What is Crowdsourced Security?

Before a new software product is released to the market, it is checked for vulnerabilities. Every responsible company performs these tests to protect both customers and the company itself from cyber threats.

In recent years, developers have increasingly relied on crowdsourcing to conduct security testing. But what exactly is Crowdsourced Security? How does it work and how is it different from other popular risk assessment methods?

How Crowdsourced Security Works

Organizations of all sizes have traditionally used penetration testing to secure their systems. Pentest is essentially a simulated cyberattack to expose security flaws, just like a real attack. But unlike in a real attack, when discovered, these vulnerabilities will be patched. This enhances the overall security profile of the organization in question. Sounds simple, right?

But there are some problems with penetration testing. It is usually only done annually, which is simply not enough, as all software is regularly updated. Second, because the cybersecurity market is already quite saturated, pentest companies sometimes "find" vulnerabilities that really don't exist to justify charging their services and stand out from the crowd. competitor. There are also budgetary concerns - these services can be quite expensive.

Crowdsourced Security operates on a completely different model. It revolves around inviting a group of individuals to test the software for security issues. Companies using Crowdsourced Security extend invitations to a group of people or the general public to explore their products. This can be done directly or through a third-party crowdsourcing platform.

Picture 1 of What is Crowdsourced Security?

While anyone can join these programs, the primary audience will be white hat hackers or researchers. There is often a well-deserved financial award for discovering a security hole. Obviously, determining the amount is up to the company, but crowdsourcing is cheaper and more effective in the long run than traditional penetration testing.

Compared to pentests and other forms of risk assessment, crowdsourcing has various advantages. First, no matter how well you hire a penetration testing company, a large group of people who are always looking for security holes will be more likely to discover them. Another obvious advantage of community service is that any such program is open-ended, which means it can run continuously, so vulnerabilities can be discovered (and patched).) year round.

3 types of Crowdsourced Security programs

Most Crowdsourced Security programs focus on the same basic concept of financially rewarding people who discover vulnerabilities, but they can be grouped into 3 main categories.

1. Get a bug bounty

Almost every tech giant - from Facebook, Apple to Google - has a bug bounty program in place. The way they work is pretty simple: Spot the bug and you'll get a reward. These rewards range from a few hundred to several million dollars, so it is not surprising that some white hat hackers earn a full-time income from discovering software vulnerabilities.

2. Vulnerability Disclosure Program

The vulnerability disclosure programs are very similar to the above group, but with one key difference: These programs are public. In other words, when a white hat hacker discovers a security hole in a software product, that vulnerability is made public for everyone to know. Cybersecurity companies often engage in these activities: They discover a security hole, write a report about it, and make recommendations to developers and end users.

3. Malware Crowdsourcing

What if you download a file but aren't sure if it's safe to run? How do you check if it's malware? Your antivirus suite may not recognize it as malicious, so what you can do is go to VirusTotal or a similar online virus scanner and upload the file there. These tools aggregate dozens of anti-virus products to check if the file in question is harmful. This is also a form of Crowdsourced Security.

Some people think that cybercrime is a form of Crowdsourced Security. This argument also makes sense, because no one is more motivated to find a vulnerability in a system than a threat actor looking to exploit it for money and reputation. After all, criminals are the ones who unwittingly force the cybersecurity industry to adapt, innovate, and improve.

The Future of Crowdsourced Security

According to analytics firm Future Market Insights, the global security market will continue to grow in the coming years. In fact, estimates say it will be worth around $243 million by 2032. This is thanks not only to private sector initiatives but also because governments around the world have adopted it. Community-sourced security measures.

These predictions can certainly be helpful if you want to gauge where the cybersecurity industry is headed, but it doesn't take an economist to figure out why corporate organizations are adopting this approach. provide community service for security purposes. No matter how you look at it, the numbers matter. Also, what harm can it do to have a team of responsible and trusted people monitoring your property for vulnerabilities 365 days a year?

In short, unless something dramatically changes the way the software is penetrated by threat actors, we are more likely to see community-sourced security programs popping up in both countries. 2 sides. This is good news for developers, white hat hackers, and consumers, but bad news for cybercriminals.