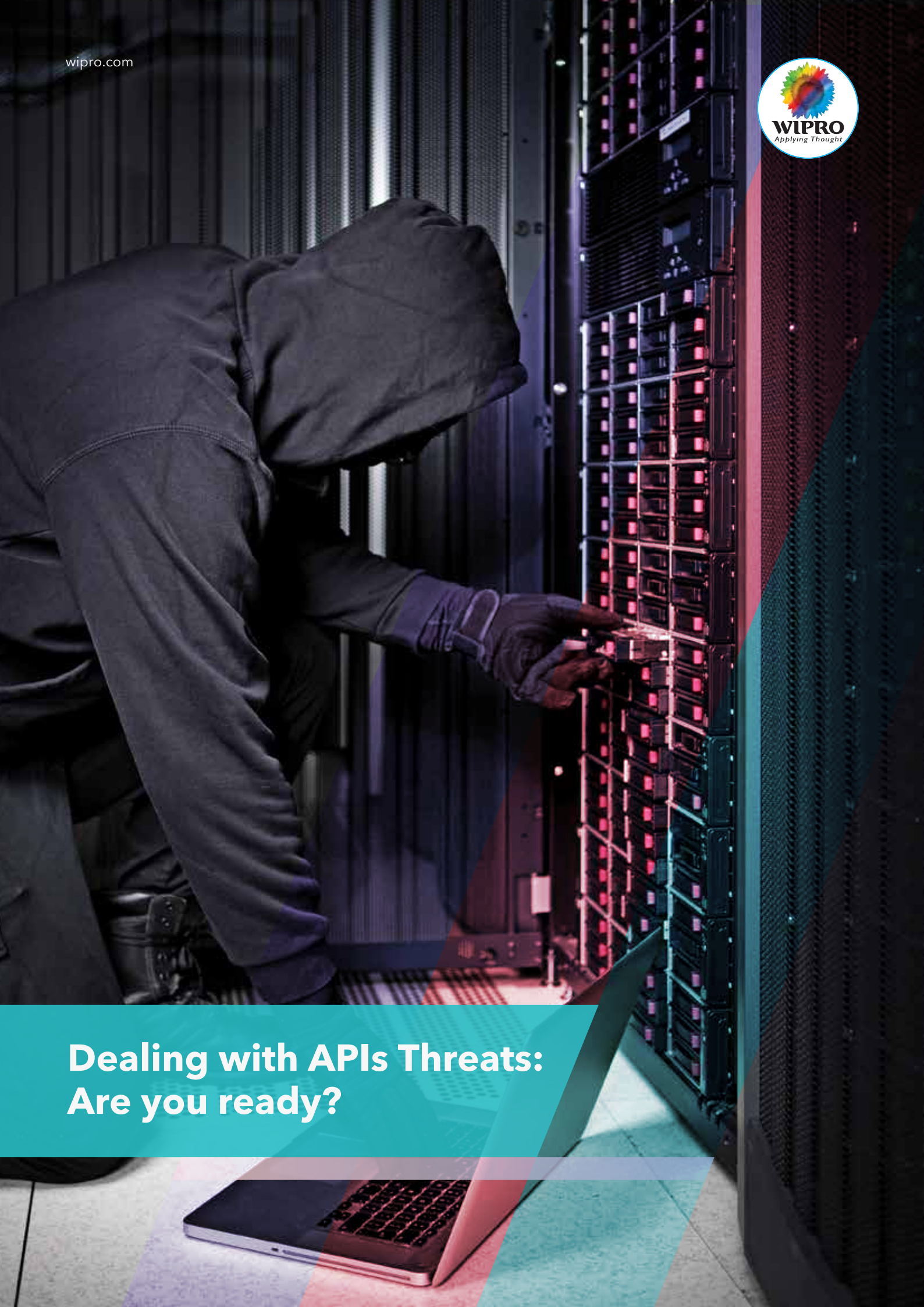
wipro.com



Dealing with APIs Threats: Are you ready?

Protect your API from Internet threat

Last couple of years, APIs have established themselves as an essential part of an enterprise architecture. Security plays a tremendous role in API management as the APIs expose enterprise assets directly to the Internet. However, there is a problem with the common approach to API security. It is highly focused on implementing OAuth and Op and tends to neglect other important aspects of a complete API security solution.

This fictional story illustrates what happens when an individual decides to hack or exploit your APIs and how the IT security manager can counteract such a threat. Two fictitious characters, John (the hacker) and Michael (the security manager) will help us to shape up our simplified storyline.

Multi-faceted aspects of API security

While focusing on threat protection, it is equally important to understand that API security is a much broader topic. The table below summarizes all areas which should be considered as part of an end-to-end API security solution:

Governance	
Compliance & Standards	Authentication
Federation	Authorization
Threat Management	Identity Propagation
Mobile Security	Kev Management
Security Analytics	Service Virtualization
Monitoring & Reporting	

The background

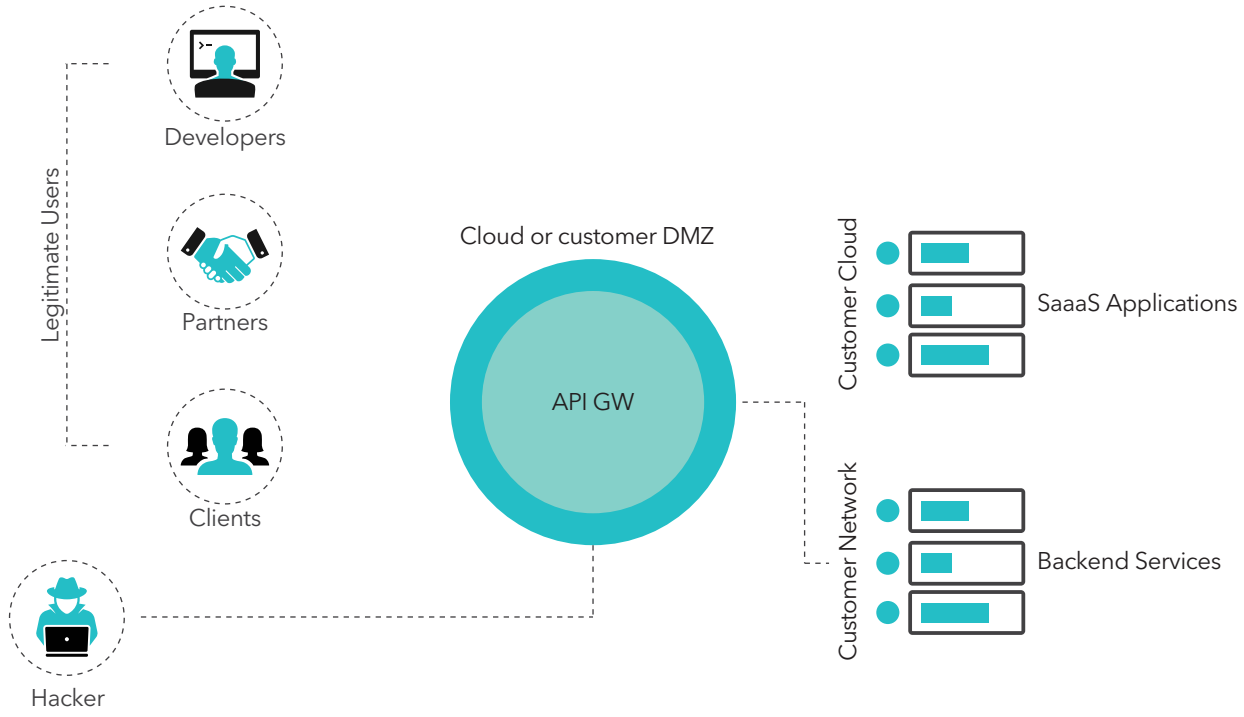
John (hacker) has heard that the company Acme Corp based out of HackMeLand, where Michael (Security Manager) works, has recently deployed the Application Programming Interface (API) version of some geo location services they used to sell as a stand-alone application. As many other Internet companies, such as Google, they realized that they can monetize the usage of their core service by making it available to developers for a fee as public API.

John's guess (and hope!) is that, as they are new to APIs, this first version of their API will be buggy and/or possibly not very well protected.

Although Michael is not an amateur in his business he is relatively new to API security. He understands that while it has much in common with Web applications security, it also has its peculiarities. Michael asks his trusted partner, ApiAcmeConsulting to help.

The battlefield

To begin with ApiAcmeConsulting provides Michael with the 'whole picture'. To protect something, it is important to understand the different layers between the hacker and the valuable assets (in the case of Acme Corp., their geo location database) and from where the attack can arrive. The diagram below reproduces a common scenario.



The hacker's weapons

John has a long and despicable record of Web application hacking during which he has developed a few techniques. The OWASP (Open Web Application Security Project) organization is the established authority in Web application security related matters. It keeps track of the vulnerabilities and attacks occurring on the Internet on their website. The list of top 10 Internet threats can be found here[1].

Let us give a closer look to the most common ones.

- **Malformed XML request** – The attack consists of malformed or recurring XML requests that throw off the XML parser.
- **Malicious Code Injection –** The objective of this attack is to exploit uncontrolled input process flow to inject[2] harmful SQL, LDAP, XPATH, or XQuery code along legitimate instructions. For instance, incorrect filtering, malicious query code string.
- **Cross-Site Scripting (XSS) –**This attack consists of malicious code into content that is delivered from the compromised site. XSS attack[3] is dangerous that the tainted content arrives at the API from a trusted source. A great example is getting high level access-privileges to confidential data, cookies from high-profiles sites.

The security manager's ammunitions

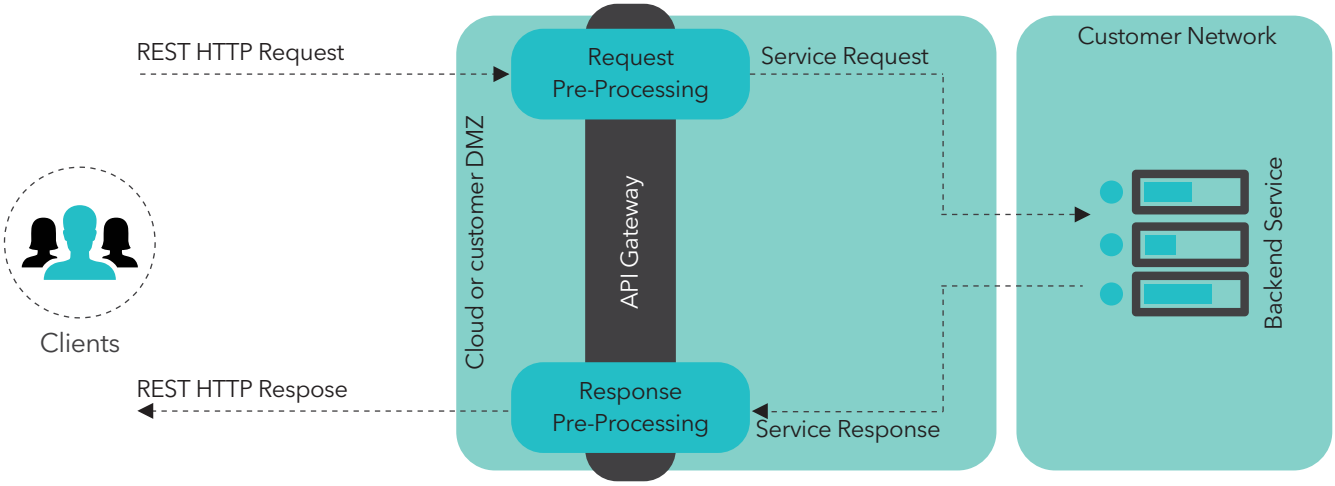
Michael and ApiAcmeConsulting decide to sit together to elaborate a strategy to counter internet threats.

ApiAcmeConsulting suggested to work on the gateway configuration, to enforce physical security and to activate all security policies designed to address the threats described in the previous section.

The API gateways implement the gateway architectural pattern . The objective is to avoid direct access to the Web services and rather have a mediation layer: the gateway.

From a security point of view this makes much sense, as with the gateway we have a single point of security policy enforcement, another common security pattern.

As per the mentioned security pattern the gateway is policy enforcement point (PEP), policy administration point (PAP) and policy decision point (PDP) in one single compon-ent (although different vendors might have different modules for those logical blocks).



API Gateways security rules called policies. Policies can be activated on proxies and implement specific controls to address the different threats. Proxies are logical containers for all the pre and post processing of client requests and might be required before they reach the service itself.

As per ApiAcmeConsulting's suggestion Michael also instructs his team to integrate the API gateway with their SOC (Security Operating Center) incident management tool. This will ensure that anomalous behaviour is detected and (depending on the gravity) an alarm is triggered.

The battle

Assuming he has previously managed to get some valid API keys, John sends a malicious request with recurring XML structures. The gateway checks the request before passing it over to the background geo-location service as part of the normal in-transit policy processing. One of the configured security policies detects that the request is malformed, drops the call and sends an alarm to the incident management tool, which in turn alerts the SOC team.

As first measure, the team can deactivate those keys, block the requestor. Off-line Michael will work with the API business manager to investigate the case further.

some of the improvements and best practices ApiConsultingAcme could recommend to their customers are:

- Enforce all security policies on the API gateway to prevent attacks from the Internet
- Periodically review the security policies and make sure they are in line with your security strategy
- Log all traffic flowing through the gateway
- Connect your gateway with the incident management tools of your SOC (Security Operations Center) or equivalent
- Perform analytics on the collected data to detect more sophisticated attacks, which can circumvent the existing policies

The way ahead

APIs give businesses a wealth of new and unforseen opportunities to amplify their reach by empowering the larger community of application developers. API security however is not an option, neither should it be treated as stand-alone. Rather the security team has to own it and make sure that API security is aligned, in terms of policies and controls, to the company's overall security strategy.

References

[Reference 1]
https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
[Reference 2]
https://www.owasp.org/index.php/Top_10_2013-A1-Injection
[Reference 3]
https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

Author details

Vamshidhar Babu Seetha is a Cloud Security Architect at Wipro. Vamshi has over 16 years of Security experience in IT Industry and has an expertise in Cloud Security and Enterprise Security Solutions designing and implementation across various industry verticals across the multiple regions He can be reached at **Vamshidhar.seetha@wipro.com**

Nicola Venditti is a Principal Security Consultant at Wipro Technologies based in Zurich, Switzerland. Nicola has over 15 years of experiences in the IT security industry and has worked on large engagements across the EMEA region.
He can be reached at **nicola.venditti@wipro.com**

About Wipro

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading information technology, consulting and business process services company that delivers solutions to enable its clients do business better. Wipro delivers winning business outcomes through its deep industry experience and a 360 degree view of "Business through Technology." By combining digital strategy, customer centric design, advanced analytics and product engineering approach, Wipro helps its clients create successful and adaptive businesses. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, Wipro has a dedicated workforce of over 170,000, serving clients across 6 continents. For more information, please visit **wipro.com** or write to us at **info@wipro.com.**

DO BUSINESS BETTER

CONSULTING | SYSTEM INTEGRATION | BUSINESS PROCESS SERVICES

IND/BRD/MAR 2017-MAR 2018