JUNGE UNION
Schleswig-Holstein

Beschluss des Schleswig-Holstein Rates am 23. Juli 2017 in Barmstedt:

IT-Sicherheit in Zeiten von E-Government

Der sich rasant entwickelnde technologische Fortschritt seit Mitte des zwanzigsten Jahrhunderts hat in jedem Bereich unseres Lebens Einzug gehalten, aber nicht im gleichen Maße der Staat. Unternehmen und Privathaushalte sind meist mit aktuelleren und leistungsstärkeren Systemen ausgestattet als die meisten Behörden. Während Privathaushalte und Unternehmen oft schon all ihre Dokumente, Daten und Erinnerungen (Fotos, Videos, etc.) digital aufbewahren, arbeiten unsere staatlichen Behörden noch überwiegend analog. Sie verursachen nicht nur einen sehr hohen Papierverbrauch, sondern auch viel umständlichen bürokratischen Aufwand. Oft müssen Daten doppelt und dreifach angegeben werden und der Austausch zwischen Bundesländern ist wenig bis gar nicht möglich. Bürger und Unternehmer müssen noch immer persönlich bei Behörden erscheinen, bei denen sie Melde- und Antragsformulare ausfüllen müssen, um staatliche Verwaltungs- und Versorgungsdienste in Anspruch zu nehmen und um entsprechenden Pflichten gerecht zu werden. In der laufenden Legislaturperiode hat die Bundesregierung unter Führung von CDU/CSU erkannt, dass der Staat in Zukunft digital effizienter funktioniert als analog. Das E-Government Gesetz der Bundesregierung sieht einen vollständigen Umstieg auf elektronische Aktenführung bis 2020 vor und stellt den Ländern und Kommunen die Art der Umsetzung der Verwaltungssoftware weitestgehend frei. An dieser Stelle soll auch das Land Schleswig-Holstein anknüpfen und die gesamte Verwaltung weiterentwickeln. Statt einer aufwendigen neuen einheitlichen Software für alle, fordern wir agile und modulare Lösungen. Dienste sollen nach und nach online angeboten werden und lose gekoppelt sein. Das heißt, dass es nur wenige Abhängigkeiten zwischen den Diensten geben soll, so dass ein fehlerhafter Dienst nicht alle anderen Funktionen blockiert. Damit Behörden untereinander Informationen austauschen können, müssen Standards für Schnittstellen festgelegt werden, so dass jede Software diese leicht verarbeiten kann. Die Investitionen, die Behörden in Schleswig-Holstein noch tätigen müssten, beziehen sich dann nur noch auf den Ausbau und die Anbindung der Schnittstellen. Dadurch wird keine komplett neue Software gebraucht. So können kommunale Dienste zu kreis-, landes- und bundesweiten Portalen nach und nach verbunden werden.

Daher fordert die Junge Union Schleswig-Holsteins:

- Standardisierte Schnittstellen bei allen Behörden
- Hohe Sicherheitsstandards bei der Absicherung dieser Schnittstellen
- Kommunen sollen ihre eigenen Software weiterhin nutzen können
- Förderung bei dem Ausbau von sicheren IT-Systemen in Behörden und öffentlichen Einrichtungen

Das Potential von E-Government wird nur dann voll ausgeschöpft, wenn das Vertrauen in die Dienste vorhanden ist. Das heißt, dass alle Daten nur vertraulich behandelt und nur im Sinne des Bürgers zwischen Behörden ausgetauscht werden dürfen, wobei hohe Sicherheits- und Datenschutzstandards erfüllt sein müssen. Die Kommunikation mit Behörden muss sowohl für Bürger als auch für Unternehmen vollständig und ausschließlich über von Ende-zu-Ende verschlüsselte Kanäle abgewickelt werden. Während einige Plattformen bereits über zertifizierte Protokolle abgesichert sind, werden Nachrichten und Dateien noch immer nicht ausreichend vor dem Zugriff Dritter gesichert. Daher fordern wir für alle Bürger eine eigene Ende-zu-Ende verschlüsselte E-Mail-Adresse. Diese E-Mail-Adresse darf, anders als die aktuelle DE-Mail, nicht auf Zwischenstationen entschlüsselt und auf den Inhalt überprüft werden. Denn jede Entschlüsselung zwischen Start und Ziel ist eine potentielle Sicherheitslücke, die von Dritten ausgenutzt werden kann. Die Kommunikation mit Behörden kann über diese E-Mail-Adresse oder über einen persönliche Zugang, gebunden an den Personalausweis, erfolgen. Dadurch stellen wir sicher, dass jeder Bürger einen persönlichen Zugang für Behördengänge hat. Jeder Bürger muss ohne Mühe oder IT-Kenntnisse in der Lage sein, diese E-Mail-Adressen oder den Zugang einzurichten. Trotz des abgesicherten Zugangs könnten kompromittierte Rechner innerhalb der Behörde Daten abfangen und die Behörde ausspionieren. Aus diesem Grund muss der Datenaustausch innerhalb der Behörden ebenfalls komplett verschlüsselt erfolgen.

Daher fordert die Junge Union Schleswig-Holsteins:

- Zertifizierte Ende-zu-Ende verschlüsselte E-Mail-Dienste
- Einen an den Personalausweis gebundenen persönlichen Zugang bei Behördenportalen
- Ausschließlich Ende-zu-Ende verschlüsselte Kommunikation mit Behörden
- Die gesamte Kommunikation innerhalb von Behörden muss verschlüsselt erfolgen
- Ende-zu-Ende verschlüsselte E-Mail-Adressen für alle Bürger, Behörden und Unternehmen
- Modernisierung der IT-Infrastruktur und Geräte in Behörden auf ein zeitgemäßes Niveau

Der digitale Schutz unserer Bürger, unserer Infrastruktur und unserer Wirtschaft ist eine der größten Herausforderungen der Gegenwart. Während Länder wie China, Russland, aber auch Partner wie die USA, große Zentren für Aufklärung, Spionage und Cyber-Angriffe betreiben, vertrauen wir darauf,

dass wir nicht angegriffen werden. Am Beispiel der russischen Attacken im Wahlkampf in den USA sehen wir, wie ein unzureichend Schutz selbst Weltmächte schnell ins Wanken bringen kann. Aber auch in Deutschland gab es bereits große Angriffe, beispielsweise auf das Herzstück unserer Demokratie: den deutschen Bundestag. Die Reichweite und das Ausmaß von Cyberangriffen nimmt von Jahr zu Jahr zu und betrifft sowohl die Bürger unseres Landes als auch unsere Wirtschaft. Unternehmen verlieren bereits heute Milliarden an Einnahmen durch Wirtschaftsspionage anderer Staaten. Am stärksten betroffen ist unser Mittelstand, der leider noch sehr zögerlich mit dem Thema IT-Sicherheit umgeht. Von einem Unternehmen, das nur auf Attacken reagiert, statt für seinen Schutz vorsorgt, können wichtige Firmengeheimnisse gestohlen werden. Eine vernachlässigte IT-Infrastruktur in Unternehmen kann den gesamten Erfolg und das Überleben aufs Spiel setzen. Hier ist der Staat gefragt, mehr Aufklärungsarbeit zu leisten und Unternehmen bei der Umsetzung des IT-Sicherheitsgesetzes zu begleiten. Die fehlende IT-Sicherheit darf nicht mehr zur vermeintlichen Terrorismusbekämpfung genutzt werden. IT-Sicherheit muss als ein Schutz des Bürgers vor fremden Mächten wahrgenommen werden. Daher müssen wir deutlich mehr in die Umsetzung von bereits vorhandenen Technologien investieren. Die kryptographischen Verfahren zum effektiven Schutz von IT-Systemen und zum sicheren Verschlüsseln von Daten sind bereits vorhanden, aber an vielen Stellen nicht umgesetzt. Auch die Polizei und Bundeswehr müssen einen großen Rückstand in diesem Bereich aufholen. Das Ziel der Nato Staaten, 2% des BIPs in Rüstung zu investieren, sollte auch dazu genutzt werden, im Bereich Cyber Security und Cyber Attack aufzuholen und ein hohes Maß an Sicherheit gewährleisten zu können. Das bewusste Offenhalten von Sicherheitslücken für Spionagezwecke halten wir für falsch. Die Polizei muss jedoch dazu befähigt werden, Straftaten im Internet aufklären zu können. Dazu müssen Spezialisten entweder durch geeignete Vergütungsstrukturen angeworben oder Kooperationen mit zertifizierten privaten Sicherheitsexperten eingegangen werden. Der Staat soll auf digitaler Ebene genauso gut funktionieren wie in der analogen Welt. Langfristig soll sich Deutschland innerhalb der EU und NATO zu (einer) der führenden Nationen im Bereich der Cybersicherheit und -abwehr entwickeln. Somit würde die Bundeswehr einen wichtigen Beitrag zu den Bündnissen leisten, ohne dafür deutsche Soldaten in gefährlichen Missionen im Ausland einsetzen zu müssen.

Daher fordert die Junge Union Schleswig-Holsteins:

- Programme zur Aufklärung über IT-Sicherheit für Bürger und Unternehmen
- Förderung beim Ausbau von sicheren IT-Systemen in kleinen und mittelständischen Unternehmen
- Die Investitionen im Rahmen des 2%-Nato-Ziels unbedingt auch darauf zu verwenden die Wehrhaftigkeit der BRD gegen Cyberangriffe auf ein angemessenes Maß zu erhöhen.
- Stärkung der Cyberfähigkeiten der Polizei

- Möglichkeiten für die Polizei der Kooperation mit zertifizierten privaten Sicherheitsfirmen zur Aufklärung von Straftaten im Internet .

Unsere digitale Infrastruktur wird nicht nur von anderen Staaten angegriffen, sondern auch immer öfter von autonom handelnden Hackern und Hacker-Gruppen. Diese Angriffe werden oft über so genannte Bot-Netzwerke gestartet und koordiniert. Diese Netzwerke bestehen teilweise aus Millionen von Viren befallenen Rechnern, bei denen die Nutzer nicht wissen, dass ihr Computer im Hintergrund von Dritten gesteuert wird. In vielen Fällen sind Sicherheitslücken in Hard- und Software für dieses Problem verantwortlich. Besonders bedrohlich sind Distributed-Denial-of-Services (DDoS) Attacken, die versuchen mit möglichst vielen Anfragen Server zu überlasten und so einen Dienst von der Außenwelt abzutrennen. Eine der größten Attacken fand im Oktober 2016 statt, bei der Schwachstellen in Software für IoT (Internet-of-Things) Geräte ausgenutzt wurden, um Millionen von Geräten für eine gezielte Attacke zu verbinden. Die Schadsoftware heißt Mirai, diese führte zu einem Ausfall der Homepages von vielen großen amerikanischen Unternehmen (Twitter, Netflix, Amazon, Google, etc.). Die Software hat primär Geräte von einem chinesischen Hersteller befallen und konnte von diesem nicht entfernt werden, weil die Möglichkeit eines späteren Software-Updates nicht in die Gerätekonstruktion eingeplant und eine Schließung der Sicherheitslücke nach Auslieferung an den Kunden nicht möglich war. Heute existieren Milliarden von internetfähigen Geräten, von denen viele Sicherheitsupdates bekommen. Hersteller, die diese Funktion nicht integrieren, gefährden unsere Infrastruktur. Es besteht bereits die Möglichkeit für Hersteller von IT-Systemen, ihre Produkte auf Sicherheitskriterien zertifizieren zu lassen, wie die Common Criteria (ISO 15408 - Die Common Criteria for Information Technology Security Evaluation; zu deutsch: *Allgemeine Kriterien für die Bewertung der Sicherheit von Informationstechnologie*) sind ein internationaler Standard zur Prüfung und Bewertung der Sicherheitseigenschaften von IT-Produkten. Diese Möglichkeit besteht für Hersteller bisher nur auf einer freiwilligen Basis, es wäre sinnvoll, ein für den Verbraucher sichtbares Gütesiegel zu erstellen, das schon vor dem Kauf eines internetfähigen Gerätes für den Kunden sichtbar ist.

Daher fordert die Junge Union Schleswig-Holsteins:

- Neue IoT Geräte müssen leicht updatebar sein.
- Eine Garantie von mind. 2 Jahren, dass neue Software wartbar ist.
- Ein Gütesiegel/Qualitätsstandard für IT-Sicherheit von internetfähigen Geräten

Diese Forderungen beinhalten ein Ziel:

Alle Bürger, Behörden, staatliche Einrichtungen und die Wirtschaft in Deutschland vor Schaden zu bewahren. Die notwendigen Technologien sind bereits vorhanden, sie werden von privaten Unternehmen in jedem neuen System integriert, aber vom Staat bisher weitestgehend ignoriert. An

dieser Stelle wollen wir anknüpfen. Statt privaten Unternehmen den Schutz der Bürger im digitalen Zeitalter des World Wide Web zu überlassen, muss der Staat diese elementare Aufgabe, den Schutz der Bürger, nicht nur im analogen Alltag, sondern auch in der digitalen Welt, wahrnehmen und die Sicherheit jedes einzelnen Bürgers und der Behörden so gut und nachhaltig wie möglich gewährleisten.