Discussion Post: You are the CISO for a publicly traded company. What protections would you implement to ensure availability of your systems and why?

If i were the CISO of a publicly traded company I would ensure availability by using redundancy and access control, and by ensuring systems remain up-to-date in terms of security.

To support availability, I would emphasize redundancy and backups. Redundancy means having multiple critical components—such as servers, storage, or network paths—so if one fails, another can immediately take over and keep the service running. Regular backups ensure that important data is copied and stored safely, including an offsite or cloud copy, so the company can restore systems and data after events like hardware failures, ransomware, or accidental deletions.

Access control and least privilege are also important for availability. Strong authentication and role-based access ensure that only authorized users can make changes to critical systems, reducing the chance of mistakes or malicious actions that could bring systems down. Least privilege, where users and services get only the access they truly need, limits the damage if an account is compromised and helps keep systems online.

Finally, I would focus on regular updates and secure configuration. Keeping operating systems and applications up to date fixes known issues that attackers could exploit to crash systems or disrupt services. Secure configuration baselines, following guides such as those from NIST, help ensure systems are set up in a stable and hardened way from the beginning, reducing misconfigurations that might cause outages. Together, understanding availability in the CIA triad, using redundancy and backups, applying strong access control and least privilege, and maintaining good updates and configurations create a solid foundation for keeping systems available.