Risk matrix – Hackernews clone

Group E

	Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
Certain					
Likely	- Open ports - Public Github codebase			DDOS attack	
Possible		Jenkins/CI supply chain[i]		Database breakdown – data loss[ii]	Server breakdown – whole system offline[iii]
Unlikely	Developer fraud[iv]	Unwanted database *read* access[v]		- Exploited code - Unwanted CI-tools access - Unwanted data *modify* access	
Rare					Outage[vi]

Endnotes:

[i] As mentioned in our threat modeling, our continuous integration tools need to run some commands at 'sudo'-level with admin rights. This could potentially execute hazardous code directly in the server.

[ii] All of our data is simulated. So, while it's not a good thing if we lose data, it's not critical.

[iii] If our server providers (Hetzner or DigitalOcean) systems goes offline, that means so do ours.

[iv] A situation where one of our own developers compromises the system or the data to his own benefit.
[v] Again, our data is simulated. Therefore, the importance of keeping its details private is not very high.
[vi] If the datacentres that hosts our servers gets destroyed completely (earthquake, meteor attack, tsunami etc.), we lose the entire system.