Vulnerabilities and Ethics: A Code of Ethics for the Private-Sector

Alfonso De Gregorio
Zeronomicon

Zero--day vulnerabilities — weaknesses in software or hardware that are unknown to the parties who can mitigate their specific negative effects — are gaining a prominent role in the modern-day intelligence, national-security, and law-enforcement operations.

At the same time, the lack of transparency and accountability in their trade and adoption, their possible overexploitation or abuse, the latent conflict of interests by entities handling them, and their potential double effect may pose societal risks or lead to the breach of human rights.

If left unaddressed, these usage-related challenges call into question the legitimacy of zero-day vulnerabilities as enablers of national security and law-enforcement operations and erode the benefits that their proportionate use have for the judiciary, defence, and intelligence purposes.

This work explores what the private sector involved in the trade of zero-day vulnerabilities can do to ensure the respect human rights and the benign and societally beneficial use of those capabilities. After reviewing what can go wrong in the acquisition of zero-day vulnerabilities, the article contributes the first code of ethics focused on the trade of vulnerability information, where the author sets forth six principles and eight corresponding ethical standards aimed at guiding and regulating the conduct of this business.