The critical role of vulnerability disclosure policies (VDP) in cybersecurity

BY ANNA HAMMOND · MAY 28, 2024 · LAST UPDATED ON MARCH 6, 2025

Cybercrime is projected to cost global enterprises a staggering $10.5 trillion annually by 2025, meaning the importance of robust cybersecurity measures cannot be overstated. To enhance organizational security postures, having a vulnerability disclosure policy (VDP) in place is fundamental.

In this blog, we'll further explore the role of VDPs in cybersecurity, their significance, and the best practices for implementing an effective policy. Read on to learn how to create a VDP that will help you reduce security risk and improve your overall security posture.

What is a vulnerability disclosure policy?

A VDP is a formalized process for receiving, reviewing, and responding to external reports of security vulnerabilities. It outlines how external parties like ethical hackers and security researchers can report vulnerabilities in systems, applications, or products. The primary aim of a VDP is to foster a structured, transparent, and efficient process for the identification, communication, and remediation of security vulnerabilities.

VDPs in cybersecurity strategies are fundamental for organizations

Why implement a vulnerability disclosure policy?

The implementation of a VDP is not just about improving security measures; it's a multifaceted strategy that benefits an organization in several ways. Let's dive into some of these benefits below.

VDPs encourage responsible reporting

VDPs provide a clear and secure channel for the disclosure of vulnerabilities, encouraging external parties to report rather than publicly disclose vulnerabilities. There are several ways a VDP helps achieves this goal:

1. Clear guidelines

VDPs provide explicit instructions on how security researchers should report vulnerabilities. This includes the types of vulnerabilities that are in scope, the proper channels for submission, and the format to report vulnerabilities.

2. Legal safe harbor

This element assures researchers that if they act in good faith and within the program's guidelines, they will not face legal repercussions. Researchers feel safe to report vulnerabilities without fear of legal

action.

3. Transparent timelines

VDPs typically outline a responsible disclosure timeline, allowing the organization time to address the vulnerability before public disclosure. This practice helps mitigate the risk of malicious actors exploiting vulnerabilities before security teams fix them. It encourages researchers to coordinate with the organization rather than disclosing vulnerabilities immediately.

4. Collaborative approach

VDPs foster a collaborative relationship between organizations and security researchers. By treating researchers as partners in security rather than adversaries, organizations can build trust and encourage ongoing, responsible vulnerability reporting.

5. Feedback mechanisms

Effective VDPs include mechanisms for providing feedback to researchers about the status and resolution of their reports. This transparency reassures researchers that their findings are taken seriously and acted upon, which promotes engagement and responsible behavior.

Enhanced security posture through better collaboration

By leveraging the expertise of external security researchers, organizations can identify and remediate vulnerabilities that might have been overlooked, thereby strengthening their security posture. VDPs also establish a foundation for ongoing communication and knowledge exchange with the global security community, keeping organizations informed about emerging threats.

Having a VDP in place demonstrates commitment to security

As Intigriti's Head of Security and IT, Niels Hofmans explains, "many researchers do not report vulnerabilities because they are unsure if they are allowed to do so legally. Without a VDP, a significant number of vulnerabilities go unreported or don't reach the right person within the organization, posing a security risk."

A well-defined VDP signals an organization's dedication to cybersecurity, enhancing its reputation and building trust among customers, partners, and stakeholders.

A VDP helps ensure legal compliance and mitigates legal risks

Various compliance frameworks mandate stringent security and data protection measures. A VDP helps in aligning with standards such as GDPR, HIPAA, and PCI DSS, among others. By setting clear guidelines and legal protections for reporters, a VDP also minimizes the risk of legal disputes and encourages more open collaboration with the security community.

The impact of not having a VDP

Not having a clear process for reporting bugs can leave your security team in the dark about vulnerabilities found by external stakeholders. During a recent poll of Intigriti's community, 65% of

respondents said they've found a vulnerability for a company without a vulnerability disclosure policy. Of those, 23% couldn't or chose not to report it. However, 42% still tried to through other means:

- 71% chose to report through customer service
- 32% guessed an email address
- 26% reported via social media
- 30% used a third-party such as disclosure assistance or CERT
- 13% chose to report the vulnerability via public disclosure.

A third of these researchers weren't informed of whether the report was received. Of the 66% who did receive acknowledgement, 29% said they could have been communicated with faster.

Keeping up with new demands creates a situation whereby security is performed in firefight mode rather than proactively addressing vulnerabilities before they can be exploited by cybercriminals. By working with security communities to find weaknesses, companies can better protect themselves from cyber threats—and VDPs let companies control how the vulnerabilities are reported.

Key components of an effective vulnerability disclosure policy

Crafting an effective VDP requires careful consideration of several elements to ensure clarity, efficiency, and compliance:

1. **Scope and background**: Clearly define which systems, applications, or products the policy covers. Provide context about what is critical from a security perspective.
2. **Reporting channels**: Specify how to report vulnerabilities, whether through email, online forms, or dedicated platforms like bug bounty programs.
3. **Responsible disclosure guidelines**: Outline the expectations for responsible disclosure, including guidelines on how to avoid unauthorized access, data exfiltration, or disruption of services during vulnerability testing.
4. **Acknowledgment and response**: Commit to acknowledging received reports promptly and provide timely updates to the reporters on the status of their submissions.
5. **Assessment and validation**: Describe the process for how reported vulnerabilities will be evaluated and prioritized based on their severity and potential impact.
6. **Remediation and public disclosure**: Explain the process for fixing vulnerabilities and the circumstances under which to disclose information about the vulnerability publicly.
7. **Legal protections**: Clarify any legal safeguards provided to researchers who comply with the policy's guidelines.
8. **Communication and transparency**: Emphasize the importance of maintaining open lines of communication with reporters throughout the process.

Hosting options for a VDP

Deciding where to host a VDP involves weighing the pros and cons of different approaches. The first is to host the policy on your own website. This approach offers full control and direct communication but may be resource-intensive and limit the policy's visibility.

Another option is to host your VDP on a bug bounty platform, such as Intigriti. Hosting a VDP on Intigriti's platform provides access to a skilled pool of researchers and ensures structured reporting and triage. Organizations might also consider a hybrid approach, maintaining a VDP on their own website while also utilizing platforms for broader engagement. Let's dive into this topic a little deeper.

The value of hosting VDPs on bug bounty platforms

Bug bounty platforms simplify and streamline the process for reporting security vulnerabilities. These platforms offer a centralized and user-friendly interface for researchers to submit vulnerability reports. Moreover, bug bounty platforms typically have established processes and procedures for handling vulnerability reports, which can enable organizations to respond to vulnerabilities in a timely and efficient manner.

Furthermore, the utilization of bug bounty platforms for VDPs offers access to a broad spectrum of security researchers. These platforms attract a diverse community of experts with varied levels of experience and backgrounds. By engaging with this community, organizations can tap into a collective pool of knowledge and skills, thereby enhancing the likelihood of effectively identifying and resolving vulnerabilities.

Having a VDP enhances an organizations cybersecurity resilience

The use of bug bounty platforms to host VDPs can significantly enhance an organization's security posture. It allows for the prioritization and resolution of vulnerabilities based on their severity and potential impact, while also fostering trust within the security community. These platforms serve as a valuable tool for organizations seeking to bolster their vulnerability management practices and safeguard their assets from potential threats.

Ready to start with vulnerability disclosure policies? Discover how our tailored solutions can protect your organization. Request your demo today!