Abgeordnetenhaus BERLIN

**Drucksache 19/1026**
13.06.2023

19. Wahlperiode

# Antrag

der Fraktion Bündnis 90/Die Grünen

**IT-Sicherheitslücken suchen und finden – Ein Bug-Bounty-Programm für Berlin**

Das Abgeordnetenhaus wolle beschließen:

Der Senat wird aufgefordert, ein Bug-Bounty-Programm für Berlin zu erarbeiten und rechtssichere Wege zu etablieren, um Sicherheitslücken in der vom Land Berlin eingesetzten Software zu melden. Insbesondere sollen über die bisherigen Anstrengungen hinaus folgende Maßnahmen umgesetzt werden:

- In Zusammenarbeit mit Berliner Universitäten oder anderen Forschungseinrichtungen sowie gemeinnützigen Vereinen wie dem CCC soll ein rechtssicheres öffentliches Bug-Bounty-Programm zur Entdeckung von Sicherheitslücken und Sicherheitsvorfällen in der digitalen Infrastruktur und eingesetzten Software der Berliner Verwaltung geschaffen werden. Die Aufdeckung von Sicherheitslücken wird mit einem „Berliner Awareness-Preis für IT-Sicherheit“ (nach Vorbild von Bug-Bounty-Programmen im Unternehmensbereich) belohnt. In künftigen Verträgen mit Softwareanbieter*innen sind hierfür entsprechende Regelungen zu schaffen, um die nötigen Preisgelder als Malus geltend machen zu können.

- Ein regelmäßiger Wettbewerb für Beschäftigte der Berliner Verwaltung, die auf Sicherheitslücken in Infrastruktur oder Software hinweisen, ist zu etablieren. Mit dieser Maßnahme soll die aktive Beteiligung von Beschäftigten an der Beseitigung von Schwachstellen in der Informationssicherheit gefördert werden.

- Vulnerability-Disclosure-Policy für ganz Berlin: In Zusammenarbeit mit Sicherheitsforscher*innen und Zivilgesellschaft soll eine Vulnerability-Disclosure-Policy für die gesamte Berliner Verwaltung erstellt werden. Ihre Regeln sollen rechtssicher garantieren, dass Sicherheitslücken in Infrastruktur und Software gemeldet

und schnellstmöglich behoben werden können. Verträge mit Dritten werden dahingehend angepasst.

Dem Abgeordnetenhaus ist zum 1. September 2023 zu berichten.

***Begründung***

Die öffentliche Verwaltung steht vor der beständigen Aufgabe für die Informationssicherheit der internen Nutzer*innen (also dem Öffentlichen Dienst) und der externen Kund*innen (also der Berliner Bürger*innen) zu sorgen. Um dieses Anliegen zu unterstützen, ist auch externer Sachverstand von Sicherheitsexpert*innen aus Universitäten, Forschungseinrichtungen und der freien IT-Szene notwendig. Ein Bug-Bounty-Programm für das Land Berlin wird diese Einbindung unterstützen und mit dem Awareness-Preisgeld Anreize für die Suche und vertrauliche Meldung von Sicherheitslücken schaffen.

Mit einem Bug-Bounty-Programm etabliert Berlin eine Lösung zur schnellen und rechtssicheren Meldung von IT-Sicherheitslücke, welche in der Wirtschaft und anderen Ländern bereits genutzt wird. Zum Beispiel wurde 2021 in der Schweiz ein Pilotprojekt durchgeführt und zehn Sicherheitslücken durch ein Bug-Bounty-Projekt identifiziert.[1]

Ein verwaltungsinterner Wettbewerb soll Mitarbeiter*innen der Berliner Verwaltung motivieren, Programmfehler, Sicherheitslücken und Sicherheitsvorfälle zu melden. Ein Wettbewerb würdigt Engagement und Courage der Teilnehmenden und fördert die Sensibilisierung für IKT-Sicherheit durch praktische Beispiele.

Gerade beim Identifizieren von Sicherheitslücken besteht Rechtsunsicherheit. Eine berlinweite Vulnerability-Disclosure-Policy schafft Sicherheit für Sicherheitsforscher*innen, Angestellte und Zivilgesellschaft, identifizierte Sicherheitslücken melden. Eine Vulnerability-Disclosure-Policy beschreibt den Vorgang der Meldung von Sicherheitslücken, garantiert Anonymität der meldenden Person und dass von einer Strafanzeige im Sinne des § 202c StGB (sogenannte Hackerparagraph) im Fall von ethischem Hacking abgesehen wird. Das Land Berlin führt bereits eine Vulnerability-Disclosure-Policy für Berlin.de und Berlinonline.net.[2] Auf Bundesebene verwendet die Bundeswehr eine solche Regelung.[3] In Ergänzung der aktuellen Sicherheitsforschung und der Bemühungen der Zivilgesellschaft sorgt eine berlinweite Regelung für Rechtssicherheit und eine schnelle Meldung von Sicherheitslücken in IT-Infrastruktur und -Anwendungen des Landes Berlin.

Mit einem Bug-Bounty Programm schafft das Land Berlin einen rechtssicheren Rahmen für einen modernen Umgang mit Sicherheitslücken in Infrastruktur und Software. Zudem wird eine positive Fehlerkultur in allen Untergliederungen der Berliner Verwaltung etabliert. Ein transparenter und offener Umgang mit IKT-Sicherheit stärkt die digitale Resilienz und das Vertrauen der Bürger*innen in eine sichere digitale Verwaltung von Berlin.

[1] https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/abschlussbericht-bb.html

[2] https://www.berlin.de/wir-ueber-uns/7470309-4219174-vulnerability-disclosure-policy.html

[3] https://www.bundeswehr.de/de/security-policy

Berlin, 13. Juni 2023

Jarasch Graf Ziller
und die übrigen Mitglieder
der Fraktion Bündnis 90/Die Grünen