CROWDSOURCING CYBERSECURITY 101: COORDINATED VULNERABILITY DISCLOSURE

How to identify and fix cybersecurity vunlerabilities before adversaries can exploit them by encouraging outside experts to discover and report vulnerabilities in good faith.

Right now, cyber criminals and foreign nations are probing state systems for vulnerabilities. Malicious actors exploit errors in software code and other design flaws—some widely known, some unknown—to steal data and disrupt services. Defenders guard against attackers by trying to avoid, find, and fix these vulnerabilities before adversaries can use them to launch an attack.

These adversaries have competition. A global community of engineers, professors, entrepreneurs, high school students, and others regularly uncover security problems. Some do so accidentally, stumbling on vulnerabilities while they tinker with software for fun. Others publish research to gain recognition and respect. Many cybersecurity professionals are paid to test computer systems for flaws. Still others are altruists, hunting down vulnerabilities so they can help potential victims close a security gap before it is too late. Yet while many of these "white hat" hackers disclose vulnerabilities they find, many others do not.

Despite good intentions, white hats can face legal risks. Unclear language in computer crime laws may inadvertently apply to good faith research conducted by white hats. This legal ambiguity can dissuade white hats from reporting vulnerabilities to government and businesses.

Legal risks aside, disclosing a vulnerability is always a delicate process. A white hat who finds a software vulnerability faces a practical dilemma: Who should they tell, and when? Total secrecy means the problem cannot be fixed, leaving defenders (including government) exposed. Publicizing a vulnerability widely would let cyber criminals exploit it before stakeholders can repair the problem.

A CVD PROGRAM AIMS TO REDUCE RISK BY ALLOWING STATE AGENCIES TO:

Manage security vulnerabilities by encouraging outside parties to identify and share them with the state—while retaining the right to punish malicious behavior.

Maximize control over who knows what and when, minimizing the chance that criminals will exploit vulnerabilities before they can be repaired.

KEY BENEFITS OF A CVD PROGRAM

GET THERE FIRST – Cyber criminals are already probing state systems for weaknesses. Encouraging ethical, white hat hackers to find these flaws and report them to defenders will give states a better chance of closing security gaps before criminal slip through.

ACHIEVE LEVERAGE – A CVD program can lower the costs of preventing cyberattacks, and they can scale well with appropriate resourcing.

ACCESS RARE TALENT – A CVD policy invites a global community of volunteer experts to use their skills to spot cybersecurity problems. Crowdsourcing cybersecurity in this way taps into a worldwide talent pool that is normally out-of-reach for state hiring managers.

BUILD CYBERSECURITY EXPERTISE – A CVD program can boost the maturity of a cybersecurity program and offer metrics for assessing return-on-investment. If targeted toward a local or regional audience, it will help train people in high-demand skills that can grow the state economy.

CVD is not a turnkey solution. Success requires time, planning, and commitment. A "crawl, walk, run" attitude is essential: start small, manage expectations, and borrow from others.

For more information please contact David Forscey at dforscey@nga.org.