Security Leftovers

By *Roy Schestowitz*
Created *13/10/2021 - 2:35pm*
Submitted by Roy Schestowitz on Wednesday 13th of October 2021 02:35:16 PM Filed under Security [1]

- **10 Most Commonly Used FOSS Packages [2]**

  The Core Infrastructure Initiative Census Program II report released earlier this year identified the most commonly used FOSS components in production applications, with the goal of understanding potential vulnerabilities in these components and better securing the open source software supply chain.

- **Don?t penalise cybersecurity researchers! [3]**

  We wrote to the Indian Computer Emergency Response Team regarding a provision in their new Responsible Vulnerability Disclosure and Coordination Policy that penalises cybersecurity researchers for vulnerability disclosures. In our representation, we highlighted how such provisions would create an atmosphere in which researchers would be reluctant about reporting vulnerabilities and recommended that a robust disclosure mechanism be implemented that protects researchers from harm.

  [...]

  Such provisions contribute to a disclosure regime in which security researchers would be liable under the Information Technology Act, 2000 (?IT Act?), and are penalised for disclosures of genuine security vulnerabilities. Section 43 of the Information Technology Act, 2000 penalizes anyone who gains unauthorized access to a computer resource without permission of the owner, and so fails to draw a distinction between malicious hackers and ethical security researchers. Thus, even when researchers have acted in good faith they may be charged under the IT Act. As we have mentioned earlier, companies have exploited this loophole in the said provision to press charges against cybersecurity researchers who expose data breaches in their companies. The Personal Data Protection Bill, 2019, currently being

considered by a Joint Parliamentary Committee, also fails to protect security researchers and whistleblowers. All of this leads to situations in which researchers are reluctant to report vulnerabilities for fear of being sued.

Clause 7 of the Policy is also in conflict with the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (?2013 IT Rules?) which adapts a cooperative and collaborative approach. Rule 10 requires CERT-IN to interact with stakeholders including research organisations and security experts for preventing cyber security incidents. Under Rule 11(2), CERT-IN is obligated to collaborate with, among others, organisations and individuals engaged in preventing and protecting against cyber security attacks. Thus, by imposing complete and sole responsibility on cyber security researchers for actions undertaken during the discovery of a vulnerability, the policy is in conflict with the collaborative spirit of the 2013 IT Rules and so is a genuine impediment to effective collaboration.

- **Airline Passenger Mistakes Vintage Camera for a Bomb [4]**

Back in 2007, I called this the ?war on the unexpected.? It?s why ?see something, say something? doesn?t work. If you put amateurs in the front lines of security, don?t be surprised when you get amateur security. I have lots of examples.

- **How to create an effective security policy: 6 tips [5]**

Are your security policies boring? OK, that?s not entirely fair. Security policies are boring, especially to people outside of IT ? in the way that children find their parents? or teachers? rules ?boring.? There?s a limit to how interesting one can make ?best practices for creating strong passwords? sound to the masses.

The point of such policies is to educate people on organizational rules and the habits of good security hygiene. This is the administrative layer of security controls: all of the rules, standards, guidelines, and training an organization puts in place as part of its overall security program. It?s the human-focused component that rounds out the other two general categories of security controls, according to Terumi Laskowsky, an IT security consultant and cybersecurity instructor at DevelopIntelligence. The other two categories are technical/logical controls (your hardware and software tools) and physical controls (things like building or site access).

Laskowsky notes that people tend to question the value of administrative controls. That?s partly because it can be difficult to measure or ?see? their effectiveness, especially relative to technical or physical controls. But Laskowsky and other security experts generally agree that they are necessary. Security is not a steady-state affair ? while our security tooling and processes are becoming more automated, a strong posture still requires human awareness, intelligence, and adaptability.

?Raising our security awareness through administrative controls allows us to start seeing the patterns of unsafe behavior,? Laskowsky says. ?We can then generalize and respond to new threats faster than security companies can come up with software to handle them.?

Security

Source URL: http://www.tuxmachines.org/node/156737

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://www.fosslife.org/10-most-commonly-used-foss-packages
[3] https://internetfreedom.in/dont-penalise-cybersecurity-researchers/
[4] https://www.schneier.com/blog/archives/2021/10/airline-passenger-mistakes-vintage-camera-for-a-bomb.html
[5] https://enterprisersproject.com/article/2021/10/security-policy-how-to-create