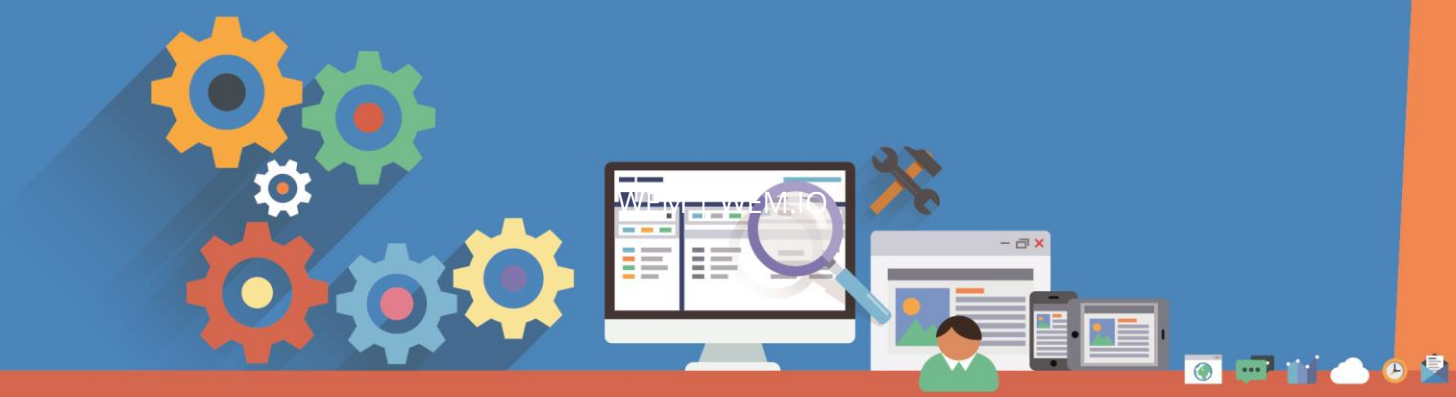
WEM

WEM
SAFETY AND SECURITY
&
GDPR



1 Legal

1.1 GDPR

The General Data Protection Regulation (AVG) will apply as of May 25th 2018. This means that from that date onwards, the same privacy legislation applies throughout the European Union (EU). The Personal Data Protection Act (Wbp) then no longer applies.
ZoomBIM has researched what consequences are of complying with this new legislation. In line with this, a plan has been drawn up which indicates where risks lie and how to eliminate these risks with which ZoomBIM ultimately complies with the new legislation.
Characteristics against which we measure risk?

- Do we need the data;
- Is current access 'allowed/justified' (by current contract - role - etc.);
- Is current format in which we keep data, justifiable and safe;
- Does the current process creates a risk on data leakage;
- What are generic processes we recognize (leave data on printer, lock screen when away from keyboard, keep door unlocked, Data storage procedures, …);
- Is data secure (enough) on location and format?

1.2 Data leakage

ZoomBIM recognizes the importance of keeping data safe and secure. Therefor there are several technical and organizational measures in place to prevent data from 'leaking'.
Should there accidentally be a suspicion or proof of data loss, there is a procedure in place to prevent further leakage and inform all stakeholders. All recordings are gathered and stored in one place and will be handled by one department and its current duty officer. This officer states the impact and will, according to protocol:

- take all necessary steps to prevent data from further loss;
- report to all stakeholders, based on the impact of the recorded event;
- take all necessary steps to prevent an event from ever happening again.

1.3 Non Disclosure Agreements

Should it be necessary to share certain data like privacy information, security information, etc, with others we require a completed Non Disclosure Agreement with all involved parties.

1.4 SLA

Service Level Agreements are generally available on two levels:

- WEM Platform
- WEM Project

The platform SLA is provided by ZoomBIM has three available categories:

Nr.	Description	Notes WEM Platform	Notes WEM Project
1.	Basic	Free of charge	25% of building cost
2.	14x6	6 days a week at 14 hours a day. 35% of annual license cost	35% of building cost
3.	24x7	50% of annual license cost	50% of building cost

The SLA support documents provide information on availability, response times, ways to report incidents, how incidents are handled, availability, etc.

WEM Project SLA's are generally offered by the WEM partner and are outside the scope of this document.

1.5 Data Processing Agreements

A Data Processing Agreement (DPA) is an agreement between a data owner (Responsible) and the data modifier (Modifier). A DPA usually will be offered at request of a ZoomBIM Customer, Distributer or Partner.
All relations are invited to request a signed DPA. Should a party not have such an agreement of its own, ZoomBIM is able happy to provide one.
Traditionally a DPA provides boundaries on what data the Modifier is allowed to handle.

1.6 Certification

ISO 27001/NEN 7510 Certification

Regarding The Netherlands, WEM's entire infrastructure is situated with the Dutch data center provider CloudVPS, located at Delftsestraat 5B, 3013 AB in Rotterdam. CloudVPS is ISO 27001 (ISO/IEC 27001:2013) and NEN 7510 certified. The ISO 27001 security management certification is the most widely used outside the United States. This certification consists of 133 controls and is applicable to the decor of the entire Information Security Management System. CloudVPS has implemented the 2005 version in 2012, the ISO 27001:2005. In 2015, CloudVPS has been certified again based upon the 2013 version: ISO27001:2013. The certificate, Statement of Applicability and the audit report are available for inspection.

NEN 7510

The Dutch healthcare sector modifies and saves important medical and patient information on patients. To ensure that medical information is kept save, the NEN (the Dutch Standardization Institute) created the NEN 7510 security standard. CloudVPS has the NEN 7510 implemented at the same time as the ISO 27001 and was audited accordingly. CloudVPS has implemented technical and organizational measures to ensure the integrity of its patient data and pass the audit. With the use of firewalls and technical and physical separation of networks, it is not possible to inappropriately access data.

Regarding countries outside The Netherlands, ZoomBIM will only contract hosts that are certified. ZoomBIM is currently in the preparation process to getting certified on ISO 27001 and SOC2.

2 Technology

2.1 WEM around the world

Whilst WEM is developed in the Netherlands, each release is deployed worldwide to all of our hosting partners. Therefore all users are guaranteed to be able to benefit from the latest WEM features with each new release. All regionally selected hosting partners have the same setup and meet the same, strict safety and security protocols as described in this document.

Currently selected, worldwide hosting partners are:

- Microsoft Azure
- AWS

2.2 WEM

Regarding access to data and the technology of WEM itself, there are several measures in place as part of the WEM platform and the infrastructure setup.
For starters, we'll explain how the WEM platform has been setup.
The WEM platform has 4 distinct elements:

1) Modeling (Development)
2) Preview (Test)
3) Staging (Acceptance)
4) Live (Production)

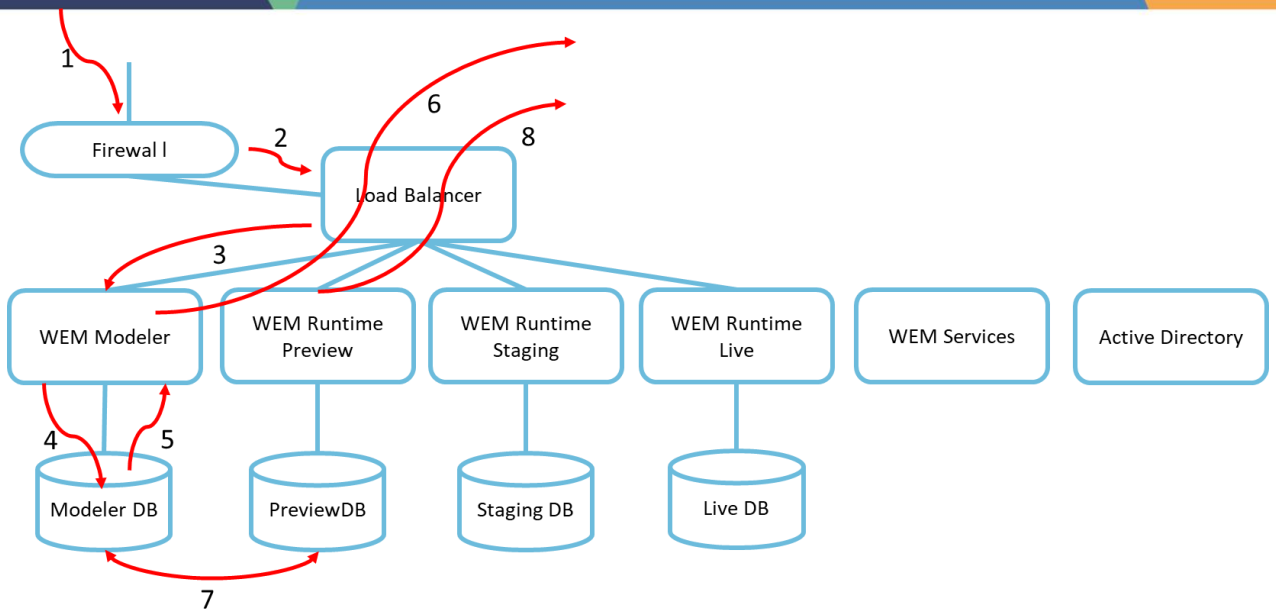
2.2.1 WEM Modeler

The WEM modeler is the authoring environment where you create (model) your WEM projects.

The WEM Modeler is secured with SSL encryption, based on the highest available standard supported by the client device and access is based on username and password combination.

The WEM modeler is internally linked with the my.wem environment for single-sign-on (SSO) purposes.

The WEM modeler creates a database based model of your application logic, from the modeler the application is published to the run-time environments. The publication happens in real time to the Preview environment and on request to the Staging and Live environments.



The process elements of the WEM Modeler environment include:

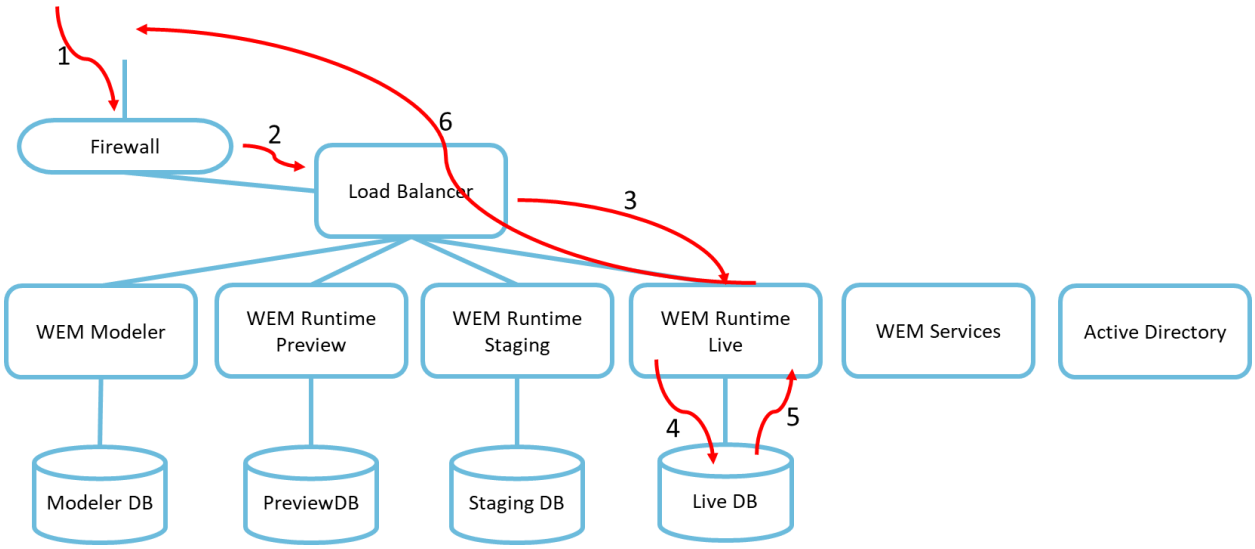
1. Request from WEM Modeler user is screened for reputation to stop DDoS and alike attacks
2. Request is forwarded to the load balancer, this is where the session is created with the end-user device, ssl decryption and encryption takes place and request format is validated. All malformed requests are denied and logged.
3. Valid requests are forwarded to a cluster of WEM Modeler servers.
4. The required WEM model information is retrieved from and updated in the Modeler DB
5. The updates to the WEM modeler database are fed back into the WEM modeler server to provide a real-time view of the status to the modeler.
6. The Modeler server provides an SSL encrypted HTML session back to the Modeler user.
7. The WEM Modeler database is synchronized in real-time with the Preview WEM Runtime to enable real-time application testing and debugging.
8. The test version of the application is send to the customer browser over an SSL encrypted connection.

WEM Modeler below version 4 is based on a combined HTML3 and HTML4 application with an important element dependent on a browser based installation of Adobe Flash.

WEM Modeler from version 4 (generally available in September 2018) is an HTML5 application that requires no additional software to use.

2.2.2 The Runtime environments

Stages 'Preview', 'Staging' and 'Live' are unrelated and exist on separate server clusters.
This means that no one cluster can access another.



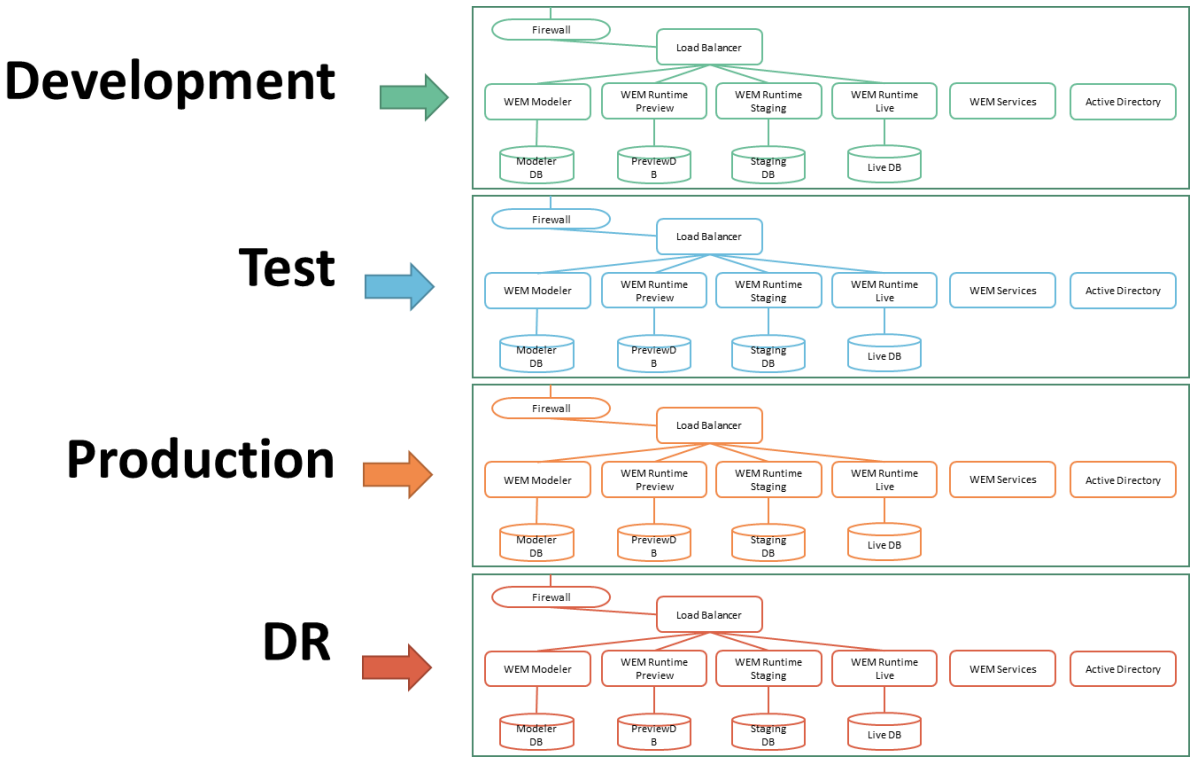
The process elements of the WEM Runtime environment include:

1. Request from WEM application user is screened for reputation to stop DDoS and alike attacks
2. Request is forwarded to the load balancer, this is where the session is created with the end-user device, ssl decryption and encryption takes place and request format is validated. All malformed requests are denied and logged.
3. Valid requests are forwarded to a cluster of WEM runtime servers. There are separate WEM instances for Staging and Live and for geographic/geopolitical regions.
4. The required WEM model information is retrieved from the WEM Runtime Model database.
5. The requested functionality and required data is provided to the WEM Runtime server where it is processed.
6. The WEM Runtime server provides an SSL encrypted HTML session back to the Modeler user.

There are four distinct and completely separate WEM environments to enable continuous development and operation. These complete instances are not connected in any way, no communication is possible between them and no services or data are shared.

The development environment normally exists in multiple simultaneously active versions depending on the current development projects.

Production and DR have multiple instances of the complete environment in various geographic and geopolitical locations.



2.2.3 Networks

Every network connection is “for purpose” only and where possible separate logical networks are used to further limit non-required communications. Routing is disabled on all devices and both incoming and outgoing firewall restricting traffic to and from other devices is managed on both device and port level.

2.2.4 Server setup

All WEM servers, both modeler and runtime are completely stateless, all session status and all user models and data are stored on the database servers only.
All servers are updated to the latest version of any installed software.
All data is backup up in real time with full backups occurring daily at minimum.
The WEM platform is developed to provide a scale-out growth path, new servers can de added or servers can be removed from a cluster without impacting the user experience and providing near linear growth.

2.2.5 Onboard safety features

Built in WEM, there are numerous measures in place. This document will only mention those measures ZoomBIM feels comfortable in sharing publicly. Should there be questions that are unanswered throughout this document, please contact us. Please note that some of the security information can only be provided under personal and specific NDA.

2.2.5.1 Authorization/Authentication

Access to any part of the WEM Modeler platform is provided by means of username & password.
Projects that are built by using WEM, can be provisioned with multifactor authentication.
Possible authentication technologies currently supported by WEM:

- Username password
- Challenge
- Captcha
- Geofencing
- Device qualifications
- IP/network firewalling
- Email code
- SMS code (using your own external provider)

WEM supports single sign on (SSO) support for the SAML and OAuth protocols for all applications created with WEM.

2.2.5.2 SSL

The WEM platform supports SSL (HTTP**S**), for the modeler and preview environments this requirement is enforced by the platform, for staging and live the option is provided but can be optionally disabled per portal to provide compatibility with your equipment or software that does not support the SSL standards.
By default strong encryption is selected if supported by the client device accessing the WEM environment. For compatibility reasons lower encryption standards are also supported to enable older devices and software to access your WEM projects.

2.2.5.3 Hash

By default WEM password are Hashed. No one who uses WEM on any level is able to access passwords of any kind, used in our WEM Projects or used to access WEM Modeler. We do not store passwords in plaintext or other human readable formats and the used hash protocols are single direction only.

Within you own WEM project, it is possible to Hash database content using SHA256, SHA512, and other standards.

2.2.5.4 API – SOAP – Rest – oData

WEM offers several options to connect to other date sources through API's. Per API and per runtime environment it is possible to enable certificates or username/password security as well as require SSL encryption. Certificates can be generated within/by the WEM Modeler.

2.2.5.5 Blueprint

The Blueprint is a build-in security mechanism that will create expectations regarding data consumption based on the accessed WEM project and current context. This expectation will be compared with data requests, both input and output, and anything that doesn't match expectation, will be discarded.

2.2.6 Code Review

All WEM software is developed in house by employees working to strict guidelines. Before any code is committed to production all projects will be reviewed by team members for:

- Efficiency;
- Quality;
- Fit for function;
- Impact on existing code;
- Security;
- Performance.

2.2.7 Matrix isolation

Look at our setup as rows and columns.
Each row is an online environment
Each column is (in most cases) a cluster of servers which can be duplicated on demand, depending on server load. We call this 'Matrix Isolation' because each environment is completely isolated from the environment next to it.

Serverpark setup

Online environments	AD	Wsus	Modeler App - DB	Preview App - DB	Staging App - DB	Live App - DB
Development	✓	✓	✓	✓	✓	✓
Test	✓	✓	✓	✓	✓	✓
Prod	✓	✓	✓	✓	✓	✓
DR	✓	✓	✓	✓	✓	✓
SW Development	✓	✓	✓	✓	✓	✓
Office	✓	✓	✓	✓	✓	✓
O365	✓	✓	✓	✓	✓	✓

3 Physical

Besides the technical security, several physical measures are in place to ensure our (and your) data is secure.

3.1 Storage of data

Just like other browser based web application there is no storage of data on the local device beyond what is currently displayed on the screen. WEM Project models and data are always only stored on the WEM database cluster you are currently working with and only accessible through your WEM project.

When using the native application option of the WEM platform (available Q3 2018) there may be local storage of data on the device for offline use. This data is encrypted locally and normally only available to access using the purpose build WEM application.

3.2 Storage of WEM platform code

No source code is stored on any local device, used to develop WEM. The development environment is completely virtual and only accessible to authorized personal through strong encryption and authentication.

Local devices are where applicable equipped with hardware encryption devices and employ full drive encryption for all storage.

3.3 Physical access

Access to the ZoomBIM building and the office floors is restricted. People only have purpose assigned keys which allows access to rooms and floors they require.

3.3.1 Host buildings

Access to buildings where data and logic is stored is restricted. Access is only allowed by appointment and only for people who are known.

ZoomBIM it's distributors, partners and clients do not have access to the physical locations hosting the applications.

4 People

Regarding Safety & Security, people are our most critical and precious factor.

4.1 Background check

Every WEM employee we know to be trustworthy for every person we onboard is subjugated to a background check which consists of reaching at least two referents. A statement of conduct of good behavior issued by the Dutch authorities is required in order to work at ZoomBIM/WEM.

4.2 Employment Agreement

Every employer's contract includes standard paragraphs on responsibilities on secrecy, security and intellectual property.

4.3 Employee Manual

A key part of the every employment agreement is the Employee Manual which documents expected behavior and requirements in key situations. This includes subjects including:

- Data leakage procedure;
- Intellectual property and Secrecy;
- How to act on Data Security;
- Behavioral code on social media

These topics will still be effective, even when leaving the organization.

There are also measures in place to help people make the right decisions when tempted by external influences.

5 Risk Management

5.1 Proactive vulnerability assessment

On a regular base but at least every 6 months a proactive assessment on our safety measures is conducted. All parties that are involved around Safety & Security will gather and review all aspects of our logical, physical and procedural safety, security and data.

As part of this review new developments in state of the art as well as possible new threats are reviewed and assessed for impact and applicability.

Results from this review are commonly further research or active improvement efforts carried out by individual team members with results reported back to the full group.

5.1.1 Penetration Tests

To be able to trust on our inhouse expertise, we invite a partner to perform penetration tests on a regular interval but at least monthly.

Several different penetration tests are performed on both the WEM modeler and runtime environment testing both the infrastructure as well as the WEM projects application security for numerous known attack vectors. Any findings are processed and countered resulting in an immediate re-test.

Customers can request a Pentest on their specific projects, but by default only on our Staging environment to prevent performance issues on our live environment. Our Staging environment is of course an exact match to our Live environment. The customer will be charged for the cost of these customer specific WEM project pen tests.

5.1.2 Uphold Knowledge

All of our employees (involved in Safety & Security) actively keep their knowledge on applicable topics up-to-date and are given the time and budget to do so as part of their regular work duties.

5.2 External Factors

Security is an ever-evolving area and new information and threats can come to our attention at any time. All periodic review described in this document and all existing measures to ensure security, safety and privacy of data can and will be updated at any time if and when we received new or updated information that challenged our current solutions. This is a reactive policy as you can not plan for unknown events.

5.2.1 DDOS

A DDOS attack is a typical event that cannot be predicted but we can anticipate on. There are mechanisms that quickly recognize an attack and take counter measures immediately, without human interaction.

DDOS and similar attacks are a constant in the normal day-to-day operation of the WEM platform, we have taken numerous steps to ensure that the impact of these external factors is minimized, including;

- Multiple network paths
- Active and reactive filtering early in the process
- Data abstraction layers to easily recognize malformed request
- Over provisioned capacity
- And others.

We will not discuss the details of these security measures as those would provide potential attackers with potential knowledge to perform a precise disruption attempt.

5.2.2 Viruses and mall-ware

Creators of viruses are always ahead of the game for one cannot react on something that isn't there yet. Therefor it is important to select an antivirus company with the shortest reaction time and that is exactly what WEM did.

Because of the single function setups of all of the serves in the WEM environment the likelihood if virus or malware infection is small, we have however taken the necessary precautions to limit the risk and limit the impact if such an event may occur.

5.3 Disaster Recovery

Disaster can always strike at a moment one least expects. Such an event is impossible to predict and so we don't try. What we did do however is setup a system that seamless takes over should our entire infrastructure fail.

The key infrastructure is hosted in at least 2 active sites at any one time, the DR infrastructure is hosted with another provider and completely separated, logically, legally and physically the DR infrastructure again is hosted in at least 2 active sites.

5.3.1 WEM Waarborg

As a failsafe, WEM uses a totally different environment which is a shadow setup of our production environment. This mirrors with a 15 second delay all of WEM consisting of our company valuables as well as all of our customer data.

This environment is managed by an independent trust, WEM Waarborgfonds, that provides continuity of services in case of operational, legal or financial issues with the ZoomBIM holding group of companies.

All customers that have signed on to the no-cost standard SLA are covered as part of the DR and WEM Waarborg services.

5.3.2 Backup

Besides de WEM Waarborg, we keep backups:

- Once an hour – Transactional backup
- Once a day – Differential backup
- Once a week – Complete backup

We keep our backups for 28 days.

5.4 OWASP

The **O**pen **W**eb **A**pplication **S**ecurity **P**roject
"Online community in the field of web application security"

Nr.	Topic	Description	WEM Response
1	Injection	Adjust queries to execute commands	WEM has a validation mechanism that excludes such interference.
2	Broken Authentication and Session Management	exploit implementation flaws to assume other users' identities	WEM Platform: we use 'Salt' and 'Pepper' WEM Project: Solution Template
3	Cross-Site Scripting	Abuse Browser ability to script to hijack user sessions.	Filter scipts + 'Escaping' to show, not execute script
4	Broken Access Control	Case: A Datagrid with a delete button in a conditional.	Blueprint.
5	Security Misconfiguration	Good security requires having a secure configuration defined and deployed	User Knowledge, discipline, combined with common sense are stored in WEM (Deploy user)
6	Sensitive Data Exposure	Common sense is to use SSL in projects.	On WEM domains we use SSL by default.
7	Insufficient Attack Protection	…	Detecting strange and unusual behavior is handled by statistics in our dashboards.
8	Cross-Site Request Forgery (CSRF)	A CSRF attack forces a logged-on victim's browser to send a forged HTTP request…	Blueprint.
9	Using Components with Known Vulnerabilities	Exploited vulnerable components (libraries, frameworks), run with the same privileges as the application, can facilitate data loss or server takeover.	Requests pass multiple systems (firewalls, reversed proxys, back end webservers). False requests only pass when all of these have the same vulnerabilities.
10	Underprotected APIs	APIs (SOAP/XML, stop/JSON, RPC, etc.)are often unprotected and contain numerous vulnerabilities.	Blueprint.

Ad. 1 - Injection
Injection flaws, such as SQL, OS, XXE, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization

WEM Response
User interaction between WEM and the database could be 'enriched' with extra commands. WEM has a validation mechanism that excludes such interference.

Ad. 2 - Broken Authentication and Session Management
Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities (temporarily or permanently)

WEM Response
WEM Modeler. No passwords are stored in plain text.
Besides that, we use 'Salt' and we use 'Pepper'
WEM Project: my.wem provides a basic 'Authorization and Authentication Project' which is safe.
One could expand this project with 'Two Phase authentication'.

Ad. 3 - Cross-Site Scripting (XSS)
XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user supplied data using a browser API that can create JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites

WEM Response
Modern browsers are able to script. Therefore free text could be used for executing unattended/unwanted/unauthorized actions. Sending someone your script to an authorized person with proper authorization could cause script execution.
WEM filters scripts (not 100% proof)[]+() used to be enough to execute commands.
Script filtering is nog 100% proof. Therefore WEM has a mechanism that show scripts ('escaping') instead of executing them.

Ad. 4 - Broken Access Control
stoprictions on what authenticated users are allowed to do are not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

WEM Response
Case: A Datagrid with a delete button in a conditional.
Click results in request on specific row. One could fake a request to delete all.

WEM renders each page with a blueprint (rendered, based on what's on the screen) containing all that is supposed to happen on that page. WEM matches this blueprint with the delivered input and anything that doesn't fit the expectation, does not get through.

Ad. 5 - Security Misconfiguration
Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, platform, etc. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.

WEM Response
This is mainly user interaction. knowledge and discipline is key, combined with common sense. All these experiences are stored in WEM so the WEM expert doesn't need to have them.
For example: WEM has a 'Deploy User' with just enough authorization to do just that.

Ad. 6 - Sensitive Data Exposure
Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at stop or in transit, as well as special precautions when exchanged with the browser.

WEM Response
Common sense is to use SSL in your projects.
On WEM domains we use SSL by default.
For any other domain we'll arrange it for you on request (a feature which will be automated in the future).

Ad. 7 - Insufficient Attack Protection
The majority of applications and APIs lack the basic ability to detect, prevent, and respond to both manual and automated attacks. Attack protection goes far beyond basic input validation and involves automatically detecting, logging, responding, and even blocking exploit attempts. Application owners also need to be able to deploy patches quickly to protect against attacks.

WEM Response
Detecting strange and unusual behavior is handled by statistics in our dashboards.

Ad. 8 - Cross-Site Request Forgery (CSRF)
A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. Such an attack allows the attacker to force a victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

WEM Response
For applications where one is always logged on (Facebook). A script could be forged for use within ones user rights.
In WEM: If it does not match the rendered blueprint (from what's on screen), it will not be executed but merely displayed as plain text.

Ad. 9 - Using Components with Known Vulnerabilities
Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

WEM Response
The issue here could be, 'how do you prepare for what is unknown'? So, we don't use such components.
Requests to our servers pass multiple systems (firewalls, reversed proxys, back end webservers). False requests only pass through when all of these have the same vulnerabilities (which they haven't).

Ad. 10 - Underprotected APIs
Modern applications often involve rich client applications and APIs, such as JavaScript in the browser and mobile apps, that connect to an API of some kind (SOAP/XML, stop/JSON, RPC, GWT, etc.). These APIs are often unprotected and contain numerous vulnerabilities.

WEM Response
We have our blueprint.