



Position paper proposal

Information

Title: The crowdsourcing of cybersecurity
Subtitle: Current situation and challenges facing Swiss organisations
Author: Luca Perrig
Affiliation: University of St.Gallen

Abstract

The information security industry has been undergoing major developments in the past few years. With the increasing digitisation of our economy, comes an ever more worrying vulnerability. Switzerland has been the target of attacks from criminal and governmental actors. Universities have been targeted for their research on covid vaccines, local administrations and companies have seen their data encrypted by ransomware, and users are increasingly threatened by online criminal activity. In order to cope with this situation, ethical hacking is regarded by many governments as a promising solution. Numerous platforms have been emerging in the past five years, which offer organisations to secure their information systems by relying on a crowd of self-employed “ethical hackers”. This novel industry is called bug bounty, and advocates for opening information systems of organisations and reward hackers in exchange for the responsible disclosure of the vulnerabilities they find. Stories abound of successful bug hunters earning good money on these platforms. Information security workers learn new skills about offensive security by practicing on these programs. And overall, the industry seems to agree that this new transparency is effective at securing systems.

Since 2020, three platforms have emerged in Switzerland which offer bug bounty services, and the industry is constantly growing. All types of organisations are crowdsourcing their cybersecurity. It involves big corporations such as Nestlé or Roche, but also smaller companies such as Proton or Zweifel. Public administrations have also set up bug bounty programs, for instance the Federal Administration, as well as semi-public organisations (SBB, SwissPost, Swisscom), many higher education institutions and numerous financial institutions. The industry is relatively well organized, with tight professional collaboration among the platforms and security managers. Since 2023, the institutionalization of ethical hacking is also mentioned in the National Cyberstrategy report of the Federal Council.

However, this promising solution to cyber-threats implies deep organisational changes. Instead of relying on internal employees for their security, organisations now crowdsource this task to a crowd of hackers scattered around the world. This raises three main questions for scholars of security and organisations:



First is the question of labour and the nature of this new form of security work. And what consequences does this shift have on “security sovereignty”? Some see this new organizational arrangement as a form of gig labour. Bug hunters face considerable uncertainty, as they conduct their search for vulnerabilities without the assurance of ever finding one. Moreover, this form of digital labour can be performed remotely, which means that it might attract an overwhelmingly precarious workforce from abroad and reproduce an unequal international division of labour. The incentive structure of bug bounty programs is also reminiscent of gig work. However, most actors in this industry seem satisfied, including the hackers. Could the situation evolve and are Swiss organisations heading towards the constitution of a precarious workforce of outsourced hackers in the Global South?

Second is the question vulnerability management. By opening their systems and asking for the world to hack them, organisations are operating a significant shift in the traditional way of practicing vulnerability management. Whereas in the past vulnerabilities might have been hidden from the public, bug bounty programs force organisations to advertise them openly. This development is in line with a wider trend towards opening organisations. But how well can it translate into the realm of security, where vulnerabilities are best kept secret?

Third is the question of the effects of this crowdsourcing within organisations. Security teams are now working with a crowd of hackers from abroad. Their work now consists increasingly in managing this new workforce. Software development is also affected, as they increasingly receive vulnerability reports from outside hackers. Bug bounty also changes the development process. Whereas in the past applications were screened by professional security experts before launch, they can now launch more rapidly with a bug bounty program which will ensure an ongoing process of security research. Bug bounty thus comes with significant disruption within the organisations, as it involves communicating with a crowd of undefined and anonymous “colleagues”, it disrupts the normal flow of software development and allows novel forms of software deployment.

For these reasons, the crowdsourcing of cybersecurity should force scholars to revisit the role of security management within organisations.

These insights draw from an ongoing study of the bug bounty industry in Switzerland. The data includes interviews with hackers, information security employees, and platform managers.