An die Verlagsetage

Die Jagd nach Fehlern im Programmcode ist eröffnet

Wir laden Hackerinnen dazu ein, in unsere Systeme einzudringen. Warum das eine gute Idee ist.

Von Patrick Venetz, 07.12.2021

Täglich nutzen viele tausend Menschen die Republik.

Sie schreiben Dialogbeiträge, verlängern ihre Mitgliedschaft – und lesen Beiträge. So, wie Sie das gerade tun.

Dabei stossen Nutzer täglich viele tausend Zeilen Programmcode an.

Sie geben damit unseren Systemen die Anweisungen, welche Texte und Bilder aus den Datenbanken geladen werden sollen oder welches Konto seinen Republik-Zugang teilen will.

Wir nutzen dafür eigens für unsere Zwecke geschaffene Software, die für alle einsehbar ist. Darin zu finden sind unter anderem der Programmcode der Website, der App und der Schnittstelle, die Inhalte wie Texte oder Bilder an die Website und die App ausliefert.

Jede Woche ändern sich Hunderte Zeilen dieses Programmcodes, um neue Funktionalitäten zu unterstützen oder Fehler zu entfernen, denen Sie oder wir auf die Schliche gekommen sind.

Fehlern auf die Schliche zu kommen, ist nicht einfach.

Im Tech-Team der Republik besitzen wir Instrumente, um Fehler überhaupt erst zu vermeiden. Uns helfen gute Planung, die Nutzung von Industriestandards, technisches Verständnis, Tests und ein Vier-Augen-Prinzip, bevor wir Änderungen auf unseren Systemen ausrollen.

Aber es gibt unzählige Beispiele, wie schnell sich die gemeine Softwareentwicklerin in falscher Sicherheit wiegen kann. Uns graut davor, eines Tages eine Mitteilung an Nutzer verschicken zu müssen, in der steht, dass Kundendaten abgegriffen wurden.

Um einer solchen Situation vorzubeugen, brauchen wir etwas anderes: einen geschulten Blick von aussen.

Deshalb legen wir ab sofort ein sogenanntes Bug-Bounty-Programm auf (also ein «Softwarefehler-Kopfgeld-Programm»). In Zusammenarbeit mit der Bug Bounty Hub AG laden wir wohlgesinnte Hackerinnen aus aller Welt ein, Sicherheitslücken in den Systemen der Republik zu finden.

Innerhalb eines nach Schweizer Recht abgestützten Rahmens können sie die Systeme der Republik «penetrieren» und gefundene Sicherheitslücken melden – und erhalten dafür eine monetäre Belohnung.

Dabei haben diese *friendly hacker* auf nichts anderes Zugriff, als Sie auch hätten. Bloss können sie tiefer graben. Sie versuchen, an Rechte und Daten zu gelangen, die wir nicht für Aussenstehende vorgesehen haben. Das hört sich gruselig an, ist aber eigentlich sehr zuvorkommend. Sie geben den Bösewicht, bevor echte Bösewichte gewollt Ungewolltes tun.

Um zu verstehen, wie heftig das ganze Vorhaben für uns werden könnte, haben wir bereits eine Art Probelauf gestartet, einen «Penetrationstest».

Während zweier Tage im November sahen sich von Bug Bounty Hub ausgewählte Hacker in unserem Code und in unserer technischen Infrastruktur um. Sie versuchten, auf der Website Defekte zu finden, und starteten automatisierte Angriffsversuche gegen unsere Infrastruktur. Anschliessend gaben sie uns eine Einschätzung über kritische Bereiche und Möglichkeiten zur Optimierung.

Der daraus entstandene, sehr technisch geratene Bericht hat bereits zu Verbesserungen geführt.

Nun startet das eigentliche Bug-Bounty-Programm, und wir hoffen, tiefer liegende, nicht offensichtliche Schwachstellen und Programmfehler zu finden – fortlaufend und bevor sie ausgenutzt werden.

Falls Sie zufällig zur Gilde der Hackerinnen gehören, hier finden Sie Einlass.