BRIT

writing the future

learn more about APIs

Educating yourself on the importance of APIs can help you to have a better understanding of how data is consumed and how to protect for specific vulnerabilities. Getting your head around this terminology can be tricky. Luckily, Richard@Cygenta is on hand to share his thoughts on APIs and why they should be on your radar when discussing cyber security with your clients.

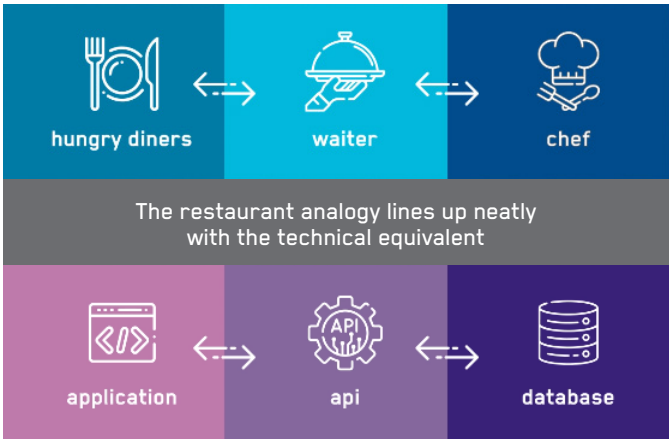
APIs defined

APIs have been around since the 1940s, yet they only really became used as we know them in the 1960s. Unfortunately, they've taken a while to become recognised for the powerful tool they are.

So, what is an API? In technical terms, it's an Application Programming Interface: a standardised communication method between computer systems or an intermediary between two applications.

The restaurant analogy

An effective way to build your understanding of how APIs work is with the restaurant analogy. A restaurant (service provider) offers meals (services) and needs a way to tell their customers (end users) what they offer. Since they don't want to let the customer into the kitchen to see their secret recipes, they share their services with a menu (documentation). The customer (API client) selects from the menu and tells the waiter (API call), who then relays the order to the chef (API server) and returns with the meal (API response) – all without the customer entering the kitchen.



The actual technology used to serve and respond doesn't matter: it's the standardised method that's important. Just as you can send Morse code via light or sound, it's the code itself that's important, not the process of sending and receiving.

continued

APIs strip away unnecessary code

Another considerable benefit of APIs is that they strip away everything that's not needed. For example, take a website that allows you to search for a recipe. The page is made from HTML and other code; it contains forms, photos and maybe adverts. A single page might be around 2-3MB once you add all the menus with JavaScript and CSS required to make it look appealing on screen. An API version of the same site has none of these: the API call requests a recipe – and only the recipe is sent back at a fraction of the size, amounting to a few kilobytes.

The fact that APIs deal only in the data actually needed makes them sleek and fast. They also have another invaluable benefit: flexibility for the end-user.

Take streaming media services such as Netflix, Amazon Prime or Disney+ as an example. They all offer the same type of data (movies and TV shows), searching and favourites lists, but they display the end results differently. What if you wanted to change the look and feel – and even the functions offered? If they provided direct access to their API, you could build any front-end system you wish. APIs simply provide the data; what you do with it is up to you – and no one is forced to use it in a specific way. Allowing end-users to do what they want creates innovation opportunities.

Security considerations for APIs

But what about the security considerations when building your own API? We've seen data breaches in the past due to a lack of API security from companies such as Facebook, Google, Venmo, T-Mobile and even the US postal service.

Most attacks against APIs are not the standard ones prevalent in web applications. They're mostly business logic flaws or access control failures. Automated tools tend not to pick up on these; hence professional testing should be sought.

The first step in helping secure an API endpoint is to require an API key. This is essentially a unique code given to the end application builder, which the API checks before processing the call. It's also important to document all endpoint functions – but not as important as checking what the function returns.
In the Facebook data breach, the API returned private data that exposed millions of users for over 20 months before it was fixed. Google's API breach resulted in a shutdown of Google+; T-Mobile users were victims of SIM-swapping.

So, whilst APIs are extremely powerful, just like any other technology, they require vigilance and security since a data exposure can be catastrophic.

We hope this article has been helpful in expanding your knowledge of APIs and how they need to be protected from cyber risks. If you want to find out more about how Brit can help your clients stay protected from cyber threats, check out our cyber security page.