SAYFER LITEPAPER

A New Approach for Web3 Projects’ Security

Table of Contents

The Problem

Web3 hacks are on the rise, every few days another major project is getting hacked. The problem is that at best the only security measure Web3 projects take is an audit of their contracts. This approach leaves many other aspects of the business vulnerable to attacks. We've seen this many times in hacks like $120M BadgerDao hack, $650M Ronin Bridge hack, and Pretty much every CEX that lost its private keys.

THIS APPROACH CONTAINS MANY SECURITY BAD PRACTICES THAT WILL INCREASE THE CHANCE OF GETTING HACKED:

01

Single point of failure

02

Lack of security layers

03

One time testing.

We believe that in order for projects to gain mass adoption from "mainstream" users, they have to be much more stable in terms of cybersecurity. Today, most of the crypto market are early adopters but that is changing and the new type of clients will not accept such risk.

SINGLE POINT OF FAILURE

When creating complex projects and protocols you want to make sure that even if one component of your system is compromised you don't lose all of your funds. This is easier said than done.

Sometimes it is easy to know where the points of failure are but very hard to find a way to mitigate the risk.

Let's imagine that you develop a contract token, how can you not lose all of your investors' money if the contract gets hacked? How will you know if something bad happens? Which component of your system is the weakest?

It is very hard to find the not-so-obvious point of failure.

Let's say you have a very secure contract, but your new employee's phone got stolen. This phone is connected to a GitHub account that can commit and push new code.

Without proper monitoring tools, a backdoor can be inserted into your contract without you even knowing about it.

LACK OF SECURITY LAYERS

The only way to create a secured project is by having multiple security layers, this was true before the computer era and is very much relevant in today's Web3 project and protocols architectures.

Projects should have many components, and each component should be able to face compromise by itself without risking the entire project's integrity. Each component should be monitored, and when abnormal behavior is detected, relevant people should be informed, and based on predefined policies transactions should be blocked.

The theory is nice but what does it mean in practice?

Security is not a binary outcome, it is layers. You can not lock the door and leave the window open. Different projects have different needs and different levels of risk, if your risk is high you should mitigate it with more security layers.

ONE TIME TESTING

When building a complex project you need to take into account that the project is a living evergrowing creature. However, the nature of audits is to happen once every N months. Yet, projects can not take the risk of being less secure because it's that time of the year. Projects need an ongoing security process.

The Wormhole bridge exploit is a great example of the problem - 8 hours after a commit with a deprecated function was deployed to the blockchain 300M$ were stolen, such an incident would be easily prevented with the proper CI/CD tools that would block the commit, along with other ongoing security measures that can detect vulnerabilities on the go and not only on the audit day. This problem is so common even projects that have just done an audit a few days ago tend to add a "last feature" after the audit which can cause harm.

The Problem

The Solution

A 360° cyber approach. Projects and protocols aren't just contracts, they are complex system that requires complex solutions.

By being a native Web3 company Sayfer can understand the architecture of your platform, the structure of your business, and the budget and development hours you can afford to allocate to a project. We will provide a tailor-made complete cybersecurity solution for you.

After you implement all our findings, which will resemble more ongoing support rather than a one-time shot, the security of your project will grow at the same pace that your project grows.

This way, security will not be a soft spot that will harm your growth in the future.

What are the steps to have 360° cyber security protection for your business?

ACTIVE & PASSIVE ASSESSMENT

HISTORICAL HACKS ANALYSIS

BUILD A SECURITY ROADMAP

IMPLEMENTATION GUIDANCE

Active & Passive Assessment

During the first phase of our process to make your project secure, we will perform a full assessment of your business cyber security posture. This part is very important because we need to know your starting point in order to build a correct security roadmap tailored for you.

We will first use the passive approach. We will talk to you, and understand your project. In this part, you will tell as much details as possible about your applications, architecture, employees, potential known security vulnerabilities, and the risks you now pose to your system.

We will then proceed to an active approach. We will "test" your claims with our own eyes by trying to hack into your system. This will be done either by security audit to the contracts, a standard penetration test to test the web or mobile application security, or a red-team style penetration test to find novel breaches to your system.

After performing both types of assessments we will have a high understanding of your current business cybersecurity posture and potential risks to it.

Historical Hacks Analysis

Hackers are not different from any other human being. They see what their colleagues are doing, and if it works, they will try to do the same.

So in order to predict where the next attack on your system will come from we need to understand what are the current common practices in the hacker community.

We will do that by performing analysis for any project that has a similar structure and features to yours.

A practical example of such behavior is the centralized exchange hack, which almost always involves the loss of the exchange's private keys. This tells us that strong custodian services with strict policies need to be implemented.

NFT projects, Discord communities, and Twitter accounts are a petri dish for social engineering and advanced phishing attacks. Sometimes the art is getting copied and published in a different marketplace as well, depending on the NFT art type and popularity. By understanding these we will take the educational approach alongside using detection tools for the malicious links in the Discord communities and crawlers detection tools to find stolen art and notify the marketplaces.

There are many more examples of this and every project has its own nuances, this is why it is important we understand the current behavior of the hackers' communities.

The Solution

Build a Cybersecurity Roadmap

After gaining all of the above information about your project, such as valuable assets and their risk potential, the market, and the potential security risks your system poses, we are ready to build a security roadmap for you.

Why Is a Cybersecurity Roadmap?

It is hard for a project to transition from a non-secure to a fully-secure state. You can't simply do it by adding two tasks to your project management platform and forgetting all about it.

There will be many tasks, some are more urgent than others, some are blocked by development tasks and some are complex and you have no idea how to do these (no worries, this is why we are here). By building a roadmap for the upcoming months, you will have the opportunity to implement cybersecurity without delaying your main development project's roadmap.

Why Is a Cybersecurity Roadmap?

Each roadmap is different and tailor-made for the specific project, based on our initial assessment work, but the goal is always the same - map all valuable assets and their corresponding attack vectors, and then protect them from several angles, in multiple layers, in runtime, and to make sure we eliminate the single point of failure at the development phase, the lack of security layers and the one-time testing problems.

THERE ARE SIMILARITIES AND COMMON STEPS THAT WILL BE IN MOST PROJECTS IN ORDER TO ACHIEVE 360° PROTECTION:

01 Fixing known vulnerabilities - during our assessment, we will find major security vulnerabilities, so the first step is to fix these and make sure hackers can't exploit them.

02 Mapping assets and their attack vectors

03 Implement Security Layers to protect these attack vectors
a. 3rd party products
b. Internal modules

04 Implement a secure software development process

05 Security architecture modification

06 Develop secure business processes

07 Educate employees about potential risks

Implementation Guidance

As mentioned above, cybersecurity is not a one-time show - this is a live process like any other development process of a crypto project.

In order to correctly implement our roadmap, we will provide as much guidance as needed, we will escort you every step of the way. This includes:

- Helping you to implement 3rd party tools, and write their policies.
- Consult and provide our knowledge when you design new modules that are directly affecting security or indirectly affecting the security of your project.
- Perform modifications to the roadmap to always stay aligned with shifting business requirements and help find and eliminate new security breaches.
- Helping you in case of an incident, if something did happen we will be with you to help you understand what happened, what got lost, and what we can do about it.

The Solution

Summary

Web3 security is hard, and almost any project is a victim of some sort of cyber security attack.

Using our unique approach to a 360° cyber protection we will take your project to the highest possible level of cyber security standards and make sure the bad guys won't hack you.

In order to do so, we will first actively and passively find the security assets and breaches of your system. We will also analyze historical hacks for projects similar to yours to better know what are the common hacks in the market.

We will then build with you a security roadmap that will add additional layers of security, prevent a single point of failure in your system and integrate an ongoing security testing scheme to make sure your system stays secure even after we are done.

After the security roadmap blueprint is done we will stay by your side to help you correctly implement our findings to make sure that everything is at the highest level of security.

Get in touch

Find out more	Phone	Location	Email
https://sayfer.io/	(404) 687-5228	Tel Aviv, Israel	info@sayfer.io