IS YOUR CORPORATE PORTAL SUFFICIENTLY PROTECTED?

GROUP IB

According to a study conducted by Group-IB, 84% of respondents switched to working from home (either fully or partially) as a result of the pandemic. At the same time, 71% of respondents provided employees with access to internal corporate systems and portals that are accessible online. Yet failure to comply with information security rules can create opportunities for attackers to infiltrate the organization's local network...

	Take our quiz and find out whether your corporate portal is sufficiently protected	**Yes**
1.	Does your company use reCAPTCHA v3 to protect against bots (if the corporate portal is accessible online)?	☐
2.	Does your company use a firewall (WAF) to protect web applications?	☐
3.	Does your company use a solution to protect against DDoS attacks (if the corporate portal is accessible online)?	☐
4.	Does your company use separate servers for different purposes, i.e. front-end and back-end operations or applications?	☐
5.	Was an external audit or penetration test conducted in the last 6 months?	☐
6.	Does the company require two-factor authentication (2FA) to access personal accounts?	☐
7.	Are databases stored in encrypted form, even at rest (Encryption at Rest)?	☐
8.	Is HTTPS SSL/TLS version 1.3 used to access the portal?	☐
9.	Does your company use any systems for analyzing behavioral profiles? (i.e. does authentication involve analysis of a user profile that is the same for all channels of interaction with an online resource; if the profile is different, the system will require additional confirmation of access).	☐
10.	Are portal access logs, system logs, and web server application logs stored for a long time (e.g. 1 month) on separate storage media and are they analyzed automatically?	☐

	Take our quiz and find out whether your corporate portal is sufficiently protected	**Yes**
11.	Does your company monitor the health of equipment and services responsible for the portal's operation by means of automated services such as Zabbix (including monitoring of the following indicators: disk, memory, processor, and the health of web server services)?	☐
12.	Does the web server run under a separate account with limited access rights to prevent attack propagation if the server is compromised?	☐
13.	Is the web server located in a separate network segment (DMZ) that is not connected to the corporate network infrastructure and corporate services?	☐
14.	Does your company use stored procedures (as opposed to direct SQL queries) to interact with databases?	☐
15.	Does your company use session tokens and other means (e.g. CSRF tokens) to prevent replay attacks and other similar threats?	☐
16.	Has your company introduced a policy to back up databases and the website itself in two modes: full backup (e.g. weekly) and incremental backup (e.g. daily)?	☐
17.	Does your company follow the 3-2-1 rule for all backups: keep at least 3 copies of your data, and store 2 backup copies on different storage media, with 1 of them located offsite?	☐
18.	Does the company have a backup site and a Disaster Recovery Plan in place that will be activated if the main site is unavailable? Is the plan reviewed regularly (e.g. monthly)?	☐

Check your result:

0-12 Your corporate portal is not protected!

Uh-oh, it looks like you need to urgently review your security policies and procedures... We recommend that you get in touch with information security specialists. Additional information on how to protect your online resources can be found at

www.group-ib.ru/secure-portal.html

13-16 Your corporate portal is not sufficiently protected,

but you're on the right track. You have already taken many steps to optimize security levels – keep it up! Yet there is still room for improvement in your security policy. We recommend that you regularly exchange information with professionals from your industry. If you think it might help, feel free to contact us and find out who to get in touch with for additional advice:

sp@group-ib.com

17-18 Your corporate portal is sufficiently protected.

Congratulations! You are proficiently versed in cybersecurity trends and clearly understand the processes required to ensure information security. Don't let your guard down, though. Attackers are always coming up with new ways to compromise infrastructures. Keep up-to-date with the latest information by visiting Group-IB's website and the StayCyberSafe portal