Die Senatorin für Finanzen

29.10.2012

Dr. Hagen

Tel. 4746

Vorlage für die Sitzung des Senats am 6.11.2012

„IT-Sicherheit im Land Bremen“

Die Fraktion der CDU hat folgende Kleine Anfrage an den Senat gerichtet:

IT-Sicherheit im Land Bremen

Heutzutage benutzen nicht nur private Unternehmen, sondern auch die Behörden das Internet. Vielfach wird das Internet zur Kommunikation genutzt. Neben den vielen guten Möglichkeiten, die das Internet und die Informationstechnik (IT) im Allgemeinen mit sich bringen, gibt es leider auch steigende Gefahren, die für das Land Bremen von Bedeutung sind. Der Begriff der inneren Sicherheit beschränkt sich somit nicht mehr nur auf den Bereich der bisher realen Welt, sondern umfasst längst auch den Bereich der IT.

Der Senat plant die Einführung von Voice over IP (VoIP), auch Internettelefonie genannt. Mit diesem weiteren Schritt wird deutlich, dass die Frage nach der IT-Sicherheit auch in den Behörden und den Infrastrukturen des Landes Bremen zunehmend relevanter wird.

Wir fragen den Senat:

1. In welcher Art und Weise nutzen die Behörden im Land Bremen das Internet und inwiefern soll sich dies in der nächsten Zeit ändern?

2. Welche Risiken sind mit dieser Nutzung verbunden? Inwiefern können die Bürger durch diese Risiken betroffen sein?

3. Wie stellt der Senat für die Behörden, wie beispielsweise die Polizei, dem Landesamt für Verfassungsschutz, den Gerichten und der Staatsanwaltschaft, den Finanzämtern, den Senatsressorts, dem Stadtamt und dem Magistrat im Land Bremen ein angemessenes Sicherheitsniveau im Bereich der IT sicher?

4. Wie stellt der Senat für die Infrastrukturen im Land Bremen, wie beispielsweise der Energieversorgung, dem öffentlichen Nahverkehr, der Telekommunikation, der Krankenhäuser und Versicherungen ein angemessenes Sicherheitsniveau im Bereich der IT sicher?

5. Wie viele Angriffe (erfolgreiche/nicht erfolgreiche) auf die Behörden und die Infrastrukturen des Landes Bremen wurden seit 2009 bis heute registriert, welche Auswirkungen hatten diese und kam es zu Einschränkungen für die Beschäftigten und/oder für die Bürger Bremens?

6. Wie werden die Mitarbeiter der Behörden über die Risiken solcher Angriffe und die Gefahren des Internets aufgeklärt? Inwiefern finden hierzu verpflichtende Fortbildungen oder gezielte Gespräche seitens der Behörden statt?

7. Inwiefern werden durch den Senat und in den Behörden mobile Geräte wie Smartphones und Tablets benutzt, und welche Maßnahmen ergreift der Senat, um diese Geräte in ähnlicher Weise wie PCs zu schützen?

8. Wie sehen die Planungen des Senats zum Schutz der Behörden und der Infrastrukturen des Landes Bremen in Anbetracht der wachsenden Bedeutung der IT-Sicherheit für die Jahre 2012-2015 aus?

Der Senat beantwortet die Kleine Anfrage wie folgt:

1. In welcher Art und Weise nutzen die Behörden im Land Bremen das Internet und inwiefern soll sich dies in der nächsten Zeit ändern?

Das Internet wird von Behörden der Freien Hansestadt Bremen für verschiedenste Anforderungsbereiche umfangreich genutzt. Es werden Präsentationen der Organisation der FHB dargestellt (Webauftritte), elektronische Dienstleistungen für die Bürgerinnen und Bürger im Rahmen des E-Governments angeboten, Informationen bereitgestellt (u.a. auch zur Umsetzung des Informationsfreiheitsgesetzes) und, durch die Nutzerinnen und Nutzer in den Dienststellen, Informationen aus dem Internet abgerufen. Einen großen Anteil stellt die interne und die externe Kommunikation mittels E-Mail dar. Auch ist es den bremischen Bediensteten gestattet, den dienstlichen Internetzugang in geringem Umfang für private Zwecke zu nutzen. Es ist davon auszugehen, dass sich der Umfang der Nutzung weiter erhöhen wird. Die mittelfristigen Auswirkungen neuer Nutzungsformen des Internets, wie z.B. die neuen Angebote für mobile Endgeräte („Apps“ für Smartphones u.a.) sind derzeit noch nicht absehbar.

Der Senat lässt gegenwärtig prüfen, wie die Telekommunikation zukünftig gestaltet werden kann. Diesbezügliche Fragen, auch zur Nutzung von VoIP, wird ein Sollkonzept beantworten, das Anfang 2013 präsentiert wird.

2. Welche Risiken sind mit dieser Nutzung verbunden? Inwiefern können die Bürger durch diese Risiken betroffen sein?

Durch die Nutzung des Internets in der Verwaltung als auch beim Bürger selbst entstehen typische Risiken, die auch für alle anderen das Internet nutzende Institutionen oder Personen bestehen. Vornehmlich handelt es sich dabei um die Gefährdung der Informationssicherheit durch gezielte Manipulationen oder durch Ausnutzung informationstechnischer Schwächen bzw. Fehlern von IT-Systemen durch Kriminelle. Um die Risiken zu minimieren, sind in der Verwaltung entsprechende Maßnahmen getroffen worden, s.u.

3. Wie stellt der Senat für die Behörden, wie beispielsweise die Polizei, dem Landesamt für Verfassungsschutz, den Gerichten und der Staatsanwaltschaft, den Finanzämtern, den Senatsressorts, dem Stadtamt und dem Magistrat im Land Bremen ein angemessenes Sicherheitsniveau im Bereich der IT sicher?

Die FHB hat zum Schutz gegen diese Bedrohungen Sicherheitsmechanismen etabliert, welche den Empfehlungen des Bundesamtes für Informationstechnik (BSI) folgen.

Das allgemein gültige Sicherheitsniveau der landesbremischen Dienststellen wird grundsätzlich von der Senatorin für Finanzen vorgegeben und kontrolliert. Die IT-Dienstleister Dataport (Anstalt öffentlichen Rechts) und die BREKOM GmbH (BREKOM), welche für den Betrieb der PC-Infrastruktur und des Landesnetzes in der FHB zuständig sind, halten entsprechende Regelungen und Maßnahmen vor, um die IT-Sicherheit zu gewährleisten. Die BREKOM hat erheblichen Anteil daran, dass es seit 2010 zu keinen nennenswerten IT-Sicherheitsvorfällen im Bremer Verwaltungsnetz kam. Dataport wird für seine Trägerländer – also auch Bremen – ein gemeinsames CERT (Computer Emergency Response Team) aufbauen. Dies ist eine Gruppe von IT-Sicherheitsfachleuten, die bei der Lösung von konkreten IT-Sicherheitsvorfällen als Koordinator mitwirkt, Warnungen vor Sicherheitslücken herausgibt und Lösungsansätze anbietet. Den Dienststellen mit eigener IT-Infrastruktur wie z.B. der Polizei oder dem Bildungsbereich obliegt es, das Niveau ihres individuellen Sicherheitsmanagements anzupassen, bis hin zum generellen Abschalten des Internetzugangs für bestimmte Computerarbeitsplätze. Die Schulen sind physikalisch vom Netz der Verwaltung separiert, da dort das Gefährdungspotenzial für Attacken von "innen" deutlich höher eingeschätzt werden muss.

In Bremerhaven ist für den Betrieb des Verwaltungsnetzes der Betrieb für Informationstechnologie (BIT), Wirtschaftsbetrieb der Stadt Bremerhaven, zuständig. Das Verwaltungsnetz wird regelmäßig einer Sicherheitsüberprüfung durch unabhängige externe Dienstleister unterzogen.

4. Wie stellt der Senat für die Infrastrukturen im Land Bremen, wie beispielsweise der Energieversorgung, dem öffentlichen Nahverkehr, der Telekommunikation, der Krankenhäuser und Versicherungen ein angemessenes Sicherheitsniveau im Bereich der IT sicher?

Die hier genannten Dienstleister müssen eigenständig für die notwendige Sicherheit ihrer IT sorgen. Diese Aufgabe obliegt nicht der Freien Hansestadt Bremen.

Die Teilnahme an der LÜKEX Übung im Jahr 2011, die den Angriff auf und folgenden Ausfall von IT-Systemen simulierte, erfolgte exemplarisch für die Dataport-Trägerländer durch Hamburg. Die dort gemachten Erfahrungen werden von Dataport zurzeit an die anderen Trägerländer weitergegeben.

Der IT-Planungsrat, in dem das Land Bremen vertreten ist, ist wiederum Mitglied im Nationalen Cyber-Sicherheitsrat, über dessen Beratungen zu aktuellen Problemen und Maßnahmen der IT-Sicherheit in den kritischen Informations-Infrastrukturen Bremen regelmäßig informiert wird.

5. Wie viele Angriffe (erfolgreiche/nicht erfolgreiche) auf die Behörden und die Infrastrukturen des Landes Bremen wurden seit 2009 bis heute registriert, welche Auswirkungen hatten diese und kam es zu Einschränkungen für die Beschäftigten und/oder für die Bürger Bremens?

Die BREKOM stellt mehrmals täglich Angriffe auf das BVN fest. Diese Werte sind aber kein Maßstab für die zu bewertende Bedrohung. Hierzu bedarf es einer differenzierten Betrachtung über Vorfälle, Gefährdungen und Schäden. Die Auswirkungen sind in der Mehrzahl der Fälle bisher nicht geschäftskritisch gewesen. Der letzte Ausfall, bei dem es zu einem Abschalten einzelner interner Informationssysteme über längere Zeit kam, war 2009. Die vom Senat als Folge beschlossenen Maßnahmen sind in der Umsetzung (s.u. Antwort zu Frage 8). Dies sind im Wesentlichen die Standardisierung der IT und der Aufbau eines IT-Sicherheitsmanagements.

6. Wie werden die Mitarbeiter der Behörden über die Risiken solcher Angriffe und die Gefahren des Internets aufgeklärt? Inwiefern finden hierzu verpflichtende Fortbildungen oder gezielte Gespräche seitens der Behörden statt?

Seit 2011 organisiert die Senatorin für Finanzen im Rahmen der Zusammenarbeit mit Dataport ein Jour Fixe „IT-Sicherheit“. Die Ressorts sind hier vertreten und können über diese Plattform aktuelle Sicherheitsthematiken problematisieren. Aus gegebenen Anlässen werden Rundschreiben bzw. Empfehlungen per E-Mail verteilt. Verpflichtende Fortbildungen werden dazu nicht angeboten, jedoch sind die Dienststellen verpflichtet, den ordnungsgemäßen Betrieb der IT-Systeme in ihrem Verantwortungsbereich sicherzustellen. Einzelne Behörden haben bereits IT-Sicherheitsbeauftragte benannt, lassen ihre IT-Systeme extern auditieren und sensibilisieren für dieses Thema.

7. Inwiefern werden durch den Senat und in den Behörden mobile Geräte wie Smartphones und Tablets benutzt, und welche Maßnahmen ergreift der Senat, um diese Geräte in ähnlicher Weise wie PCs zu schützen?

Die Senatorin für Finanzen hat in Abstimmung mit den Ressorts ein Pilotprojekt initiiert, in dem Tablets und Smartphones, die mit den zentralen IT-Systemen der FHB direkt kommunizieren, eingesetzt werden. Die Verbindung dieser Geräte mit dem Verwaltungsnetz wird durch Policies (feste technische Regeln) auf den zentralen Servern geschützt, sowie durch die eingebauten Geräteschutzmechanismen, wie z.B. die Verwendung von PINs.
Ob der so zu gewährleistende Schutz der Geräte und der über sie genutzten Anwendungen unter Praxisbedingungen ähnlich wie bei „normalen“ PCs und Notebooks möglich und sinnvoll ist, wird in diesem Projekt ermittelt.

8. Wie sehen die Planungen des Senats zum Schutz der Behörden und der Infrastrukturen des Landes Bremen in Anbetracht der wachsenden Bedeutung der IT-Sicherheit für die Jahre 2012-2015 aus?

Die bereits begonnene und durch BASIS.bremen erheblich intensivierte Standardisierung der IT-Systeme in der FHB hilft, Sicherheitsrisiken transparent zu machen, und durchgehende Schutzmechanismen ergreifen zu können.

Um auch ein zukünftig qualitativ ausreichendes Informationssicherheitsmanagement sicherstellen zu können, soll die Kooperation der mit den entsprechenden Aufgaben befassten Stellen innerhalb und außerhalb der Bremer Verwaltung verstärkt werden. Dazu hilft auch die durch BASIS.bremen bewirkte Entlastung von operativen IT-Aufgaben in den Ressorts.

Außerdem ist eine verstärkte Zusammenarbeit mit den anderen Trägerländern von Dataport, den übrigen Bundesländern und dem Bund notwendig. Das wird z.B. beim Aufbau des CERT (s. o. Antwort zu Frage 3) bereits praktiziert.