hvg Állásbörze

Firewall and IT security information

URL: https://allasborze.hvg.hu

Modules affected by IT security issues:

- Firewall settings
- Chat&videochat
- Webinars
- Website

17-19 April 2024

Firewall settings

The Online Job Fair uses external modules as well. In order to reach these modules by a computer and by the company admin user, the firewall of the given computer and/or the local network the computer uses, needs to be set up properly by the IT administrator of the company.

The firewall must be properly set up to enable two-way communication with the following componennts:

Google Firebase (Website operation and storage)
*.googleapis.com

Talkjs (chat component)
https://app.talkjs.com/
https://cdn.talkjs.com/talk.js

Videochat
https://daily.co
(in and outcoming data enablement) webRTC – this is the technology that the service uses P2P (peer to peer) – this must be also enabled on the firewall to make the videochat event possible

Forum (shared chatroom)
https://talk.hyvor.com
https://hyvor.com
*.hyvor.com – this doman with all its subdomains need to be opened ont he firewall

Web services
Besides all the above, you need to enable the following urls, too:
https://hvg-allasborze-backend.herokuapp.com
https://hvg-allasborze-service.herokuapp.com
https://gstatic.com/
https://bootstrapcdn.com/

Chat, videochat

We use the **TalkJS** application for the chat service. TalkJS stores the chat messages. To send chat messages, the websocket technology must work.

Security info:

Chat:
https://talkjs.com/resources/article/what-about-user-data-security/

Videochat:
https://hyvor.com/privacy-policy

For authentication and data storing we use **Google Firebase**.

Security info:
https://firebase.google.com/support/privacy

Webinars

We use the **Cisco Webex** solution for the webinars. It works in **browsers** and via **desktop/mobile application**.

The IT security info are given by the service provider:

Zero-Trust Security for Webex White Paper

https://www.cisco.com/c/en/us/solutions/collateral/collaboration/white-paper-c11-744553.html

Cisco Webex Security

Webex Security and Strong Encryption - Cisco

Cisco Webex Meetings Security

Cisco Webex Meetings - Cisco Webex Meetings Security - Cisco

Webex | Installation and Automatic Upgrade

Webex App - Installation and automatic upgrade

A default 80/443-s portokat használja a böngészőben és a kliensként futó alkalmazás is.

https://www.dell.com/support/kbdoc/hu-hu/000136478/how-do-i-allow-webex-meetings-traffic-on-my-network

Webex website, Webex Desktop App/Productivity Tools, Webex Meetings for Android/iOS, Webex Web App				
Protocol	**Port Number(s)**	**Direction**	**Access Type**	**Comments**
TCP	80 / 443	Outbound	Webex Client Access port	The Webex Client makes the majority of its data transfers and loading using HTTPS over port 443. In some cases, port 80 will also be used before being redirected to a secure connection.
TCP/UDP	53	Outbound	DNS	In order to connect to Webex you must have a working DNS server. Most DNS queries are made over UDP; however, DNS queries may use TCP as well.
UDP	9000	Outbound	Webex Client Media for Webex Events (Audio Streaming)	Webex utilizes port 9000 for the Webex Events Audio Broadcast feature. If unable to connect, it will use TCP 443.
UDP	9000	Outbound	Webex Client Media (VoIP and Video RTP)	The Webex client will try to connect to a Multimedia server over UDP port 9000. If unable to establish a connection over UDP 9000, it will use TCP port 443. Due to the nature of TCP and how lost delayed packets are retransmitted, it is not recommended to use TCP. We recommend allowing UDP port 9000 whenever possible. (This media is sent over standard RTP. Firewalls should not manipulate the RTP being sent or received.)
TCP / UDP	Operating System Specific Ephemeral Ports	Inbound	Return traffic from Webex	Webex will communicate to the destination port received when the client makes its connection. A firewall should be configured to allow these return connections through.

Website application

The HVG Online Job Fair website uses only cloud based services, and only European, EU-West-1 region (GDPR compilant) servers, therefore third party IT sercurity solutions work in every case. We use **HTTPS TLS 1.2+** protocol.

Infrastructure: Amazon (AWS) and Heroku based on it

Cloud Security – Amazon Web Services (AWS)

Heroku Security | Heroku

Heroku Security, Privacy, and Compliance | Heroku Dev Center

Cloudflare - Gateway and security roles

Website Security | Services and Solutions | Cloudflare

AWS S3

Contents uploaded by partners are stored on AWS S3 (storage server)

Amazon S3 Security Features - Amazon Web Services