hvg Állásbörze

IT biztonsági információi és a működéshez szükséges beállítások

Az állásbörze weboldal url-je: https://allasborze.hvg.hu

Az állásbörze IT-biztonsági kérdéseket érintő moduljai, területei:

- Tűzfalbeállítások
- Chat & videochat
- Webinárium
- Website

2024. április 17-19.

Tűzfal-beállítások

Az online állásbörze weboldal külső szervereken elérhető komponenseket is használ. Annak érdekében, hogy ezek elérhetőek legyenek a céges adminok számára, a céges számítóképek tűzfalát fel kell készíteni arra, hogy ezeket a külső webhelyeket ne blokkolja, hogy a céges admin tudja használni a szolgáltatásokat.

Az állásbörze céges userei számára a tűzfalat a következő oldalak felé (oda-vissza kommunikáció) kell megnyitni:

Google Firebase (Weboldali működés és tárhely)
*.googleapis.com

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

Videochat
https://daily.co
(ezen a domainen jövő és menő adatoknak át kell jutniuk a tűzfalon)
WebRTC technológiát alkalmaz a szolgáltatás. P2P (peer to peer) kapcsolaton keresztül megy a videóhívás, ezt is engedélyezni kell a céges tűzfalakon.

Fórum (közös chat fal)
https://talk.hyvor.com
https://hyvor.com
*.hyvor.com – érdemes a domaint minden aldomainnel együtt átengedni a tűzfalon

Webszolgáltatások
A fentieken felül engedélyezni kell az következő két urt-t is:
https://hvg-allasborze-backend.herokuapp.com
https://hvg-allasborze-service.herokuapp.com
https://gstatic.com/
https://bootstrapcdn.com/

Chat, videochat - biztonsági információk

A chat funkcióhoz a TalkJS alkalmazást használjuk. A **TalkJS** tárolja a user chat üzeneteit. A chat üzenetek sikeres továbbításához a websocket technológiának kell működnie (mint minden instant messaging szolgáltatás esetén).

Biztonsági információk:

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

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

Az autentikácó kezelésére, a felhasználói adatok és CV-k tárolására a **Google Firebase**-t használjuk.

Biztonsági információk:
https://firebase.google.com/support/privacy

Webinárium - biztonsági információk

A Webinárium szolgáltatáshoz a **Cisco Webex** megoldását használjuk. A Webex működik **böngészőben** és **desktop- valamint mobil alkalmazással** is.

A biztonsággal kapcsolatos információk mindkét eszköz használata során a Cisco által alkalmazott szigorú security megoldások érvényesek:

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.

Weboldali alkalmazás - biztonsági információk

A HVG online állásbörze weboldal kizárólag felhő-alapú szolgáltatásokat használ, ezen belül is európai, EU-West-1 régiós (GDPR compilant) szervereket, ezért a harmadik-feles IT security megoldások érvényesek minden esetben.
A **HTTPS TLS 1.2+** protokollt használjuk.

Infrastruktúra: Amazon (AWS) és az arra épülő Heroku
Cloud Security – Amazon Web Services (AWS)
Heroku Security | Heroku
Heroku Security, Privacy, and Compliance | Heroku Dev Center

Cloudflare - Gateway és biztonsági szerep
Website Security | Services and Solutions | Cloudflare

AWS S3
A partnerek által feltöltött tartalom az AWS S3-on (storage szerver) tárolódik
Amazon S3 Security Features - Amazon Web Services