'Just Fix the Bug, and Nobody Will Get Hurt:'
HackerOne’s Mårten Mickos on Bug Bounties and Their Place in Government

Because everyone will be hacked — eventually.

Amanda Ziadeh
Fri, 08/17/2018 - 17:15

When it comes to detecting and fixing system vulnerabilities, bug bounties are gaining traction for their scalability, success and cost efficiency. But while patching the hole is technically enough, organizations and agencies should go the extra mile.

That’s what HackerOne CEO Mårten Mickos advised when GovernmentCIO Media caught up with him at Black Hat on Aug. 9. HackerOne is a bug bounty platform that connects businesses and government agencies with its 200,000-strong global
network of hackers hunting for vulnerabilities. You may recognize HackerOne from the Defense Department’s six bug bounty programs: Hack the Pentagon, Hack the Air Force (twice), Hack the Army, Hack the Defense Travel System, and most recently, Hack the Marine Corps.

To date, HackerOne has exposed 77,000 vulnerabilities that have been fixed. And it all starts with that first small step.

“Just start the program, start getting the reports, and over time, we will help you become faster,” Mickos said, referring to a quicker time-to-resolution after an incident occurs, because “true security will not happen until you act as quickly as the adversaries act.”

And ultimately, everyone will be hacked. But with the proper incident response team, response procedures (contact legal aid, public relations, workload backup, etc.) and strong threat intelligence, organizations can act fast. So, while time-to-resolution is post-incident, it shares the same principles with bug bounties.

“The faster you can fix things, the more secure you will be,” Mickos said.

So, Why Ethical Hacking Over Everything Else?

If you could completely secure code, that would be the best option. Unfortunately, “nobody can do that,” Mickos said.

White hat hacking and bug bounties slash cyberrisk by reducing the risk of a breach, because they up the cost for attackers, find the flaws and plug them so adversaries have fewer ways to break in.

Scanners catch the low-hanging fruit, and Mickos advises using them, too. But scanners won’t find the more elusive vulnerabilities, so they fall short.

Penetration testing is another option, where people come in to test internal networks. But in pentesting, you pay for effort, not for results.

“You end up paying for a lot of people who are just sitting there,” Mickos said, and it’s only for that point-in-time. So again, they fall short.

With bug bounty programs, Mickos said a vulnerability is typically found in 24 hours, from a varied and diverse group of unbiased hackers. Plus, “they find things
pentesters can never find, or an internal person can never find,” Mickos said. And considering the cost-per-vulnerability found, it can be a tenth of what it would be in pentesting, using a scanner or an internal asset.

“The model is fast, it’s productive and the cost-per-unit is low,” Mickos said. You only pay when something is found, so there’s no way to really waste money on a bug bounty program. And the program is continuous, meaning hackers around the country can look anytime for vulnerabilities.

**Agencies are Catching On**

The Pentagon is the largest government program HackerOne is a part of, but the company works with foreign public sector organizations, too.

“It is growing, but it’s typically the federal or the state-level agencies who come to us,” Mickos said. In fact, he said, agencies are more “pioneering and progressive,” whereas corporations can be more conservative.

“But the government is saying, ‘we need to do this’— that’s pretty cool,” he added.

Mickos was asked to testify before the U.S. Senate in February, providing it with the previous copy of HackerOne’s [Hacker-Powered Security Report](#). The members and staffers were “genuine, sincere, honest and have a goal that’s good for security,” he said.

In fact, the House Foreign Affairs Committee approved a bill in May called [Hack Your State Department Act](#), which would design and establish a Vulnerability Disclosure Program and a bug bounty program to improve the State Department’s cybersecurity. The White House also included bug bounty program recommendations in its December IT modernization [report](#), and the Senate Homeland Security and Governmental Affairs Committee advanced a Homeland Security Department reauthorization [bill](#) in March that includes a Hack DHS Bug Bounty Pilot Program.

But Mickos wouldn’t recommend the government mandate bug bounties into cybersecurity procedures, but rather, mandate vulnerability disclosure programs, which are bug bounties without the bounty.
He also recommends mandating agencies fix the bugs.

“If your company or organization holds customer information in your system, or you’re operating things that are for the benefit of consumers, you must have a way of fixing bugs,” Mickos said. “And I think the government should pass such a law — it would be very useful.”

And of course, these programs have their own challenges for government. Agencies have to make sure they patch vulnerabilities in a timely manner, and have the staff and resources to do so. Plus, it’ll take the IT staff time to sift through the slew of invalid reports. For example, Hack the Army received 416 reports, but only 118 were valid, according to HackerOne.

**Going the Extra Mile**

Fixing flaws is the one and only task Mickos said must be done after they’re found.

“If you just fix the bug, you’re in good shape,” he said. But if you are smart, responsible and eager to engage with the broader community, go public, he added. Disclosing the found bugs and publishing the hacker’s report mean other organizations can be aware of the flaws, learn from the report and fix their own vulnerabilities ahead of time.

“We also recommend customers to write a blog posting or an article about how they did it — people love to hear about this, and their customers will then respect the company more,” Mickos said.

And that’s part of the reason DOD has had such great results. Hackers see DOD recognizes them by name in a press release, motivating other hackers to work harder to find those vulnerabilities.

And if an organization is really diligent, it will go a step further by talking with its software engineers about they’ve learned, how to design or redesign software going forward, review system weaknesses and changes that need to be made in the framework, and find ways to ensure there are fewer of these vulnerabilities in the future.

But, ultimately, Mickos said to “just fix the bug, and nobody will get hurt.”