FMBusinessDaily

Pen testing vs bug bounties: which one is right for your business

2 years ago

Insight from Anders Reeves, CEO at CovertSwarm, a leading global ethical hacking, and red team cyber security solution provider

Over the past five years, ransomware attacks have risen exponentially worldwide and high-profile attacks dominated the headlines last year.

The statistics are concerning, with IT Governance's 'Data Breaches and Cyber Attacks' list showing that, in the UK alone, there have been 528 data breaches, resulting in 451,724,931 breached records.

Cybercrime is here to stay, and to reduce the risk of breach it is up to companies themselves to employ the services of a skilled cyber partner to ensure they are best protected from a cyber attack.

Penetration Testing – otherwise known as 'pen testing' – and Bug Bounties are a great place to start.

But what are they and how do they differ? What are the pros and cons of what a business will get from investing in either service?

So, let's get into it.

Firstly, what is a bug bounty?

It wasn't that many years ago that ethical hackers, in their spare time, would explore other people's web applications, websites, and other areas of technology infrastructure for the purpose of discovering vulnerabilities ahead of genuine bad actors.

What they would then normally do is proverbially knock on that business' door and inform them they had found something that needs fixing.

It was a process that wasn't commercialised, until early commercial zero-day vendors – and more recently mainstream companies like Google, Microsoft, and other SaaS vendors – started to introduce Terms and Conditions that encouraged ethical hackers to freely test the security of their applications or web apps to discover underlying vulnerabilities without falling foul of any computer misuse legislation.

The reward for finding, reporting, and supporting these initiatives led to the birth of bug bounties.

However, it's far from common for companies to have these types of programmes in place. Most of the time, this activity happens sporadically, beginning with an ethical hacker sending a friendly email alerting a business to an issue they have spotted on the website, of their own accord.

That tends to skirt a little bit on the grey areas of what's legal because they're testing without permission. But usually, it's well received – with the CEO or CTO generally being appreciative of the effort and responsible disclosure.

That said, it can also be quite unnerving for some companies to receive those types of approaches. They're never sure whether the approach is genuine or whether it's actually a bad actor seeking to extort or exploit.

Properly established bug bounty providers are a little different – and help take the risk and fear factor off the table for users of their service. In a formal, managed bug bounty programme, a company contracts with a third party who manages the entire process on their behalf, offering a walled-garden approach to how a business can go to the outside world and expose its estate for cyber testing against a set of curated rules of engagement. They're specific about who the door is open to and what doors of the estate they can test.

One of the major challenges with bug bounty is that they only focus on the external digital aspects of an organisation. The social, physical, and wider internal threats are a huge blind spot.

Bug bounties require engagement and openness or will fall short in value

Bug bounties are valuable and immensely useful but they do come with their flaws.

While a managed bug bounty programme can address a lot of problems, the variability of reporting quality of the delivered cyber testing, and the limited reality of what a business chooses to expose to faceless/unknown cyber testers, do hinder it.

If you're a business that is going to invest in a bug bounty programme, you should consider:

- Working with a third party that acts as a marketplace provider doesn't have the same level of assurance or quality rigour that a more dedicated agency or service provider deploys services by fully-employed staff members. If they're not very well managed, marketplace-delivered services can end up producing highly variable findings. The quality of their ethical hackers can be strikingly different.

- You also have the important issue of variable reporting quality. Not everyone's written word is going to be able to meet the standard required to effectively communicate their findings, and associated risks, to you. They don't necessarily have the same QA processes that a dedicated ethical hacker would have available to them as part of a more stable, vetted, and uniformly skilled workforce.

- Clients tend to hold back a little bit so as to not expose the things that might seriously damage their reputation or that might really impact their brand if it was found to be hugely vulnerable. This means genuine cyber risks may lay unrecognised if a client holds the vulnerable systems back from being scrutinised.

- Bug bounty programmes can often be very shallow as people tend to focus on the common vulnerabilities that can be addressed quickly, so they can go on and make the next £250, rather than work for a year and maybe get the million-pound hit that may actually be lying underneath the surface somewhere.

Companies need to think beyond the low-hanging fruit if they're to be truly protected

There's an analogy we can use here relating to how real estate agents operate:

The economics of a real estate agency tends to be that it makes more sense to flip as many properties as you possibly can than to try and get the best possible deal on every property in your portfolio on behalf of the seller.

It's much better to flip 10 today than flip five at a slightly inflated price and then delay the sale of the next bite.

The lowest-hanging fruit mentality tends to win in the real estate agency world and that's the case in the bug bounty world as well. What you tend to find is a focus on the common vulnerabilities that can be addressed quickly – essentially like a top 10 – to tick a set of most frequently detected boxes.

They're usually low value but they will address some security issues and make a business more secure, meaning it looks like a worthwhile engagement.

However, taking that approach means a huge area gets neglected. It's not bespoke. You could do those top 10 vulnerabilities and get on top of them but if you miss number 11 or 12, or perhaps even your own unique zero-day, it could lead to something devastating.

On the other end of the scale is pen testing

Pen testing is typically carried out over an agreed (limited) scope – a short number of days – and will, normally, be delivered by an agency or consultancy that a business has worked with before that has got specialisms in specific technological areas.

They will have a reputation and you will heavily rely upon that reputation to make sure the work they do doesn't bring down your estate or website or web app – whatever it might be through their testing.

But, also, there'll be a level of quality that you'll be looking for from them, which again will be reputation based. Maybe they are CREST certified, or they have other industry-recognised accreditations that make you gain a sense of professionalism from that pen test outfit.

If the scope and the number of days for a pen test have been adequately provisioned, they have the capability to go deeper. It's not that bug bounty programmes can't go deeper, it's just not often in the tester's economic interest to do so.

Of the testers to go that deep, they could be chipping away for 50 days and find nothing. Unless a business is really cherry-picking ethical hackers that are coming through the bug bounty programme – who's got a tried and tested method that provides that assurance of depth and perseverance – you're much better off going down the more traditional route of pen testing.

How to decide what's right for your business

The reality is that both pen testing and bug bounties are very important parts of a complete comprehensive security programme.

It's not that one is necessarily better than the other. If you have a reasonable budget and you can afford to take a blended approach, you should.

Bug bounties can be really effective because if all you're doing is paying for the detection of an issue, then arguably, there is zero cost to the business until there's something worth paying for. That said, I'm not sure a business owner would be able to sleep particularly well at night, knowing that nothing has been reported. The absence of reported issues doesn't equal the absence of issues.

Meanwhile, within the traditional pen testing engagement world, you know it's going to cost you say, $30,000, whether something or nothing is found. The costs vary depending on the third party you employ for the test. Remember, however, that failure to detect issues can be equally valuable as it provides assurance that what has been deployed or configured is 'secure' in its current form.

Each has its advantages and disadvantages but both are necessary in today's environment and in combating the growing cyber security threat.

Final thoughts

Organisations make the mistake of thinking that they can just go and buy a cyber security product or service and it will be a silver bullet.

No matter how big of an organisation you operate, whether it is a one or two person-band or a company with thousands of employees, there isn’t such a thing as a silver bullet, especially in the cyber security world.

One of the best ways to secure and protect your business and its people is to get in the mindset of how an attacker would approach the challenge of subverting your security controls.

Appreciating no business or organisation ever stands still, you should recognise how every change incurs a new point of risk that could lead to a breach, and so employing a security partner that applies constant ethical hacker’s eyes on your estate is a must if you are to outpace the threat of a genuine cyber attack.

Remember also that from a cyber perspective, an effective attack may not necessarily be physical, but could come in the form of digital or social, too and you need to be prepared.