INSTRUCTIONS

Security hardening guide

Reverse Proxy

- Consider a DMZ with a reverse proxy
- Tune a rate limiter to mitigate DDOS attacks: https://www.nginx.com/blog/rate-limiting-nginx/
- Consider using a web application firewall (WAF)
- Set-up NAT hairpinning for internal traffic
- SSL termination on your reverse proxy is only suitable when unencrypted traffic between your reverse proxy and Live's NGINX server is acceptable (for example if they coexist on the same server, with Live's NGINX only listening on localhost).

Reverse Proxy Configuration

- To prevent Live from triggering the brute-force protection incorrectly your reverse proxy **must** forward the client's IP to the Live server using the header `X-Forwarded-For`
  The IP of the reverse proxy **must** also be added as a regular expression to Tomcat's configuration file `conf/server.xml`: look for the element `Valve` of class `RemoteIpValve` and set the IP in the attribute `internalProxies`. Check Tomcat's documentation for further details on the syntax to be followed for this attribute.
- Prevent Cross-origin attacks setting HTTP Headers
  - `X-Frame-Options: SAMEORIGIN`
  - `Content-Security-Policy: default-src ‘self’;`
- Disable Reverse Proxy's version header printing
- Introduce any SSL Hardening settings deemed necessary from the following section.

SSL Hardening

- Only allow TLS >= 1.2
- Strong Diffie-Hellman Parameters (4096 bit)
- Use a strong key for the certificate (RSA 4096 bit)
- Disable weak ciphers (use verifier tool below to identify weak ones)
- Enable HTTP Strict Transport Security
- Verify SSL hardening and check cyphers: https://www.ssllabs.com/ssltest/index.html

BORM-INFORMATIK AG
03.03.2022

INSTRUCTIONS

Security hardening guide

User-based access control

- Create and configure a separate non-privileged Windows user for running the Tomcat service
    - This user must also have rights to execute BGBormScriptServer.exe from bin\ subdirectory of Borm/Evo
    - Read/Write access to Borm/Evo folder
    - Read/Write access to configured Temp folder (as configured in META_WEB_SETTINGS) and IMG_CACHE folder (by default under Temp folder)
    - Read/Write access to Tomcat program folder
    - Read/Write access to %PROGRAMDATA%/Borm
    - Read/Write access to DOKV folders if you want to allow document viewing/editing/uploading with Live
    - Read access to SSL certificate keystore (if applicable/necessary)
- Create another non-privileged Windows user for running NGINX service (if applicable)
    - This user should have read access to SSL Certificate files when used to provide SSL termination for Tomcat
    - This user should also have Read/Write access to the NGINX's folder and to Read/Execute the NSSM executable
- Further hardening is available and can be discussed for each customer on request

Database connection

- Create a dedicated low-privileged SQL user for Tomcat to connect to SQL Server
- Restrict this SQL Server user's rights (Read/Write) to the BORM Database and TempDB only
- Adjust connection parameters in Tomcat's context.xml to use this dedicated SQL user
- Adjust the ODBC Connection for the Windows user which runs Tomcat, so that these use the dedicated SQL user
- Further table-level hardening is available but customer-specific and can be discussed on request