// KI-Hub VON STRUKTURAFLOW

IT-SECURITY

Bug-Bounty-Programme schließen: Was das für Ihre IT-Sicherheit bedeutet

cURL stoppt. HackerOne pausiert. Cloudflare zieht sich zurück. Warum die KI-Flut die Bug-Bounty-Welt umbaut — und was das für KMU-Sicherheit bedeutet.

AUTOR
Natascha Reiner

VERÖFFENTLICHT
26. April 2026

ONLINE LESEN
https://wissen.strukturaflow.it.com/bug-bounty-schliessungen-it-security-kmu/

Fast täglich erreichen uns in der IT-Branche Meldungen, die vor einem Jahr noch undenkbar gewesen wären: Ein weiteres Bug-Bounty-Programm schließt. Eines pausiert. Ein anderes zieht sich hinter geschlossene Türen zurück und ist für normale Sicherheitsforscher nicht mehr zugänglich.

Das klingt nach einem internen Problem der Tech-Welt. Es ist keines. Es ist ein strukturelles Signal — und ich möchte Ihnen erklären, warum Sie das als Unternehmen, als IT-Verantwortliche oder als Betreiber digitaler Infrastruktur direkt betrifft.

Was ist ein Bug-Bounty-Programm – und warum sollte mich das interessieren?

Bug-Bounty-Programme sind bezahlte Sicherheitsprüfungen durch externe Experten. Unternehmen und Open-Source-Projekte laden unabhängige Sicherheitsforscher ein, ihre Software auf Schwachstellen zu untersuchen — und zahlen für jeden validen Fund eine Belohnung (englisch: Bounty). Das Modell ist seit über zwei Jahrzehnten eine der effektivsten Methoden der koordinierten Sicherheitsforschung. Tausende Augen schauen auf Code, den das eigene Entwicklerteam nicht mehr neutral betrachten kann.

Vereinfacht gesagt: Bug Bounties sind das Gegenteil von Vogel-Strauß-Politik in der Softwaresicherheit. Firmen sagen aktiv: „Bitte findet unsere Fehler, bevor Kriminelle es tun — und wir zahlen euch dafür.„

Wenn dieses System kollabiert, fällt eine wichtige Schutzschicht weg. Nicht nur für die großen Anbieter. Sondern für alle, die deren Software einsetzen.

Die Fälle, die 2026 das System erschüttern

cURL: Ende eines sechsjährigen Programms

cURL ist eine Softwarebibliothek, die auf nahezu jedem Webserver der Welt läuft — Sie nutzen sie täglich, ohne es zu wissen. Im Januar 2026 stellte Projektgründer Daniel Stenberg das Bug-Bounty-Programm nach sechs Jahren und rund 86.000 USD ausgezahlter Belohnungen ein.

Der Grund war kein finanzieller. Es war Erschöpfung.

In den ersten drei Wochen des Jahres 2026 gingen 20 Sicherheitsmeldungen ein. Keine einzige enthielt eine echte Schwachstelle. Alle waren von KI generiert — technisch klingend, oberflächlich plausibel, inhaltlich wertlos. Das Kernteam verbrachte hunderte Stunden damit, KI-Halluzinationen über fiktive Codepfade zu widerlegen.

Seit dem 1. Februar 2026 gibt es für cURL keine monetären Belohnungen mehr. Meldungen werden direkt über GitHub abgewickelt — der finanzielle Anreiz für massenhafte, automatisierte Einreichungen ist bewusst entfernt.

METRIK	PHASE 2019-2024	PHASE 2025	STAND JANUAR 2026
Gesamtauszahlungen	~$80.000	~$6.000	$0 (eingestellt)
Anteil KI-generierter Meldungen	< 2 %	~20 %	> 95 %
Triage-Status	handhabbar	überlastet	abgebrochen

Internet Bug Bounty: Vollständiger Stopp im März 2026

Die Internet Bug Bounty (IBB), betrieben von HackerOne und verantwortlich für kritische Infrastrukturprojekte wie Node.js und Ruby, stoppte am 27. März 2026 alle Einreichungen. Die Begründung: KI-gestützte Forschung hat die Geschwindigkeit der Schwachstellenentdeckung so weit beschleunigt, dass das Gleichgewicht zwischen Fund und Behebungskapazität fundamental gestört ist.

HackerOne formulierte es ungewöhnlich direkt: Das Modell der offenen Einreichung sei „gebrochen", wenn ein KI-System in Sekunden hunderte potenzielle Probleme markieren kann, für deren Bearbeitung ein menschliches Team Monate braucht.

Cloudflare & Mozilla: Rückzug hinter geschlossene Türen

Cloudflare und Mozilla schließen ihre Programme nicht — sie machen sie exklusiv. Cloudflare hat ein VIP-Bug-Bounty eingeführt: ein geschlossener Kreis handverlesener Forscher mit tiefgehender Nischenexpertise. Belohnungen für kritische Lücken liegen bei bis zu 15.000 USD — aber der Zugang ist nicht öffentlich.

Mozilla verlangt seit 2026 zwingend reproduzierbare Testfälle. Theoretische Bedenken ohne Beweis werden kategorisch niedriger priorisiert. Die Messlatte steigt — und damit scheiden viele Einreicher aus, die früher noch mitgespielt haben.

Das Signal ist eindeutig: Der offene Marktplatz für Sicherheitsfunde schließt sich. Was bleibt, sind geschlossene Expertennetzwerke.

Die eigentliche Frage: Werden Bugs überhaupt noch gemeldet?

Hier liegt der Kern des Problems — und ich möchte ihn direkt ansprechen, weil er in der öffentlichen Debatte zu wenig Raum bekommt.

Sicherheitsforschung ist zeitintensiv, komplex und erfordert tiefes technisches Wissen. Bug-Bounty-Programme haben über Jahre ein Ökosystem von spezialisierten Forschern finanziert, die genau diese Arbeit leisten. Wenn der monetäre Anreiz wegfällt oder der Zugang verschlossen wird — was passiert dann mit dem Wissen, das diese Forscher finden?

Es gibt drei mögliche Wege für eine ungemeldete Schwachstelle:

1. **Sie bleibt unentdeckt** — bis ein Angreifer sie findet.
2. **Sie wird intern gemeldet** — wenn die Forscher guten Willen haben und einen zugänglichen Kanal finden.
3. **Sie landet auf dem Darknet-Markt** — wo für kritische Zero-Days in weitverbreiteter Software fünf- bis sechsstellige Summen bezahlt werden.

Die Schließung öffentlicher Programme treibt einen Teil dieser Funde in Richtung Option 1 und 3. Das ist keine Spekulation. Das ist eine wirtschaftliche Logik.

Die KI-Flut und das Paradox dahinter

Verstehen Sie mich nicht falsch: Künstliche Intelligenz ist kein Feind der IT-Sicherheit. Sie ist einer der mächtigsten Verbündeten, die wir haben.

Aber das, was gerade passiert, ist ein klassisches Überlastungsproblem mit einer neuen Dimension.

KI-Systeme können heute tausende Zeilen Code in Sekunden auf potenzielle Fehler scannen. Das ist gut. Das Problem: Die Verifizierung, ob ein gefundenes Muster wirklich eine ausnutzbare Schwachstelle ist — und das anschließende Patching — bleibt zutiefst menschlich, zeitintensiv und ressourcengebunden.

Aus meiner täglichen Arbeit mit Entwicklerteams in der Region weiß ich: Die verfügbaren Ressourcen für Bug-Fixing sind in den meisten Betrieben chronisch knapp. Das ist keine Kritik — es ist Realität. Entwicklerinnen und Entwickler arbeiten an neuen Features, halten laufende Systeme am Leben, managen Updates. Die Kapazität für systematische Sicherheitsarbeit ist begrenzt.

Was passiert, wenn diese Teams jetzt mit einer Flut von KI-generierten Meldungen konfrontiert werden — von denen ein Teil valide ist, ein Großteil aber nicht?

Eigenschaft	Traditionelles Hacking	KI-gestütztes Hacking 2026
Geschwindigkeit	Stunden bis Tage pro Bug	Sekunden bis Minuten
Skalierbarkeit	limitiert durch Expertise	nahezu unbegrenzt
Kosten pro Meldung	hoch	marginal
Triage-Aufwand	normal	extrem hoch

Das Ergebnis ist ein schwieriger Kreislauf, den ich in meiner Arbeit immer wieder beobachte: Sicherheitslücken haben — zu Recht — höchste Priorität. Aber je mehr Ressourcen in die Triage und das Patching fließen, desto weniger bleibt für Weiterentwicklung. Der technische Fortschritt verlangsamt sich. Gleichzeitig steigt der Druck durch neue Meldungen weiter.

Das ist kein Versagen einzelner Teams. Das ist ein systemisches Problem, das durch die Asymmetrie zwischen automatisierter Entdeckung und manueller Behebung entsteht.

Was das für Ihr Unternehmen bedeutet

Sie setzen täglich Software ein — ob als Cloud-Dienst, als gehostete Anwendung oder als lokal installiertes System. Diese Software enthält Abhängigkeiten: Open-Source-Bibliotheken, Frameworks, externe Komponenten. Viele davon waren bisher durch aktive Bug-Bounty-Programme abgesichert.

Wenn diese Programme wegfallen oder sich in geschlossene Elitekreise zurückziehen, entstehen konkrete Risiken:

Kleinere Projekte fallen durchs Raster. Hochkapitalisierte Unternehmen wie Cloudflare oder Google bauen sich mit VIP-Programmen und KI-gestützter Eigenentwicklung eine Sicherheitselite auf. Open-Source-Projekte und kleinere Softwareanbieter, die ihre öffentlichen Programme einstellen, verlieren dagegen eine wichtige Schutzschicht — ohne direkten Ersatz.

Die Remediation Gap wächst. Weniger als 1 % der durch moderne KI-Modelle entdeckten Schwachstellen können zeitnah behoben werden. Die Frage, wie schnell eine Organisation patchen kann, wird wichtiger als die Frage, wie viele Bugs gefunden werden.

Abhängigkeiten von externen Sicherheitsmodellen werden riskanter. Wer ausschließlich auf Cloud-Software von Drittanbietern setzt, ist direkt abhängig davon, wie gut diese Anbieter ihre Sicherheitsinfrastruktur in diesem veränderten Umfeld aufrechterhalten.

Die DACH-Perspektive: Regulatorik trifft auf Realität

Im deutschsprachigen Raum kommt ein weiterer Faktor hinzu. Die rechtliche Grauzone rund um den sogenannten „Hacking-Paragrafen„ (§ 202a StGB) macht unabhängige Sicherheitsforschung in Deutschland rechtlich risikoreich — selbst wenn sie gutgläubig und im Interesse der Allgemeinheit erfolgt.

Gleichzeitig verschärfen NIS-2 und der Cyber Resilience Act der EU die Anforderungen an strukturierte Schwachstellen-Meldewege. Vulnerability Disclosure Policies (VDPs) werden zur regulatorischen Pflicht — unabhängig davon, ob monetäre Belohnungen damit verbunden sind.

Das bedeutet: Unternehmen müssen Meldewege für Sicherheitslücken definieren und dokumentieren. Wer das nicht tut, riskiert Compliance-Probleme — und wer es tut, muss gleichzeitig die Kapazität haben, eingehende Meldungen ernsthaft zu bearbeiten.

REGELUNG	INHALT	AUSWIRKUNG
§ 202a StGB	Strafbarkeit des Ausspähens	erfordert klare Befugnisregelung
NIS-2-Richtlinie	Meldepflichten kritischer Sektoren	erhöht Druck zur VDP-Implementierung
Cyber Resilience Act	Produktsicherheit & Schwachstellen-Management	verpflichtet Hersteller zu Meldewegen

Kontrolle beginnt dort, wo Sie die Infrastruktur selbst in der Hand halten

Hier möchte ich einen Punkt ansprechen, der mir in Kundengesprächen immer wieder begegnet — und der direkt mit dem zusammenhängt, was wir gerade besprochen haben.

Bei Strukturaflow hosten wir unsere eigene IT-Infrastruktur selbst. On-Premise. Das ist keine nostalgische Entscheidung gegen die Cloud — es ist eine bewusste Sicherheitsentscheidung. Und es ist eine Entscheidung, die wir auch für Kunden umsetzen, wenn die Anforderungen es nahelegen.

Was bedeutet das im Kontext dieses Artikels?

Wer seine IT selbst hostet oder unter kontrollierter Verwaltung betreibt, hat eine direkte Möglichkeit auf die Software-Auswahl, die eingesetzten Versionen und die Update-Zyklen Einfluss zu nehmen. Die Abhängigkeit davon, ob ein Drittanbieter sein Bug-Bounty-Programm noch aktiv betreibt oder ob dessen Sicherheitsinfrastruktur der KI-Flut standhält, wird reduziert.

Das schafft keine vollständige Immunität. Sicherheitslücken existieren in jeder Software, egal wo sie läuft. Aber es schafft etwas Wichtiges: **Handlungsfähigkeit**. Die Möglichkeit, auf Meldungen zu reagieren, Patches eigenständig einzuspielen, Software-Abhängigkeiten aktiv zu managen — anstatt auf einen externen Anbieter zu warten, der möglicherweise gerade mit hunderten anderen Meldungen beschäftigt ist.

Was Sie jetzt konkret prüfen sollten

Sie müssen kein IT-Sicherheitsexperte sein, um die richtigen Fragen zu stellen:

1. Welche Software setzt Ihr Unternehmen ein — und wer pflegt sie? Gibt es für die eingesetzten Systeme einen aktiven Wartungskanal? Wer ist verantwortlich für Security-Updates?

2. Wie schnell werden kritische Patches in Ihrer Umgebung eingespielt? Die Remediation Gap — die Zeit zwischen Bekanntwerden einer Lücke und dem Patch — ist oft das entscheidende Angriffsfenster.

3. Haben Sie eine Vulnerability Disclosure Policy (VDP)? Nicht nur aus Compliance-Gründen, sondern weil Sie damit einen strukturierten Kanal schaffen für den Fall, dass jemand eine Schwachstelle in Ihren Systemen findet.

4. Kennen Sie die Open-Source-Abhängigkeiten in Ihrer Software? Viele Unternehmen nutzen Bibliotheken und Frameworks, ohne zu wissen, wer dahintersteht — und ob dieses Projekt noch aktiv gewartet wird.

Fazit: Die Ära der offenen Bug Bounties geht zu Ende – was kommt danach?

Die Schließung und Transformation von Bug-Bounty-Programmen ist kein vorübergehendes Phänomen. Sie ist das sichtbare Symptom einer strukturellen Verschiebung: Die automatisierte Schwachstellenentdeckung durch KI hat ein Tempo erreicht, das die manuelle Triage menschlicher Teams überfordert. Die Antwort der Branche ist Exklusivität — geschlossene Netzwerke, höhere Hürden, selektiverer Zugang.

Das ist für hochkapitalisierte Tech-Konzerne eine handhabbare Lösung. Für das breite Ökosystem aus Open-Source-Projekten, mittelständischen Softwareanbietern und den Unternehmen, die deren Produkte einsetzen, entstehen neue Risiken.

Die Konsequenz ist keine Apokalypse — aber sie ist eine Einladung, die eigene IT-Infrastruktur nüchtern zu betrachten. Wer kontrolliert Ihre Systeme? Wer entscheidet, wann gepatcht wird? Wie transparent sind Ihre Software-Abhängigkeiten?

Diese Fragen haben keine universelle Antwort. Aber sie sind die richtigen Fragen — und die Antworten sollten Sie kennen.

Haben Sie Fragen zu On-Premise-Infrastruktur oder zur Absicherung Ihrer IT-Umgebung?

Vereinbaren Sie ein unverbindliches Beratungsgespräch mit unserem Team: Kontakt aufnehmen.