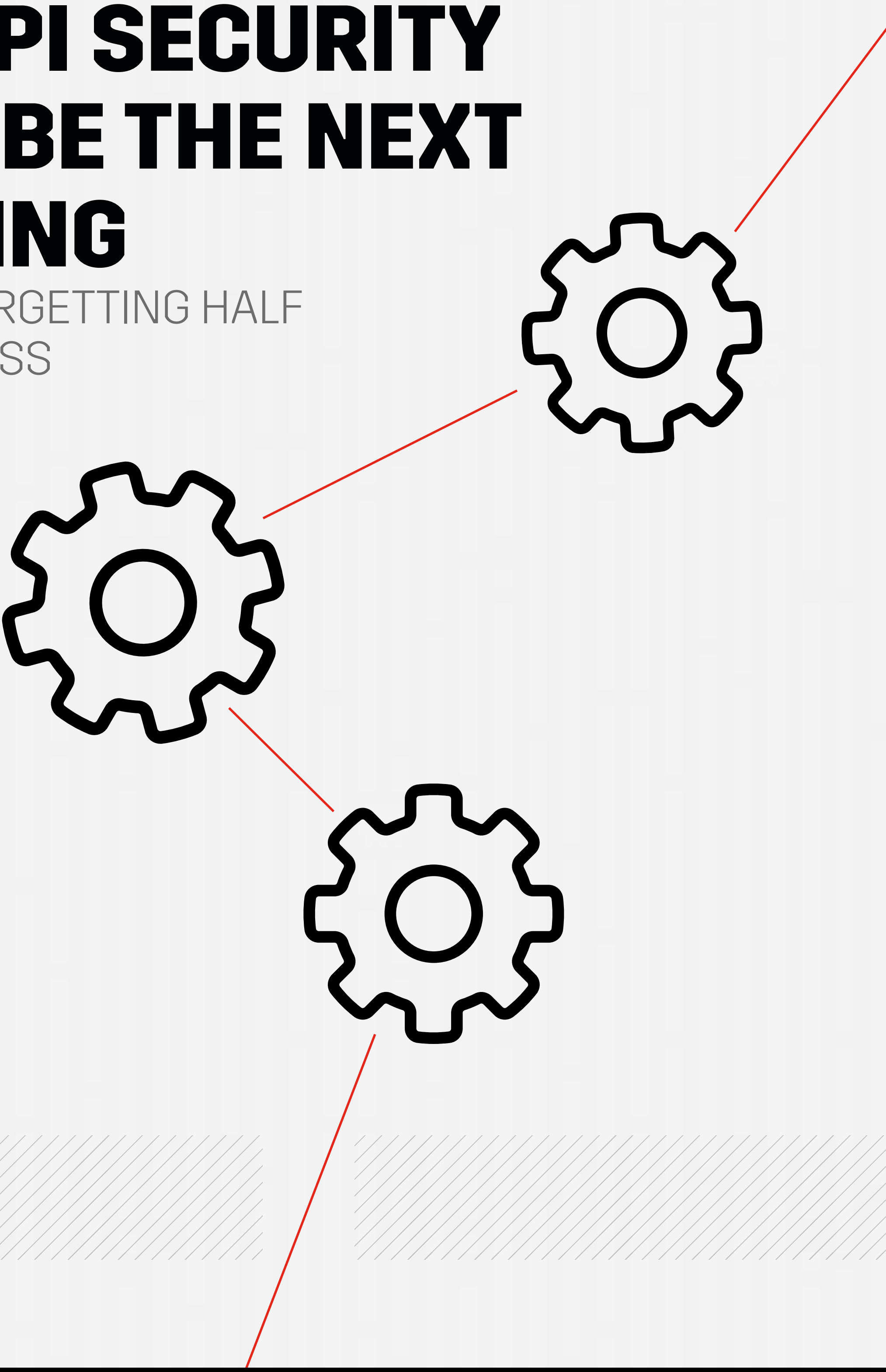
WHY API SECURITY MIGHT BE THE NEXT BIG THING

BUT WE'RE FORGETTING HALF OF THE PROCESS



BY **EWARD DRIEHUIS**
SVP STRATEGY CYBERSPRINT

BY E. DRIEHUIS
SVP Strategy

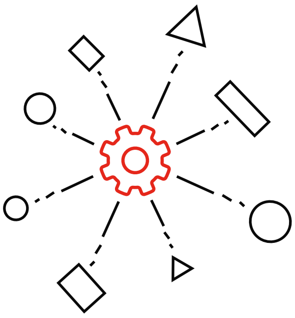
WHY API SECURITY MIGHT BE THE NEXT BIG THING

BUT WE'RE FORGETTING HALF OF THE PROCESS

API security is one of those essential elements, as it's rooted in so many processes. Yet, it's still easily overlooked. API security needs a second component to be effective. In this insight, I will outline what that is and why you need it.

APIs POWER EVERYTHING

APIs, Application Programming Interfaces, are the gateways to applications, their software components, and the data they serve. Your bank, payments, socials, authentication, and your news outlet all use APIs to serve you the requested functionality. Whether you're connecting through an app on your mobile, or through your desktop web browser, most large tech infrastructures are served via APIs.



Needless to say, there's a lot of them.

13,042 APIs

in Europe alone
(API type; Swagger)

API ABUNDANCY

When there are so many APIs, there are bound to be security misconfigurations among them. We've researched API discovery[1] and found 13,042 APIs in Europe alone. Since we only looked for a certain type (Swagger - the most widely used) and didn't look in the Americas, MEA or APAC regions, it would be a safe assumption that over 100,000 APIs are available for anyone to query and tinker with today.

COMMON ISSUES

That "tinkering" might lead to problems. In our research, we found hundreds of severe issues related to authentication alone. The three most common problems are:

/ **ABSENCE OF AUTHENTICATION**
While many APIs are meant to be publicly available, we found many offering functions returning vast amounts of payment data, personal identifiable information (PII), and other data that probably should be hidden from public scrutiny.

/ **PRESENCE OF API KEYS**
We found many APIs with an API key, thus giving access to hidden functions. These were likely used in a testing phase, forgotten and left in, where they can easily be extracted and used for authentication. In most cases, these keys still work.

/ **HALF-HEARTED AUTHENTICATION IMPLEMENTATION**
We found many APIs which had authentication, but the underlying functions were accessible anyway. Obviously, the mere presence of authentication is not as important as the functional dependencies on it.

All of these issues lead to data leaks, some small, but some extremely large. We found invoices, home addresses, payment data, and much more by the thousands.

This leads to the question:

What else could be wrong with APIs, on top of their apparent authentication issues?

CRIMINAL ADOPTION

There are no conclusive numbers on how often APIs are part of attacks. We know social engineering is still the most popular initial attack vector. Automated vulnerability scanning and exploiting is on the rise. Whenever a zero day hits the streets, such as the recent Microsoft Exchange zero day[2], white hats and black hats go on a scanning rampage, trying to be the first to find access - although the black hats immediately exploit it.

APIs aren't often cited as the source of a data leak or hack. This is inconsistent with our research findings - there seem to be a lot of opportunities.

INNOVATE WHEN NEEDED

What's going on here? APIs are abundant, open all kinds of opportunities to malicious actors, but they're not a problem? I believe the bad guys just haven't gotten around to it yet. If this sounds silly, please remember that criminals, and even nation-states, have no economical incentive to innovate new attack vectors if the old ones still work. They work, so they use them until they don't work anymore. Then they'll find new ones.

And find it, they will. As organisations double down on cybersecurity essentials, their resilience will go up, forcing bad guys to innovate.

In the meantime, compliance might be the best economic driver for API security. Based on our research, we estimate these breaches would result in GDPR fines worth tens of millions of dollars or euros. Mind you, this was in a 20-hour discovery timebox. We will find more if we invest more time.

> AS ORGANISATIONS DOUBLE DOWN ON CYBERSECURITY ESSENTIALS, THEIR RESILIENCE WILL GO UP, FORCING BAD GUYS TO INNOVATE.

FIRST THINGS FIRST

Application security might be on your mind now. What if we pentest the heck out of them, red team periodically, do code reviews, and all that good stuff. Great thinking! But there's a big catch.

Organisations don't always know where their APIs are, or if they even have them, or how many they have. Sounds strange? Just think about the "forgotten" API keys. If an organisation can forget an API key, they can forget an API. They have, and they will. Out of the hundreds we checked, a large percentage (maybe even half) gave us the impression their owners weren't aware of their existence.

In other words, you need complete visibility over your attack surface. The process will discover your APIs for you. You can then forward the data to your red team or code reviewers.

Red teaming will work in combination with complete visibility of your attack surface. An incomplete scope introduces blind spots and huge risks, as the bad guys don't have scopes.

In other words, knowing where your APIs are is a prerequisite to securing them. Put the two steps together, and you have the best defence possible.

FURTHER READING

1. https://www.cybersprint.com/blog/swagger-api-discovery-of-api-data-and-security-flaws
2. https://threatpost.com/microsoft-exchange-zero-day-attackers-spy/164438/

ABOUT THE AUTHOR

EWARD DRIEHUIS has been a security veteran for over 24 years, describing himself as having a "tech heart, design mentality, business drive". He's got a proven track record in innovative leadership in start-ups and large enterprises. Eward is an established speaker in the media and at international events such as RSA and FS-ISAC, drawing upon his years of experience of fighting cyber-threats together with banks, law enforcement and corporates.

Before joining Cybersprint, Eward spent three years as CMO at SecureLink, Europe's largest cybersecurity provider, including being responsible for research. He has also spent nine years at Fox-IT heading their Threat Intelligence and Advanced Analytics products. Earlier in his career, Eward's roles included CTO and Business Director in several IT and software companies.

ABOUT CYBERSPRINT

Cybersprint helps organisations achieve instant control over their visible and hidden digital risks to mitigate cyber threats related to their business, brand, online data and employees.

Our Our Attack Surface Management platform provides a continuous and automated process of identifying and managing your attack surface and associated external digital threats.

Visit www.cybersprint.com