**API Security Requirements:**

I choose to carry out this assignment considering the X API which enables access to data on the social network X. More specifically, among the different APIs that are available on the X site, I choose to analyse the API that enables access to public posts and replies. This API is used by developers to receive information about posts by searching for key words or requesting a sample of posts from given accounts. It is, e.g., used by NGOs like the UNO to counter misinformation about public health programs. [X, n. d.]

In order to keep this API secure, several protection mechanisms should be in place. Due to Nordic APIs (n. d.), the API should have transport layer security which is shown by having an httpts:// connection. This is a secure way of encrypting data transmissions over the internet.

While backend servers typically will have a limitation of the number of requests they can handle at the same time, it is important to ensure that the API is able to handle the traffic it is faced with at all times. Thus, it might make sense to limit the number of requests each individual can submit to, e.g., prevent DDoS attacks and ensure that all real user traffic can still be served. [Nordic APIs, n.d.] Furthermore, it is of importance to introduce a routing system to route approximately the same amount of traffic to each server. E.g., Google Cloud Armor, one of the most proficient products for the prevention of DDoS attacks, follows this approach which is called load balancing. [Google Cloud, n. d.]

A way of authenticating and authorizing the usage of the API must be defined. As Postman (n. d.) argues, in many cases it is important to ensure that different users get different permissions for how they are allowed to use the API. Here, it must me ensured that these different allocated roles are checked by keeping up a dedicated authentication and authorization structure. This is rather easy in the example of the X API. As the API enables the access to already publicly available information, no differentiation in the access level for different user groups is necessary. However, it is still necessary for X to track who accesses the API. Thus, due to X (n.d.) an application for the usage of the API is used before the data can be accessed and connected to other applications by users.

Postman (n. d.) furthermore stresses the importance of using Web Application Firewalls to validate inputs, sanitization and encoding for methods used in order to prevent malicious data from entering the workflow. This prevents attacks from causing harm at both the server side through SQL queries of harmful code or at the customer side by embedding harmful content in the HTML structure.

As the X API I am here considering does not enable a connection to sensitive data because it only presents a connection to already publicly available data, no additional encryption or masking of sensitive data is necessary in this specific example. However, as already mentioned this does not mean that any of the other security measures are less important than in a case where sensitive data would be handled.

**References:**

Google Cloud (n. d.) Cloud Armour Enterprise overview. Available from: <https://cloud.google.com/armor/docs/armor-enterprise-overview#:~:text=Google%20Cloud%20Armor%20offers%20the%20following%20options%20to,protection%20is%20configured%20on%20a%20per-region%20basis.%20> [Accessed 03. October 2024]

Nordic APIs (n. d.) Seven Must-Have Security Policies for Your APIs. Available from: <https://nordicapis.com/seven-must-have-security-policies-for-your-apis/#:~:text=Seven%20Must-Have%20Security%20Policies%20for%20Your%20APIs%201,Data%20...%207%207.%20Data%20Signature%20Verifications%20> [Accessed 03. October 2024]

Postman (n. d.) API Security. Available from: <https://www.postman.com/api-platform/api-security/#:~:text=Enforce%20security%20rules%20on%20API%20definitions%20and%20requests:%20Postman%20API> [Accessed 03. October 2024]

X (n.d.) About X’s APIs. Available from: <https://help.x.com/en/rules-and-policies/x-api#:~:text=When%20someone%20wants%20to%20access%20our%20APIs%2C%20they,from%20you%20before%20they%20can%20access%20your%20information>. [Accessed 03. October 2024]