SECURE CODE
WARRIOR

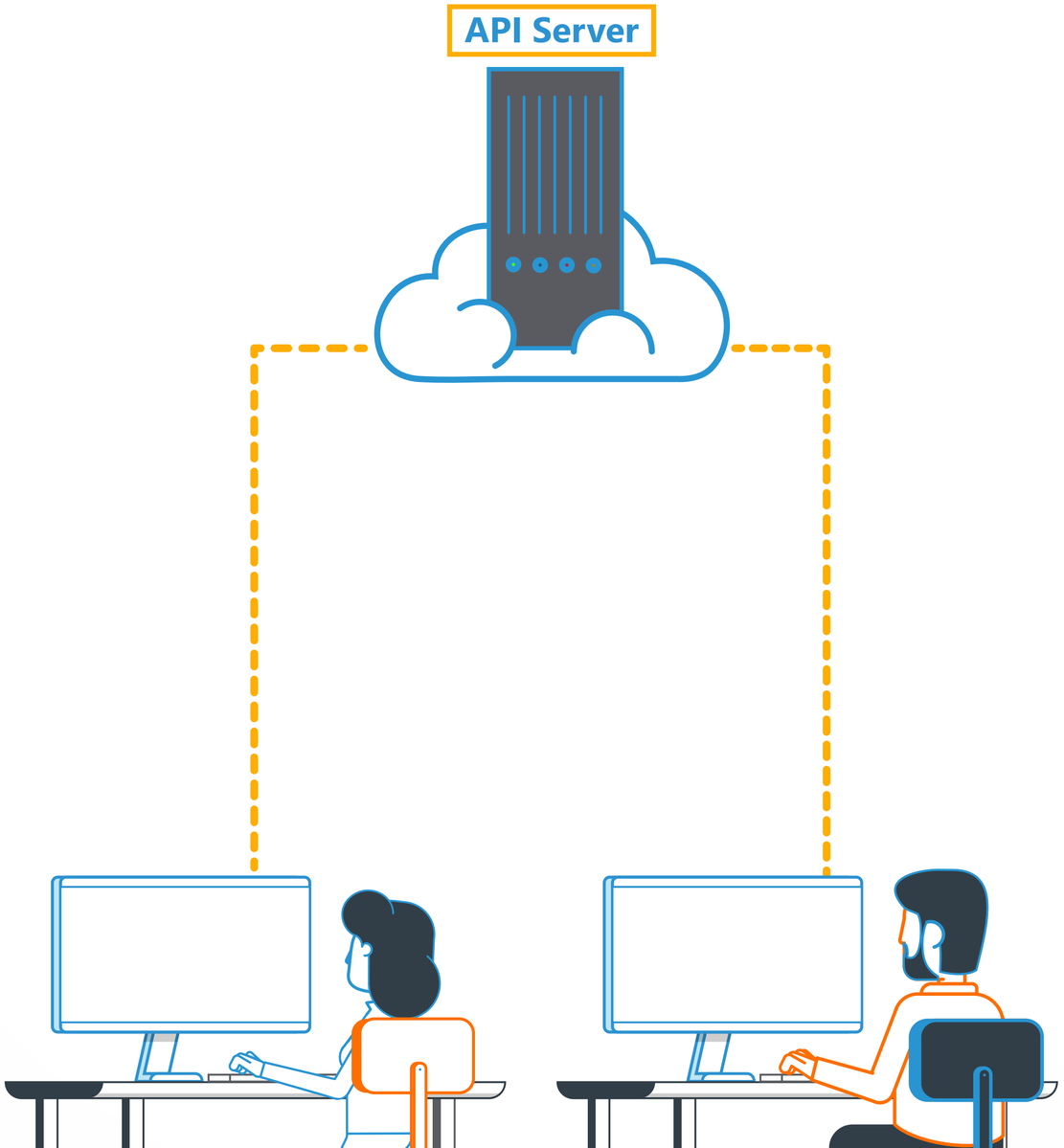
LACK OF RESOURCES & RATE LIMITING VULNERABILITY

We'll go through

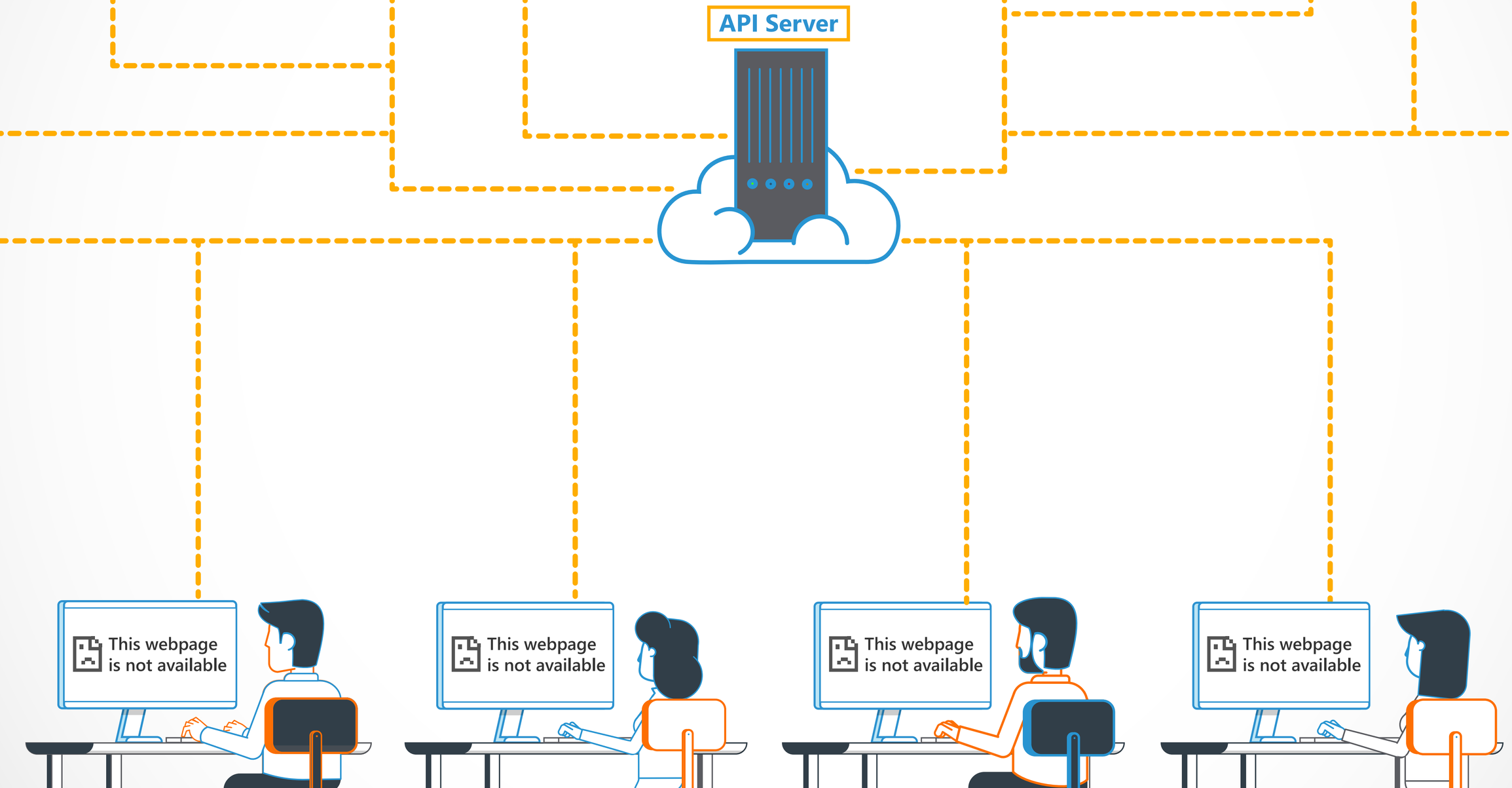
some causes and preventions of vulnerabilities in this category

THE LACK OF RESOURCES & RATE LIMITING VULNERABILITY AFFECTS APIS

All APIs have limited resources and are being called by multiple clients simultaneously.

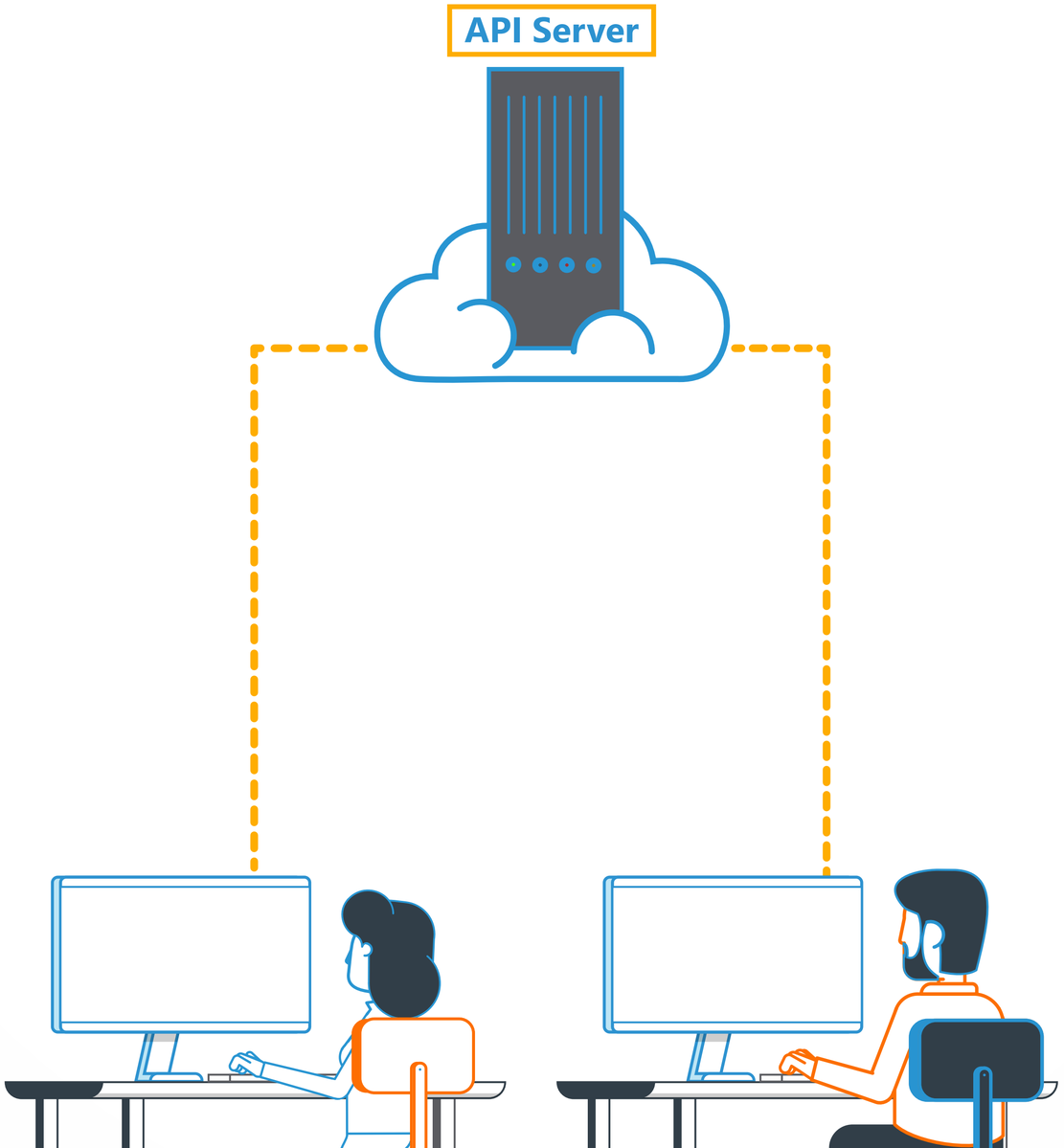


The risk occurs when the API is unable to effectively limit the number of requests or deliverables handled in a given time period.

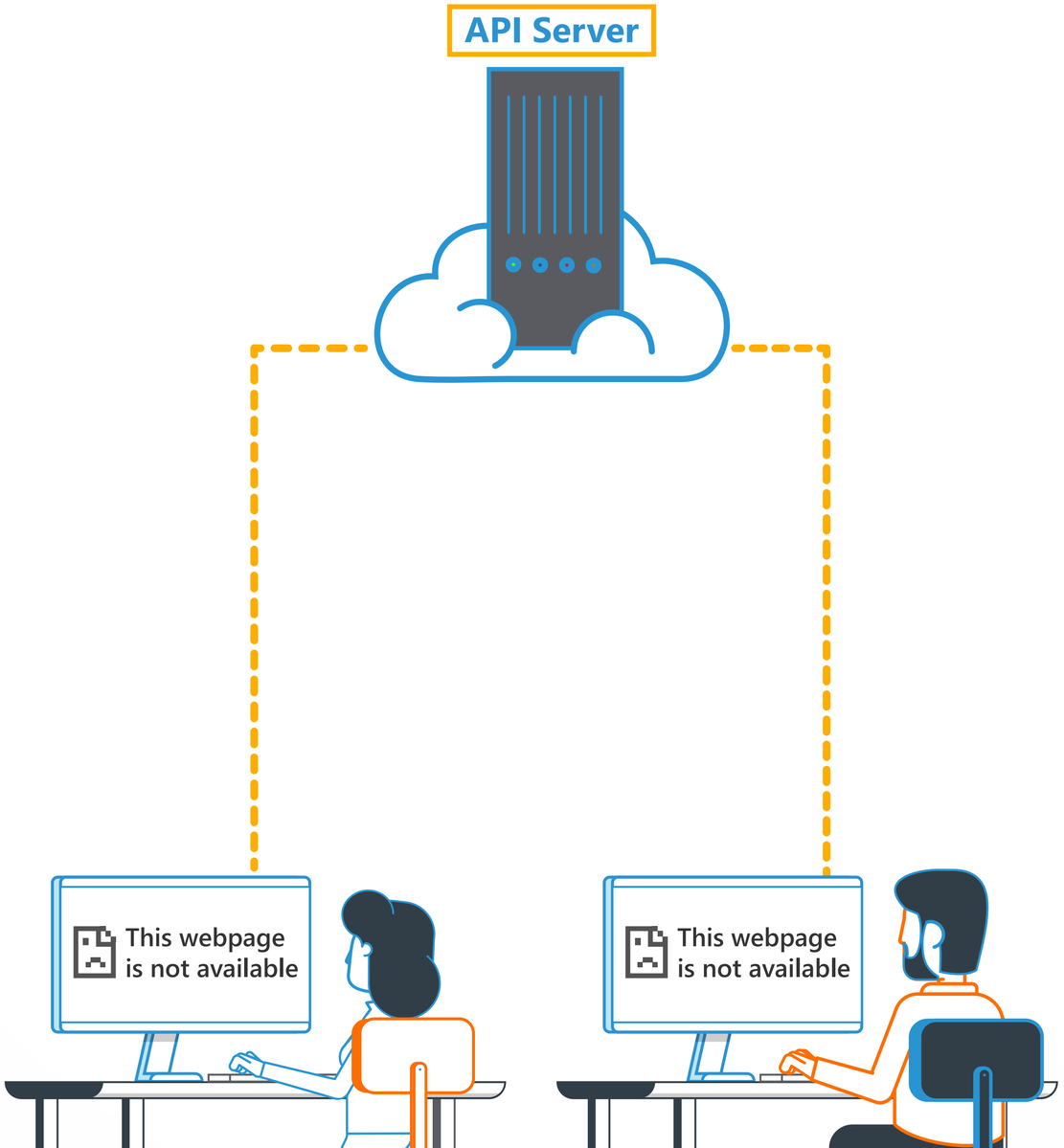


HOW CAN THE LACK OF RESOURCES & RATE LIMITING VULNERABILITY HAPPEN?

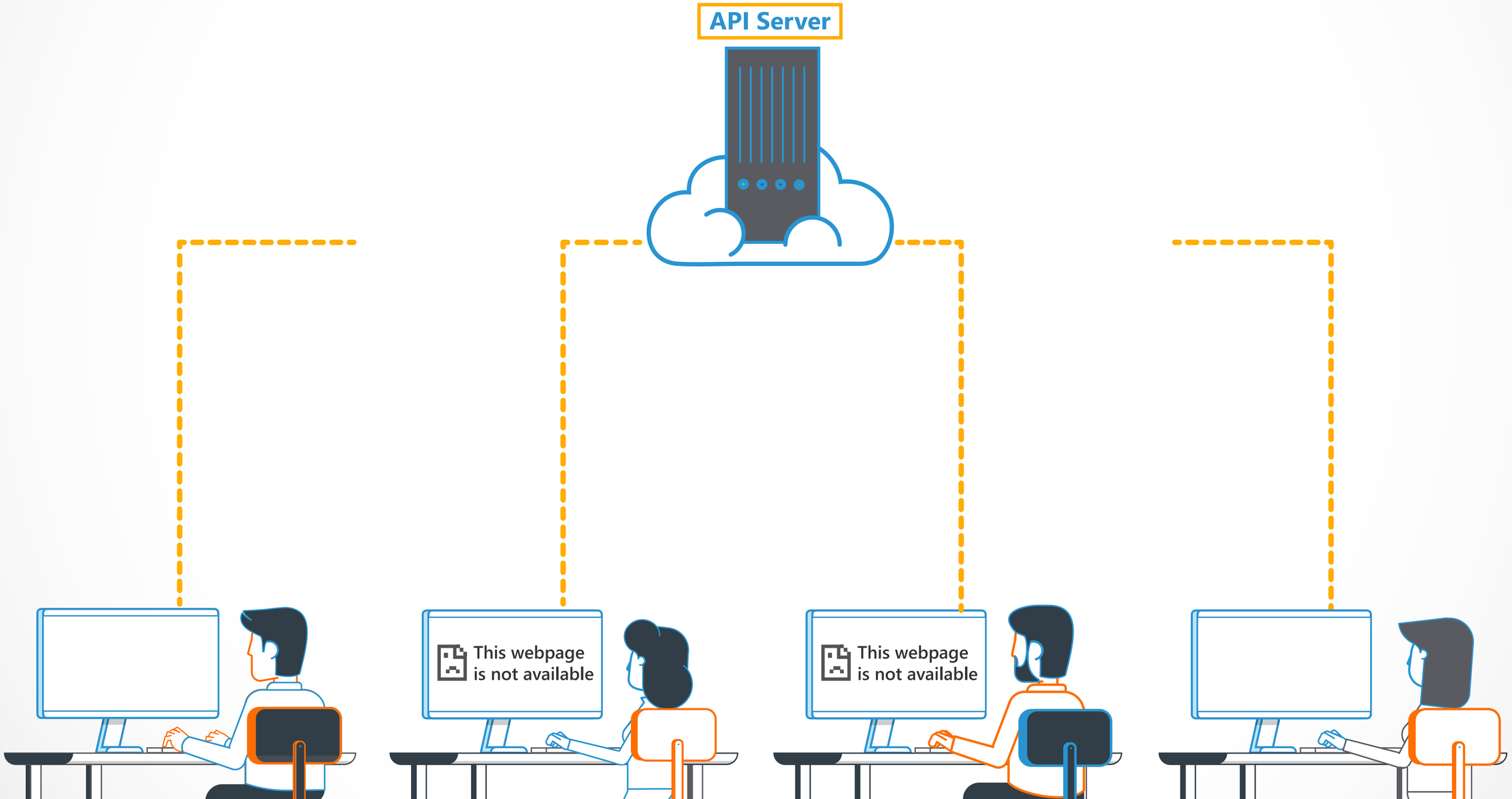
This vulnerability occurs when an API's rate limits or resource limits are not set correctly, or not set at all.



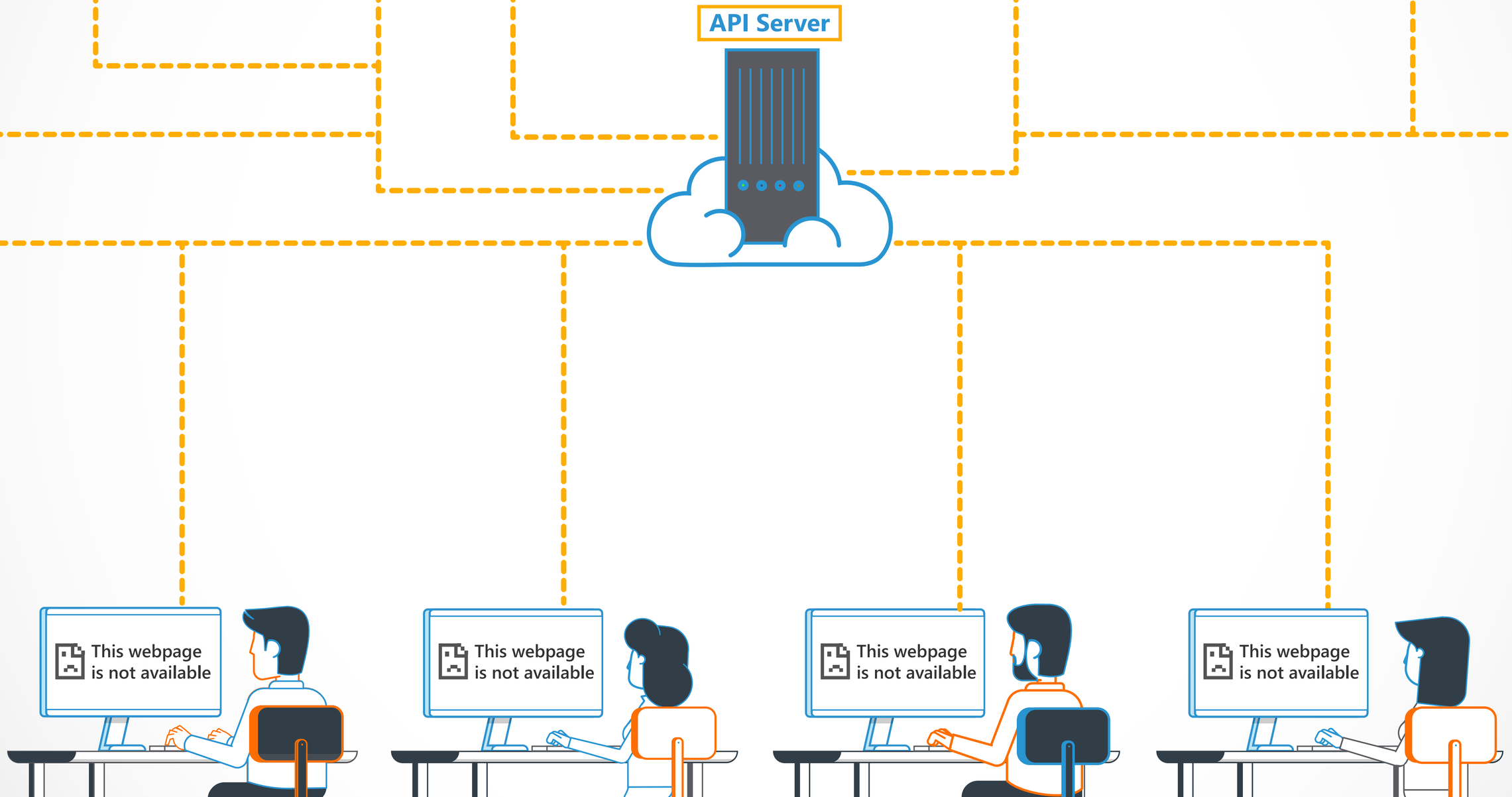
As a result, the API can become unresponsive or unavailable



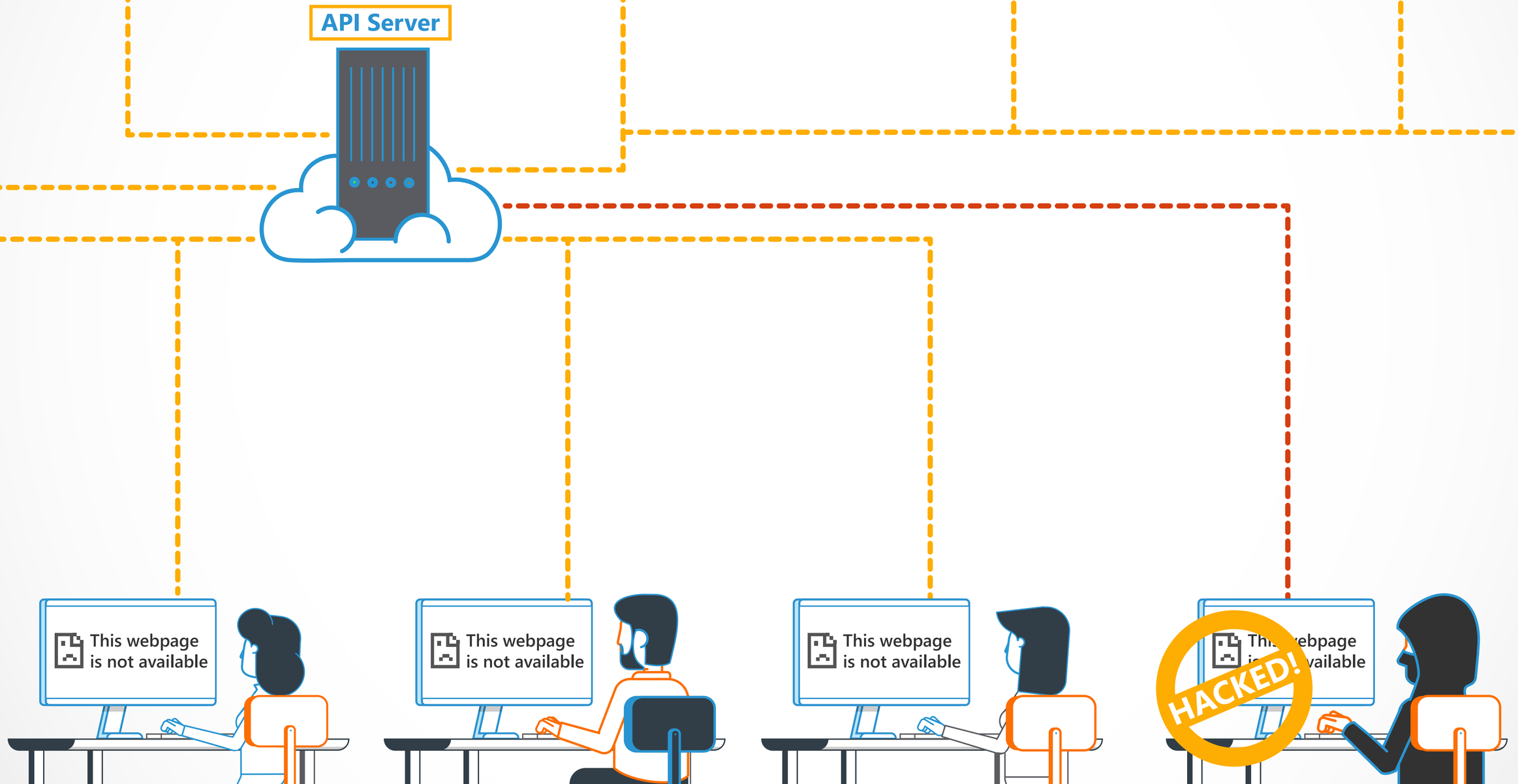
when overloaded with unexpectedly high traffic, or a spike in calls.



This could be because a company grows faster than anticipated or is experiencing a particularly busy season.



Alternatively, attackers can intentionally monopolise an API's resources by using malicious scripts.



To prevent Lack of Resources & Rate Limiting vulnerabilities, ensure the following limits are set properly:

- Execution timeouts
- Maximum allocable memory
- The number processes permitted within a defined timeframe
- Maximum number of file descriptors

To prevent Lack of Resources & Rate Limiting vulnerabilities, ensure the following limits are set properly:

- Maximum number of requests allowed per client
- The number of records per page, which can be returned per request
- Be sure to display a notification when these limits are met and include the time when the limit will be reset

Congratulations, you have now completed this module!

SECURE CODE
WARRIOR

www.securecodewarrior.com