Abgeordnetenhaus BERLIN

Drucksache 19 / 15 562
Schriftliche Anfrage

19. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Stefan Ziller (GRÜNE)

vom 11. Mai 2023 (Eingang beim Abgeordnetenhaus am 15. Mai 2023)

zum Thema:

Umsetzung der IT-Sicherheitsstrategie in der Berliner Verwaltung

und **Antwort** vom 05. Juni 2023 (Eingang beim Abgeordnetenhaus am 06. Juni 2023)

Der Regierende Bürgermeister von Berlin
Senatskanzlei

Herrn Abgeordneten Stefan Ziller (GRÜNE)
über
die Präsidentin des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

Antwort
auf die Schriftliche Anfrage Nr. 19/15 562
vom 11. Mai 2023
über Umsetzung der IT-Sicherheitsstrategie in der Berliner Verwaltung

---

Im Namen des Senats von Berlin beantworte ich Ihre Schriftliche Anfrage wie folgt:

1. Wie viele Live-Hacking-Veranstaltungen wurden seit dem 1. Juni 2019 in der Berliner Verwaltung durchgeführt und wie viele Mitarbeiter*innen haben dabei teilgenommen? (Bitte jeweils Jahr, Anzahl der Teilnehmer*innen und Verwaltungseinheit angeben).

Zu 1.:
Gemäß § 23 EGovG Bln sind die Behörden verpflichtet, einmal jährlich für alle Beschäftigten eine Fortbildungsveranstaltung im Themenbereich IKT-Sicherheit durchzuführen. Die einzelnen Behörden führen diese ihrerseits eigenständig durch. Eine behördenübergreifende Übersicht wird dabei aus Datensparsamkeitsgründen nicht durchgeführt. Als Unterstützung zur Durchführung und Bewertung dieser Maßnahme wird derzeit im Awarenesskonzept-Berlin erarbeitet.

2. In welchen Verwaltungen von Berlin wird seit 1. Juni 2019 das Behörden Informationssicherheitstraining (BITS) durchgeführt und wie sind die Teilnehmendenzahlen?

Zu 2.:
Gemäß § 23 EGovG Bln sind die Behörden verpflichtet, ein ISMS aufzubauen, in dem das auf Open Source basierende BITS Training eine sinnvolle Maßnahme sein kann, aber nicht sein muss. Einige Behörden haben separate Instanzen eingerichtet und für ihre eigenen Bedürfnisse konfiguriert. Das BITS wird weiterhin landesweit als Dienstleistung durch das Berlin CERT bereitgestellt und kann innerhalb der Berliner Behörden über https://bits.berlin-cert.verwalt-berlin.de/ genutzt werden. Eine zentrale Protokollierung der Nutzer erfolgt aus Datensparsamkeitsgründen nicht.

3. Wo können Sicherheitsforscher*innen und Zivilgesellschaft Sicherheitslücken in Software und Websiten der Berliner Verwaltung melden? (bitte einzeln auflisten mit jeweiliger Internetpräsenz oder anderweitiger Kontaktmöglichkeit)

Zu 3.:
Sicherheitsforscher und Zivilgesellschaft können bei Webseiten oder damit zusammenhängenden Softwareprodukten über den Impressum-Button der jeweils verantwortlichen Behörde die Sicherheitsprobleme melden. Diese wird dann über die etablierten Meldewege die Abarbeitung initiieren.

Bei davon losgelösten Sicherheitsproblemen kann eine Meldung an

a) das Schwachstellenportal des BSI unter
https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/IT-Schwachstellen/Schwachstellenmeldungen/Schwachstellenmeldungen_node.html
(Über den CERT Verbund erfolgt dann gegebenenfalls eine Information über die etablierten Meldewege an das Land Berlin.)

b) den Bereich IKT-Sicherheit
https://www.berlin.de/moderne-verwaltung/prozesse-und-technik/ikt-sicherheit/informationssicherheit/artikel.947470.php
E-Mail: IKT-Sicherheit@seninnds.berlin.de

c) das CERT Berlin
https://www.itdz-berlin.de/dienstleistungen/it-infrastruktur/sicherheit/

erfolgen.

4. Was ist der aktuelle Stand zur Ausarbeitung eines Durchführungskonzepts (angekündigt in Drucksache 18/1999) für regelmäßige Informationssicherheitsübungen nach Drucksache 18/1674?

Zu 4.:
Seit 2020 wird jährlich die im § 23 EGovG Bln festgeschriebene, übergreifende jährliche Sicherheitsübung durchgeführt. Ausnahme bildete das Jahr 2021. 2021 wurde die Übung aufgrund der Pandemiebeschränkungen nicht durchgeführt.

5. Was ist der aktuelle Stand der Umsetzung eines Wettbewerbs für Beschäftigte, die auf Informationssicherheitslücken hinweisen? (Drucksache 18/1674)

Zu 5.:
Mit der Planung zu einem Wettbewerb für Beschäftigte, die auf Informationssicherheitslücken hinweisen, wird begonnen, wenn personelle Ressourcen im verantwortlichen Bereich zur Verfügung stehen. Bei der gegenwärtigen personellen Situation ist eine Umsetzung nur mit einer Ausschreibung für entsprechende Unterstützungsleistungen durchführbar. Die Anmeldung dafür erforderlicher Mittel ist im Rahmen zukünftiger haushaltswirtschaftlicher Maßnahmen in die Planung aufgenommen. Es ist beabsichtigt, den Wettbewerb als Bestandteil im derzeit in Erstellung befindlichen Awarenesskonzept-Berlin zu berücksichtigen. Die Finalisierung des Konzepts ist für Q4 2023 geplant.

6. Was ist der aktuelle Stand der Umsetzung eines Bug-Bounty-Programms für Berliner Universitäten? (Drucksache 18/1674)

Zu 6.:
Zur Umsetzung eines Bug-Bounty-Programms für Berliner Universitäten oder Forschungseinrichtungen sowie gemeinnützigen Vereinen wie dem CCC sind umfangreiche rechtliche Bewertungen zur Machbarkeit erforderlich - einschließlich der Anpassung von Vergabevorschriften. Mit der Planung und Umsetzung wird durch den Fachbereich begonnen, wenn personelle Ressourcen im verantwortlichen Bereich zu dem komplexen Thema zur Verfügung stehen.

7. Welche Bug-Bounty-Programme des Bundes, der Bundesländer und Kommunen sind dem Senat bekannt, deren Konzepte für Berlin übernommen werden könnten?

Zu 7.:

Derzeit sind keine Bug-Bounty-Programme des Bundes oder anderer Länder bekannt.

Berlin, den 5. Juni 2023

Der Regierende Bürgermeister von Berlin
In Vertretung

Martina Klement
Staatssekretärin für Digitalisierung und Verwaltungsmodernisierung / CDO