bugcrowd

CASE STUDY

VULNERABILITY DISCLOSURE PROGRAM

The Office of the Minnesota Secretary of State takes a proactive approach to security

Industry Government

Founding Date 1858

Website sos.state.mn.us

Headquarters St. Paul, MN

The Situation

The Minnesota Secretary of State is an executive-branch statewide office serving Minnesotans in the areas of business services, elections and voting, address confidentiality, and other functions of state government. It has always taken a proactive approach to cybersecurity and saw an opportunity to expand its security posture by adopting a vulnerability disclosure program (VDP).

The Challenge

The Office of the Minnesota Secretary of State serves a broad range of customers through various divisions, including voters and potential voters, political candidates for office, business owners, and many others. Given that much of the information pertaining to such individuals and businesses must be kept confidential, it is crucial that the Office does everything possible to keep its data secure.

The Office of the Minnesota Secretary of State prioritizes proactively reducing risk exposure by innovating in security instead of just checking boxes. “We want to visibly demonstrate our commitment to security, build productive relationships with the hacker community, and leverage security testing and remediation that keep pace with innovation,” Dan Auger said.

It was the first time the Office had considered using a VDP, and it wanted to spend time objectively assessing the idea of working with hackers. Ultimately, it concluded that systems are already constantly being probed, so there are many benefits to proactively engaging the help of ethical hackers who are skilled in the same techniques.

Success Snapshot

Identified and addressed vulnerabilities, reducing the risk of security incidents.

Strengthened security operations by partnering with the hacker community.

Demonstrated a proactive commitment to cybersecurity, boosting customer trust.

Received vulnerability submissions quickly, with an average of 1.8 days in triage.

Received actionable findings via its VDP.

The Bugcrowd Solution

Once it decided to move forward with a VDP and work with the hacker community, the Office reached out to other states' offices and federal and regional security partners to gather a list of recommended VDP providers. It ultimately gravitated toward Bugcrowd because Bugcrowd has extensive experience and an excellent track record in this area, and Bugcrowd's programs emphasize long-term customer success.

The Office really has its finger on the pulse of trends, considering Bugcrowd is currently seeing a boom in hacker participation in government programs. In 2023, Bugcrowd saw a 151% increase in vulnerability submissions to government sector programs.

The Outcome

Thanks to Bugcrowd, the Office of the Minnesota Secretary of State has discovered hidden high-impact vulnerabilities, reduced noise, built productive relationships with hackers, improved its security brand, and defined a consistent way for the public to submit vulnerabilities. It has achieved its goals and received legitimate vulnerabilities that it can take action on.

Moving forward, it intends to expand on the scope of its current program.

Products involved

VULNERABILITY DISCLOSURE PROGRAM

"We have found our engagement with Bugcrowd to be **valuable.** We have received useful submissions that we would never have found with our automated scanning tools. It has been a great addition to our overall **security toolkit."**

— **DAN AUGER** Enterprise Architect • Office of the Minnesota Secretary of State