

KLEINE ANFRAGE

des Abgeordneten Jens-Holger Schneider, Fraktion der AfD

Verwendung von proprietärer und quelloffener Software in Behörden des Landes Mecklenburg-Vorpommern

und

ANTWORT

der Landesregierung

Die Frage der Cyberkriminalität dringt zunehmend in den Verwaltungsalltag staatlicher Behörden ein. Exemplarisch und aktuell steht hierfür der Hackerangriff auf das Auswärtige Amt. (Quelle: [BR2 - Auswärtiges Amt und Verteidigungsministerium gehackt](#))

In einer Dokumentation des Rundfunk Berlin-Brandenburg (RBB) kritisiert der ehemalige IT-Chef der Bundesregierung die Abhängigkeit staatlicher Stellen von Microsoftprodukten. (Quelle: [Das Erste - Die Story im Ersten: Das Microsoft-Dilemma](#))

1. Ist die Landesregierung der Ansicht, dass durch Cyber-Angriffe auf das Auswärtige Amt oder andere staatliche Stellen die Datensicherheit, Vertraulichkeit und Integrität der informationstechnischen Systeme des Landes und der öffentlichen Landesverwaltung gefährdet oder in nicht mehr hinreichendem Maß gegeben ist (bitte begründen)?

Für die Landesregierung ist die Gewährleistung der Informationssicherheit ein kontinuierlicher Prozess. Damit wird ein bestmöglicher Schutz der drei Grundwerte der Informationssicherheit - Vertraulichkeit, Verfügbarkeit und Integrität - auch bei sich verändernden Gefährdungslagen angestrebt. Bislang geht die Landesregierung davon aus, dass es keine erfolgreichen Cyberangriffe auf die informationstechnischen Systeme des Landes gab. Da es unter anderem aufgrund geltender Sicherheitsrichtlinien und aufgrund umgesetzter Sicherheitsmaßnahmen grundsätzlich nicht möglich ist, vom Internet oder von anderen Netzen aus direkt auf die informationstechnischen Systeme der Landesverwaltung und insbesondere auf die darauf abgelegten Informationen zuzugreifen, haben die Cyberangriffe auf das Auswärtige Amt keine unmittelbaren Auswirkungen auf die Sicherheit der informationstechnischen Systeme der Landesverwaltung.

2. Welche Initiativen hat die Landesregierung vor dem Hintergrund der in der RBB-Dokumentation geäußerten Kritik gegenüber Microsoft geplant oder bereits ergriffen, um im Rahmen des IT-Sicherheitsmanagements die Datensicherheit, Vertraulichkeit und Integrität der von der Landesverwaltung verwendeten informationstechnischen Systeme sicherzustellen?

Für die Landesregierung bedarf es keines besonderen Anlasses, um der Sicherheit der Informationstechnik (IT) eine essenzielle Bedeutung beizumessen. So setzt die Landesregierung die Sicherheitsleitlinie des IT-Planungsrates (Beschluss 2013/01 des IT-Planungsrates) um. Dazu hat die Landesregierung am 12. Mai 2014 die Leitlinie zur Gewährleistung der Informationssicherheit in der Landesverwaltung von Mecklenburg-Vorpommern (IS-Leitlinie M-V) beschlossen. Gemäß dieser Leitlinie wurde ein ressortübergreifendes Informationssicherheitsmanagement mit einheitlichen Sicherheitsstandards, einschließlich eines Computer-Notfall-Teams zur gemeinsamen Abwehr von Angriffen auf die Informationstechnik aufgebaut und ständig weiterentwickelt.

3. Wie viele identifizierte Angriffe auf die IT-Infrastruktur der Landesverwaltung in den Jahren 2014 bis 2018 sind der Landesregierung bekannt?
Wie viele konnten abgewehrt werden?
(Bitte aufschlüsseln nach Art des Angriffs, Anzahl, Jahr und Anzahl der abgewehrten Angriffe.)

Zum Schutz vor IT-Angriffen nutzen die Behörden der Landesverwaltung für ihre Internetzugänge unter anderem ein zentrales Sicherheitssystem, das aus mehreren Firewall- und Viruswallsystemen besteht und durch die DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ M-V GmbH) betrieben wird. Dieses zentrale Sicherheitssystem ermöglicht eine konzentrierte Gefahrenkontrolle und Gefahrenabwehr.

Nach Auskunft der DVZ M-V GmbH verarbeiten die zentralen Firewall-Systeme der Landesregierung je nach Aufkommen bis zu 150.000 Datenpakete je Sekunde. In jeder Sekunde verursachen durchschnittlich rund 20 dieser Pakete Warnmeldungen, die von den Herstellern der Firewall-Systeme mit dem Level „kritisch“ eingestuft sind. Auf diese Weise summiert sich die Zahl der pro Tag möglichen Angriffsversuche auf mehrere Hunderttausend.

Zu den Angriffsversuchen zählen unter anderem die folgenden Angriffsarten:

- SPAM/E-Mail mit schadhafte Anhängen, zum Beispiel Viren, Trojanern oder Würmern: An einem durchschnittlichen Arbeitstag erreichen circa 350.000 E-Mails das zentrale Sicherheitssystem in der DVZ M-V GmbH. Von diesen E-Mails werden durch das zentrale Sicherheitssystem circa 302.500 E-Mails als SPAM erkannt; 2.500 E-Mails sind mit gefährlichen Anlagen belastet. Lediglich 45.000 E-Mails (rund 12,85 Prozent) stellen das „normale“ E-Mailaufkommen der Landesverwaltung dar.
In Spitzenzeiten (Feiertage, Wahlen, bundesweite/internationale Kongresse oder Besuche von Staatsoberhäuptern) potenzieren sich diese Zahlen um ein Vielfaches.

- Port-Scans: Hacker suchen gezielt nach verwundbaren IT-Systemen, um diese unter anderem für den SPAM-Versand, für die Verbreitung von zumeist urheberrechtlich geschützten Inhalten oder zur Vorbereitung von Denial-of-Service-Angriffen gegen Dritte zu missbrauchen.

Bei Denial-of-Service-Angriffen (Verfügbarkeitsangriffen) soll durch Überlastung der IT-Infrastruktursysteme ein Ausfall von Netzwerkdiensten erreicht werden.

Konkrete Statistiken darüber, wie viele IT-Angriffe, welcher Art und in welchem Zeitraum festgestellt wurden, liegen nicht vor. Aufgrund der hohen IT-Sicherheitsstandards konnten die Angriffsversuche auf das zentrale Sicherheitssystem bisher abgewehrt werden.

4. Welche strategischen Vorteile und Nachteile sieht die Landesregierung im Einsatz von proprietären Softwareanwendungen in der Landesverwaltung?
 - a) Wie bewertet sie den Einsatz proprietärer Software hinsichtlich der Sicherheit, Wirtschaftlichkeit, Nachhaltigkeit und Effizienz?
 - b) Welche strategischen Vorteile und Nachteile sieht die Landesregierung im Einsatz von quelloffenen Softwareanwendungen in der Landesverwaltung?
 - c) Wie bewertet sie den Einsatz quelloffener Software hinsichtlich der Sicherheit, Wirtschaftlichkeit, Nachhaltigkeit und Effizienz?

Die Fragen 4, a), b) und c) werden zusammenhängend beantwortet.

Die IT-Strategie der Landesverwaltung ist darauf ausgerichtet, einen wirtschaftlich effizienten IT-Einsatz zu gewährleisten und den Anforderungen einer modernen Verwaltung langfristig gerecht zu werden. Der wirtschaftlich effiziente Einsatz wird insbesondere durch die Verwendung einheitlicher Standards, die im IT-Strukturrahmen der Landesverwaltung festgelegt sind, sichergestellt. Ob diese Standards den Einsatz proprietärer oder quelloffener Software vorsehen, hängt sowohl von den bestehenden fachlichen Anforderungen als auch von wirtschaftlichen Gesichtspunkten ab. Da ein großer Anteil der in der Landesverwaltung eingesetzten Fachverfahren den Einsatz von Microsoft-Betriebssystemen und Microsoft-Office-Produkten voraussetzt (unter anderem betrifft dies das Vorgangsbearbeitungssystem DOMEA[®]), wird an den Endarbeitsplätzen der Behörden vorrangig mit proprietärer Software gearbeitet. Im Serverbereich kommt jedoch auch quelloffene Software zum Einsatz.

Der standardisierte Einsatz von Microsoft-Betriebssystemen und Microsoft-Office-Produkten an den Endarbeitsplätzen ermöglicht unter anderem den zentralen Einsatz eines Softwareverteilungssystems in der DVZ M-V GmbH, mit welchem bereits etwa 4.400 Endarbeitsplätze der Landesverwaltung gemanagt werden. Das bedeutet, dass die benötigte Software nur an einer Stelle für die Installation vorbereitet und konfiguriert, dann am Endarbeitsplatz bereitgestellt und anschließend regelmäßig gepflegt und mit Sicherheitsupdates versorgt wird. Von daher ist der Einsatz dieser Software im Hinblick auf Sicherheit, Wirtschaftlichkeit, Nachhaltigkeit und Effizienz positiv zu bewerten.

Ebenso wie das Bundesamt für die Sicherheit in der Informationstechnik vertritt die Landesregierung hierzu die Auffassung, dass freie und quelloffene Software inzwischen eine anerkannte Alternative zu proprietären Angeboten darstellt. Gleichwohl unterliegen die Einsatzmöglichkeiten dieser Software gewissen Rahmenbedingungen, die beachtet werden müssen. Wie zu den vorherigen Fragen bereits ausgeführt, sind hierbei insbesondere Abhängigkeiten zu den Fachverfahren zu berücksichtigen. Auch müssen die Wirtschaftlichkeitsaspekte ganzheitlich betrachtet werden, da den Einsparmöglichkeiten bei den Lizenzkosten meist erhöhte Schulungs-, Umstellungs-, und gegebenenfalls auch Anpassungsaufwände gegenüberstehen. Zudem haben die bisherigen Praxisbeispiele gezeigt, dass die Kosten für die Absicherung eines kontinuierlichen Supports bei Open-Source-Lösungen potentiell höher liegen als bei den derzeit verbreiteten Closed-Source-Lösungen.

5. Welche Rolle spielen freie und quelloffene Software sowie offene Standards und deren Verwendung in der öffentlichen Verwaltung in der strategischen Ausrichtung der IT-Politik der Landesregierung und im IT-Masterplan des Landes?

Die E-Government-Strategie der Landesverwaltung orientiert sich an der bundesweiten E-Government-Strategie. Ein grundlegendes Ziel der bundesweiten E-Government-Strategie ist eine weitestgehende Standardisierung der in der gemeinsamen Zusammenarbeit eingesetzten Architekturen und Anwendungen, um Folgendes zu erreichen:

- Interoperabilität - Gewährleistung der Zusammenarbeit verschiedener E-Government-Anwendungen, um effizient Informationen zwischen Bund, Ländern, Kommunen, Unternehmen und Partnern des Bundes auszutauschen,
- Wiederverwendbarkeit - mehrfache Nutzung von Prozess- und Datenmodellen, Systemen, Diensten und Komponenten in verschiedenen E-Government-Projekten, um Synergieeffekte zu erzeugen,
- Offenheit - Einbindung offener Standards in E-Government-Anwendungen, um deren langfristige Nutzbarkeit zu fördern,
- Reduktion von Kosten und Risiken - Berücksichtigung investitionssicherer Entwicklungen am Markt und im Bereich der Standardisierung,
- Skalierbarkeit - Sicherstellung der Nutzbarkeit von Anwendungen bei sich ändernden Anforderungen hinsichtlich Volumen und Transaktionshäufigkeit.

Auf dieser Grundlage entstanden die „Standards und Architekturen für E-Government-Anwendungen“ (SAGA). SAGA beschreibt Standards, Technologien und Methoden für den Einsatz von Informationstechnik. Die hierin referenzierten Standards bilden eine Grundlage für den reibungslosen Datenaustausch im deutschen E-Government - eine wichtige Voraussetzung für eine moderne und dienstleistungsorientierte Verwaltung. Daher strebt der IT-Planungsrat einen deutschlandweit gültigen Standard auf der Basis von SAGA an, der dann auch für die Behörden der Landesverwaltung von Mecklenburg-Vorpommern zur Geltung kommen wird.

6. In welchem Umfang wird derzeit bereits freie und quelloffene Software in der öffentlichen Landesverwaltung eingesetzt (z. B. Betriebssysteme, Officeanwendungen, Fachanwendungen usw.)?
In welchem Umfang wird derzeit bereits freie und quelloffene Software in der öffentlichen kommunalen Verwaltung eingesetzt (z. B. Betriebssysteme, Officeanwendungen, Fachanwendungen usw.)?

Auf den Endarbeitsplätzen wird freie und quelloffene Software nur begrenzt eingesetzt. Verbreitet sind hier beispielsweise der Internetbrowser Mozilla Firefox und Hilfsprogramme wie Mediaplayer, Bildbearbeitungsprogramme, Brennwerkzeuge und Programme zum Erstellen von PDF-Dateien. Bei Office-Produkten ist Open-Source-Software aus den in der Antwort zu Frage 4 genannten Gründen kaum im Einsatz. Im Serverbereich sind neben quelloffenen Betriebssystemen wie Linux auch quelloffene Werkzeuge zur Programmentwicklung, Netzwerküberwachung und Netzwerkbetreuung sowie quelloffene Web-Server im Einsatz. Auch für zentrale Verfahren, die von der DVZ M-V GmbH betrieben werden, sind Linux-Server im Einsatz. In welchem konkreten Umfang aktuell freie und quelloffene Software in den einzelnen Ressorts der Landesregierung für Fachverfahren genutzt wird, ist nicht bekannt.

In welchem konkreten Umfang aktuell freie und quelloffene Software in den einzelnen Kommunen sowohl für Betriebssysteme und Office-Anwendungen als auch für Fachverfahren genutzt wird, ist der Landesregierung nicht bekannt.

7. Plant die Landesregierung, zukünftig proprietäre Software durch freie und quelloffene Software und offene Standards in der Landesverwaltung zu ersetzen?

Die Landesregierung sieht derzeit keine Veranlassung, von der gegenwärtigen Strategie, die zu den vorherigen Fragen bereits erläutert wurde, abzuweichen. Dem Anliegen wird aber Rechnung getragen, indem sie sich im E-Government-Bereich an den „Standards und Architekturen für E-Government-Anwendungen“ - SAGA orientiert und weiter orientieren wird.