Die Robustheit der kalkulierten Demokratie

Abraxas sammelt seit einigen Monaten Erfahrungen mit einem eigenen Bug-Bounty-Programm und der Offenlegung des Quellcodes einer Software zur Ermittlung von Wahl- und Abstimmungsergebnissen. Das verantwortliche Team sieht positive Effekte bis in die eigene Organisation hinein. Ein Zwischenstand.

Der Autor
Peter Gassmann, Head of Solution Engineering und Mitglied der Geschäftsleitung, Abraxas Informatik AG

Die ICT-Welt wandelt sich in immer dichter aufeinanderfolgenden Zyklen. Die Digitalisierung nimmt auch im Staat an Fahrt auf. Traditionelle Methoden und Mindsets stehen auf dem Prüfstand. Die digitale Kriminalität ist so aktiv wie nie. Die altbekannte Methode der Softwareentwicklung genügt nicht mehr.

Den eigenen Code geheim zu halten, um sich vor Angriffen zu schützen, das erweist sich im gegenwärtigen Cybersecurity-Umfeld als kontraproduktiv. Darum braucht es neue Ansätze und Methoden – das hat Abraxas erkannt und mit der Entwicklung des neuen Ergebnisermittlungssystems für die Kantone St. Gallen und Thurgau neue Wege beschritten.

Vorbereitung auf das Unbekannte

Bug-Bounty-Programme sind nichts Unbekanntes, seit Jahren sind sie üblich, zum Beispiel bei den Grossen der Cloud-Branche. Im Umfeld der öffentlichen Hand in der Schweiz sind sie jedoch ein Novum; der Bund war hier Vorreiter mit dem ersten Pilotprogramm im Frühjahr 2021. Abraxas als Organisation tat sich anfänglich schwer mit dem Gedanken, Bugs künftig nicht mehr nur intern zu behandeln.

Schwachstellen entdecken und beheben, das sollte im anspruchsvollen Umfeld und mit immer komplexerer Software nicht mehr hinter einem Paravent geschehen, sondern mit Unterstützung von aussen. Ohne falsche Scham wegen der Fehler, sondern mit Stolz auf eine Software, die einen wesentlichen Beitrag an die Digitalisierung von Verwaltung, Wirtschaft und Gesellschaft leistet. Die Kantone St. Gallen und Thurgau hatten bei der Ausschreibung der Nachfolgegeneration ihres Ergebnisermittlungssystems im Sinn, mit einer transparenten Softwareentwicklung die Diskussion um die Digitalisierung der Demokratie anzuregen und die Software so sicher wie nur möglich zu machen.

Private Bug Bounty: Attacken im kontrollierten Umfeld

Das Abraxas-Team unter der Leitung von Chief Software Architect Daniel Scherrer erhielt im August 2021 die Freigabe für ein Bug-Bounty-Programm mit Prägung durch Abraxas, geführt vom Team, mit Unterstützung durch Bug Bounty Switzerland (bugbounty.ch), die Monate früher auch das erste Bundesprogramm begleitet hatte. Es beschleunigte die Entwicklung des Abraxas Security Frameworks, das sich im Kern aus einem Bündel an Methoden zur sicheren Softwareentwicklung und Tools sowie Tests in drei Phasen zusammensetzt: Auf die interne Phase des Testens und Überarbeitens des Codes folgt das Abraxas-Bug-Bounty-Programm in zwei Teilen mit schrittweiser Code-Offenlegung.

Den Beitrag finden Sie auch online
www.netzwoche.ch

Es war für das Team essenziell, gut vorbereitet in das Programm zu gehen. Jeder virtuelle Stein im Code wurde vor dem Start des privaten Programms am 23. Mai umgedreht, jedes Szenario bedacht und jeder denkbare Angriffsversuch schon einmal gestartet. Doch … Hacker denken anders. Der erste Angriff galt nicht dem definierten Ziel, dem Fachteil der Lösung, sondern der Komponente für die Verwaltung der Berechtigungen und Identitäten.

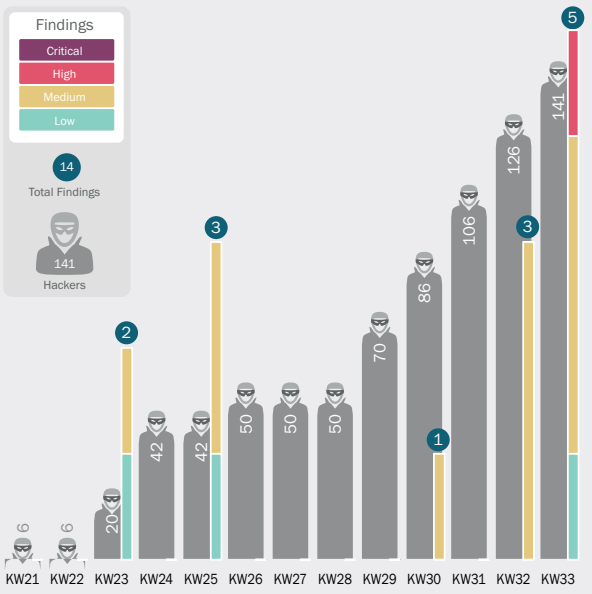
Software ist heute eben kein Monolith, sondern bildhaft gesprochen eine Bausteinsammlung verschiedener Codes, Teams, mit unterschiedlichen Ressourcen – und unter Umständen auch noch geprägt durch althergebrachte Muster. Rasch erweiterte das Abraxas-Bug-Bounty-Team seinen Fokus und holte die Komponente mit den Entwicklern vor den bildhaften Paravent. «Diese schnelle Reaktion belegt den Nutzen eines solchen Programms nicht nur hinsichtlich des Schwachstellen-Managements», sagt Daniel Scherrer. «Die Organisation hinter den Entwicklern kann sich neu ausrichten.» Das Programm startete mit einem «rejected» und einer Sonderprämie für den Researcher, der die Scope-Erweiterung angeregt hatte.

Öffnung für die ganze Welt

Mehr als 140 Researcher waren in der privaten Phase in unterschiedlicher Intensität aktiv. Daraus resultierten 28 Findings, von denen 12 akzeptiert werden konnten und zu einer Auszahlung von Prämien in der Gesamthöhe von 12 400 Franken führten. Es gab mit Blick auf den Scope genau eine Schwachstelle, die als «high» eingestuft, jedoch nicht als «critical» beurteilt

ERGEBNISSE

Anzahl Security-Researcher und akzeptierte Findings in der Private-Bug-Bounty-Phase bis Ende KW 33



Quelle: Abraxas

wurde. Der CVSS (eine standardisierte Berechnung der Kritikalität einer Schwachstelle) wird vom Security Researcher selbst eingeschätzt und danach im Dialog mit dem Team realistisch fixiert. So sind etwa gewisse Schwachstellen weniger gewichtet, weil das Ergebnisermittlungssystem selbst nicht mit dem Internet verbunden ist, sondern nur im privaten Netzwerk der Kantone läuft.

Das seit dem 22. August laufende öffentliche Programm hat nicht zu einem markanten Anstieg von Registrierungen von Security-Researchern geführt – Voraussetzung für das Einstreichen einer Prämie, wenn eine Lücke gefunden wurde. Auch von einer Findings-Flut kann keine Rede sein. Das Team bearbeitet sie normalerweise innerhalb eines Arbeitstages und stellt eine ausführliche Analyse bereit. Möglicherweise benötigen die Security-Researcher mehr Zeit, um das anspruchsvolle Ergebnisermittlungssystem zu untersuchen. Dazu steht ihnen auch der Quellcode zur Verfügung, im öffentlichen Programm in mehreren Schritten auf GitHub publiziert. Damit gleichen sie ihre Erkenntnisse mit dem Code ab, was zu besseren Reports führt.

Erstes Fazit und Erkenntnisse

Das Abraxas-Bug-Bounty-Programm für das Ergebnisermittlungssystem dauert noch einige Monate; berücksichtigt werden dabei auch Erkenntnisse aus dem Parallelbetrieb an realen Wahl- und Abstimmungssonntagen. Dabei berechnet das neu entwickelte System die Resultate, während das bisherige System weiterhin das rechtlich abgesicherte Schlussresultat liefert. Die Rückmeldungen aus den Gemeinden sind positiv. Und im Bug-Bounty-Programm werden die neu entdeckten Schwachstellen laufend behoben. Wird das System in wenigen Monaten den nötigen Grad an Robustheit erreicht haben, steht einer Ablösung aus technischer Sicht nichts mehr im Weg. Im Frühling 2023 soll es nach heutigem Stand so weit sein.

Schon jetzt lassen sich einige Erkenntnisse gewinnen. Ist die Software sicher? Sie ist durch das Programm robuster geworden, enthält weniger Schwachstellen. Damit steigt der Aufwand auf Hacker-Seite, es braucht mehr Know-how, Mittel und Energie, eine Kampagne erfolgreich abzuschliessen. Hacken ist ein Geschäftsmodell. Stimmen Aufwand und potenzieller Ertrag nicht, wenden sich die Kriminellen einem neuen Opfer zu.

Software ist eben niemals fehlerfrei, doch es braucht für eine Balance zwischen nicht entdeckten und relevanten entdeckten Schwachstellen eine ausreichend grosse, durchmischte Basis an Security-Researchern. Dabei ist ein erfahrener externer Dienstleister mit Zugriff auf die Ethical-Hacker-Community wertvoll. Mit ihr sollte ein ständiger Dialog auf Augenhöhe stattfinden. Rückstufungen des prämienrelevanten CVSS sowie Ablehnungen von Findings müssen nachvollziehbar begründet werden. Innerhalb kurzer Zeit sollte auf Einsendungen der Community reagiert werden – mit etwas mehr als einem Tag zählt Abraxas zu den schnellen Partnern der Security-Researcher. Das schätzt laut einer Umfrage die Community ebenso wie die klaren und starken Analysen. Eine gute Vorbereitung umfasst nicht nur technische Aspekte, sondern auch die Kommunikation. Es gilt, Szenarien vorzubereiten und Kommunikationsbausteine zu entwickeln: Je nach Finding und Verlauf des Programms müssen die Hintergründe rechtzeitig ausgeleuchtet werden. Wir haben dazu einen Blog aufgebaut: blog.abraxas.ch. Ein durchgehender Informationsfluss vom Arbeitsplatz bis zum Entwicklerteam und weiteren Anspruchspersonen stärkt die Kultur der Sicherheit generell. Das Abraxas-Bug-Bounty-Programm hat bereits einige Wirkung gezeigt, Silos aufgebrochen und das Wissen um die aktuellen Gefahren im Cyberraum gefestigt. Doch der Weg ist noch lang.

Eines ist nämlich sicher: Software ohne Schwachstellen gibt es nicht. Auch in Zukunft werden wir darum nur mit Offenheit, sicheren Prozessen, kontrollierten Angriffen und Mut zur ausbalancierten Lücke die Digitalisierung meistern.

DAS ABRAXAS-BUG-BOUNTY-PROGRAMM

Seit Frühling 2022 prüfen mehr als 140 Security-Researcher das Ergebnisermittlungssystem inkl. Identitäts- und Berechtigungssystem auf Herz und Nieren. Das Programm soll mit dem ersten offiziellen Einsatz des Ergebnisermittlungssystems an einem Wahl- und Abstimmungssonntag im nächsten Frühling 2023 vorläufig abgeschlossen werden. Aufgrund der positiven Wirkung will Abraxas künftig weitere Bug-Bounty-Programme auflegen.