Beschluss der Fraktion Bündnis 90/Die Grünen im Abgeordnetenhaus von Berlin, 15.01.2019

IT-SICHERHEIT FÜR BERLIN

Sicherheit im Digitalen ist zu einer zentralen Herausforderung unserer Infrastrukturen und Kommunikationssysteme geworden ist. Das Zusammenwirken der immer komplexer werdenden Netzwerke und der Sicherheit unserer IT-Infrastruktur ist heute wesentliche Bedingung unserer grundrechtlichen Freiheiten sowie unserer verfassungsrechtlichen Ordnung.

Berlin ist nicht nur ein gesellschaftlicher, wirtschaftlicher und politischer Knotenpunkt von einzigartiger Bedeutung in Europa, es ist auch in der IT-Infrastruktur ein bedeutender Hub, das den vielfältigen Anforderungen an diese Stadt gerecht werden muss. Gleichzeitig steigen in diesem komplexen Netzwerk die Gefahren für einzelne Punkte im Netz als auch dem Gesamtverbund: ob es um digitale Risiken für einzelne Bürger, für Behörden, für Wirtschaftsunternehmen oder für die kritische Infrastruktur geht – Berlin muss Sicherheit im digitalen Raum bieten.

Ein zentraler Grundgedanke der bündnisgrünen Perspektive auf IT-Sicherheit ist das **Vorsorge- und Verhütungsprinzip**: IT-Sicherheit entsteht, wenn wir vor einem Krisenfall absichernde Maßnahmen treffen. Oder anders gesagt: es ist besser, wenn wir mit Rauchmeldern und Feuerlöschern den Brandfall vorneweg verhindern, als wenn der Brand schon lodert und wir das Feuer nur noch löschen können.

Die aktuellen Ereignisse machen gleichfalls deutlich, dass IT-Sicherheit uns alle betrifft. Denn es ist auch der Mensch, der ein wesentliches Risiko bei Angriffen auf unsere IT-Systeme darstellt. In diesem Sinne ist IT-Sicherheit auch Führungsverantwortung. Denn das Führungspersonal muss das Thema mit der nötigen Aufmerksamkeit vorleben.

Sicherheit der Netzinfrastruktur

Der Berliner Großraum ist der Raum für vielfältige große und kleine Netze. Die Anbindung der Universitäten im internationalen akademischen Raum steht dabei genauso im Raum, wie die Einwahl der einzelnen Bürger in das öffentliche WLAN oder der heimische Internetzugang. Digitale Zugänge, sei es über das „klassische Internet“ (www), Bibliotheks- und Ausbildungsnetzwerke oder die Verlagerung von Kultur- und Medienangeboten auf die IPTV-Distribution und DVB-T2, sind einerseits das sprichwörtliche Tor zur globalisierten und vernetzen Welt und andererseits ein Hauptfaktor für die gesellschaftliche Teilhabe in der modernen Stadtgesellschaft.

Sicherheit der Netzinfrastruktur ist nicht nur eine Frage der digitalen Angriffspunkte, sondern muss auch physisch gewährleistet werden. Die „Ostkreuz“-Anschläge auf das S-Bahn- und Fernbahn-Netz trafen nicht

nur den Zugverkehr, sondern sorgten bei einem großen Telekommunikationsdienstleister für tagelange Ausfälle.

Das Land Berlin muss in Zusammenarbeit und im Dialog mit den Netzbetreibern dafür Sorge tragen, dass die Sicherheitskonzepte sich mit den Bedrohungen weiterentwickeln. Redundante Systeme zum Schutz der Berliner*innen und der hier angesiedelten Unternehmen, der Schutz neuralgischer Orte sowie ein dezentraler Netzaufbau sind Bausteine, um Angriffen vorzubeugen.

Netzzugänge als digitale Türöffner, sind kritische Punkte und damit beliebte Angriffsziele. Als im November 2016 während eines Versuchs, ein weltweites Botnetz aufzubauen, über eine Million Router der Telekom ausfielen, saßen auch hunderttausende Berliner*innen ohne Internet da.

Die Berlin-Cloud als zentrales Netzwerk der Berliner Behördenstruktur muss gegen großflächige Ausfälle abgesichert werden und in Zusammenarbeit mit anderen Bundesländern müssen Sicherungskopien außerhalb des Landes Berlin aufbewahrt werden, um im digitalen Krisenfall einen schnellen Zugriff auf unbeschädigte Daten zu haben und der kompromittierten Stadt zu helfen.

Sicherheit der Verwaltung

Maßgeblich für das Vertrauen der Bürger*innen in die Berliner Verwaltung und ihren Digitalisierungsprozess ist die Absicherung der Daten. Während wir mit der Umsetzung des E-Government-Gesetz Berlins das zentrale Großprojekt der Reformierung der Berliner Verwaltung angehen, müssen wir auf zwei übergeordnete Grundsätze hinwirken: „**Security by Design**“ und „**Form follows Function follows Security**“.

Denn auch wenn in manchen IT-Stellen die Vorstellung vorherrschend ist, dass Behörden keine lohnenswerten Ziele wären, ist die öffentliche Verwaltung im starken Fokus von Datenhändlern und Kriminellen: Die erhobenen Daten durch die Verwaltung sind hochverifiziert, aktuell, umfassend und abschließend. Das macht sie besonders wertvoll und besonders sensibel, seien es persönliche Daten des Melderegisters, Kita-Plätze oder Bußgeldverfahren. Berliner Behörden sind für den Datendiebstahl ein attraktives Ziel und sie sind aufgrund dieser Umstände hoch gefährdet. Schließlich geht es nicht nur um den illegalen Zugang auf geschützte private Daten, sondern zunehmend auch um den Schutz digitaler Identitäten.

Dabei ist die im Berliner E-Government-Gesetz angelegte Zentralisierung ein großer Durchbruch für „**Security by Design**“. Mit der Aufhebung der IT-Planungshoheit in den einzelnen Behörden und in der Zusammenführung eines Großteiles der Berliner Behörden unter der Aufsicht und dem Sicherheits-management des ITDZ wurde der Gefahr der Kompromittierung einzelner Dienststellen entgegengewirkt. Nunmehr haben sich alle abnahmepflichtigen Behörden den strengen Sicherheitsanforderungen der zentralen IT-Verwaltung zu stellen – eine Verschleppung der Verantwortung ist damit nicht möglich. Die innovative Sicherheitskultur des ITDZ – z.B. der Hacktober als Awareness-Maßnahme – muss immer wieder überprüft und weiterentwickelt werden.

Die Fraktion Bündnis 90/Die Grünen setzt auf eine **Landes-Awareness-Strategie der IT-Sicherheit**. Verpflichtende und regelmäßige Weiterbildungen sowie eine erlebnisorientierte Sensibilisierung der Berliner Mitarbeiter*innen im Öffentlichen Dienst sind in einer digitalen Verwaltung unabdingbar. Dabei muss die Weiterbildung zertifiziert und qualifiziert erfolgen. Alle weiteren Schulungen im digitalen Bereich

sollen außerdem verpflichtend ein IT-Sicherheitsmodul beinhalten. Daneben braucht es ein ständig aktualisiertes und verständlich aufbereitetes Warnsystem.

Mit dem Computer Emergency Response Team (CERT) des ITDZ ist Berlin Institutionell schon gut aufgestellt. Das CERT arbeitet präventiv und reaktiv. Zum einen prüft es in den Dienststellen der Verwaltung die Infrastruktur auf verwundbare Stellen und sensibilisiert Sachbearbeiter zum Umgang mit Hard- und Software. Im Ernstfall eines Angriffs von außen analysiert das CERT sofort die Situation, sichert die Spuren und leitet entsprechende Gegenmaßnahmen ein.
Mit regelmäßigen **Sicherheitsübungen** nach Vorbild der Brandschutzübungen der Feuerwehr wollen wir den Ernstfall proben und das Bewusstsein über IT-Sicherheit erhöhen. Die Einbindung des LKA und des **Berlin-CERT** beim ITDZ soll dafür sorgen, reale Angriffsszenarien zu erfahren, damit im digitalen Krisenfall jeder Handgriff sitzt und die Arbeitsfähigkeit schnell wiederhergestellt werden kann. Erfahrungen dazu bestehen auf europäischer Ebene mit den erfolgreichen Sicherheitsübungen der ENISA.

Die heutigen Angriffe im IT-Bereich sind längst nicht mehr gezielte und präzise Eingriffe, sondern vornehmlich die automatisierte und massenhafte Ausnutzung von Programmfehlern durch zentrale Steuerungssysteme.Es ist daher eine Notwendigkeit die **Zentralisierung von Sicherheitsmaßnahmen** in Berliner Behörden voranzutreiben.

Gleichzeitig müssen **Sicherheitsvorfälle** in Berlin transparent gemeldet werden. Dazu müssen dass die Meldepflichten der Dienststellen an das ITDZ konsequent umgesetzt werden und andererseits relevante Sicherheitsvorfälle (wie z.B. Datenverlust) in der Berliner Verwaltung im Rahmen der Open-Data-Strategie transparent gemeldet werden. Denn Behördendaten sind nicht nur Daten über Bürger, sie sind auch Daten der Bürger!

Wir brauchen im Rahmen der landesweiten Sicherheitskultur eine behördeninterne Belohnungsstrategie für das Melden von Sicherheitslücken und Fehlern durch die Mitarbeiter*innen nach dem Vorbild von „**Bug Bounty**"-Programmen. Eine außerordentliche Prämie für das Melden von besonders schwerwiegenden Lücken soll die behördeninterne Bewusstsein stärken und die Mitarbeiter*innen zu einem reflektierten Umgang mit den verwendeten Programmen anregen.

Alle Vorfälle, Maßnahmen und Entwicklungen sind in einem umfangreichen **Sicherheitsbericht** jährlich durch die zuständigen Stellen zusammenzufassen und der Öffentlichkeit sowie dem Parlament zugänglich zu machen, um die **Transparenz** in diesem Bereich auf hohem Niveau zu halten.

Damit im Digitalisierungsprozess der Berliner Verwaltung eine neutrale Stelle unvoreingenommenen die Sicherheitsmaßnahmen kontrollieren kann, treten wir schließlich dafür ein, die im Berliner E-Government-Gesetz vorgesehene Stelle des **Chief Information Security Officers** (CISO) zu besetzen. Wir erwarten, dass mit dem zunehmenden Umfang von Digitalisierungsaufgaben im Land Berlin es zu Abwägungskonflikten zwischen Sicherheit und Fortschritt der Umsetzung kommen wird. Hinzu tritt die Herausforderung, nicht nur bei unberechtigten Zugriffen durch behördenexterne Personen, sondern auch bei behördeninterne Sicherheitsverstöße tätig zu werden. Perspektivisch streben wir die Schaffung einer **unabhängigen Stelle für IT-Sicherheit** nach Vorbild der Berliner Datenschutzbeauftragten an.

Sicherheit der Wirtschaft

Berlin lebt von den vielen innovativen Ideen und der technischen Raffinesse seiner Gründer*innen und der guten und zielgenauen Arbeit seiner alteingesessenen Unternehmen. Start-Up-Ideen und Arbeitsprozesse sind genauso wertvolle Diebstahlsziele wie Transaktionsdaten und Finanzgeheimnisse; sie werden bedroht von Online-Betrügern, von Datenhändlern und von Industriespionage.

Um den Standort Berlin und seine gewerblichen Träger*innen vor bösen Überraschungen zu schützen, haben wir in dem Koalitionsvertrag die Fokussierung von Internet-Kriminalität durch Strafverfolgungs-behörden niedergelegt und den Aufbau einer **Beratungs- und Informationsstelle für IT-Sicherheit** durch die Senatsverwaltung für Wirtschaft, Energie und Betriebe geplant. Mit der **Digitalagentur** hat die bündnisgrüne Senatsverwaltung dieses Projekt bereits angestoßen.

Dabei ist der Schwerpunkt der Digitalagentur die nachhaltige Information und Beratung insbesondere der kleinen und mittelständischen Unternehmen, denen es oft an eigenen Ressourcen für eine zielgenaue Absicherung ihrer Infrastruktur fehlt. Die Digitalagentur soll sich außerdem mit weiteren Expert*innen in der IT-Sicherheit, insbesondere den aufgebauten Kompetenzen an den Universitäten, vernetzen und gemeinsame Projekte mit wissenschaftlicher Evaluierung planen und durchführen. Ein effektives Netzwerk der öffentlichen Hand stärkt dem Berliner Standort den Rücken und unterstützt eine reibungsarme Digitalisierungstransformation der Berliner Gewerbelandschaft.

Auch die landeseigenen Betriebe müssen ihrer Verpflichtung zur Wahrung von effektiven Sicherheitsplänen nachkommen. Dafür muss für alle landeseigenen Betriebe ein mit der Aufsichtsbehörde abgestimmten IT-Sicherheitsplan geschaffen werden und die Umsetzung fachkundig und unabhängig evaluiert und zertifiziert werden.

Wichtig für den Transformationsprozess in Wirtschaftsleben Berlins ist der Einsatz moderner Kollaborationsformate, der die sicherheitstechnische Kreativität und Produktivität der verschiedenen Institutionen zusammenbringt und praktische Probleme für alltägliche, digitale Sicherheitsprobleme findet. Wir werden einen berlinweiten, jährlichen **Hackathon initiieren**, in dem ehrenamtlich und gemeinsam die Stärkung unser IT-Sicherheit vorangetrieben werden wird. Mit Unternehmen, mit Behörden, mit zivilgesellschaftlichen Initiativen und vor allem mit all dem technischen Potenzial unserer Bürger*innen. Von Berlin – für Berlin.

Sicherheit der Bürger*innen

IT-Sicherheit ist nicht nur eine Herausforderung für die Berliner Institutionen, sondern für jeden einzelnen Bürger. Wir nutzen PCs, Laptops, Tablets und Smartphones über alle Bevölkerungsschichten hinweg jeden Tag zu jeder Zeit – und setzen uns damit einem Labyrinth aus technischen, digitalen und sozialen Gefahren aus. Nicht jede*r kann mit den Begriffen Scamming, Hacking, Phishing und Spam was anfangen – manches klingt mehr nach einer britischen Dinnergestaltung als nach realen Gefahren.

Und gerade deshalb müssen wir hier auch die Möglichkeiten zur Beratung und Information schaffen. Dabei zeigen Studien, dass Jugendliche als vermeintliche „digital natives“ genauso betroffen sind von Informationsschwächen im Bereich der digitalen Sicherheit wie Senioren*innen.

Wir setzen auf möglichst umfangreiche Bildungs- und Beratungsangebote und sorgen für eine gesamtheitliche Vermittlung von Medienkompetenz und Sachverständnis in der schulischen Bildung

ebenso wie in der Erwachsenenbildung. In den Berliner Schulen muss IT-Sicherheit innovativ und spielerisch vermittelt werden und dabei selbst durchgängig abgesichert sein. Mit der Schaffung von IT-Administratoren an jeder Berliner Schule unterlegen wir diesen Anspruch auch personell.

Im Bereich der **Erwachsenenbildung** sind insbesondere die **Volkshochschulen** und die **Hochschulen** gefordert. IT- und Medienkompetenz mit einem ständigen Schwerpunkt auf Sicherheit können nach unserer Vorstellung durch öffentlich und kostenfrei zugängliche „**Digital Summer Schools**" im Land Berlin in der Ferienzeit für alle Bürger*innen vermittelt werden. Die Vermeidung von menschlichen Fehlern oder Fehlgebrauch von IT ist ein zentraler Gewinn von IT-Sicherheit für die gesamte Stadtgesellschaft – und darüber hinaus.

Ein weiterer Baustein für IT-Sicherheit sind vielfältige Erfahrungen mit der Digitalisierung. Dazu soll eine „**Digitale Woche Berlin"** beitragen. Vom digitalen Klassenzimmer über die Werteentwicklung einer digitalen Gesellschaft bis hin zum Einsatz von Robotern in der Pflege soll die Themenvielfalt interessierte Bürgerinnen und Bürger eine Woche lang zu einem intensiven Dialog mit den digitalen Gestaltern einladen. Öffentliche Orte wie Stadtteilzentren, Bibliotheken und Rathäuser sollen dabei ebenso ihre Tore für Veranstaltungen öffnen wie private Vereine und Firmen, die ihre Fortschritte und Bildungsmöglich-keiten präsentieren wollen.

Berliner Institutionen stehen im Auftrag der Berliner Bürger*innen und haben daher eine Verantwortung für die Schaffung eines effektiven und nachhaltigen digitalen Verbraucherschutzes: Technologien, die in Berlin entwickelt werden, sollen die Verschlüsselung von z.B. WLAN-Routern stärken und die Landschaft des „Internet of Things" auf Dauer in seiner Benutzung sicher machen. Berlin ist vieles, aber kein Bot-Netz.

Sicherheit im Katastrophenfall

Mit detailreichen Aufschlägen zum Schutz der Kritischen Infrastruktur hat der Bundesgesetzgeber eine umfassende Regelung über die Erweiterungen der KritV geschaffen. Stichtag für die Umsetzung der KritV-Bestimmungen war der 3. Mai 2018 – Unternehmen, die dann nicht sicher sind, müssen mit empfindlichen Maßnahmen zur Einhaltung der Standards gebracht werden. Das Land Berlin ist hier in der Pflicht, genau hinzuschauen. In enger Abstimmung mit der Bundesebene muss das Land Berlin außerdem die eigenen Katastrophenschutz-Programme in ständiger Revision so überarbeiten, dass Risiken für die Berliner Bevölkerung minimiert werden.

Denn für Berlin mit seiner hohen Bevölkerungsdichte ist die Funktionsfähigkeit und Integrität unserer Katastrophenschutzmaßnahmen, unserer Krankenhäuser und unserer Energieinfrastruktur ein unerlässlicher Kernpunkt im Hinblick auf die IT-Sicherheit. Vorfälle wie die Auswirkung des WannaCry-Trojaners in Großbritannien, der in dutzenden Krankenhäusern die Rechner in digitale Geiselhaft nahm, zeigen, wie alltäglich und real die Bedrohungsszenarien für hochsensible Bereiche wie z.B. die Gesundheitsversorgung werden können.

Insbesondere die Charité als zentrales Forschungs- und Ausbildungskrankenhaus in Berlin hat hier die Pflicht, ihre digitale Infrastruktur umfangreich zu schützen und Sicherheitsmaßnahmen so bald wie möglich umfangreich und – im wahrsten Sinne des Wortes – abschließend umzusetzen. Das betrifft nicht nur ihre elementare Stellung als kritische Infrastruktur, sondern auch den alltäglichen Schutz von Patientendaten vor internen und externen unberechtigten Zugriffen.

Wir fordern, neben den Umsetzungen der bundesweiten Sicherheitsvorschriften auch regelmäßig den Rückfall auf analoge Strukturen zu planen und in einem jährlichen „**Aktionstag Netzausfall**“ zu testen. Hierfür braucht es ein integriertes Konzept zwischen Betreiber*innen kritischer Infrastruktur, den Berliner Behörden und dem ITDZ.

IT-Sicherheit im Spannungsfeld zwischen Strafverfolgung und Bürger*innenschutz

Sicherheit hat der Freiheit zu dienen. Das heißt, dass IT-Sicherheit auch über staatlichen Maßnahmen stehen muss und insbesondere durch diese nicht gefährdet werden darf. Es ist ein grundlegender Bestandteil bündnisgrüner Politik, dass digitale Handlungsfreiheit erst durch die Integrität der Systeme zu erreichen ist.

Ein Ankauf und die Ausnutzung von Sicherheitslücken durch die Berliner Strafverfolgungsorgane und den Verfassungsschutz schließen wir insbesondere dort aus, wo sie massenhaft für Systemunsicherheiten bei Bürger*innen sorgen. Der Trojaner „WannaCry“ hat gezeigt, dass wir eine neue Verantwortungskultur bei dem Ankauf von Sicherheitslücken durch Sicherheitsbehörden brauchen. Sicherheitslücken die viele Millionen Menschen betreffen - beispielsweise im Betriebssystem Windows 10, Android oder iOS, die das Rückgrat unseres digitalen Lebens ist, müssen geschlossen und nicht offen gehalten werden.

Es muss eine zentrale Aufgabe und unser aller Interesse sein, freie und staatlich unabhängige Forschung zu Verschlüsselungstechnologien zu fördern und sie den Berliner*innen zugänglich zu machen. Hierbei nehmen insbesondere die Berliner Hochschulen und die außeruniversitären Forschungseinrichten eine zentrale Rolle ein. Starke Verschlüsselung bedeutet nicht nur starke Bürgerrechte, sondern auch eine Absicherung der E-Government-Angebote des Landes Berlin: Nur mit einer starken und ungebrochenen Verschlüsselung ist die Vertraulichkeit und Integrität der versendeten und gespeicherten Daten der Berliner Bürger*innen gewahrt. Förderung von quelloffener Kryptografie ist eine konstante Investition in die Sicherheit der Zukunft.

Für eine nachhaltige Sicherheitspolitik im digitalen Raum ist eine stärkere und funktionierende Zusammenarbeit zwischen den bearbeitenden Stellen für Sicherheitsvorfälle in den Berliner Behörden und den **Strafverfolgungsbehörden** sicherzustellen. Ein standardisiertes **Meldesystem** ist Grundlage, um eine Nachermittlung der Urheber von Angriffen auf die Berliner Systeme zu ermöglichen. Hierzu müssen die **Sicherheitsbehörden** auf Landes-, aber auch auf Bundesebene ihre Arbeitsweisen regelmäßig koordiniert hinterfragen und wenn nötig die entsprechenden Ressourcen bündeln. Voraussetzung dafür ist eine belastbare Klärung und Realisierung der **Verantwortlichkeiten** sowohl zwischen als auch innerhalb von Bundes- und Landesbehörden.