

V27 IT-Sicherheit in Berlin voranbringen

Antragsteller*in: Christopher Philipp (KV Berlin-Mitte)
Tagesordnungspunkt: TOP 9 Weitere Anträge
Status: Zurückgezogen

1 IT-Sicherheit in Berlin voranbringen

2 In den letzten Monaten gab es in Deutschland zahlreiche folgenschwere Cyberangriffe.
3 Krankenhäuser, Altenpflegeeinrichtungen, Unternehmen, Behörden und Universitäten waren
4 betroffen. So musste beispielsweise das Rathaus Potsdam über eine Woche vom Netz getrennt
5 werden und konnte seine Verwaltungsaufgaben nur eingeschränkt erfüllen. Nach einer
6 repräsentativen Umfrage des Digitalverbands Bitkom unter mehr als 1000 Geschäftsführern
7 deutscher Unternehmen verursachten Cyberangriffe für die befragten Unternehmen einen
8 wirtschaftlichen Gesamtschaden von 102,9 Milliarden Euro jährlich. Teilweise war es Glück,
9 dass erfolgte Cyberangriffe keine schlimmeren Auswirkungen hatten: So waren bei einem
10 Angriff auf elf Krankenhäuser in Rheinland-Pfalz und im Saarland medizinische Geräte nicht
11 betroffen - dass dies unmittelbar eine Gefahr für Leib und Leben der dortigen Patient*innen
12 bedeutet hätte, ist offensichtlich.

13 Auch das Berliner Kammergericht ist im letzten Jahr Opfer eines schwerwiegenden
14 Cyberangriffs geworden. Dies führte dazu, dass die komplette Internetkommunikation des
15 Kammergerichts abgeschaltet werden musste.

16 Nicht zuletzt der Fall des Cyberangriffs auf das Kammergericht zeigt: Berlin muss sich im
17 Bereich Cybersicherheit auf neue Herausforderungen und häufigere Angriffe einstellen. Wenn
18 es uns nicht gelingt, ein hohes Maß an IT-Sicherheit zu gewährleisten, kann dies negative
19 Auswirkungen auf alle Menschen in der Stadt haben. Ein Cyberangriff kann dazu führen, dass
20 Dienstleistungen der Verwaltung nicht erbracht werden können, sensible Daten von
21 Bürger*innen abfließen, Arbeitsplätze bedroht sind und im schlimmsten Fall Menschenleben
22 gefährdet werden.

23 Wir schlagen daher folgende Maßnahmen vor, mit denen wir das Land Berlin im Bereich der IT-
24 Sicherheit besser aufstellen wollen und den Menschen in Berlin und dort ansässigen
25 Unternehmen verbesserte Angebote unterbreiten möchten:

26 1. Wir wollen eine **IT-Sicherheitsstrategie** für das Land Berlin erarbeiten!

27 Für eine gelungene Neuaufstellung im Bereich der IT-Sicherheit braucht es zunächst eine
28 gemeinsame Strategie. Einzelne Maßnahmen können nur dann erfolgreich sein, wenn sie sich in
29 ein stimmiges Gesamtkonzept einbetten. Ein solches fehlt bislang. Ausgangspunkt einer
30 Strategie muss für uns das *Vorsorge- und Verhütungs-Prinzip* sein. IT-Sicherheit darf kein
31 reaktiver Vorgang auf schwerwiegende Sicherheitsvorfälle sein, sondern muss Vorfälle auf
32 allen Ebenen antizipieren und ihnen mit einer umfassenden präventiven Strategie begegnen.
33 Wir sehen dabei verschiedene zentrale Aspekte einer IT-Sicherheitsstrategie: die Sicherheit
34 der Bürger*innen, die Sicherheit der Netze, die Sicherheit der Verwaltung, die Sicherheit
35 der Wirtschaft und die Sicherheit im Katastrophenfall. Jeder dieser Aspekte erfordert dabei
36 eine individuelle Betrachtung, um dem sicherheitspolitischen Anforderungsprofil gerecht zu
37 werden. In einem weiteren Schritt müssen die Schwachstellen der gegenwärtigen
38 Zuständigkeitsaufteilung für die IT-Sicherheit in Berlin analysiert werden, um auf dieser
39 Basis die Prioritäten für deren Weiterentwicklung zu identifizieren. Die IT-
40 Sicherheitsstrategie Berlin muss unter Einbindung aller zuständigen Ressorts, der

41 Zivilgesellschaft und der Wirtschaft erarbeitet werden. Nur so ist sichergestellt, dass sie
42 den nötigen ganzheitlichen Ansatz abbildet.

43 2. Wir wollen ein **BerlinerIT-Sicherheitsgesetz** schaffen!

44 Ein zentraler Punkt der IT-Sicherheitsstrategie müssen die Eckpunkte eines Berliner IT-
45 Sicherheitsgesetzes sein, welches das entsprechende Bundesgesetz ergänzt. Dieses muss in
46 einem nächsten Schritt ausgearbeitet und zügig verabschiedet werden. Um IT-Sicherheit auf
47 einem hohen Niveau in Berlin gewährleisten zu können, braucht es eine klare
48 Aufgabenverteilung und klar beschriebene Befugnisse der handelnden Behörden. Beides kann nur
49 auf gesetzlicher Basis vorgenommen werden - denn nur der Gesetzgeber kann solch wesentlichen
50 Entscheidungen demokratische Legitimation verschaffen. Eine Verlagerung dieser
51 Entscheidungen auf die Verwaltung wird einem transparenten Verfahren nicht gerecht. Die
52 vorgesehenen Maßnahmen müssen so gestaltet werden, dass sie den Gefahren wirkungsvoll
53 begegnen, dabei aber die Grundrechte der Bürger*innen wahren.

54 3. Wir wollen ein **Kompetenzzentrum IT-Sicherheit** einrichten!

55 Bei einem IT-Sicherheitsvorfall sind die Zuständigkeiten verschiedener Stellen betroffen. In
56 der Regel sind personenbezogene Daten involviert, so dass die Landesbeauftragte für
57 Datenschutz und Informationsfreiheit ins Spiel kommt. Cyberangriffe sind strafbar - deren
58 Verfolgung Sache der Strafverfolgungsbehörden. Erste Schutz- und Bereinigungsmaßnahmen von
59 Cyberangriffen wird das Berliner Computer Emergency Response Team (sog. CERT) vornehmen.
60 Wichtig ist, dass die involvierten Beteiligten sich eng abstimmen und das wichtige
61 Informationen ausgetauscht werden. Hierfür muss ein Kompetenzzentrum IT-Sicherheit als
62 Informations-, Kooperations- und Koordinationsplattform in Berlin eingerichtet werden. Auch
63 dieses sollte auf einer gesetzlichen Grundlage beruhen, welche die vorgesehenen
64 Verantwortlichkeiten, Informations- und Benachrichtigungspflichten festlegt.

65 4. Wir wollen **Wissensvermittlung und Sensibilisierungen** für die Gesellschaft fördern!

66 IT-Sicherheit kann durch staatliche Akteure allein nicht sichergestellt werden. Vielmehr ist
67 von entscheidender Bedeutung, dass alle Menschen für die Risiken im Netz sensibilisiert
68 werden und wissen, wie sie sich vor ihnen schützen können. Der Staat kann hierbei aber
69 unterstützen. Zusammen mit der Berliner Wirtschaft werden wir einen *Hackathon* initiieren,
70 bei dem kollektiv die Stärkung der IT-Sicherheit vorangetrieben wird. Für die Bürger*innen
71 setzen wir außerdem auf umfangreiche Wissensvermittlung. Wir wollen *Digital Summer Schools*
72 für Berlin schaffen und uns aktiv am Digitaltag 2020 (<https://digitaltag.eu>) beteiligen, der
73 am 19. Juni 2020, stattfindet. Damit wollen wir die Digitalisierung und IT-Sicherheit
74 niedrigschwellig in der Stadt erfahrbar machen. Da der Digitaltag von Beteiligung lebt,
75 rufen wir auch alle Kreisverbände dazu auf, Aktionen für den Digitaltag 2020 anzumelden.

76 Wir setzen auf möglichst umfangreiche Bildungs- und Beratungsangebote und sorgen für eine
77 ganzheitliche Vermittlung von Medienkompetenz und Sachverständnis in der schulischen
78 Bildung. Im Bereich der Erwachsenenbildung setzen wir insbesondere auf die Volkshochschulen
79 und Hochschulen. Zudem wollen wir prüfen, den Auftrag der Landeszentrale für politische
80 Bildung als anerkannte Akteurin in der Bildungsarbeit um die digitale Bildung zu erweitern.
81 Denn aus unserer Sicht ist digitale Bildung heute wesentlich, um sich in der Welt
82 selbstbestimmt zu bewegen.

83 5. Wir wollen mehr **IT-Sicherheit in der Verwaltung!**

84 Maßgeblich für das Vertrauen der Bürger*innen in die Berliner Verwaltung und ihren
85 Digitalisierungsprozess ist die Absicherung der Daten. Dabei müssen wir auf zwei
86 übergeordnete Grundsätze hinwirken: „Security by Design“ und „Form follows Function, follows
87 Security“.

88 Ebenso bedeutsam für die Vermeidung von IT-Sicherheitsvorfällen innerhalb der Verwaltung ist
89 das Bewusstsein aller Beschäftigten für die Relevanz der IT-Sicherheit. Hier setzen wir auf
90 eine Landes-Awarness-Strategie der IT-Sicherheit. Verpflichtende und regelmäßige
91 Weiterbildungen sowie das Angebot von E-Learning-Tools, sowie erlebnisorientierte
92 Sensibilisierungen wie die Durchführung regelmäßiger IT-Sicherheitsübungen und Live-Hackings
93 sind in einer digitalen Verwaltung unabdingbar. Zudem machen wir uns dafür stark, dass
94 Beschäftigte, die IT-Sicherheitsprobleme melden, dafür belohnt werden und wir werden die
95 Kooperation mit den Berliner Universitäten suchen, um durch Bug-Bounty-Programme
96 Sicherheitslücken zu finden bevor sie zu Sicherheitsvorfällen werden.

Unterstützer*innen

Jan Fährmann (KV Berlin-Kreisfrei); Sebastian Weise (KV Berlin-Charlottenburg/Wilmersdorf); Lara Liese (KV Berlin-Mitte); Jelisaweta Kamm (KV Berlin-Mitte); Stefan Ziller (KV Berlin-Marzahn/Hellersdorf); Esra Celebi (KV Berlin-Mitte); Claudia Fechner (KV Berlin-Treptow/Köpenick); Silke Gebel (KV Berlin-Mitte)