

mms

ns.wow

Information Security



Informationssicherheit / Information Security

Document Version 3.1

March 2024

mms solutions ag
Dorfstrasse 29
CH-8037 Zurich
T +41 44 446 83 30

mms solutions gmbh
TechQuartier, Platz der Einheit 2
DE-60327 Frankfurt a. M.
T +49 69 247 43 62 00

Office an register court
Frankfurt a. M.
HRB 107996
Managing director: Rolf Traber

A member of
Neidhart + Schön Group
mmssolutions.io



Übersicht / Overview

Über ns.wow / About ns.wow	4
Betriebskonzept / Operational concept	6
Rechenzentren vor Go-Live / Data centers before Go-Live	8
1 Physische Sicherheit / 1 Physical security	8
2 Zertifikate / 2 Certificates	9
3 Connection / 3 Connection	10
4 Architektur / 4 Architecture	11
5 Netzwerk- und Systemsicherheit / 5 Network and system security	12
6 Applikationssicherheit / 6 Application security	16
7 Organisation / 7 Organization	17
8 Überwachung / 8 Monitoring	18
Rechenzentren nach Go-Live / Datacenters after go-live	19
1 Systemübersicht / 1 System overview	19
2 Backup / 2 Backup	22
3 Überwachung / 3 Monitoring	22
4 Organisation / 4 Organization	22

Sicherheit auf Enterprise-Level

Mit der Nutzung von ns.wow, den damit zusammenhängenden IT-Dienstleistungen und Software-Services vertrauen Unternehmen global ihre noch nicht veröffentlichten, streng vertraulichen Jahresabschlüsse und Geschäftsberichte der mms solutions (im Folgenden «mms» genannt) an.

Über ns.wow

ns.wow ist das moderne Tool für das Publizieren im Web. Selbstverständlich «fully responsive» auf allen digitalen Kanälen. Für autonomes und individuelles digitales Storytelling. Gearbeitet wird nach dem «Online first»-Prinzip, das heisst, Inhalte werden direkt im Webbrowser erfasst und in erster Priorität auf einer Website publiziert.

Einsatzzwecke

ns.wow eignet sich vor allem für die Erstellung und Veröffentlichung von redaktionellen Beiträgen und Storys im Web. Klassische Produkte sind z.B. Online-Geschäftsberichte und Nachhaltigkeitsberichte, Online-Magazine, Blogs, Microsites oder Newsportale. Auch Corporate Websites können mit ns.wow umgesetzt werden.

Funktionsweise

Das Funktionsprinzip ist ähnlich wie bei einem Web-Content-Management-System. Struktur und Form werden strikt voneinander getrennt und ermöglichen die Verwaltung/Aktualisierung einer Website ohne Programmierkenntnisse. Im Gegensatz zu einem herkömmlichen Web-Content-Management-System werden Inhalte aber nicht in Form von starren Templates erfasst, sondern anhand flexibler HTML-Komponenten per Drag & Drop zusammengestellt und als Artikel publiziert.

Enterprise-level security

By using ns.wow, the related IT services and software services, companies globally entrust their none-disclosed, highly confidential financial statements and annual reports to mms solutions (hereinafter referred to as "mms")

About ns.wow

ns.wow is the modern tool for publishing to the web. Of course, "fully responsive" on all digital channels. For autonomous and individual digital storytelling. Work is carried out according to the "online first" principle, that is, content is captured directly in the web browser and published on a website primarily.

Purpose

ns.wow is particularly suitable for the creation and publication of editorial articles and stories on the web. Classic products are e.g. online business reports and sustainability reports, online magazines, blogs, microsites or news portals. Corporate websites can also be implemented with ns.wow.

How it works

The functional principle is similar to that of a Web Content Management System. Structure and form are strictly separated and allow the administration/updating of a website without programming knowledge. In contrast to a conventional web content management system, however, content is not captured in the form of rigid templates, but rather compiled using flexible HTML components using drag & drop and published as articles.

Die wesentlichen Merkmale im Überblick:

- WYSIWYG-Editor auf Basis von frei definierbaren Komponenten
- Läuft vollständig im Browser
- Flexible Designs – keine starren Templates
- Sehr einfache und intuitive Bedienung (keine Schulung für Endanwender notwendig)
- Artikel können flexibel zusammengestellt und jederzeit angepasst werden
- Strikte Einhaltung von Corporate-Design-Vorgaben
- Erweiterbar mit spezifischen Modulen speziell für Geschäftsberichte (z.B. finance plus)
- Weitere Output-Formate (PDF und Word)

Aufbau

ns.wow setzt sich aus zwei unterschiedlichen Komponenten zusammen, dem **Editor** und dem **Zielsystem**.

Editor

ns.wow ist in erster Linie der Online-WYSIWYG-Editor, der mit zahlreichen Funktionen und Modulen erweitert wird, um den gesamten Redaktionsprozess möglichst effizient abzubilden. Ein Anwender von ns.wow arbeitet ausschliesslich mit dem Editor, das Zielsystem wird lediglich als optionale Präsentationsschicht (Preview) verwendet.

Zielsystem

Inhalte werden innerhalb von ns.wow in Form von einzelnen Artikeln erfasst und per Knopfdruck an ein Zielsystem übergeben. Im Zielsystem werden die Artikel in ihrer finalen Ausprägung dargestellt (komplette Microsite inkl. Header, Footer, Navigation usw.). Das Zielsystem wird als eigene Microsite betrieben.

The essential features at a glance:

- WYSIWYG editor based on freely definable components
- Runs completely in the browser
- Flexible designs - no rigid templates
- Very simple and intuitive operation (no training required for end users)
- Articles can be flexibly compiled and adapted at any time
- Strict compliance with corporate design guidelines
- Expandable with specific modules especially for business reports (e.g. finance plus)
- Other output formats (PDF and Word)

Superstructure

ns.wow consists of two different components, the **editor** and the **system for presentation**.

Editor

ns.wow is first and foremost the online WYSIWYG editor, which is extended with numerous functions and modules in order to map the entire editorial process as efficiently as possible. A user of ns.wow works exclusively with the editor, the target system is only used as an optional presentation layer (preview).

System for presentation

Content is recorded within ns.wow in the form of individual articles and passed on to a target system at the push of a button. In the target system the articles are displayed in their final form (complete microsite incl. header, footer, navigation etc.). The target system is operated as a separate microsite.

Betriebskonzept

ns.wow wird ausschliesslich im SaaS-Modell betrieben (Software-as-a-Service). Sämtliche Aufwände bezüglich Betrieb und Wartung fallen auf Seite des Systemanbieters an. Der Zugriff auf die hochspezialisierte IT-Infrastruktur ist orts- und zeitunabhängig möglich und setzt lediglich Internetzugang und einen Webbrowser voraus.

Hosting

Bei einer Publikation unterscheidet die mms bezogen auf die Informationssicherheit zwei Phasen:

- **vor dem Go-Live:** Die Systeme für Programmierung und inhaltliche Bearbeitung einer Publikation wird in den hochspezialisierten Rechenzentren der mms bereitgestellt.
- Aus Gründen der Produktionssicherheit während der Produktion wird auch das Zielsystem ausschliesslich innerhalb dieser geschützten Infrastruktur gehostet und ist daher nur für autorisierte Benutzer zugänglich.
- Hier werden die vertraulichen Daten gehalten und durch den Kunden und seine Beauftragten bearbeitet und schlussendlich für die Veröffentlichung auf einen vordefinierten Zeitpunkt hin freigegeben.
- Die dafür von der mms bereitgestellten Systeme werden in den Rechenzentren wie weiter unten (Rechenzentrum vor Go-Live, ab Seite 8) beschrieben bereitgestellt.
- nach dem Go-Live: Ab dem Zeitpunkt der Veröffentlichung wird die Microsite zu einem kommerziellen Hoster übertragen und ist für jedermann zugänglich.

Die dafür von der mms bereitgestellten Systeme werden in den Rechenzentren (Rechenzentrum nach Go-Live, ab Seite 19) wie weiter unten beschrieben.

Operational concept

ns.wow is operated exclusively in the SaaS model (Software-as-a-Service). All expenses regarding operation and maintenance are incurred by the system provider. Access to the highly specialized IT infrastructure is possible regardless of location and time and requires only Internet access and a web browser.

Hosting

In the publishing process, mms differentiates between two phases with regard to information security:

- **Before going live:** The systems for programming and editing the content of a publication are provided in the highly specialised data-centers of mms.
- For reasons of security during production, the target system is also hosted exclusively within this protected infrastructure and is therefore only accessible to authorized users.
- Here the confidential data is kept and processed by the customer and his authorised representatives and finally released for publication at a predefined point in time.
- The systems provided by mms for this purpose are provided in the data centers as described later (Datacenter before Go-Live, starting on page 8).
- After Go-Live: From the time of publication, the microsite will be transferred to a commercial hoster and will be accessible to everyone.

The systems provided by mms for this purpose will be located in the data centers (Datacenter after Go-Live, starting on page 19) as described later

Veröffentlichungsprozess (Go-Live)

Während dem Erstellungsprozess des Geschäftsberichts werden die Daten wie oben beschrieben, ausschliesslich innerhalb der Rechenzentren vor Go-Live gehalten. Dies betrifft sowohl den ns.wow-Editor wie auch das Zielsystem. Erst unmittelbar vor der Veröffentlichung verlassen die Daten diese Rechenzentren und werden in das öffentlich zugängliche Hosting (Rechenzentren nach Go-Live) übertragen. Dieser Schritt betrifft nur das Zielsystem, der ns.wow-Editor wird immer innerhalb der vor Go-Live Datacenter betrieben.

Der Auslieferungsprozess des Zielsystems, wie auch weitere Anpassungen vor und nach der Veröffentlichung, unterliegen vollständig der Verantwortung der mms.

Go-Live (Standardprozess)

Beim Standardprozess ist sowohl das Zielsystem als auch die Rechenzentren vorgegeben.

Bei diesem Prozess wird das in den vor Go-Live Rechenzentren befindliche Zielsystem über einen standardisierten und wiederholbaren Deployment-Prozess über eine verschlüsselte Datenleitung zu den nach Go-Live Rechenzentren übertragen. Dies geschieht im Normalfall am Vorabend vor dem Veröffentlichungstermin, und immer erst nach Börsenschluss.

Das Zielsystem wird zu diesem Zeitpunkt öffentlich noch nicht zugänglich sein und mit mehreren Methoden gegen den unerlaubten Zugriff von aussen geschützt (Passwortschutz, Verzeichnisberechtigungen, Security-Plug-Ins, usw.). Die Entfernung dieser Schutzmechanismen geschieht erst unmittelbar zum Zeitpunkt der offiziellen Veröffentlichung der Inhalte.

Publishing Process (Go-Live)

During the preparation process of the annual report, the data will be held as described above, exclusively within the data centres before Go-Live. This applies to both the ns.wow editor and the target system. Only immediately before publication do the data leave these data centers and are transferred to the publicly accessible hosting (data centers after go-live). This step only affects the target system, the ns.wow editor is always operated within the pre-Go-Live datacenter.

The delivery process of the target system, as well as further adjustments before and after the publication, are fully the responsibility of mms.

Go-Live (standard process)

In the standard process, both the target system and the data centers are predefined.

In this process, the target system in the data centers before Go-Live is transferred via a standardized and repeatable deployment process via an encrypted data line to the data centers after Go-Live. This is usually done the evening before the publication date, and always after the close of trading.

At this point, the target system will not yet be publicly accessible and will be protected against unauthorized access from outside with several methods (password protection, directory permissions, security plug-ins, etc.). The removal of these protection mechanisms takes place only immediately at the time of the official publication of the contents.

Go-Live (Individualprozess)

Bei Bedarf kann das öffentliche Hosting auch nach spezifischen Kundenvorgaben abgebildet werden (Hosting inhouse, Hosters nach Wahl). Die Machbarkeit muss dazu für jede Anforderung vorab geprüft werden.

Beim einem solchen Individualprozess ist nur das Zielsystem fix vorgegeben. Es muss ein spezifischer individueller Veröffentlichungsprozess definiert werden. Es ist mit Mehrkosten zu rechnen und die Verantwortung für den Prozess liegt beim Kunden.

Korrekturen nach dem Go-Live

Nachträgliche inhaltliche Änderungen durch den Kunden werden über den ns.wow-Editor immer zuerst in das Zielsystem in den vor Go-Live Rechenzentren geschrieben (Preview-Umgebung). Von dort wird dann ein neuer Deployment-Prozess angestoßen damit die Änderungen öffentlich werden.

Rechenzentren vor Go-Live

1 Physische Sicherheit

Standort

Die mms verfügt über zwei georedundante Rechenzentren, beide befinden sich in der Schweiz

Das primäre Rechenzentrum befindet sich in CH-5242 Lupfig und wird von Green Datacenter AG betrieben, das sekundäre Rechenzentrum befindet sich in CH-8048 Zürich und wird von Atlas Edge betrieben.

Konformität

Beide Rechenzentren sind nach der Tier-Norm gemäss Uptime Institute gebaut, das primäre Rechenzentrum nach Tier IV, das sekundäre Rechenzentrum nach Tier III.

Go-Live (individual process)

If required, public hosting can also be mapped according to specific customer specifications (in-house hosting, hoster of choice). The feasibility of each requirement must be checked in advance.

With such an individual process, only the target system is fixed. A specific individual publication process must be defined. Additional costs are to be expected and the responsibility for the process lies with the customer.

Corrections after go-live

Later changes in content by the customer are always written via the ns.wow editor first into the target system in the pre-Go-Live data centers (preview environment). From there, a new deployment process is triggered to make the changes public.

Data centers before Go-Live

1 Physical security

Location

mms operates with two georedundant data centers, both sites are located in Switzerland.

The primary data center is located in Lupfig and is operated by Green Datacenter AG, the secondary data center is located in Zurich and is operated by Atlas Edge.

Compliance

Both data centers are built compliant with the Tier Norm according to Uptime Institute. The primary data center according to Tier IV, the secondary data center according to Tier III.

Zutrittsschutz

- Elektronische Überwachung sämtlicher Türen
- Aufzeichnung sämtlicher Zutritte
- Überwachungskameras innen und aussen
- Zutrittsberechtigung nur für autorisierte und registrierte Personen
- Biometrische Zutrittskontrolle
- Getrennte Sicherheitszonen
- Separate Personen- und Warenschleuse

Strom und Kühlung

- Redundante Klimatisierung in zwei Kreisläufen und redundante Kühlgeräte
- Eigene Trafos und vier Dieselgeneratoren (beides im Gebäude) für autarken Notstrombetrieb während mindestens sieben Tagen
- Stromeinspeisung über redundante Infrastruktur, getrennt geführt (Feed A / Feed B)

Brandschutz

- Brandhemmende Materialien
- Getrennte Brandschutzzonen und -wände
- 7x24 h elektronisch überwachte Räumlichkeiten mit Rauch-/Wärmemeldern
- Brandfrüherkennung
- Automatische Löschung

2 Zertifikate

ISO 27001

Die Informationssicherheit bei mms selbst und in den beiden Rechenzentren ist nach ISO 27001 zertifiziert.

Access protection

- Electronic surveillance of all doors
- All entries logged
- Surveillance cameras inside and out
- Access granted only to authorized and registered persons
- Biometric access control
- Separated security areas
- Separate personnel and goods airlock

Electricity and cooling

- Redundant air conditioning in two cycles and redundant cooling units
- Own transformers and four diesel generators (both inside the building) for self-sufficient emergency power lasting at least seven days
- Electricity feed-in via redundant infrastructure, managed separately (feed A / feed B)

Fire protection

- Flame-retardant materials
- Separate fire protection zones and walls
- 24/7 electronically monitored premises with smoke and heat detectors
- Early fire detection
- Automatic extinguishers

2 Certificates

ISO 27001

Information security at mms itself and at both data centers is certified in accordance with ISO 27001.

SOC 1 Report nach ISAE 3402

Die mms verfügt über einen auditierten SOC1 Type 2 Report, welcher gegen Gebühr erhältlich ist.

Energiemanagement

Beide Rechenzentren sind bezüglich Energiemanagement zertifiziert und nutzen ausschliesslich erneuerbare Energie.

3 Connection

Internetanbindung

Die Rechenzentren sind über physikalisch redundante Leitungen von zwei unterschiedlichen Providern ans Internet angebunden. Die beiden Rechenzentren sind über eine dedizierte 10-Gbit-Verbindung zusammengeschlossen. Der gesamte Datenverkehr ist verschlüsselt.

DDoS Schutz

Der Schutz vor DDoS-Attacken wird über den Internet-Service-Provider mit einem Team von Spezialisten rund um die Uhr gewährleistet.

SOC 1 Report according to ISAE 3402

The mms has an audited SOC1 type 2 report, which is available for a fee.

Energy management

Both data centers are certified for energy management and use only renewable energy.

3 Connection

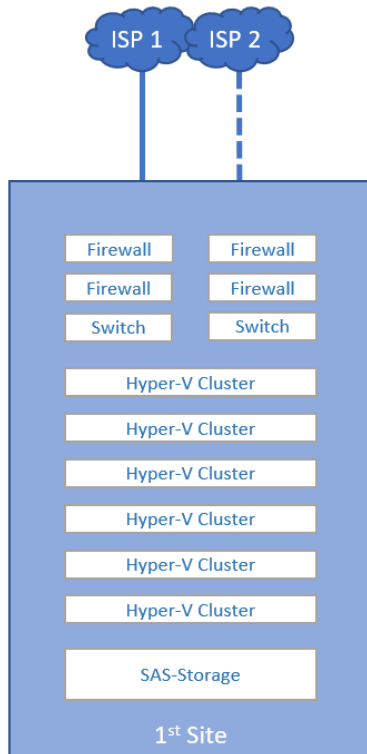
Internet connection

The data centers are connected to the internet via physically redundant lines from two different providers. The two data centers are connected via a dedicated 10 GBit connection. All data traffic is encrypted.

DDoS Protection

Protection against DDoS attacks is provided through the internet service provider with a team of specialists, operating around the clock.

4 Architektur



Eigene Hardware

Wir haben die volle Kontrolle über die eingesetzte Hardware, weil sie ausschliesslich von der mms verwendet und nicht mit anderen geteilt wird.

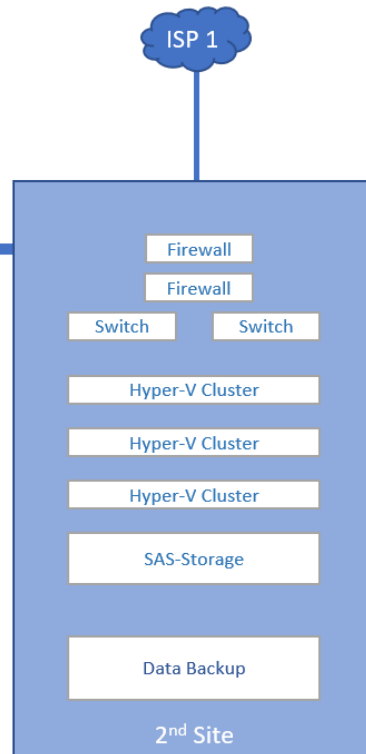
Ohne Single Point of Failure

Sämtliche Komponenten sind redundant ausgelegt, sodass kein einzelner Ausfall zu einem Ausfall des Gesamtsystems führen kann.

Redundantes Rechenzentrum

mms verfügt über ein georedundantes zweites Datacenter (das Notfallsystem). Das Notfallkonzept der mms sieht für Kunden mit der Option «2nd Site» vor, im Katastrophenfall auf das Notfallsystem im zweiten Datacenter zu wechseln.

4 Architecture



Dedicated hardware

We have full control over the hardware since it is used exclusively by mms and is not shared with others

No single point of failure

All components are designed redundantly so that no single failure can lead to a full collapse of the entire system.

Redundant data center

mms disposes of a georedundant second data center (the emergency system). The emergency concept of mms provides for customers with the “2nd Site” option to switch to the emergency system in the second data center in the event of a disaster.

Georedundantes Backup

Zur Sicherung der Business Continuity in einem Worst-Case-Szenario werden die täglich erstellten Backups im zweiten Rechenzentrum vorgehalten.

Die mms führt regelmässige Restore-Tests durch und dokumentiert diese.

Georedundant back-up

To ensure business continuity in a worst-case scenario, the daily back-ups are stored in the second data center.

mms carries out and documents regular restore tests

5 Netzwerk- und Systemsicherheit

Netzwerktrennung

mms verwendet entsprechend den hohen Sicherheitsanforderungen geeignete Netzschutzverfahren und trennt die Netzwerke durch VLANs.

5 Network and system security

Network separation

mms uses suitable network protection methods according to the high security requirements and separates the networks by VLANs.

Verschlüsselte Datenübertragung

Die Datenübertragung zwischen dem Kunden und dem System ns.wow erfolgt ausschliesslich verschlüsselt (TLS 1.2 oder TLS 1.3).

Encrypted data transmission

Data transmission between the customer and the ns.wow system is strictly encrypted (TLS 1.2 or TLS 1.3).

Verschlüsselung im Speicherzustand

Die Verschlüsselung der gespeicherten Daten ist nach FIPS 140-2 level 2 zertifiziert, der Storage nutzt hierzu AES256.

Encryption at rest

The encryption of the data at rest is certified according to FIPS 140-2 level 2, and for this the storage uses AES256.

Mehrstufige Firewall

Wir verfügen über mehrfache Firewall-Cluster, der äussere Firewall-Cluster wird durch die Partnerfirma verwaltet, der innere durch das IT-Team der mms (Segregation of Duties).

Multi-stage firewall

We have multiple firewall clusters: external firewalls are managed by the partner company; internal firewalls by the mms IT team (segregation of duties).

Lastausgleich und Proxy

Alle für Kunden zugreifbaren Services sind über Lastausgleich und Proxy-Server hochverfügbar ausgelegt

Load balancing and proxy

All customer-accessible services are designed for high availability via load balancing and proxy servers.

Intrusion Prevention

Unser IPS prüft den Datenverkehr auf unterster Ebene, um durch den Abgleich von Datenverkehrsmustern mit einer umfassenden und ständig aktualisierten Signaturdatenbank bekannte Bedrohungen zu erkennen und blockiert nötigenfalls den Vorgang.

Malware-Schutz

Die ganze Plattform ist mit State-of-the-Art-Antivirussoftware geschützt (mehrere Sicherungen in Serie mit Werkzeugen unterschiedlicher Anbieter).

Updates und Patch-Management

Alle eingesetzten Komponenten werden regelmäßig gepatcht, entweder in den angekündigten Wartungsfenstern oder – bei kritischen Schwachstellen – unmittelbar. Updates werden auf einem Testsystem vor dem produktiven Rollout ausführlichen Tests unterzogen.

Zugriff

Der Zugriff auf ns.wow erfolgt über einen Webbrowser, in dem sich die Benutzer über ein zweistufiges Login (Benutzername, Passwort, MFA-Token) authentifizieren. Sämtliche Applikationen, wie auch ein kundenspezifisches Austauschlaufwerk, sind erst nach dieser Anmeldung abrufbar. Das Passwort kann jederzeit durch den User selbst geändert werden. Es ist maximal 120 Tage gültig und muss folgende Minimalvoraussetzungen erfüllen: 10 Zeichen, bestehend aus Gross- und Kleinbuchstaben sowie Zahl oder Sonderzeichen. Es darf keinen Teil des eigenen Benutzernamens enthalten. Werden die Minimalvoraussetzungen beim Ändern des Passworts nicht eingehalten, ist diese Änderung nicht möglich. Nach fünf falschen Passworteingaben wird der Useraccount automatisch für mehrere Minuten gesperrt, nach zehn falschen MFA-Eingaben dauerhaft.

Intrusion prevention

IPS examines traffic at the lowest level to identify known threats by matching traffic patterns to a comprehensive and continuously updated signature database and blocks the process if necessary.

Malware protection

The entire platform is protected with state-of-the-art antivirus software (multiple layers in series with tools from different providers).

Updates and patch management

All components will be patched regularly, either in the announced maintenance windows or immediately in case of critical vulnerabilities. Updates are subjected to extensive testing on a test system before the productive rollout.

Access

ns.wow is accessed via a web browser in which the user is authenticated by a two-stage login procedure (username, password, MFA token). All applications, as well as a customer-specific replacement drive, can be accessed only after login. The user may change his password at any time. It is valid for a maximum of 120 days and must meet the following minimum requirements: 10 characters, consisting of lower and upper-case letters, and numbers or special characters. It may not contain part of the username. The password cannot be changed if these minimum requirements are not met. After five failed password entries, the user account is automatically blocked for several minutes, after ten failed MFA entries it is blocked permanently.

Kundendaten

Vertrauliche Kundendaten werden ausschliesslich in den geschützten Datacenter gehalten und mittels geprüfter, mehrstufiger Rechtevergabe vor unberechtigten Zugriffen geschützt

Trennung der Kundendaten

Für Kunden in der shared Umgebung werden die Daten einzelner Kunden applikatorisch getrennt. Für Kunden in einer Premium Umgebung werden die Daten in getrennten Netzwerksegmenten gehalten.

Customer data

Confidential customer data is kept only in the protected data center and protected from unauthorized access by verified, multi-level access rights assignment.

Segregation of customer data

For customers in the shared environment, the data of individual customers is segregated applicative. For customers in a premium environment, the data is kept in separate network segments.

Schema

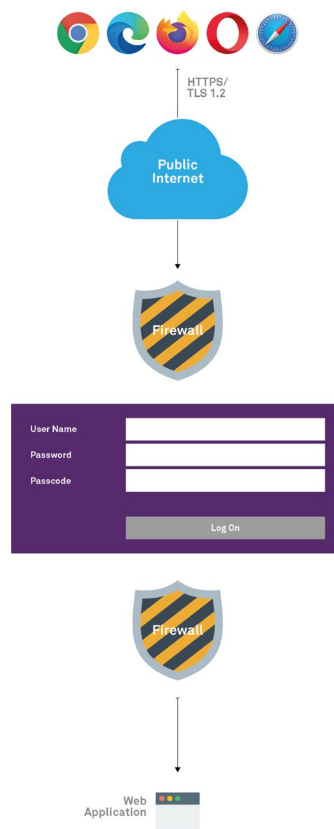
Client-Applikationen

- Citrix Receiver / Workspace App
- Webbrowser mit aktiviertem JS
(Google Chrome / MS Edge / Firefox; jeweils die aktuelle Version)

Scheme

Client applications:

- Citrix Receiver / Workspace App
- Web browser with JS enabled
(Google Chrome / MS Edge / Firefox; the latest version for each)



Zugriff auf das Redaktionssystem

- Webbasierte Applikation
- HTTPS-verschlüsselte Verbindung (EV-Zertifikat)
- 2-Faktor-Authentifizierung
 - Benutzername
 - Passwort
 - MFA-Token
- Textbearbeitung webbasiert
- Abgesicherter Dateiaustausch (webbasiert) zugreifbar nach 2-Faktor-Authentifizierung
- Finanzschnittstelle und alle weiteren Module (webbasiert) zugreifbar nach 2-Faktor-Authentifizierung

Access to the editorial system

- Web-based application
- HTTPS-encrypted connection (EV certificate)
- Two-factor authentication
 - Username
 - Password
 - MFA token
- Text editing Web-based
- Secured data exchange (Web-based) accessible after a two-factor authentication
- Financial interface and all other modules (Web-based) accessible after a two-factor authentication

6 Applikationssicherheit

Applikationssicherheitsprozess

Ein detaillierter Application-Security-Lifecycle-Prozess ist vollständig in den Software Development Lifecycle von mms integriert, einschliesslich:

- definierter interner Sicherheitsanforderungen, Richtlinien und Best Practices für die Branchensicherheit, die in jeder Phase des Lebenszyklus angewendet werden;
- laufender Überprüfung von Architekturen, Designfunktionen und Lösungen;
- Iterativer manueller und automatisierter (mit statischen Codeanalysatoren) Quellcode-Überprüfung auf Schwächen und Codequalität;
- regelmässiger manueller Bewertung der Vorproduktionsumgebung;
- Sicherheitsschulungen für die Mitarbeitenden entsprechend ihrer jeweiligen Aufgabenbereiche.

Rechte und Rollen

Der Zugriff auf die Dokumente innerhalb der Redaktionssystem-Datenbank kann über detaillierte Gruppenrechte gesteuert werden. Jedem Benutzer wird somit eine bestimmte Rolle zuteil, die auf einer Verantwortlichkeitsmatrix abgestützt ist, die individuell mit jedem Kunden erarbeitet wird.

Die Zuteilung von Benutzerrechten erfolgt in einem mehrstufigen Prozess mit Kontrollen nach jedem Prozessschritt.

6 Application security

Application security process

An in-depth application security lifecycle process is fully integrated into mms's software development lifecycle, including:

- defined in-house security requirements, policies, and industry security best practices applied in every stage of the lifecycle;
- ongoing review of architectures, design features, and solutions;
- iterative manual and automated (using static code analysers) source code review for weaknesses and code quality;
- regular manual assessment of pre-production environment;
- security trainings for employees according to their respective job roles.

Rights and roles

Access to documents within the editorial system database can be controlled with detailed group permissions; each user is assigned a certain role, based on a responsibility matrix which is developed individually for each customer.

The assignment of user rights is done in a multi-level process with checks after each process step.

Administratorenberechtigung

Für administrative Aufgaben und Wartung wird Dritten nur soweit nötig und nur im Beisein von internen Mitarbeitern Zugriff auf die Infrastruktur gegeben. Unser IaaS Provider hat keinen logischen Zugriff auf die Kundendaten.

Ausschliesslich benannte Mitarbeiter haben physischen Zutritt.

Datenzugriff

Eine Weiterleitung der Daten ausserhalb des ns.wow-Systems während der Produktion erfolgt nicht ohne spezielle Anweisung durch den Kunden. Die involvierten Mitarbeiter arbeiten alle direkt auf dem System. Somit erfolgt keine Datenspeicherung auf dem lokalen Client. Der Upload der Daten erfolgt über den unter dem Punkt «Verschlüsselung» beschriebenen sicheren Kanal, wie auch der allfällige Download von PDFs oder anderen Daten.

7 Organisation

Personal

Alle Mitarbeiter der mms haben eine umfassende Vertraulichkeitsklausel im Arbeitsvertrag, welche auch die einschlägigen Bestimmungen u.a. des Bankgeheimnisses, der Gesetze der Börsenaufsichten sowie der Datenschutzgesetzgebung einschliessen.

Des Weiteren werden alle Mitarbeiter regelmässig vor Produktionsbeginn auf die geltenden Verhaltensregeln, Prozesse und Standards hingewiesen und jährlich bezüglich IT-Security und Umgang mit vertraulichen Daten geschult.

Administrator privileges

For administrative and maintenance work, third parties may access the infrastructure only to the extent necessary and only in the presence of internal staff members. Our IaaS provider does not have logical access to customer data.

Only designated staff have physical access.

Access to data

Data is not shared outside the ns.wow system during production, unless specifically requested by the customer. All participating staff work directly in the system; thus no data is stored on the local client. The data is uploaded, and PDFs and other files downloaded via the secure channel described in the “Encryption” section.

7 Organization

Personnel

All mms employees have a comprehensive confidentiality clause in their employment contract, which also includes the relevant provisions of banking secrecy, stock exchange supervisory laws and data protection legislation, among others.

In addition, all employees are made aware regularly of the applicable rules of conduct, processes and standards before the start of production, and receive regular training in IT security issues and handling of confidential data.

Beauftragte / Unterakkordanten

Mit Dritten, die im Rahmen eines Projekts in unserem Auftrag mit Ihren Daten in Berührung kommen, schliessen wir entsprechende Geheimhaltungserklärungen ab. Geschäftspartner mit regelmässiger Tätigkeit auf Kundenprojekten werden jährlich durch uns zertifiziert. Während dieser Zertifizierung werden die Partner auch im Umgang mit vertraulichen Daten instruiert.

Exit-Vereinbarung

Bei einer Vertragsauflösung (und zu jedem beliebigen weiteren Zeitpunkt) können die bei mms gehaltenen Daten exportiert werden.

Umgang mit Sicherheitsvorfällen

Vorfälle jeder Art werden über das Ticketsystem erfasst und bearbeitet. Sicherheitsrelevante Vorfälle werden entsprechend markiert, beurteilt und dem CISO vorgelegt nach festgelegtem Prozedere bearbeitet.

8 Überwachung

Monitoring

Die Plattform wird konstant mit über 1'000 Sensoren überwacht und löst automatisch Alarmierung aus.

Threat Protection

Die Systeme werden automatisch auf Anomalien hin untersucht.

Logging

Die Logs werden zentral zusammengezogen und automatisch ausgewertet.
Optional können Audit-Logs regelmässig an Kunden ausgeliefert werden.

Contractors / subcontractors

We conclude appropriate confidentiality agreements with our assigned third parties who come into contact with your data during a project. Business partners that work regularly on customer projects are certified annually by us. During this certification, partners are also briefed on how to handle confidential data.

Exit agreement

When a contract is terminated (and at any other time), the data held at mms can be exported.

Handling security incidents

Incidents of any kind are recorded and processed via the ticket system. Security-related incidents are marked accordingly, assessed and submitted to the CISO and processed according to a defined procedure.

8 Monitoring

Monitoring

The platform is monitored continuously with more than 1'000 sensors that automatically trigger an alarm.

Threat Protection

The systems are automatically checked for anomalies.

Logging

The logs are aggregated centrally and evaluated automatically.
Optionally, audit logs can be provided to customers on a regular basis.

Externe Audits

Die ns.wow-IT-Infrastruktur wird regelmässig auditiert. Diese Überprüfung beinhaltet die Beantwortung komplexer Fragestellungen zu den verschiedenen Bereichen unserer Dienstleistung, inklusive der Beurteilung unserer technischen und organisatorischen Infrastruktur nach aktuellen Gesichtspunkten.

Schwachstellen-Scans

Die Möglichkeit eines unautorisierten Zugriffs wird mittels automatisierter Vulnerability Scans durch einen unabhängigen Service-Provider überprüft. Die Tests erfolgen wöchentlich.

Penetrationstests

Jährlich wird eine Sicherheitsfirma mit einem umfassenden Penetrationstest beauftragt. Diese prüfen einerseits die Sicherheit von aussen. Zusätzlich bekommen sie privilegierten Zugang auf eine für sie bereitgestellte standardisierte Kundeninstanz und prüfen so die Sicherheit der Abschottung gegenüber anderen Kundeninstanzen.

Kunden-Audits

Kunden-Audits sind auf Anfrage unter Einhaltung von Auflagen möglich.

Rechenzentren nach Go-Live

1 Systemübersicht

Provider

Die öffentlich zugänglichen Reports werden in der AWS Cloud gehostet. Die mms nutzt die Standorte Frankfurt (Deutschland) und Dublin (Irland).

AWS verfügt über eine Reihe von Zertifikaten, auch über ein ISO-27001 Zertifikat für alle von mms eingesetzten Services.

External audit

The ns.wow IT infrastructure is audited regularly. This audit involves complex questions on the various aspects of our service and includes an assessment of our technical and organizational infrastructure from current perspectives.

Vulnerability scans

The possibility of unauthorized access is checked by an independent service provider by means of an automated penetration test. The test is performed weekly.

Penetration test

On an annual basis, a security company is charged with a comprehensive penetration test. On one hand, they check the security from the outside. In addition, they are given privileged access to a standardized customer instance provided for them and thus check the security of the foreclosure against other customer instances.

Customer audit

Customer audits are possible on request and subject to compliance with conditions.

Datacenters after go-live

1 System overview

Provider

The publicly available reports are hosted in the AWS Cloud. mms uses the sites Frankfurt (Germany) and Dublin (Ireland).

AWS is certified with a number of standards, including an ISO-27001 certificate for all services used by mms.

Eingesetzte Services

Die von AWS bereitgestellten Dienste sind:

- Elastic Compute Cloud (EC2)
- Simple Storage Service (S3)
- Relational Database Service (RDS)

Installierte Applikationen

mms verwendet einen Lamp-Stack mit Ubuntu, Apache2 und HAProxy. Als Datenbankschnittstelle fungiert der RDS-Service.

Technische Struktur

mms betreibt mehrere Linux Nodes mit Lastausgleich, auf der Firewall werden nach aussen nur die notwendigen Ports (HTTP/HTTPS) zugelassen. SSH-Zugriff ist nur von wenigen IPs aus zugelassen.

Physische Sicherheit

Physische Sicherheit wird durch AWS gewährleistet und beinhaltet Zäune um das Gelände, Überwachungskameras, Einsatz von Sicherheitspersonal u.v.m.

Hardening

Das Betriebssystem ist gehärtet, SSH-Zugriff ist nur von definierten Umgebungen aus mittels Private/Public-Key ansprechbar, ein Zugang nur mit Passwort ist deaktiviert, nicht benötigte Dienste sind deaktiviert, Login-Seite und allfällige Administrations-Backend sind gesperrt und nicht benötigte Schnittstelle sind deaktiviert, bösartige Zugriffe führen nach einer Kulanzschwelle zur kompletten Sperre der angreifenden IP.

Services used

The services provided by AWS are:

- Elastic Compute Cloud (EC2)
- Simple Storage Service (S3)
- Relational Database Service (RDS)

Installed applications

mms uses a lamp stack with Ubuntu, Apache2 and HAProxy. The RDS service acts as the database interface.

Technical structure

mms operates several Linux nodes with load balancing, on the firewall only the necessary ports (HTTP/HTTPS) are allowed to the outside. SSH access is only permitted from a few IPs.

Physical Security

Physical security is ensured by AWS and includes fences around the site, surveillance cameras, security personnel and much more.

Hardening

The operating system is hardened, SSH access is only accessible from defined environments using a private/public key, password-only access is deactivated, services that are not required are deactivated, the login page and any administration backend are blocked and interfaces that are not required are deactivated, malicious access leads to the complete blocking of the attacking IP after a goodwill threshold.

Zielsystem Security

Bei einigen Projekten wird eine speziell durch mms entwickelte WordPress-Installation eingesetzt, welche nicht benötigte Funktionalität deaktiviert und sicherstellt, dass die benutzte Funktionalität den sicherheitstechnischen Vorgaben entspricht.

Die Standard-Funktionalität wird durch selbst entwickelte WordPress-Plugins erweitert, die ebenfalls die geforderten Sicherheitsrichtlinien erfüllen. Plugins von Drittanbietern werden nur nach eingehender Qualitätsprüfung und nach gegenseitiger Absprache mit dem Kunden integriert.

Bei den übrigen Projekten werden ausschliesslich statische Inhalte gehostet, der Angriffsvektor somit eingeschränkt und engmaschig überprüft.

Provisioning

Provisioning wird automatisiert mittels Scripting ausgeführt.

Patchmanagement

Patches zu kritischen Issues werden unmittelbar aufgespielt, die unkritischen in den geplanten Wartungsfenstern.

Zugriffskontrolle

Zugriffe auf die Server sind ausschliesslich über public/private Key (Zertifikat) möglich; nur berechtigte User an berechtigten Standorten können sich einloggen und Systembefehle ausführen und Dienste neu starten.

Security of the system for presentation

A WordPress installation specially developed by mms is used, which deactivates unneeded functionality and ensures that the functionality used corresponds to the safety-related specifications.

The standard functionality is extended by self-developed WordPress plug-ins, which also meet the required security guidelines. Third-party plug-ins are only integrated after a thorough quality check and mutual agreement with the customer.

The other projects only host static content, so the attack vector is limited and closely monitored.

Provisioning

Provisioning is automated using scripting.

Patchmanagement

Patches for critical issues are applied immediately, the uncritical ones in the planned maintenance windows.

Access control

Access to the servers is only possible via public/private key (certificate); only authorized users at authorized locations can log in and execute system commands and restart services.

Betriebsrollen

Auf den Systemen gibt es drei Klassen von Betriebsrollen: Service User, benannte Administrator User und benannte Entwickler User. Entwickler können Deployments ausführen, Service User können provisionieren, Administratoren können das System verwalten.

Logging

Ereignisse und Zugriffe werden geloggt, die Logs werden für mindestens einen Monat vorgehalten.

2 Backup

Es werden tägliche Snapshot pro Node erstellt und georedundant gehalten, lokale Datenbank Dumps werden täglich erstellt und eine Woche lang aufbewahrt.

3 Überwachung

Eine automatisierte Überwachung mit PRTG sowie Überwachung der Erreichbarkeit von außerhalb alarmieren bei Abweichung.

4 Organisation

Personal

Alle Mitarbeiter der mms haben eine umfassende Vertraulichkeitsklausel im Arbeitsvertrag, welche auch die einschlägigen Bestimmungen u.a. des Bankgeheimnisses, der Gesetze der Börsenaufsichten sowie der Datenschutzgesetzgebung einschliessen.

Des Weiteren werden alle Mitarbeiter regelmässig vor Produktionsbeginn auf die geltenden Verhaltensregeln, Prozesse und Standards hingewiesen und jährlich bezüglich IT-Security und Umgang mit vertraulichen Daten geschult.

Operational roles

There are three classes of operational roles on the systems: Service User, Named Administrator User, and Named Developer User. Developers can perform deployments, service users can do provisioning, administrators can manage the system.

Logging

Events and accesses are logged, the logs are kept for at least one month.

2 Backup

Daily snapshots are created per node and kept georedundant, local database dumps are created daily and kept for one week.

3 Monitoring

An automated monitoring with PRTG as well as monitoring the accessibility from outside alert in case of deviation.

4 Organization

Personnel

All mms employees have a comprehensive confidentiality clause in their employment contract, which also includes the relevant provisions of banking secrecy, stock exchange supervisory laws and data protection legislation, among others.

In addition, all employees are made aware regularly of the applicable rules of conduct, processes and standards before the start of production, and receive regular training in IT security issues and handling of confidential data.

Beauftragte / Unterakkordanten

Mit Dritten, die im Rahmen eines Projekts in unserem Auftrag mit Ihren Daten in Berührung kommen, schliessen wir entsprechende Geheimhaltungserklärungen ab. Geschäftspartner mit regelmässiger Tätigkeit auf Kundenprojekten werden jährlich durch uns zertifiziert. Während dieser Zertifizierung werden die Partner auch im Umgang mit vertraulichen Daten instruiert.

Contractors / subcontractors

We conclude appropriate confidentiality agreements with our assigned third parties who come into contact with your data during a project. Business partners that work regularly on customer projects are certified annually by us. During this certification, partners are also briefed on how to handle confidential data.

Dieses Dokument wurde in deutscher Sprache verfasst und auf Englisch übersetzt. Verbindlich ist die deutsche Version. Die in diesem Dokument enthaltenen Informationen sind ausschliesslich den Kunden der mms solutions vorbehalten. Eine Weitergabe an Dritte ist untersagt.

This document is originally prepared in German and translated into English. In the event of any discrepancy, the German version prevails. The information contained in this document is reserved exclusively for the customers of mms solutions. Any disclosure to third parties is prohibited.