- **den begrenzten, bedarfsorientierten Zugang der Systemadministratoren (Root-Ebene) auf die Produktionshosts; dieser Zugang wird nur einer speziellen Gruppe von Mitarbeitern gewährt, deren Zugriffe genau überwacht werden**

Diese Aspekte der Webfleet-Sicherheitsmethodik werden in den folgenden Abschnitten dieses Whitepapers ausführlicher behandelt.

Authentifizierung

Jeder Mitarbeiter von Webfleet muss eine eindeutige Nutzer-ID verwenden. Über das entsprechende Nutzerkonto werden die Aktivitäten jeder Person im Webfleet-Netzwerk erkannt, insbesondere Zugriffe auf Mitarbeiter- oder Kundendaten. Das eindeutige Nutzerkonto wird für jedes System bei Webfleet verwendet. Bei der Einstellung eines Mitarbeiters erhält dieser von der Personalabteilung eine Nutzer-ID mit einer Reihe von Standardberechtigungen, die im Folgenden beschrieben werden. Bei Beendigung des Arbeitsverhältnisses muss der Zugang des Kontos zum Webfleet-Netzwerk über das Personalsystem deaktiviert werden.

Soweit Passwörter oder Passphrasen zur Authentifizierung verwendet werden (z. B. bei der Anmeldung an Workstations), setzen die Systeme die strengen Passwortrichtlinien von Webfleet durch. Diese sehen den Ablauf von Passwörtern, eine Beschränkung der Wiederverwendung von Passwörtern sowie eine ausreichende Passwortstärke vor. Webfleet nutzt in großem Umfang die Zwei-Faktor-Authentifizierung, beispielsweise in Form von Zertifikaten und Einmal-Passwort-Generatoren.

Rechte

Welche Zugangsrechte und -ebenen ein Mitarbeiter hat, hängt von seiner Funktion und seinen Aufgaben ab. Dabei folgt Webfleet dem Prinzip der minimalen Rechtevergabe (POLP) sowie dem Grundsatz, dass jeder Mitarbeiter nur Zugang zu den Informationen und Daten hat, die er für die Erfüllung seiner Aufgaben unbedingt benötigt. Unsere Mitarbeiter haben nur eine begrenzte Anzahl von Standardberechtigungen für den Zugriff auf Unternehmensressourcen, wie z. B. das E-Mail-System, das interne Webfleet-Portal und Personalinformationen. Anträge auf weitere Zugangsrechte können im Rahmen eines

genau definierten Prozesses gestellt werden. Dieser sieht vor, dass der Antrag geprüft und ggf. von einem Daten- oder Systemverantwortlichen, dem Vorgesetzten oder einer anderen Führungskraft gemäß den Anforderungen in den Sicherheitsrichtlinien von Webfleet genehmigt wird. Genehmigungen werden mit Hilfe von Workflow-Tools verwaltet, in denen alle Änderungen durch Prüfprotokolle dokumentiert werden. Mit diesen Tools werden sowohl die Änderung von Genehmigungseinstellungen als auch der Genehmigungsprozess gesteuert, um eine einheitliche Anwendung der Genehmigungsrichtlinien zu gewährleisten. Über die Rechtekonfiguration für einen Mitarbeiter wird gesteuert, auf welche Ressourcen der jeweilige Mitarbeiter Zugriff hat. Zu diesen Ressourcen gehören insbesondere die Daten der Service-Plattform und die Produktionssysteme.

System-Protokolle

Die Webfleet-Richtlinie sieht vor, dass jeder Zugriff eines Administrators auf Systeme und Daten protokolliert wird. Die entsprechenden Protokolle können von den Webfleet-Sicherheitsmitarbeitern bei Bedarf eingesehen werden, um forensische Maßnahmen zu unterstützen oder unseren Perimeterschutz aufrecht zu erhalten. Die Protokolle werden auf einem separaten Server gespiegelt, auf dem sie nicht bearbeitet werden können.

7 VERSCHLÜSSELUNG

Webfleet investiert in hochmoderne Hardware- und Softwarelösungen, darunter bewährte kryptografische Technologien, damit Informationswerte und vertrauliche Daten mit hoher Verschlüsselung und in sicherer Form übertragen und verwaltet werden. Dies ist entscheidend, um die Sicherheit der Daten unserer Kunden sowie die betriebliche Integrität unserer Systeme zu gewährleisten.

Alle Webfleet-Umgebungen sind optimal vor Bedrohungen aller Art geschützt, und unser Betriebsteam wird in Echtzeit über alle internen und externen Eindringversuche informiert.

Sichere Datenübertragung

Webfleet bietet eine sichere SSL/TLS-Übertragung von Daten der Service-Plattform (Nutzerschnittstelle oder Plattform-APIs).

Die SSL/TLS-Zertifikate werden von einem führenden Unternehmen für kryptografische Sicherheit bereitgestellt. Die 2048-Bit-Zertifikate bieten ein perfektes Gleichgewicht zwischen Performance und hoher Sicherheit und werden auch vom US-amerikanischen National Institute of Standards and Technology (NIST) und dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlen.

Darüber hinaus unterstützen die SSL/TLS-Zertifikate folgende Sicherheitsmerkmale:

- **256-Bit und 128-Bit https AES-Verschlüsselung. Https wird standardmäßig für den Zugriff auf Daten über die Nutzeroberfläche oder die Plattform-APIs verwendet**
- **SHA-256-Verschlüsselung; diese entspricht den höchsten kryptografischen Standards der EU**
- **Extended Validation (EV)-Authentifizierungsstufe, die höchstmögliche Stufe, die erreicht werden kann**

8 PHYSISCHE SICHERHEIT UND SICHERHEIT DER UMGEBUNG

Webfleet hält eine strikte Trennung seiner physischen, logischen und umgebungsbezogenen Informationen und Infrastrukturen aufrecht, um größtmögliche Sicherheit für Kunden und Kundendaten zu erreichen.

Dazu gehört auch der Schutz der in unserem Verantwortungsbereich für die Datenverarbeitung eingesetzten Hardware.

Einige Beispiele dafür, wie Webfleet die physische Sicherheit und die Sicherheit der Umgebung gewährleistet:

- **Systemhärtung auf der Grundlage des Center for Internet Security (CIS)-Standards zur Härtung von Betriebssystemen, Datenbanken und Netzwerk-Hardware**
- **Regelmäßige Überprüfungen und Tests; Einspielung von Patches durch unser Patch-Management-Programm**
- **Zentrale Verwaltung von Zugangskontrolllisten auf der Grundlage bewährter Verfahren der rollenbasierten Zugangskontrolle (RBAC), damit nur solche Personen Zugang erhalten, die darauf angewiesen sind; die Zugriffe werden überwacht und protokolliert, damit bei Systemmanipulationen nachgewiesen kann, wer verantwortlich ist**
- **Regelmäßige Überwachungs- und Prüfvorgänge mit Dokumentation durch Protokolldateien**
- **Echtzeit-Überwachung und -Warnungen bei allen operativen Systemen (sowohl physische als auch virtuelle Systeme)**
- **Systeme zur Verhinderung von unbefugten Zugriffen mit Echtzeit-Warnung. Dazu zählen netzwerkbasierte Intrusion-Prevention-Systeme (NIPS), drahtlose Intrusion-Prevention-Systeme (WIPS), Systeme zur netzwerkbasierten Verhaltensanalyse (NBA) sowie hostbasierte Intrusion-Prevention-Systeme (HIPS). Durch die Einbindung von Intrusion-Prevention-Systemen verschiedener Hersteller können verschiedene Erkennungsmethoden genutzt werden, zum Beispiel Erkennungsmethoden, die auf Signaturen oder statistischen Anomalien beruhen oder eine zustandsabhängige Protokollanalyse.**

Geografische/physikalische Trennung

Die Rechenzentren von Webfleet sind geografisch verteilt und auf die Anforderungen des ISMS abgestimmt. In den Rechenzentren werden verschiedene physische Sicherheitsmaßnahmen umgesetzt, um unseren Perimeterschutz aufrechtzuerhalten. In Abhängigkeit von den örtlichen Gegebenheiten (z. B. Gebäudestandort, regionale Risiken) werden in den Rechenzentren unterschiedliche Technologien und Sicherheitsmechanismen eingesetzt. Wir legen jedoch großen Wert darauf, dass unsere Standorte und Anbieter nach Möglichkeit nach ISO/IEC 27001 zertifiziert sind.

Die standardmäßig in allen Rechenzentren von Webfleet implementierten physischen Sicherheitsvorkehrungen, umfassen bekannte Technologien und entsprechen den allgemein anerkannten best practices der Branche:

- **an die individuellen Anforderungen angepasste kartenbasierte elektronische Zutrittskontrollsysteme**
- **Alarmanlagen**
- **Innen- und Außenkameras**
- **Sicherheitsbestreifung**

Der physische Zutritt zu Bereichen, in denen Systeme oder Systemkomponenten installiert sind bzw. gelagert werden, ist von den allgemeinen Büro- und öffentlichen Bereichen wie Lobbys getrennt. Kameras und Alarmanlagen für jeden dieser Bereiche werden zentral auf verdächtige Vorkommnisse überwacht, und die Standorte werden routinemäßig von Sicherheitspersonal bestreift. An den Standorten von Webfleet werden hochauflösende Kameras mit Videoanalyse und andere Systeme eingesetzt, um Eindringlinge zu erkennen und zu verfolgen. Damit Vorfälle bei Bedarf untersucht werden können, werden Vorgangsprotokolle und Kameraaufzeichnungen aufbewahrt. Bei Bedarf werden zusätzliche Sicherheitsmaßnahmen wie Wärmebildkameras, Umzäunungen und biometrische Verfahren eingesetzt. Der Zugang zu allen Einrichtungen des Rechenzentrums ist auf autorisierte Webfleet-Mitarbeiter, zugelassene Besucher und zugelassene Dritte, die mit dem Betrieb des Rechenzentrums beauftragt sind, beschränkt.

Webfleet hat auch eine Richtlinie für den Zutritt von Besuchern sowie verschiedene Verfahren, die vorsehen, dass jeder Besucher im Voraus eine Genehmigung des Leiters des Rechenzentrums für die internen Bereiche haben muss, die er besuchen möchte. Die Regeln für Besucher gelten auch für alle Webfleet-Mitarbeiter, die normalerweise keinen Zutritt zum Rechenzentrum haben. Webfleet prüft regelmäßig, wer Zutritt zu den Rechenzentren hat, um sicherzustellen, dass nur diejenigen Zutritt haben, die darauf angewiesen sind, um ihre Aufgaben erfüllen zu können. Webfleet beschränkt den Zutritt zu seinen Rechenzentren auf der Grundlage der Funktion und nicht der Position des jeweiligen Mitarbeiters. Infolgedessen haben selbst die meisten Führungskräfte von Webfleet keinen Zutritt zu den Rechenzentren des Unternehmens.

Sicherheit der Umgebung

Bei der Planung der Computing-Cluster von Webfleet wurde Wert auf Ausfallsicherheit und Redundanz gelegt. Dadurch gibt es nur wenige Single Points of Failure und die Auswirkungen von üblichen Geräteausfällen und Umgebungsrisiken können minimiert werden. Doppelt ausgelegte Stromkreise, Schalter, Netzwerke und andere betriebsnotwendige Geräte sorgen für eine hohe Redundanz. Die Infrastruktur der Rechenzentren ist robust und fehlertolerant, dabei jedoch wartungsfreundlich.

Stromversorgung

Zur Gewährleistung des Dauerbetriebs (24/7) sind die Rechenzentren mit einer redundanten Stromversorgung ausgerüstet. Für jede kritische Komponente im Rechenzentrum gibt es eine Haupt- und eine alternative Stromversorgung mit jeweils gleicher Kapazität. Bei einem Ausfall der Hauptstromversorgung, z. B. aufgrund eines Stromausfalls, eines Blackouts, einer Über- oder Unterspannung oder eines Frequenzfehlers, übernimmt eine unterbrechungsfreie Stromversorgung (USV) oder eine rotierende unterbrechungsfreie Stromversorgung mit Dieselaggregat (DRUPS) die Versorgung, bis die Notstromaggregate angelaufen sind. Die USV und die DRUPS liefern genügend Strom, um das Rechenzentrum so lange mit voller Kapazität zu betreiben, bis die normale Stromversorgung wiederhergestellt wurde.

Klima und Temperatur

Da Server und andere Computerhardware auf eine konstante Betriebstemperatur angewiesen sind, müssen Rechenzentren gekühlt werden. Die Kühlung verhindert eine Überhitzung der Hardware und verringert die Gefahr von Betriebsausfällen. Die Klimaanlagen in den Serverräumen werden sowohl vom normalen als auch vom Notstromsystem gespeist. Darüber hinaus gibt es Systeme zur Sauerstoffreduzierung, die die Sauerstoffmenge in den Rechenzentren auf das für die Arbeit unserer Mitarbeiter erforderliche Minimum reduzieren. Der Sauerstoffgehalt ist dadurch nicht so hoch, dass ein Brand entstehen könnte. Mit diesen ausgewogenen Maßnahmen wird ein Höchstmaß an Sicherheit für unsere Service-Plattform erreicht.

Branderkennung und -bekämpfung

Automatische Brandmelde- und Feuerlöschanlagen tragen dazu bei, Schäden an der Hardware zu verhindern. Die Brandmeldesysteme verfügen in den Decken und unter dem Doppelboden des Rechenzentrums über Wärme-, Rauch- und Wassersensoren. Bei der Entstehung von Feuer oder Rauch löst die Brandmeldeanlage einen akustischen und visuellen Alarm in dem betroffenen Bereich, in der Brandmelderzentrale und in der entfernten Leitstelle aus. Außerdem sind die Rechenzentren mit Handfeuerlöschern ausgestattet. Die Techniker der Rechenzentren erhalten eine Schulung zur Brandverhütung und zum Löschen von Bränden, die auch den Einsatz von Feuerlöschern umfasst. Die meisten unserer Rechenzentren verfügen über eine Stickstoff-Löschanlage, die aktiviert werden kann, um den restlichen Sauerstoff aus der Luft zu verdrängen und so die Auswirkungen Brands zu minimieren.

9 BETRIEBSSICHERHEIT

Überblick über die Konfiguration unserer Active/Active-Rechenzentren

Webfleet betreibt derzeit zwei Rechenzentren im Active/Active-Betrieb. Dank der Multi-Homing-Infrastruktur und der Lastausgleichs-Hardware können Internet-Uplinks, Anwendungsserver und Dienste von beiden Standorten aus gleichzeitig genutzt werden.

Beide Rechenzentren sind über drei redundante Gigabit-Verbindungen miteinander verbunden, wodurch Webfleet über einen leistungsfähigen und stabilen Ring von Kommunikationskanälen zwischen den in beiden Zentren befindlichen Diensten verfügt. Im Normalbetrieb sind beide Rechenzentren so konfiguriert, dass sie sich die Last teilen. Gleichzeitig ist aber jedes Rechenzentrum in der Lage, alle Dienste ohne Leistungseinbußen für die Kunden bereitzustellen.

Sicherheit von Rechenzentren

Webfleet betreibt zwei unabhängige Rechenzentren in der Europäischen Union, da für Rechenzentren mit Sitz in der EU hohe Datenschutzstandards gelten. Beide Zentren befinden sich unterirdisch in zwei verschiedenen Städten in Deutschland und werden von zwei verschiedenen Anbietern in einer Active/Active-Konfiguration betrieben, die höchste Verfügbarkeit und volle Disaster-Recovery-Fähigkeiten auch bei höherer Gewalt gewährleistet.

Beide Rechenzentren bieten ein sehr hohes Maß an Sicherheit und weisen folgende Merkmale auf:

Rechenzentrum 1 (Deutschland)

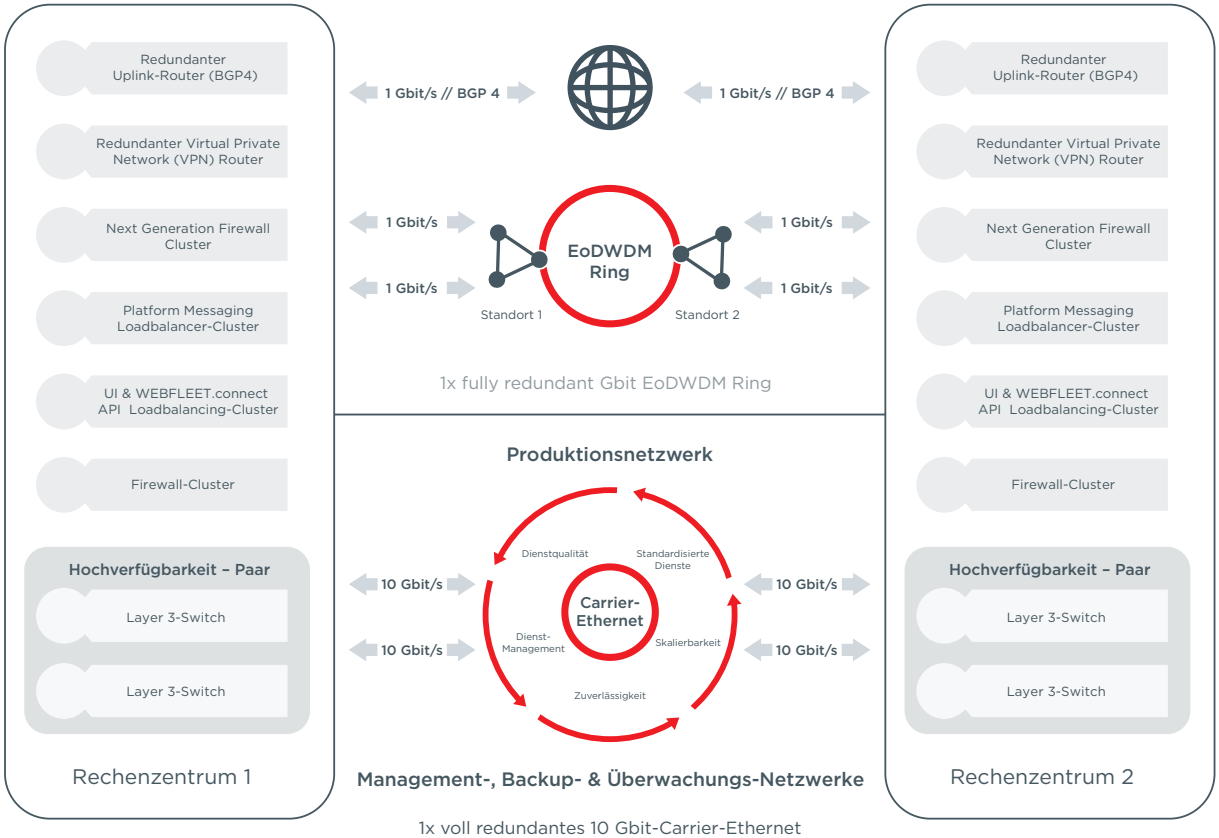
- **Separate Bereiche mit gesichertem Zutritt nur für autorisierte Webfleet-Mitarbeiter aus dem IT-Administratoren-Team**
- **Nach ISO 27001 zertifiziert**
- **Dreistufige Zutrittskontrolle**
- **N+1 redundante Hochleistungs-USV**
- **N+1 Notstromaggregat**
- **Monatliche Tests**
- **N+1 unabhängige Klimaanlagen**
- **Permanente Sauerstoffreduzierung zur Brandverhütung (~15 %)**
- **Fensterlose unterirdische Anlage**
- **Überwachung 24/7**
- **Mehrere Anbindungen ans WAN**
- **Alarmsensoren für Feuchtigkeit, Rauch, Vibration usw.**
- **Videoüberwachung mit 30-Tage-Aufzeichnung zur Unterstützung der Untersuchung von Sicherheitsvorfällen**

Rechenzentrum 2 (Deutschland)

- **Separate Bereiche mit gesichertem Zutritt nur für autorisierte IT-Administratoren von Webfleet**
- **Nach ISO 27001 zertifiziert**
- **Dreistufige Zutrittskontrolle**
- **Redundante Hochleistungs-USV**
- **Notstromaggregat**
- **Monatliche Tests**
- **Mehrere unabhängige Klimaanlagen**
- **Überwachung 24/7**
- **Mehrere Anbindungen ans WAN**
- **Alarmsensoren für Feuchtigkeit, Rauch, Vibration usw.**
- **Videoüberwachung mit 30-Tage-Aufzeichnung zur Unterstützung der Untersuchung von Sicherheitsvorfällen**

Überblick Netzwerk

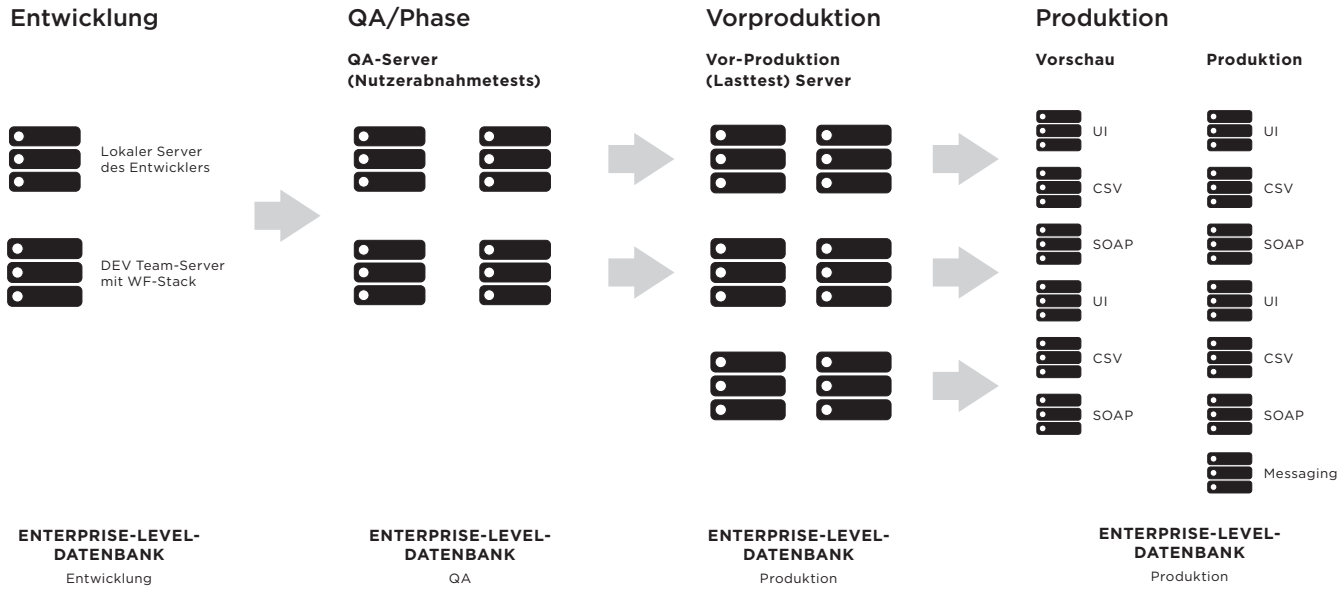
Die folgende Übersicht über unsere Netzwerkkonfiguration vermittelt einen Eindruck vom Aufbau unserer Active/Active-Rechenzentren:



Abkürzungen

EoDWDM	Ethernet over Dense Wavelength Division Multiplexing: Hochleistungsverbindung für hohe Anforderungen an die Bandbreite
BGP4	Border Gateway Protocol: Standard-Gateway-Protokoll zum Austausch von Routing- und Erreichbarkeitsinformationen zwischen autonomen Systemen im Internet. BGP4 ermöglicht die Aggregation von Routen einschließlich autonomer Systempfade
VPN	Virtuelles privates Netzwerk: ermöglicht das sichere Senden und Empfangen von Daten über gemeinsam genutzte oder öffentliche Netzwerke, so als befände sich der Nutzer innerhalb eines Unternehmensnetzwerks
UI	Nutzeroberfläche
API	Anwendungsprogrammierschnittstelle: eine Schnittstelle, mit der sich die Nutzer über verschiedene Methoden mit der Service-Plattform verbinden können
Gbit	Gigabit

Logisch getrennte Betriebsumgebungen



Sicherheit im Netz

Webfleet setzt mehrere Abwehr-Layer ein, um den Schutzperimeter vor externen und internen Angriffen zu schützen. Nur autorisierte Dienste und Protokolle, die den Sicherheitsanforderungen von Webfleet entsprechen, dürfen das Unternehmensnetzwerk durchqueren. Nicht autorisierte Pakete werden automatisch verworfen. Die Netzwerksicherheitsstrategie von Webfleet beruht auf folgenden Elementen:

- **Steuerung der Größe und des Aufbaus des Schutzperimeters. Durchsetzung der Netzwerktrennung mit Hilfe von branchenüblichen Firewalls und Zugangskontrolllisten (ACL)**
- **Systematische Verwaltung von Netzwerk-Firewalls und ACL-Regeln durch Änderungsmanagement, Peer Review und automatisierte Tests**
- **Beschränkung des Zugangs zu vernetzter Hardware auf befugte Mitarbeiter**
- **Weiterleitung des gesamten Datenverkehrs über nutzerdefinierte Front-End-Server, mit denen bösartige Anfragen erkannt und gestoppt werden können**
- **Einrichtung interner Aggregationspunkte zur Verbesserung der Überwachung**
- **Prüfung von Protokollen auf die Ausnutzung von Programmierfehlern (z. B. Cross-Site-Scripting) und Generierung von Warnmeldungen hoher Priorität, wenn ein Vorfall festgestellt wird**

Webfleet betreibt etwa 50 HP ProCurve Switches pro Rechenzentrum mit redundanten Verbindungen zu jedem Server (Bonding) und zusätzlichen getrennten Verbindungen für Backup und Management auf dedizierten Switches. Alle Verbindungen beruhen auf der Gigabit-Technologie, so dass sie eine optimale Leistung bieten und praktisch keine spürbare Netzwerklatenz aufweisen.

Logisch getrennte Netzwerkumgebungen

Webfleet gewährleistet einen optimalen Schutz vor externen und internen Bedrohungen für unsere Informationswerte. Dies wird durch die Trennung der Netzwerke (Demilitarized Zone [DMZ], Entwicklungs-, Test-, Produktions- und Büroumgebungen mit rollenbasierter Zugriffskontrolle [RBAC] u. a. Maßnahmen) und durch die Bereitstellung mehrerer NextGeneration Firewall-Cluster (NGFW) zur Trennung der verschiedenen Zonen erreicht:

- **Schichtenarchitektur mit Firewall-Clustern zur Trennung der Netzwerkbereichen**
- **Firewalls der nächsten Generation (mehrere Active/Active-Cluster pro Rechenzentrum)**
  - IPS zur Abwehr von Bedrohungen und Eindringversuchen
- **Firewall auf Anwendungsebene zum Schutz vor:**
  - Layer 7 DoS und DDoS
  - brachialer Gewalt
  - Cross-Site-Scripting (XSS)
  - Cross-Site Request Forgery
  - SQL-Einschleusung
  - Web-Scraping
  - Parameter- und HPP-Manipulationen
  - Durchsickern sensibler Daten
  - Session-Hijacking
  - Pufferüberläufen
  - Cookie-Manipulation
  - verschiedenen Verschlüsselungsangriffen
  - defekten Zugangskontrollen
  - erzwungenem Browsing
  - der Manipulation verborgener Felder
  - Request Smuggling
  - XML-Bomben/DoS
- **Restriktive Regeln und Strategien**
- **Tägliches Reporting und regelmäßige Audits**
- **Überwachung und Benachrichtigungen in Echtzeit**
- **Verschiedene Firewall-Anbieter**
- **Dreifacher Schutz vor E-Mail-Bedrohungen (Viren, SPAM, usw.)**

Systemüberwachung

Webfleet betreibt ein redundantes und verteiltes System zur Überwachung aller physischen und virtuellen Hosts und Services. Zusätzlich zu den technischen Überwachungslösungen verfügt unser System über Kontrollmechanismen, mit denen wir eine annähernde Replikation der Nutzererfahrung in Bezug auf die Verarbeitungs- oder http-Antwortzeiten erreichen.

Darüber hinaus besteht eine externe Überwachung von mehreren internationalen Standorten aus, durch die Konnektivitäts- oder Verfügbarkeitsprobleme beim Erreichen der Webfleet-Dienste (z. B. Internet-Peering-Probleme) in Echtzeit erkannt werden. Im Rahmen der Überwachung wird die Performance unsere Dienste aus Kundensicht erfasst (z. B. bei der Anmeldung an der Nutzeroberfläche), und wir erhalten regelmäßige SLA-Berichte für die interne Verwaltung der Dienste. Darüber hinaus wird das Webfleet-Betriebsteam über mehrere Kommunikationskanäle benachrichtigt, wenn Probleme festgestellt werden.

Webfleet speichert die im Zusammenhang mit der Service-Plattform erstellten Zugriffsprotokolle für unsere Web- und Anwendungsserver für bis zu neunzig (90) Tage auf unseren sicheren Protokollservern. Dadurch können die Kunden die Nutzersitzungen bis zu neunzig (90) Tage lang einsehen. Die Dauer der Speicherung hängt von den jeweils geltenden Rechtsvorschriften ab.

Überwachung

Der Fokus des Sicherheitsüberwachungsprogramms von Webfleet liegt auf Informationen, die aus dem internen Netzwerkverkehr, den Aktionen der Mitarbeiter an den Systemen und dem externen Wissen über Schwachstellen gewonnen werden. An vielen Stellen unseres Netzwerks wird der interne Datenverkehr auf verdächtige Vorkommnisse untersucht, z. B. auf Datenverkehr, der auf Botnet-Verbindungen hinweisen könnte. Diese Analyse wird mit einer Kombination aus Open-Source- und kommerziellen Tools durchgeführt.

Unterstützt wird diese Analyse durch ein proprietäres Korrelationssystem, das auf der Webfleet-Technologie aufbaut. Die Netzwerkanalyse wird durch die Untersuchung von Systemprotokollen ergänzt, um ungewöhnliche Vorkommnisse festzustellen, z. B. unerwartete Aktivitäten in den Konten ehemaliger Mitarbeiter oder Versuche, auf Kundendaten zuzugreifen. Die Sicherheitstechniker von Webfleet suchen proaktiv nach Sicherheitsvorfällen, die die Infrastruktur des Unternehmens beeinträchtigen könnten. Dazu überprüfen sie eingehende Sicherheitsberichte und überwachen öffentliche Mailinglisten, Blogbeiträge und Web-Bulletin-Board-Systeme. Die automatisierte Netzwerkanalyse unterstützt das Team dabei, unbekannte Bedrohungen zu erkennen und an das Webfleet-Sicherheitspersonal weiterzuleiten. Die Netzwerkanalyse wird durch eine automatisierte Analyse der Systemprotokolle ergänzt.

Malware-Prävention

Malware stellt ein erhebliches Risiko für heutige IT-Umgebungen dar. Ein effektiver Malware-Angriff kann zu kompromittierten Konten, Datendiebstahl und möglicherweise zusätzlich zu unerwünschten Zugriffen auf ein Netzwerk führen. Webfleet nimmt diese Bedrohungen für seine Netzwerke und seine Kunden sehr ernst und setzt eine Vielzahl von Methoden zur Verhinderung, Erkennung und Beseitigung von Malware ein.

Webfleet verwendet beispielsweise Next-Generation Firewalls (NGFW) und Intrusion Prevention Systems (IPS), um Malware vorzubeugen und andere Antiviren-Scans zu unterstützen. Unsere Betriebsteams sind darin geschult, auf alle Sicherheitsvorfälle zu reagieren, die von unseren Systemen erkannt werden und ein Handeln erfordern. Wir investieren viel in diesen Bereich, um unsere operativen Risiken und das Risiko von Datenschutzverletzungen zu Lasten der Kundendaten zu verringern.

Alle Produktionssysteme der Service-Plattform, die vor internen und externen Zugriffen geschützt sind, verfügen über einen integrierten Virenschutz. Die Signaturen werden täglich aktualisiert und von den verschiedenen Anbietern bereitgestellt. Auf einigen Nicht-Windows-Servern ist aufgrund der hohen Leistungsanforderungen kein Virenschutz installiert. Diese Systeme wurden jedoch gemäß den best practices der Branche abgesichert und mit den Benchmarking-Tools des Center for Internet Security (CIS) und anderen zusätzlichen Kontrollmechanismen überprüft, die nicht an unternehmensfremde Akteure weitergegeben werden dürfen, aber dennoch einen umfassenden Schutz bieten.

Alle Windows-basierten Server und Workstations führen stündlich Prüfungen auf neue Signaturen und Updates durch, die sofort automatisch installiert werden.

10 SICHERE VERBINDUNGEN

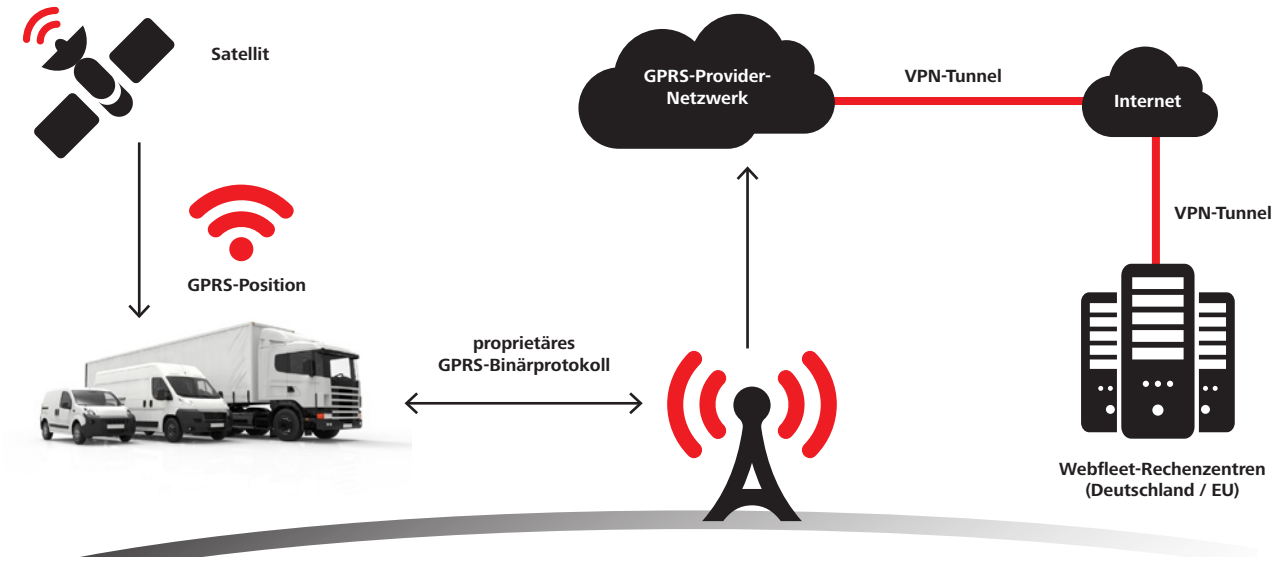
GPRS-Verbindungen

Die Webfleet-Hardware, LINK (außer LINK 105) und PRO sind über GPRS mit unserer Infrastruktur verbunden. Die Verbindungen zu den GSM-Providern beruhen auf VPN und bieten entweder eine 256- oder 128-Bit-Verschlüsselung. Die VPN-Verbindungen weisen die Vorteile der Multi-Homing-Konfiguration auf, die eine hohe Verfügbarkeit mit automatischem Failover unterstützt. Ein Beispiel ist der Ausfall des Uplinks.

Für die Messaging-Server, mit denen diese Einheiten verbunden sind, betreiben wir in jedem Rechenzentrum mehrere dedizierte Hochleistungsserver, die die volle Last bewältigen können, ohne dass unsere Kunden Performance-Einbußen bemerken. Alle Nachrichten und Daten werden über unsere Hardware-Load-Balancer-Cluster verteilt, um eine hohe Leistung und Verfügbarkeit zu gewährleisten.

Datenfluss von und zur Service-Plattform

Geolokalisierung der Flotte in Echtzeit:
Webfleet bietet für einige seiner Lösungspakete eine LINK-Ortungseinheit an, die in jedes Fahrzeug der Flotte eingebaut wird. Das Gerät nutzt die GPS-Satellitentechnologie, um seinen Standort im Durchschnitt alle 10 Sekunden zu bestimmen, und sendet dann einmal pro Minute die Koordinaten seines Standorts über GPRS an die sicheren Webfleet-Server in Deutschland, die diese Position wiederum mit den neuesten Karten für die Anzeige in Webfleet abgleichen.



Dadurch kann der Kunde alle seine Fahrzeuge auf einmal auf dem Bildschirm sehen und kann über die einfach zu bedienende Kartensteuerung oder die Maus ein einzelnes Fahrzeug auswählen. Um sich weitere Angaben zu dem ausgewählten Fahrzeug und zum Fahrzeugstandort anzeigen zu lassen, muss der Nutzer lediglich die Zoomstufe erhöhen.

Verarbeitung von Nachrichten

Der Kern der Nachrichtenverarbeitung besteht aus mehr als 20 High-End-Servern, die die Nachrichten von den JMS-Systemen abrufen, verarbeiten und die Daten in einem hochverfügbaren Enterprise Edition-Datenbanksystem speichern.

Auf jedem Messaging-Server ist ein lokal laufender Kartenserver für die umgekehrte Geokodierung zuständig, die den Längen- und Breitengrad in eine bestehende Adresse umwandelt und unseren Kunden die aktuellsten Webfleet-Kartendaten zur Verfügung stellt.

Die Messaging-Server (einschließlich der JMS-Server) umfassen mehr als 30 Hochleistungsserver in jedem Rechenzentrum und sind in der Lage, eine volle Last kontinuierlich zu verarbeiten, ohne dass es zu Verzögerungen bei der Verarbeitung oder zu Performance-Einbußen für unsere Kunden kommt.

Redundanter Uplink-Router (BGP4)

Redundanter Virtual Private Network (VPN) Router

Next Generation Firewall Cluster

Platform Messaging Loadbalancing Cluster

UI & Webfleet.connect API Loadbalancing Cluster

Firewall-Cluster

GPRS-Servers

Eingehende Schlange

Messaging-Balancer

Messaging-Dispatcher

Enterprise-Level-Datenbank

Internet-Konnektivität

Webfleet betreibt mehrere Breitband-Internet-Uplinks von verschiedenen Anbietern.

Die Internet-Uplinks für die Plattformdienste sind physisch von den Uplinks zum Internet für die Büronutzung (Webbrowsing, E-Mail usw.) getrennt, wodurch das Risiko von Abhängigkeiten bzw. negativen Auswirkungen auf Performance oder Sicherheit verringert wird.

Die redundanten Internet-Uplinks für die Service-Plattform sind als Multi-Homing-Lösung mit einem Provider-aggregierten Adressraum (AS) implementiert.

Der Vorteil einer solchen Konfiguration besteht darin, dass es mehrere Internet-Uplinks von verschiedenen Anbietern/ISPs gibt, die denselben IP-Adressbereich über alle bestehenden Uplinks verwenden/umleiten. Dies bietet zusätzliche Sicherheit und verringert die Risiken, die von physischen Problemen mit den ISP-Verbindungen, ISP-weiten Ausfällen oder nahezu allen Konfigurationsproblemen bei einem einzelnen ISP ausgehen. Außerdem ist dadurch auch das Risiko geringer, dass sich das Netzwerk als potenzieller Single Point of Failure erweist. Sollte ein Uplink ausfallen, erfolgt durch dynamisches Routing mit BGP4-Protokoll ein automatisches Failover auf einen der anderen Uplinks. Failbacks funktionieren ähnlich und sind ebenfalls vollständig automatisiert.

Lastausgleich

Webfleet betreibt mehrere Lastausgleichs-Cluster pro Rechenzentrum; dabei handelt es sich um eine Standardmethode zur Verteilung der Last auf mehrere Rechenressourcen. Darüber hinaus trennt das Setup die Lastausgleichsumgebungen von den kundenorientierten Systemen wie der Website, der Nutzeroberfläche und den APIs der Service-Plattform sowie von Systemen, die mit dem Messaging zusammenhängen, um maximale Performance und Verfügbarkeit zu gewährleisten und mögliche Abhängigkeiten zwischen den Systemen zu beseitigen.

Bei der von Webfleet eingesetzten Lastausgleichshardware handelte es sich um eine bewährte Lösung des Weltmarktführers für Lastausgleichssysteme.

Die Lösung bietet fortschrittliche Funktionen und Leistungen für den Lastausgleich, wie z. B.:

- **bis zu 10 Gbit/s L4/L7 Intelligenter Traffic-Durchsatz (pro Clusterknoten)**
- **mehr als 10 Millionen gleichzeitige Verbindungen bei 1 GB (pro Clusterknoten)**
- **maximale SSL von 9.000 TPS (2k-Schlüssel) für neue Verbindungen (pro Clusterknoten)**
- **Informationen zum Anwendungsstatus**
  - Statusprüfungen auf der L7-Anwendungsebene und automatische Deaktivierung aller Server im Pool, bei denen Probleme festgestellt wurden
- **Echtzeit-Fehlererkennung für ausgefallene Server mit detaillierten Ereignisinformationen zur Fehlerbehebung für IT-Administratoren**
- **schneller Zwischenspeicher**
  - Performance-Beschleunigung
- **erweiterte Hardware-Kompression**
  - bessere Performance und geringeres Transfervolumen
- **SSL-Hardware-Beschleunigung**

Die implementierte Architektur ermöglicht es Webfleet, die Betriebskapazität schnell zu erhöhen und zukünftige Ressourcenbeschränkungen durch eine Kombination aus erstklassiger Hardware, unserem Kapazitätsmanagementprogramm und unseren detaillierten Überwachungsmöglichkeiten frühzeitig zu verhindern, bevor unsere Kunden Performance-Probleme haben.

11 BESCHAFFUNG, ENTWICKLUNG UND WARTUNG VON SYSTEMEN

Es gehört zu den Grundsätzen von Webfleet, die sicherheitsbezogenen Eigenschaften und Auswirkungen von Anwendungen, Systemen und Diensten, die von Webfleet genutzt oder bereitgestellt werden, während des gesamten Projektlebenszyklus zu berücksichtigen. Die Sicherheitsrichtlinien von Webfleet sehen vor, dass unsere Teams und Mitarbeiter ausreichende Sicherheitsmaßnahmen in den von uns entwickelten oder erworbenen Anwendungen, Systemen und Diensten implementieren, und zwar in Übereinstimmung mit allen erkannten sicherheitsbezogenen Risiken und Bedenken. Unsere Richtlinie sieht vor, dass Webfleet ein Sicherheitsteam einsetzt, das die Aufgabe hat, sicherheitsbezogene Hinweise zu geben und Risikobewertungen zu erstellen. Webfleet trifft eine Vielzahl von Maßnahmen, um sicherzustellen, dass die für die Kunden bestimmten Softwareprodukte und Dienstleistungen in Sachen Softwaresicherheit den höchsten Branchenstandards entsprechen. In diesem Abschnitt wird das derzeitige Softwaresicherheitskonzept von Webfleet beschrieben; es wird künftig ggf. angepasst und weiterentwickelt.

Sichere Softwareentwicklung für die Service-Plattform

Im Rahmen seines Service-Management-Portfolios betreibt Webfleet ein Change-Management-Programm, das sich an den best practices von ITIL und ISO-20000 orientiert. Die entsprechenden Prozesse werden in der gesamten Entwicklungs- und Betriebslandschaft eingesetzt. Dadurch sorgen wir dafür, dass unsere Produkte so geplant, entworfen, getestet, genehmigt und implementiert werden, dass die Sicherheit gewährleistet ist. Außerdem ist dadurch sichergestellt, dass unsere gesamte interne Betriebshardware und -software sowie die Dokumentation im Zusammenhang mit dem Informationsmanagementsystem Gegenstand des Risikomanagements, der Versionskontrolle und des Änderungsmanagements ist und dass dafür getrennte Umgebungen vorgesehen sind.

Zur Umsetzung eines Secure Software Development Life Cycle (SDLC) hat Webfleet eine Methodik implementiert, die sich an den Leitlinien für sichere Codierung orientiert und die Vorteile vieler Standardmethoden der Branche vereint. Außerdem hat Webfleet ein Project Creation Framework (PCF) entwickelt, das die wichtigsten Elemente des SDLC sowie anderer Methoden wie des Wasserfall-Modells und der agilen Softwareentwicklung umfasst. Diese Methoden werden für die Entwicklung unserer Plattform und den zuverlässigen Betrieb der Software verwendet. Dabei liegt der Schwerpunkt darauf, durch Qualität, Integrität, Sicherheit und Wiederverwendbarkeit in Verbindung mit den Kundenanforderungen sowie angemessenen Markteinführungszeiten einen Wettbewerbsvorteil zu erlangen.

Bei den Releases achtet Webfleet stets auf die Trennung zwischen Feature-Releases und Bugfix-Releases. Alle Versionen werden von unserem dedizierten QA-Team auf Integrationsfähigkeit und Funktion getestet und zur Messung der Performance einem Belastungstest unterzogen.

Für unsere kundenorientierten Systeme setzen wir das erstklassige Lasttest-Tool Neoload ein, um eine höhere Last zu erzeugen, als wir sie in unserer Produktionsumgebung erleben. Dabei werden alle Layer detailliert überwacht, um etwaige Auswirkungen auf beteiligte Komponenten wie Webserver, J2EE-Server oder das Datenbank-Backend zu bewerten.

Engineering	Entwicklung abgeschlossen	Qualitäts-sicherung	Einführung
Analyse des Softwaredesigns	Statische Prüfung des Codes	Dynamische Analyse der Anwendung	Einführung und Stabilisierung der Anwendung

Bei Bugfix-Releases wird jeder Fehler auf der Grundlage der Auswirkungen auf den Kunden/das Unternehmen und der Dringlichkeit klassifiziert. Je nach Klassifizierung wird festgelegt, wie wir ein Release erstellen und testen, z. B. als Notfall-Änderung oder als Ergänzung zu einer ohnehin geplanten Bugfix-Version. Alle vom Kunden gemeldeten Fehler sowie intern gemeldete Fehler (z. B. im Rahmen der Qualitätssicherung) werden protokolliert und bearbeitet.

Für viele Komponenten veröffentlichen wir monatliche Releases, da wir durch die kontinuierliche Bereitstellung von Releases unseren Entwicklungszyklus steuern und die bestehenden Risiken begrenzen.

Dank unserer bewährten Infrastruktur, zu der auch Hardware-Load-Balancer gehören, können neue Versionen mit geringen oder ohne jegliche Auswirkungen auf die Kunden in unserer Produktionsumgebung bereitgestellt werden.

Sicherheitsberatung und -prüfung

Im Hinblick auf das Design, die Entwicklung, die Bereitstellung und den Betrieb von Anwendungen und Diensten erbringen die Produkt- und -Technikteams von Webfleet folgende Leistungen auf dem Gebiet der sicheren Kodierung:

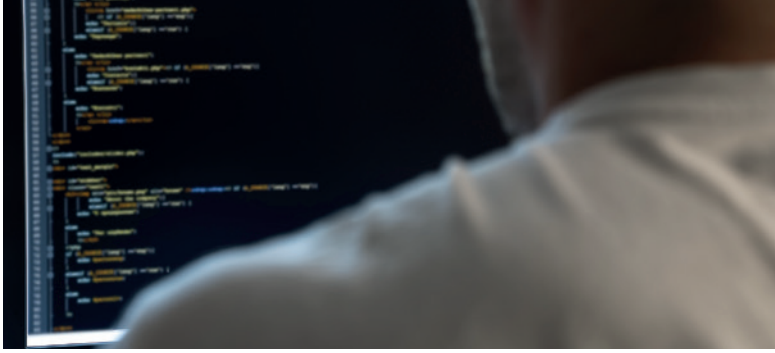
- **Sicherheitsdesign-Reviews: Bewertung der mit einem Projekt verbundenen Sicherheitsrisiken und Planung von geeigneten Risikominderungsmaßnahmen; Bewertung der Verhältnismäßigkeit und Wirksamkeit der Maßnahmen**
- **Durchführung von Sicherheitsüberprüfungen: Bewertung von Code-Artefakten auf Implementierungsebene, um deren Robustheit gegenüber relevanten Sicherheitsbedrohungen zu beurteilen**

Webfleet ist sich bewusst, dass viele Arten von Sicherheitsbedenken auf der Ebene des Produktdesigns auftreten und daher in der Designphase eines Produkts oder einer Dienstleistung berücksichtigt und behandelt werden müssen. Die Berücksichtigung solcher Überlegungen ist der Hauptzweck des Produktkontrollrahmens, mit dem wir die folgenden Ziele verfolgen:

- **Erstellung einer umfassenden Bewertung der mit dem Projekt verbundenen Sicherheitsrisiken auf der Grundlage einer Untersuchung der relevanten Bedrohungen**
- **Bereitstellung der von den Entscheidern eines Projekts benötigten Informationen, damit sie fundierte Risikomanagemententscheidungen treffen und im Rahmen der Projektziele sicherheitsbezogene Aspekte berücksichtigen können**
- **Orientierung bei der Auswahl und sachgerechten Umsetzung von geplanten Sicherheitsmaßnahmen, Authentifizierungsprotokollen oder Verschlüsselungslösungen**
- **Ausreichende Unterrichtung des Entwicklungsteams über relevante Schwachstellen, Angriffsmuster und geeignete Abhilfestrategien**

Wenn ein Projekt innovative Funktionen oder Technologien umfasst, hat das Informationssicherheitsteam die Aufgabe zu analysieren, welche Sicherheitsbedrohungen, potenziellen Angriffsmuster und technologie-spezifischen Schwachstellen vorhanden sind.

Gegebenenfalls schließt Webfleet Verträge mit externen Sicherheitsberatungsfirmen ab, um die im Unternehmen vorhandene Kompetenz im Bereich der Informationssicherheit zu ergänzen und eine unabhängige Überprüfung durch Dritte zur Validierung der internen Sicherheitsüberprüfungen zu erhalten.



Sicherheit im Zusammenhang mit dem Softwareentwicklungszyklus von Webfleet

Die Sicherheit steht im Mittelpunkt unseres Design- und Entwicklungsprozesses. Die technische Organisation von Webfleet sieht vor, dass die Produktentwicklungsteams einen bestimmten Softwareentwicklungsprozess einhalten, der Teil der historischen Sicherheitskultur von Webfleet ist und eine wichtige Grundlage für den Erfolgs unseres Softwaredesigns bildet. Die Sicherheitsüberprüfungsprozesse von Webfleet sind an die Anforderungen der Produktkontrolle angepasst. Der Erfolg dieses Prozesses beruht auf der konsequent qualitätsorientierten Entwicklungskultur von Webfleet und bestimmten Anforderungen, die das technische Management für die Projektentwicklungsprozesse definiert hat:

- **Von Fachleuten geprüfte Softwaredesigndokumentation**
- **Einhaltung von Kodierungsrichtlinien**
- **Peer Code Review**
- **Mehrschichtige Sicherheitstests**
- **Statische Codeprüfung nach OWASP Top 10 und SANS Top 25**

Die oben genannten Anforderungen verkörpern die Software-Engineering-Kultur von Webfleet, zu deren wichtigsten Zielen Softwarequalität, Robustheit und eine einfache Softwarepflege gehören. Während das Hauptziel darin besteht, die Erstellung von Software zu ermöglichen, die in allen Aspekten eine erstklassige Qualität aufweist, zeigt die Erfahrung des Webfleet-Engineering- und Sicherheitsteams auch, dass die Häufigkeit von Sicherheitsmängeln und Fehlern im Software-Design durch die Erfüllung dieser skalierbaren Anforderungen deutlich verringert wird:

- **Eine ausreichend detaillierte Dokumentation des Softwaredesigns bildet eine Voraussetzung für die Überprüfung des Sicherheitsdesigns, da die Dokumentation in frühen Projektphasen in der Regel das einzige Instrument ist, auf das sich die Sicherheitsbewertung stützen kann**
- **Viele, wenn nicht sogar die meisten, Arten von Sicherheitslücken auf Implementierungsebene unterscheiden sich grundsätzlich nicht von gewöhnlichen Funktionsmängeln mit geringem Risiko. Die meisten Sicherheitslücken auf Implementierungsebene werden durch relativ offensichtliche Versäumnisse der Entwickler verursacht**
- **Da Entwickler und Code-Prüfer in Bezug auf die Erkennung und Vermeidung von typischen Sicherheitslücken geschult sind, ist eine auf Peer-Reviews beruhende Entwicklungskultur, in der die Erstellung von qualitativ hochwertigem Code einen hohen Stellenwert einnimmt, ein sehr wichtiger und skalierbarer Faktor, um sicheren Code zu erhalten**

Die Software-Ingenieure von Webfleet arbeiten gemeinsam mit anderen Ingenieuren aus dem gesamten Unternehmen an der Entwicklung und Überprüfung von wiederverwendbaren Komponenten, mit denen Software-Projekte dabei unterstützt werden, bestimmte Arten von Schwachstellen zu vermeiden. Beispiele hierfür sind Datenbankzugriffsschichten, die so konzipiert sind, dass sie inhärent vor Einschleusungen in Abfragesprachen geschützt sind, oder HTML-Vorlagen-Frameworks mit eingebauten Schutzmechanismen gegen Cross-Site-Scripting-Schwachstellen.

Sicherheitsschulungen

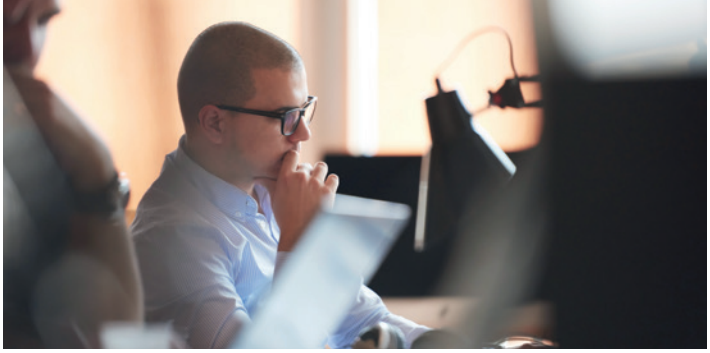
Das Sicherheitsteam von Webfleet hat erkannt, wie wichtig es ist, dass die technischen Mitarbeiter in Bezug auf sichere Programmierpraktiken geschult werden, und betreibt daher Programm zur Förderung und Schulung von Ingenieuren, das derzeit Folgende Maßnahmen umfasst:

- **Sicherheitsschulungen für alle neuen Mitarbeiter, insbesondere für die technischen und operativen Teams**
- **Erstellung und Pflege einer umfassenden Dokumentation über sichere Design- und Codierungsmethoden**
- **Gezielte, kontextgerechte Verweise auf Dokumentation und Schulungsmaterial. Tools für automatisierte Schwachstellentests verweisen beispielsweise auf Schulungen und Hintergrunddokumente zu bestimmten von den Testtools angezeigten Fehlern oder Fehlerklassen**
- **Technische Präsentationen zu sicherheitsrelevanten Themen**
- **Corporate Security Workshop – eine regelmäßig stattfindende unternehmensinterne Veranstaltung, bei der Software-Ingenieure aus verschiedenen Teilen des Unternehmens, die in sicherheitsrelevanten Bereichen arbeiten, vor unseren technischen Teams Vorträge zu sicherheitsbezogenen Themen halten**

Sicherheitstests und -überprüfungen auf Implementierungsebene

Webfleet setzt auf verschiedene Vorgehensweisen, um die Zahl der Sicherheitsschwachstellen auf Implementierungsebene in seinen Produkten und Diensten weiter zu verringern:

- **Sicherheitsüberprüfungen auf Implementierungsebene: Die Sicherheitsüberprüfungen auf Implementierungsebene werden von Mitgliedern des Webfleet-Sicherheitsteams durchgeführt (in der Regel in den späteren Phasen der Produktentwicklung), um festzustellen, ob ein Software-Artefakt tatsächlich so entwickelt wurde, dass es relevanten Sicherheitsbedrohungen standhält. Solche Überprüfungen bestehen in der Regel aus einer Neubewertung der bei den Sicherheitsüberprüfungen festgestellten Bedrohungen und Gegenmaßnahmen**
- **Automatisierte Prüfung auf Schwachstellen, die bestimmten relevanten Schwachstellenklassen zuzurechnen sind. Wir verwenden für diese Tests sowohl intern entwickelte als auch einige handelsübliche Tools**
- **Sicherheitsüberprüfungen, die von Software-Qualitätsingenieuren im Rahmen der allgemeinen Softwarequalitätsbewertung und -tests des Projekts durchgeführt werden**



Systemhärtung

Die von Grund auf intern gehärteten Produktionsserver von Webfleet basieren auf einer schlanken und gehärteten Version von Linux, die so angepasst wurde, dass sie nur die Komponenten enthält, die für den Betrieb der Service-Plattform erforderlich sind, bspw. die Dienste, die für die Verwaltung des Systems und die Bereitstellung des Nutzer-Traffic benötigt werden. Das System wurde für Webfleet entwickelt, um die Kontrolle über den gesamten Hardware- und Software-Stack zu behalten und eine sichere Anwendungsumgebung zu schaffen.

Die Produktionsserver von Webfleet basieren auf einem Standard-Linux-Betriebssystem (OS), das auf der Grundlage von Branchenstandards gehärtet wurde; die Sicherheitsfixes werden einheitlich in der gesamten Infrastruktur des Unternehmens eingesetzt. Durch den Einsatz eines robusten Änderungsmanagementsystems, das einen zentralen Mechanismus für die Registrierung, Genehmigung und Nachverfolgung von Änderungen umfasst, die sich auf alle Systeme auswirken, minimiert Webfleet die Risiken, die mit nicht autorisierten Änderungen an unserem standardmäßig installierten Betriebssystem verbunden sind.

Umgang mit Sicherheitslücken/Patches

Webfleet schützt alle seine Informationswerte durch eine umfassende Patch-Management-Politik für Sicherheits- und Viren-Patches. Sicherheitspatches für Linux, JDK oder andere Komponenten werden zunächst in einer Testumgebung installiert, bevor sie in die Produktionsumgebung eingespielt werden. Das bedeutet, dass die von unseren QA-Teams bereitgestellten Patches funktional und unter Last getestet werden, damit Sicherheit und Performance bewertet werden können.

Webfleet prüft regelmäßig alle Systeme auf Schwachstellen. Sobald Lücken entdeckt werden, wird der Vorfall an unser Patch-Management-Team gemeldet, und die entsprechenden Änderungsmanagementverfahren werden umgesetzt, um das Paket entweder für den nächsten geplanten Wartungszyklus einzuplanen oder durch Notfalländerungsverfahren Sicherheitsrisiken zu beheben.

Webfleet unterhält auch Kontakte zur Sicherheitsforschungs-Community, um sich über gemeldete Probleme und Common Vulnerabilities and Exposures (CVE) auf dem Laufenden zu halten.

Webfleet unterhält auch Kontakte zur Sicherheitsforschungs-Community, um sich über gemeldete Probleme und Common Vulnerabilities and Exposures (CVE) auf dem Laufenden zu halten.

Penetrationstests

Webfleet führt regelmäßig interne und externe Penetrationstests durch, um die Anforderungen der ISO 27001-Norm zu erfüllen und nachzuweisen, dass durch Änderungen der Norm keine unbekannten, nicht beantragten Sicherheitszugänge entstehen. Intern führen wir täglich Netzwerk-Scans und wöchentlich vollständige Schwachstellen-Scans durch, um zu gewährleisten, dass wir über jede Schwachstelle in Echtzeit informiert werden.

Ferner arbeiten wir mit externen Sicherheitsexperten zusammen, die regelmäßig externe Audits unserer Systeme durchführen, darunter auch Black- und Grey-Box-Tests für unsere nach außen gerichteten Systeme.

12 LIEFERANTENBEZIEHUNGEN

Sicherheit in den Lieferantenbeziehungen

Webfleet investiert viel in den Schutz seiner internen Informationssysteme, doch aufgrund unserer Risikoanalysen wissen wir, dass wir auch die Sicherheit an der Peripherie unseres Managementsystems im Auge behalten müssen. Daher führen wir bei unseren potenziellen Lieferanten eine Sicherheitsrisikoanalyse durch, um zu wissen, mit welchen Risiken wir an der Grenze zu unserem Schutzperimeter rechnen müssen.

Wenn möglich, wählen wir Anbieter aus, die ebenfalls nach ISO 27001 oder ähnlichen Managementsystemen zertifiziert sind oder bei denen festgestellt wurde, dass sie über ausreichende Sicherheitsmechanismen verfügen, so dass unsere Risiken vertretbar bleiben.

Außerdem überwachen wir unsere Lieferanten aktiv, so dass wir über alle Änderungen ihres Sicherheitsstatus informiert werden. Dadurch können wir jederzeit einschätzen, wie sich die von unseren Lieferanten ausgehenden Risiken ändern.

Dienstleistungen von Lieferanten

Neben der Durchführung von Hintergrundprüfungen und der Analyse von Risiken bei unseren Lieferanten prüfen wir regelmäßig die von unseren Lieferanten zu erbringenden Dienstleistungen, und zwar insbesondere im Hinblick auf die vereinbarten Sicherheitsvereinbarungen. Dadurch können wir beurteilen, ob die ausgewählten Kontrollmechanismen angemessen sind, um die Sicherheit von Informationswerten und Kundendaten zu gewährleisten.

13 MANAGEMENT VON VORFÄLLEN IM ZUSAMMENHANG MIT DER INFORMATIONSSICHERHEIT

Diese regelmäßigen Prüfungen sind auch Gegenstand der regelmäßigen ISO 27001-Zertifizierungsaudits. Dadurch wird sichergestellt, dass unsere Prüfungen den best practices und der von uns definierten Risikobereitschaft entsprechen.

Identifizieren, analysieren, korrigieren

Webfleet verfügt über einen Prozess zum Umgang mit Sicherheitsvorfällen, die die Vertraulichkeit, Integrität oder Verfügbarkeit unserer Systeme oder Daten ggf. beeinträchtigen. In diesem Prozess werden Handlungsabläufe sowie Verfahren zur Benachrichtigung, Eskalation, Schadensbegrenzung und Dokumentation festgelegt. Mitarbeiter in entscheidenden Positionen werden in forensischen Analysen und im Umgang mit Beweismaterial geschult (eigene Tools und Tools von Drittanbietern), um sich auf Vorfälle in Bezug auf die Informationssicherheit vorzubereiten. Für Schlüsselbereiche wie Systeme, in denen sensible Kundendaten gespeichert sind, werden Notfallpläne getestet. In diesen Tests wird eine Vielzahl von Szenarien berücksichtigt, darunter Bedrohungen von innen sowie Schwachstellen der Software.

Damit schnell wirkungsvolle Gegenmaßnahmen getroffen werden können, steht das Webfleet-Sicherheitsteam allen Mitarbeitern zur Verfügung. Wenn ein Informationssicherheitsvorfall eintritt, wird das Webfleet-Sicherheitsteam, den Vorfall zunächst dokumentieren und nach seiner Schwere priorisieren. Vorfälle, die direkte Auswirkungen auf die Kunden haben, werden mit höchster Priorität behandelt. Eine Person oder ein Team widmet sich der Behebung des Problems und zieht ggf. Produktexperten und Fachleute hinzu. Andere Aufgaben werden zurückgestellt, bis das Problem gelöst ist.

Die Webfleet-Sicherheitsingenieure führen bei Bedarf Post Incident Reviews (PIR) durch, um die Ursache für einzelne Vorfälle und Trends, die sich über mehrere Vorfälle im Laufe der Zeit erstrecken, zu ermitteln und neue Strategien zu entwickeln, mit denen das erneute Auftreten ähnlicher Vorfälle verhindert werden kann.

14 INFORMATIONSSICHERHEIT IM RAHMEN DES BETRIEBSKONTINUITÄTSMANAGEMENTS

Webfleet betreibt seine Service-Plattform und seine Dienstleistungen nach der ISO 27001-Norm, die einen Disaster-Recovery-Plan für verschiedene Fälle vorsieht. Wir führen regelmäßig Audits und Tests unserer Systeme durch, um sicherzustellen, dass alle Wiederherstellungsmaßnahmen erfolgreich und effizient sind, so dass wir unseren Kunden unsere Dienste möglichst schnell wieder zur Verfügung stellen können.

Aufgrund der Active/Active-Konfiguration unseres Rechenzentrums hat unser Risikomanagementteam die Wahrscheinlichkeit für einen massiven Ausfall, der beide Rechenzentren betrifft, als sehr gering eingestuft. Dennoch hat Webfleet Notfallpläne erstellt, um unabhängig von der Eintrittswahrscheinlichkeit auch auf einen solchen Ausfall vorbereitet zu sein.

Um Serviceunterbrechungen aufgrund von Hardwareausfällen, Naturkatastrophen oder anderen Katastrophen möglichst zu verhindern, hat Webfleet in allen Rechenzentren ein Disaster-Recovery-Programm eingeführt. Das Programm umfasst mehrere Komponenten zur Minderung des Ausfallrisikos, darunter:

- **Datenreplikation und -sicherung: Damit die Systeme auch im Katastrophenfall verfügbar sind, liegen die Plattformdaten innerhalb eines Rechenzentrums auf mehreren Systemen vor und werden zudem auf ein zweites Rechenzentrum repliziert**
- **Webfleet betreibt Rechenzentren an verschiedenen Standorten, die darauf ausgelegt sind, die Betriebskontinuität im Falle einer Katastrophe oder eines anderen Vorfalls in einer einzelnen Region aufrechtzuerhalten. Hochgeschwindigkeitsverbindungen zwischen den Rechenzentren sorgen für ein schnelles Failover. Das Management der Rechenzentren ist ebenfalls verteilt, um eine standortunabhängige Abdeckung sowie die Systemadministration rund um die Uhr zu gewährleisten**

Neben der Redundanz von Daten und Rechenzentren in unterschiedlichen Regionen hat Webfleet auch einen Geschäftskontinuitäts- und Informationssicherheitsplan für seine Technologiezentrale in Leipzig. In diesem Plan werden Vorkehrungen für größere Katastrophen getroffen, bspw. eine Naturkatastrophe oder eine Krise im Bereich der öffentlichen Gesundheit. Im Rahmen des Plans wird davon ausgegangen, dass Menschen und Dienstleistungen ggf. für bis zu dreißig (30) Tage nicht verfügbar sind. Mit diesem Plan wollen wir den Weiterbetrieb unserer Dienste für unsere Kunden auch im Krisenfall ermöglichen. Unser Notfallplan wird regelmäßig getestet.

Hohe Verfügbarkeit

Die Webfleet Telematics Service Platform basiert auf einer verteilten und skalierbaren Architektur mit mehreren Redundanzen, Lastausgleich und Clustern zur Unterstützung des Kapazitätsmanagements und bietet damit maximale Skalierbarkeit und eine sehr hohe Verfügbarkeit.

Die Produktionsumgebung verfügt derzeit über die folgenden Kapazitäten:

- **Mehr als 100 moderne Multicore-Server mit (Bruttokapazität) einem lokalen Festplattenspeicher von**
  - > 50 Terabyte
  - > 140 Mehrkern-CPUs
  - > 4 Terabyte RAM
- **6 Fibre-Channel-Netzwerkspeicher (SAN)**
  - ca. 200 Terabyte Bruttokapazität

Zusätzlich zur Produktionsumgebung betreibt Webfleet vollständig getrennte und redundante Entwicklungs-, Phasen- und Vorproduktionsumgebungen. Dadurch steht uns eine optimale Konfiguration für die Entwicklung und die Tests unserer erstklassigen Plattformlösung zur Verfügung und wir können mit etwa 50 weiteren Servern für diese Umgebungen ein Höchstmaß an Qualität und Leistung garantieren.

Jede Version wird von einem eigenen Team von Qualitätssicherungsexperten funktional getestet. Zu den Test zählen unter anderem statische Codeanalysen, Regressionstests sowie Lasttests, die unter Verwendung modernster Simulationssoftware durchgeführt werden. Dank dieser Tests lässt sich vorhersagen, ob und inwieweit Workloads von denjenigen abweichen, die derzeit in der Produktionsumgebung auftreten. Damit ist sichergestellt, dass unsere Service-Plattform unter allen Belastungen leistungsfähig und stabil bleibt und dass unser Code auf bekannte Schwachstellen getestet und durch unsere Change-Management-Prozesse genehmigt wird, bevor er im Produktionsbetrieb eingesetzt wird.

Server-Datenschutz

Alle Server werden mit aktivierter Festplattenspiegelung unter Verwendung von RAID-1, RAID-5 oder RAID-10 betrieben, um bei einem Ausfall einer Festplatte Datenverluste zu verhindern. Alle wichtigen Daten, insbesondere Protokoll- und Konfigurationsdateien, werden täglich auf unserem sicheren Netzwerkspeicher und zusätzlich mit Bandsicherungssystemen gesichert. Für die Netzwerkspeicherung werden die Dateien für neunzig (90) Tage auf Band gespeichert. Dabei ergeben sich keine Einschränkungen in Bezug auf die monatlichen Backups, die gemäß unseren Datensicherungsrichtlinien durchgeführt werden.

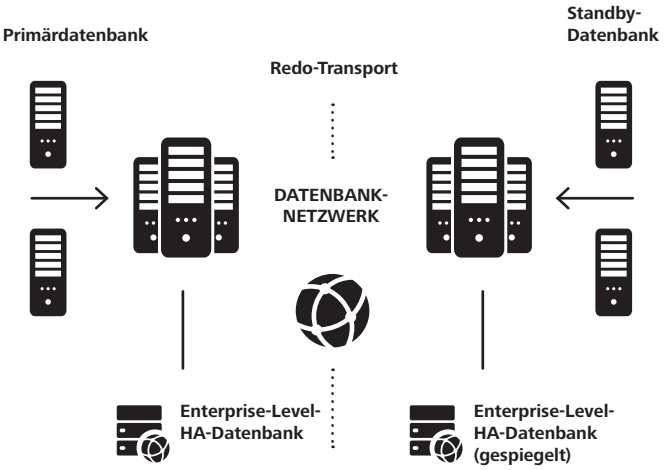
Datenbank-Backend-Datensicherung

Webfleet betreibt ein hochverfügbares Datenbank-Backend auf Enterprise-Niveau, das auf hochleistungsfähiger Server- und SAN-Hardware läuft.

Die Konfiguration wird in jedem unserer Rechenzentren für unsere Datenbankserver, redundanten SAN-Switches und SAN-Speicher mit unserer Backup-Lösung auf Unternehmensebene implementiert, so dass unsere Kunden von maximaler Verfügbarkeit profitieren.

Die Plattformdaten sowie alle vertraulichen Daten werden in einer Enterprise-Level-Datenbank gespeichert, die in Sachen Performance, Sicherheit, Zuverlässigkeit und Skalierbarkeit branchenführend ist. Darüber hinaus ist der gesamte Datenbankspeicher in unserem Storage Area Network (SAN) mit RAID-Schutz gesichert.

Enterprise-Level-Datenbanksicherung



Zur Gewährleistung einer hohen Verfügbarkeit unseres Datenbank-Backends betreiben wir in unserem zweiten Rechenzentrum eine Managed Standby-Datenbank. Dadurch kommt es selbst bei einer geplanten Wartung unseres Datenbank-Backends oder der Rechenzentrumsinfrastruktur von Webfleet nur zu minimalen Beeinträchtigungen. Alle Transaktionen aus unserer Master-Datenbank werden sofort synchronisiert und in unsere Managed Standby-Datenbank übertragen. Dank dieser Konfiguration können wir ein schnelles (automatisches und/oder erzwungenes) Failover durchführen, das automatisch oder erzwungen auf das Managed Standby-System übertragen wird – mit minimalen Auswirkungen auf den Kunden.

Das Managed Standby-System in unserem zweiten Rechenzentrum läuft auf einem ähnlichen dedizierten Server und SAN-Speicher wie im Primärrechenzentrum. Beide Standorten weisen identische Sicherheitsmechanismen auf.

Jeden Tag wird ein vollständiges Backup der Datenbank einschließlich der Transaktionsprotokolle auf dem Netzwerkspeicher (NAS) und redundant auf Band (B2D2T) durchgeführt.

Dadurch ist eine punktgenaue Wiederherstellung der Daten möglich. Mit dieser Wiederherstellungskonfiguration führen wir jeden Monat einen Wiederherstellungstest durch, um die Integrität der Daten zu gewährleisten. Auf unserem NAS archivieren wir die Sicherungen der letzten sieben (7) Tage, während die Bandsicherungen entsprechend unserer Sicherungsrichtlinie über einen längeren Zeitraum archiviert werden.

Standortferne sichere Aufbewahrung von Sicherungsbändern

Die Sicherungsbänder werden in einem 40 km von unserem Rechenzentrum in Deutschland gelegenen Hochsicherheitslager verwahrt. Der Betreiber des Lagers holt die Sicherungsbänder regelmäßig ab und bringt sie zur Wiederherstellung des Systems auch wieder ins Rechenzentrum.

Datenschutz und Datensicherung

Webfleet trägt Sorge dafür, dass das Risiko eines Verlusts oder einer Beschädigung von Kundendaten durch technische Probleme oder menschliches Versagen minimiert wird. Webfleet setzt modernste Hard- und Software sowie eine Reihe von Kontrollmechanismen ein, die größtmöglichen Schutz für Kundendaten und Informationswerte bieten. Innerhalb der Architektur der Service-Plattform wurden verschiedene Kontrollmechanismen implementiert, um unsere Informationssicherheitsstrategie und die Compliance zu unterstützen.

Beispiele:

- **Zweistufige Überprüfung**
- **Vom Kunden festgelegte Passwortlänge und -stärke**
- **Sichere Browsing-Verbindungen (HTTPS)**

15 COMPLIANCE UND DATENSCHUTZ

Rechtmäßiger Zugang zu Informationen

Webfleet hält sich bei der Beantwortung von Anfragen Dritter nach Nutzerinformationen an die üblichen rechtlichen Verfahren. Informationen können von Dritten nur durch rechtliche Verfahren wie Durchsuchungsbefehle, Gerichtsbeschlüsse, Vorladungen, durch eine gesetzliche Ausnahmeregelung oder durch die Zustimmung des Nutzers erlangt werden. Nach Eingang eines Offenlegungsverlangens prüft die Rechtsabteilung von Webfleet den Antrag darauf, ob er mit geltendem Recht in Einklang steht. Alle Daten wie Telemetrie- oder Standortdaten unterliegen Datenschutzvorschriften, und wir setzen das Verbot der Weitergabe von Daten an Dritten konsequent durch, sofern die Weitergabe nicht gesetzlich vorgeschrieben ist. Alle Daten werden innerhalb der Europäischen Union unter Beachtung der datenschutzrechtlichen Vorschriften gespeichert und verarbeitet, so dass die Daten unserer internationalen Kunden bestmöglich geschützt sind.

Datenschutz

Webfleet verpflichtet sich, die Daten seiner Kunden und alle weiteren Informationswerte unter Einsatz der derzeit leistungsfähigsten Sicherheitsmechanismen zu schützen. Damit wir unsere Tracking- und Tracing-Dienste anbieten können, müssen wir zahlreiche vertrauliche Daten auf der Grundlage von strengen Datenschutzvorschriften für jede der verschiedenen Erfassungsmethoden erheben und aufbewahren. Diese Methoden werden von unserem Datenschutzbeauftragten und im Rahmen von Zertifizierungsaudits auch von einer international akkreditierten Prüfstelle regelmäßig überprüft. Um die Anforderungen unserer Kunden an den Datenschutz und die entsprechenden Rechtsvorschriften wie die DSGVO der EU und andere relevante Datenschutzvorschriften sowie unsere internen Richtlinien mindestens einzuhalten, sieht Webfleet verschiedene physische, elektronische und verfahrensbezogene Kontrollmechanismen vor:

Maximale Sicherheit und Integrität

- **Ihre Daten sind bei Webfleet in sicheren Händen. Wir setzen auf bewährte Sicherheitsvorkehrungen, um Ihre Daten zu schützen, so dass Sie darauf vertrauen können, dass Ihre Daten bei uns sicher sind. Alle vertraulichen Daten werden in unseren sicheren Rechenzentren in Deutschland gespeichert. Dadurch ist größtmöglicher Schutz gewährleistet.**
- **Next-Generation Firewalls (NGFW) und andere Sicherheitsvorkehrungen zum Schutz vor externen und internen Datenverletzungen einschließlich Überwachung**
- **Eindeutige Nutzeranmeldedaten für die Plattform oder Kundenlogins, die mit der höchsten Verschlüsselungsstufe in unseren sicheren Datenzentren gespeichert werden**
- **Extended Validation SSL-Verschlüsselung nach höchstem Standard für die Datenübertragung und digitale Zertifikate zur Authentifizierung der Nutzer bei Transaktionen mit Webfleet**
- **Regelmäßige interne und externe Audits unserer Informationsmanagementsysteme, Rechenzentren und unserer Datenschutzverfahren**
- **Der Zugriff der Mitarbeiter auf personenbezogene Daten muss im Rahmen unserer Änderungsmanagementprozesse förmlich genehmigt werden. Zur Verarbeitung von Daten befugte Mitarbeiter unterliegen einer Mitarbeitervereinbarung, die mit den Anforderungen der DSGVO (EU) und den einschlägigen Datenschutzvorschriften in Einklang steht**

Schutz der Privatsphäre der Fahrer

1. **Sichere Daten**
   Der Zugang zu Webfleet ist nur mit einem registrierten Konto, dem Nutzernamen und dem zugehörigen Passwort möglich

2. **Sie entscheiden, wer was sieht**
   Mit Webfleet können Sie die Informationen, auf die jeder Nutzer Zugriff hat, nach dem Grundsatz der Erforderlichkeit einschränken.

3. **Fahrer haben Kontrolle über ihre Privatsphäre**
   Sobald sie außer Dienst sind, können die Fahrer auf ihren Webfleet-Geräten in den privaten Modus wechseln, damit der Standort des Fahrzeugs nicht verfolgt werden kann.

4. **Bei uns stehen Ihre Fahrer an erster Stelle, genau wie Sie**
   Alle unsere Lösungen sind auf den Fahrer ausgerichtet, so dass Sie Ihren Fahrern versichern können, dass sie die ersten sind, die von Ihrer Investition in Webfleet profitieren.

Die Plattformumgebungen sind vollständig von anderen Systemen oder Umgebungen, wie z. B. den Büro- oder Entwicklungsumgebungen, getrennt, und der Zugang zu den Servern des Produktionssystems ist streng auf die IT-Administratoren von Webfleet beschränkt und durch mehrere Firewall-Ebenen mit unterschiedlichen Anbietern und/oder Plattformen geschützt. Jeder Zugriff wird sicher protokolliert und zur Unterstützung forensischer Untersuchungen archiviert.

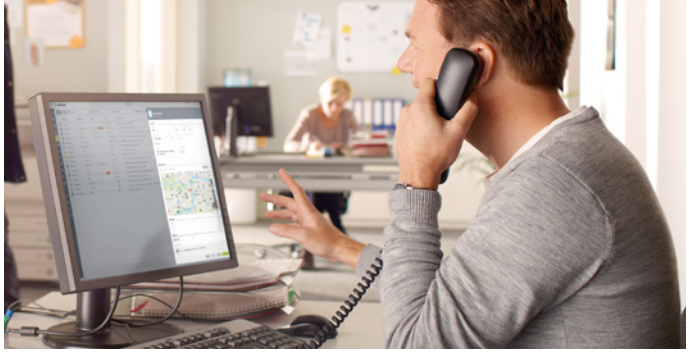
Löschung von Daten

Wenn ein Webfleet-Nutzer oder -Administrator Informationen innerhalb seines Kontos löscht, werden die betreffenden Daten entfernt und sind nicht mehr über die Webfleet-Oberfläche des Nutzers zugänglich. Die Daten werden dann dereferenziert und im Laufe der Zeit im Webfleet-Backend mit anderen Kundendaten überschrieben. Kein Kunde kann Daten anderer Kunden abrufen, wenn der zuvor zugewiesene Speicherplatz dereferenziert wird und unser Datenschutzbeauftragter festgestellt hat, dass dies kein Risiko für unsere Kunden darstellt.

Darüber hinaus gehört der Datenschutz zur Einhaltung der ISO 27001-Norm.

Dauer der Datenspeicherung

Webfleet uses the following schedule for its data Webfleet sieht folgende Zeiträume für die Datenspeicherung vor. Es handelt sich dabei um wichtige Informationen, an denen die meisten Betriebsräte oder Datenschutzbeauftragten im Zusammenhang mit der Service-Plattform interessiert sein werden.



Webfleet Telematics Service Platform
Die letzten neunzig (90) Tage: alle detaillierten Daten, einschließlich der exakten Positionsdaten

Webfleet Dashboard & Reporting
Aktuelles Jahr plus die zwei (2) vorangegangenen Kalenderjahre: Logbuch, Dashboard und Reporting

Webfleet.connect API
Die letzten neunzig (90) Tage: alle detaillierten Daten, einschließlich der exakten Positionsdaten

Webfleet.connect – API – Message Queue Service
Die letzten zwei (2) Tage: bestätigte Nachrichten: die letzten 14 Tage: nicht bestätigte Nachrichten. Die Daten werden nur gespeichert, wenn der Kunde ein Abonnement für diesen Dienst abgeschlossen hat.

Webfleet Mobile
Die letzten neunzig (90) Tage*: alle detaillierten Daten, einschließlich der exakten Positionsdaten

** Die Aufbewahrungszeiten hängen von den im jeweiligen Land geltenden Rechtsvorschriften ab.*

Digitales Vertrauen/ Datenschutzbeauftragter

Die Webfleet-Technologie erfüllt uneingeschränkt die Anforderungen der Datenschutzgrundverordnung der EU sowie der Datenschutzvorschriften anderer Länder. Unser zertifizierter Datenschutzbeauftragter widmet sich den Themen digitales Vertrauen und Datenschutz in Vollzeit, überwacht die Einhaltung der Datenschutzvorschriften und berät das Unternehmen. Dabei wird er vom Digital Trust Management Team unterstützt.

Kontaktinformationen

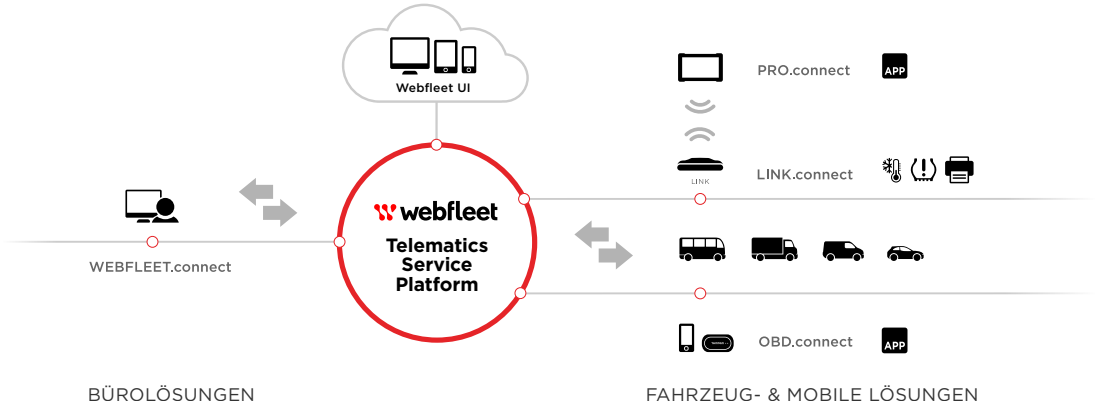
Für weitere Informationen über digitales Vertrauen, Informationssicherheit und Datenschutz wenden Sie sich bitte an:
digitaltrust@webfleet.com

Alternativ können Sie auch schreiben an:

Bridgestone Mobility Solutions B.V.
Legal Dept.
Beethovenstraat 503, 1083 HK Amsterdam, Niederlande

16 SICHERHEIT DER PLATTFORM UND COMPLIANCE

Zusätzlich zu den zuvor beschriebenen Sicherheitsmechanismen, die Webfleet zum Schutz der Sicherheit und der Privatsphäre der Kundendaten eingerichtet hat, bietet die Webfleet Telematics Service Platform zusätzliche Sicherheitsoptionen, die von den Administratoren des Kunden genutzt werden können. Wir arbeiten ständig daran, unseren Kunden weitere Möglichkeiten für die Steuerung ihrer Sicherheitskontrollanforderungen zu bieten.



Webschnittstelle (UI) und Plattform-APIs

Das Webfleet-Flottenmanagement lässt sich nahtlos in Ihre aktuelle Software und Anwendungen integrieren, so dass Sie eine umfassende und vollständig vernetzte Lösung für das Flotten- und Personalmanagement erhalten. Das bedeutet, dass Sie über Ihre bestehenden Systeme auf alle Daten zugreifen können, von mobilen Arbeitskräften über Verkehrs- und Fahrzeuginformationen bis hin zu Daten von mobilen Endgeräten. Dadurch können sie schneller und effizienter arbeiten. Wir verfügen über ein breites Netzwerk von zuverlässigen und vertrauenswürdigen Software- und Hardware-Partnern, die das Webfleet-Flottenmanagement in ihre Anwendungen integriert haben. Mit Hilfe von Webfleet und unseren Partnern haben Sie folgende Möglichkeiten:

- **Zugriff auf Dutzende Partner-Apps**
- **Schnelle und einfache Implementierung der Lösung**
- **Erstklassige API Webfleet.connect**

Mit dem Webfleet-Flottenmanagement können Sie auf das branchenweit umfangreichste Portfolio an integrierten Anwendungen zurückgreifen. Das heißt, Sie müssen Ihre Arbeitsweise nicht ändern, sondern nur verbessern.

Entdecken Sie unser App Center und finden Sie heraus, wie Sie das Webfleet-Flottenmanagement in Ihre aktuellen Lösungen integrieren können, – oder erfahren Sie mehr darüber, wie die Integration funktioniert.

Webfleet betreibt für die UI und die APIs mehrere dedizierte und leistungsstarke Server. Die verschiedenen Anwendungen befinden aus Performance- und Sicherheitsgründen in verschiedenen Zonen auf dem Server.

Die Server-Ressourcen in jedem Rechenzentrum können die volle Lastkapazität ohne spürbare Performance-Einbußen für unsere Kunden bewältigen. Alle Anfragen werden über unsere Hardware-Loadbalancer-Cluster ausgeglichen.

Webfleet Mobile

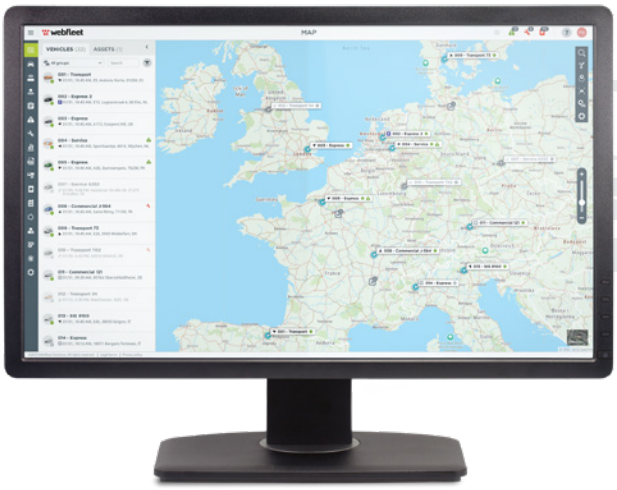
Darüber hinaus wurden die Möglichkeiten zur Anbindung an Webfleet erweitert, so dass Sie sofortigen Zugriff auf die Informationen haben, die Sie benötigen. Dadurch haben sie ihren gesamten Betrieb stets im Blick, ganz gleich ob von unterwegs oder vom Büro aus.

Webfleet Mobile bietet dasselbe hohe Maß an Sicherheit in einem flexiblen Paket. Damit:

- **verwalten sie ihre Prozesse von unterwegs aus**
- **bieten einen besseren Service**
- **behalten die Kontrolle**

Webfleet Mobile ist sowohl im Google Play Store als auch im Apple App Store erhältlich.

Weltweit führender Anbieter von Flottenmanagement-Dienstleistungen: Die meisten aktiven Abonnements in Europa.



- **ANWENDERFREUNDLICHE**
- **ZUVERLÄSSUG**
- **SCHNELL AMORTISIERT**
- **ZUKUNFTSSICHER**

Entscheiden Sie sich für Integrität. Schutz Sie die Umwelt

Zu guter Letzt möchten wir Sie daran erinnern, dass nicht nur der Schutz von Informationswerten für Webfleet eine Priorität ist. Vielmehr gibt Webfleet Ihnen die Mittel an die Hand, mit denen Sie die Daten Ihrer Mitarbeiter, die Umwelt und die Welt insgesamt schützen können.

Kann mein Unternehmen durch Assoziierung eine Zertifizierung nach ISO 27001 erlangen?

Die ISO 27001 deckt einen vereinbarten und genehmigten Geltungsbereich ab, der während des Zertifizierungsprozesses erreicht und überprüft wurde. Wenn Sie oder Ihr Unternehmen eine Zertifizierung anstreben, unterstützt Webfleet Sie als zertifizierter Anbieter dabei, das Risiko zu verringern, und kann Ihnen helfen, die Zertifizierung zu erhalten.

Die ISO 27001 deckt einen vereinbarten und genehmigten Geltungsbereich ab, der während des Zertifizierungsprozesses erreicht und überprüft wurde. Wenn Sie oder Ihr Unternehmen eine Zertifizierung anstreben, unterstützt Webfleet Sie als zertifizierter Anbieter dabei, das Risiko zu verringern, und kann Ihnen helfen, die Zertifizierung zu erhalten.

Wenn Sie bereits zertifiziert sind, können wir als starker Partner mit den bei Ihnen vorhandenen Informationsmanagementsystemen zusammenarbeiten und Ihr Betriebsrisiko weiter verringern.

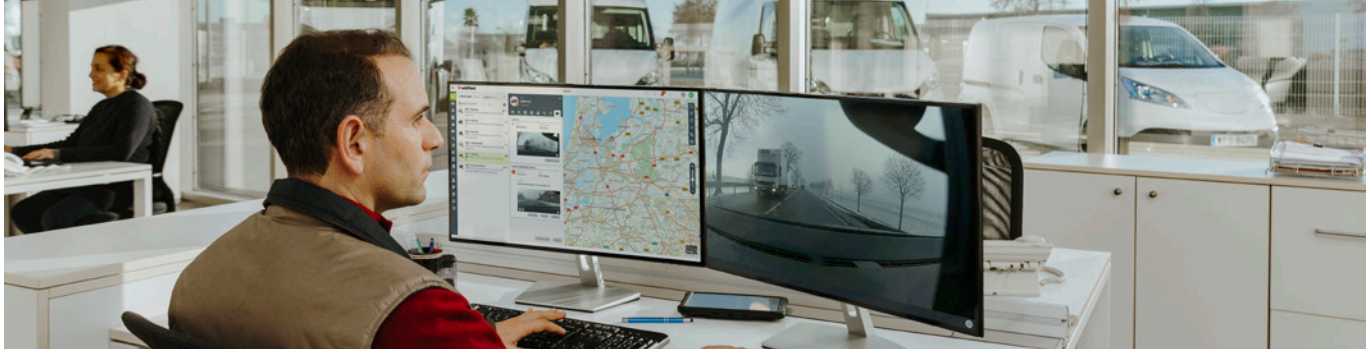
17 FAZIT

Webfleet ist entschlossen, größtmögliche Informationssicherheit für seine Computersysteme, Rechenzentren, Mitarbeiter und Kundendaten zu gewährleisten. In diesem Whitepaper wurden einige der wichtigsten Merkmale unserer Sicherheitsarchitektur behandelt. Auf einige Sicherheitsvorkehrungen sind wir bewusst nicht eingegangen, weil sie nicht bekannt werden sollen, denn dies trägt dazu bei, dass wir ein Höchstmaß an Sicherheit erreichen.

Diese Sicherheitsmaßnahmen haben jedoch weder negative Auswirkungen auf den Schutz der Daten unserer Kunden, noch verstoßen sie gegen Rechtsvorschriften innerhalb der Europäischen Union. Unsere Strategie spiegelt sich in der gesamten Organisation wider, und unsere Webfleet Telematics Service Platform bietet Mechanismen, um alle Systemebenen gezielt zu steuern, von der Datenspeicherung, über den Datenzugang bis hin zur Datenübermittlung.

Wir investieren täglich in das Vertrauen unserer Kunden. Sie können darauf vertrauen, dass wir die Privatsphäre unserer Kunden achten und die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Daten professionell schützen.

Webfleet
www.webfleet.com



18 PLATTFORM SERVICE LEVEL

Verfügbarkeit

Webfleet bietet eine vom Kunden beobachtbare durchschnittliche Verfügbarkeit von mindestens 99,95 % pro Monat.

Die Nichtverfügbarkeit im Sinne dieses Dokuments beginnt mit dem Zeitpunkt der Benachrichtigung von Webfleet durch den Kunden und endet mit dem Zeitpunkt, zu dem

- **Webfleet wieder verfügbar ist, oder**
- **Webfleet sinnvolle Abhilfe geschaffen hat**

Steht das System aufgrund von geplanten Wartungsarbeiten, die wie unten beschrieben angekündigt wurden, nicht zur Verfügung, so wird dieser geplante Ausfall bei der Ermittlung der Verfügbarkeitsquote nicht berücksichtigt.

Ausnahmen

Verfügbarkeits-, Reaktions- und Wiederherstellungszeiten gelten nur für Dienste und Komponenten, die direkt von Webfleet gesteuert werden können. Daher gelten die folgenden Ausnahmen:

- **Störungen der Telekommunikations- oder Netzwerkverbindungen (insbesondere Peering-Probleme beim Internet-Backbone)**
- **Denial-of-Service-Angriffe (DoS) aus dem Internet**
- **Hacking-Versuche oder Angriffe auf die Infrastruktur von Webfleet**
- **Höhere Gewalt**
- **Änderungen der geltenden Rechtsvorschriften**

Parameter

Gemäß der nachstehenden Tabelle, in der die Service-Level-Parameter definiert sind, werden die bei Webfleet eingehenden Nichtverfügbarkeitsmeldungen innerhalb der maximalen Reaktionszeit beantwortet oder bestätigt.

Planmäßige Wartung

- **wird auf dem Webfleet-Anmeldebildschirm angekündigt**
- **Max. 4h Ausfallzeit pro Wartungsmaßnahme**
- **Max. 8h Ausfallzeit pro Monat**
- **Benachrichtigung mindestens 5 Arbeitstage vor der geplanten Wartung**
- **Durchführung außerhalb der Geschäftszeiten (an Werktagen zwischen 22:00 und 06:00 Uhr MESZ sowie an Wochenenden und Feiertagen)**

Nichtverfügbarkeit des Dienstes

Nichtverfügbarkeit von Komponenten der Service-Plattform (Kommunikation und Messaging, Datenbank-, Anwendungsserver oder andere Module, die von Webfleet entwickelt wurden bzw. von Webfleet eingesetzt werden).

Nichtverfügbarkeit der Infrastruktur

Nichtverfügbarkeit der lokalen Netzwerkinfrastruktur, der Internetverbindung, von Firewalls, Gateways, Servern oder anderer kritischer Hardware und Ausrüstung.

SLA	GMT	Reaktionszeit	Reparaturzeit
Nichtverfügbarkeit des Dienstes	Montag bis Freitag 08:00 bis 17:00 Uhr	30 Minuten	4 Stunden
Nichtverfügbarkeit der Infrastruktur	Montag bis Freitag 08:00 bis 17:00 Uhr	30 Minuten	12 Stunden