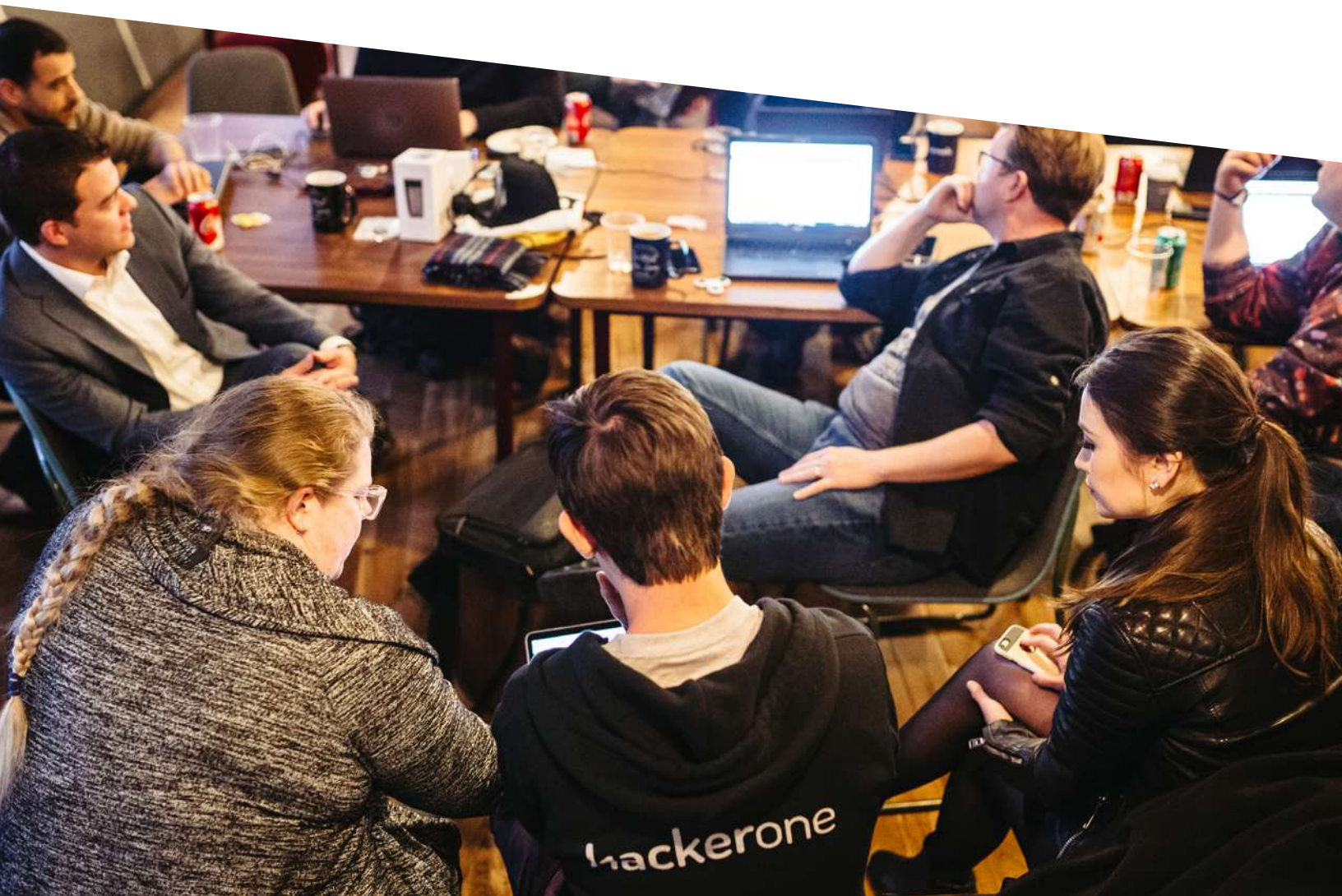
hackerone

What Percentage of Your Software Vulnerabilities Have GDPR Implications?

Published on hackerone.com Jan. 16th, 2018



GDPR is a regulation requiring organizations to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. And non-compliance will be expensive.

Do you know how many of your unknown vulnerabilities have the potential to cause a breach of consumer data? In other words, how many have GDPR implications?

We wondered the same thing, so we did some digging. Here's what we found.

UP TO A QUARTER OF YOUR BUGS COULD CAUSE GDPR ISSUES

We talked with LocalTapiola, a Finnish financial services company, about their efforts to prepare for GDPR. Their security team recently did an internal hackathon and found that 14 percent of the vulnerabilities reported during the event touched consumer data in one way or another.

Taking things one step further, to help them find more GDPR-related bugs, they guided white-hat hackers by adding a bonus bounty for GDPR-related reports submitted to their bug bounty program.

Leo Niemela
CHIEF SECURITY OFFICER

"GDPR is coming to effect in May 2018 and we want to show to our customer that we are serious about it," said Leo Niemelä, Director, ICT Risk Management and Security, CSO at LocalTapiola. "This GDPR bonus payment idea is totally new for us. We want to be proactive and we want to show our customer that we are taking information security seriously at every level."

We've seen other anecdotal data showing that a sizable portion of the vulnerabilities found via hacker-powered security programs (bug bounties, vulnerability disclosure policies, etc.) have GDPR ramifications, meaning they impact consumer data in some way.

> A quick and unscientific analysis we ran internally showed that **up to 25 percent of incoming bug reports in HackerOne bug bounty programs could impact consumer data.** That makes them relevant to GDPR, and it shows just how many bugs could be open to the exact types of breaches GDPR is targeting.

GDPR EMPHASIZES BREACHES, NOT BUGS

GDPR Article 33 states that data breaches must be disclosed to the organization's supervisory authority "without undue delay and, where feasible, not later than 72 hours after having become aware of it." It's not uncommon these days for organizations to require weeks or months to remedy a vulnerability.

In our Hacker-Powered Security Report 2017, we found that the fastest industry, ecommerce & retail, takes an average of 31 days to fix a reported vulnerability.

The slowest takes 90 days. And that's when it's reported, triaged, and managed via a known process, not in the chaos of an emergency, fire-drill-like situation immediately after a breach.

> Our advice regarding GDPR has always been to find and fix vulnerabilities before they can be exploited. There's no disclosure requirement for bugs, only for breaches, and running a bug bounty program is a great way to identify vulnerabilities before the bad guys do.

Furthermore, GDPR requires companies to maintain "...a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing," which is exactly where bug bounties fit in.

Here's another reason to start getting your GDPR-driven security processes underway: CSO predicts that GDPR regulators will be looking to make an example of someone in 2018. "The safe plan," says CSO, " is to make your best effort to be in compliance by May 25."

ALL SOFTWARE HAS BUGS, SO FIND THEM QUICKLY

Think about how many unknown vulnerabilities are lurking in your own code. One estimate says that there are between 15 and 50 errors per 1,000 lines of delivered code. Consider also that a small smartphone app has about 10,000 lines of code (on the other end of the spectrum, OS X has 86 million).

Software bugs are of course not 100% equivalent to security vulnerabilities. Many if not most bugs do not cause security vulnerabilities. However, security vulnerabilities are likely lurking in those bugs.

With the 15–25 percent rate of GDPR-relevant security vulnerabilities, it doesn't take a math wiz to figure out that every application most likely has dozens if not hundreds of GDPR-relevant bugs hiding in the code.

Even with robust security, development, and quality assurance efforts, the number of unknown bugs in your code that have GDPR ramifications is big enough to be scary.

GET AHEAD OF VULNERABILITIES TO GET AHEAD OF GDPR

Working to meet GDPR's rapidly-approaching effective date takes effort, money, and cross-organizational teamwork. At this point, if you collect any data on consumers, you should be working towards GDPR compliance. No matter where you reside or who you target, if an EU citizen leaves a data breadcrumb with you, you're bound by GDPR's rules.

If you have yet to begin working in earnest towards GDPR compliance, do not delay.

Some companies, like HackerOne customer LocalTapiola, wisely got a head start. "Our GDPR project has been in progress since April, 2016," says Leo. "Our budget for the GDPR project is estimated at €3–4 million ($3.5–4.7 million) and my team is running that project together with our legal department."

Others, however, are behind in the sprint to May 25. In the same article noted above, CSO predicts that "many, if not most, U.S. companies will not meet GDPR compliance by deadline."

If you're in that bucket, HackerOne can help you:

1. *Implement a Vulnerability Disclosure Policy (VDP). This is a great first step towards identifying vulnerabilities well before they turn into breaches.*

2. *Determine whether a bug bounty program is right for you at this time. GDPR requires regular testing and assessing of your systems. A continuous bug bounty program provides incentives to get white-hat hackers to find more bugs, so you're finding them before they turn into breaches.*

GDPR TAKES EFFECT IN 128 DAYS

May 25, 2018 is 128-days away, counting from today's date: January 16, 2018. Getting your process in place for identifying and fixing bugs in a controlled manner will help you close more gaps before they can be exploited. In about 15–25 percent of the cases, you're plugging another potential GDPR hole. Contact us to learn more about how HackerOne can help.

ABOUT HACKERONE

HackerOne is the #1 hacker-powered security platform, helping organizations receive and resolve critical vulnerabilities before they can be exploited. More than 1,000 organizations, including the U.S. Department of Defense, U.S. General Service Administration, General Motors, Twitter, GitHub, Nintendo, Panasonic Avionics, Qualcomm, Square, Starbucks, Dropbox and the CERT Coordination Center trust HackerOne to find critical software vulnerabilities. HackerOne customers have resolved over 57,000 vulnerabilities and awarded over $23M in bug bounties. HackerOne is headquartered in San Francisco with offices in London and the Netherlands.

MAKE THE INTERNET SAFER

WWW.HACKERONE.COM / SALES@HACKERONE.COM / +1 (415) 891-0777

hackerone