Safe harbor legal framework for ethical hacker officially launches in Belgium

BY INTIGRITI · FEBRUARY 15, 2023 · LAST UPDATED ON MARCH 6, 2025

As part of the Belgian Act on the Protection of Whistleblowers, dispositions were adopted to offer a safe harbor for ethical hackers who respect certain strict conditions.

Some positive developments impacting Belgium's cybersecurity industry came into effect today (February 15), with newly adopted legal dispositions serving to protect ethical hackers and bug bounty hunters.

Much like in other areas of technology, policy often fails to keep pace with developments in cybersecurity security. The gap between legislation and innovation provokes difficulties for both researchers and businesses, where the absence of legal protection can result in unfair outcomes and missed opportunities.

Fortunately, things are changing. Increasingly we're seeing new legal frameworks being brought in to safeguard ethical hacking practices. For those looking to enter the industry as researchers, this change is providing greater motivation to devote more time to hacking. For businesses, this influx can be leveraged to provide greater security assessments. Confidence in the continued growth of crowdsourced security is rising with recognition of its clear benefits at a governmental level.

We recently discussed the NIS2 Directive and how its more stringent regulations would demand greater attention to security for companies, driving demand for crowdsourced services. Elsewhere in the UK, the organization CyberUp has made progress in its campaigns for greater hacker protection.

New legislation goes live

In January, we pulled focus on the Belgian Act on the Protection of Whistleblowers, and how it was set to improve the conditions through which hackers can safely report vulnerabilities. Moreover, we're seeing how legislation is positively affecting our industry in more ways than one.

But with specifically the Belgian Whistleblowers Act officially coming into effect today, we spoke with our **Chief Hacker Officer, Inti De Ceukelaire**, who discussed the changes being made and what they mean for the future of ethical hacking and in Europe.

Prior to this new legislation, what difficulties did ethical hackers face in Belgium and how did this affect them and the businesses they were testing?

Inti De Ceukelaire: When you're trained as a hacker, it's hard to not instinctively see the potential faults and vulnerabilities present in a system. It's like being an advertising agent and seeing a bad advert. Even if there is no safe reporting process in place, a hacker may feel a sense of duty to inform a business especially if the risk was severe.

While researchers can sometimes make use of the press as a mediator or tools such as disclose.io, you were still at the mercy of the laws of the country you resided in. Hackers faced little motivation for acting

on their urges when there was so much legal risk. Why would you bother hacking when it could potentially land you in serious trouble?

The rise of bug bounties offers a safer, and much more rewarded way of hacking, so hackers would be directed this way rather than bothering to look at companies that didn't have a policy.

This proclivity towards seeing potential vulnerabilities is of course present in malicious hackers as well, so during this time businesses that did not engage in any kind of vulnerability disclosure practice simply put themselves at greater risk of breaches.

RELATED The ultimate guide to VDP: How to write a vulnerability disclosure policy

What immediate effect do you think it will have?

Inti De Ceukelaire: I'm expecting a huge influx of reports now that hackers are better protected. There are plenty of companies who have never had any kind of policy in place before, and so would not have had much attention from researchers.

For companies, making it clear what you can and cannot do as a hacker is essential. Without some basic rules, people can only assume, which can lead to bad consequences. With the new hacker protections in place, the responsibility and ownership of those consequences have shifted to the businesses.

We can look at the Netherlands to understand what the picture looks like with these rules in place, as they've been hosting similar protections for several years. There are individuals in this region such as Victor Gevers, known as 0xDUDE, who have become globally famous for their extensive vulnerability reporting.

The removal of barriers around vulnerability disclosure will inevitably lead to more introspections by hackers. For businesses, this means if you haven't got a policy in place yet, you better get one because either way your security will more likely be tested.

What first actions could businesses take considering these new rules? For those interested in wading into crowdsourced security, how best can they dip their feet in?

Inti De Ceukelaire: Starting with a simple Vulnerability Disclosure Policy might simply mean you initially provide a single channel through which a few kinds of report can be submitted. This can follow the basic checklist as an effective starting point.

You should of course give at least some kind of scope, even if it is not in detail, of which assets and parts of your business you would like to guide hackers towards. Secondly, you may want to decide whether you pay out for any disclosed vulnerabilities. If you do want to, you'll need to be sure you're not paying out to hackers who have been sanctioned. Using a bounty service can help remove the headaches that go along with paying out bounties.

Moving from here, proper bounty programs will of course attract much more attention, and so you can start to make a more proactive effort to strengthen your defenses.

How important is this legislation in the wider context of the European bug bounty and crowdsourced security space? Do you feel this will set a precedent that other countries will follow?

Inti De Ceukelaire: In many ways, the rules had been a long time coming. Similar protections have existed in Lithuania, Poland, Slovakia, and France. With Belgium now joining the fray, the visibility around these kinds of legal frameworks will continue to accelerate. The hope is that one day we will see an EU-wide rule that protects hackers. Ultimately, reporting will continue even where a rule isn't yet in place, so it's simply a matter of time.

What steps remain on the road towards protecting and encouraging ethical hacking?

Inti De Ceukelaire: Other than a more widespread adoption of this rule that will come no doubt in time, a continued rise in transparency from companies will improve the situation.

You can often find a general attitude around security that involves putting your head in the sand until a problem arises, which then demands a fix. But these new protections will change this attitude. With hackers being able to inform businesses with their express interest, it will demand change from them much more than it has in the past. They won't be able to stay naïve about their security issues.

In the future, I would like to see this transparency grow as the standard choice for most companies. In a similar way that investor reports are publicly published, why shouldn't we expect the same for pentest reports?