bitkom

Cybersicherheit im Public Sector

8 Thesen der digitalen Wirtschaft für eine sichere und resiliente öffentliche Verwaltung

November 2024

Cybersicherheit im Public Sector: 8 Thesen der digitalen Wirtschaft für eine sichere und resiliente öffentliche Verwaltung

Cybersicherheit im Public Sector – Deshalb sollten wir häufiger darüber sprechen:

- **Schutz sensibler Daten**: Cybersicherheit in der öffentlichen Hand ist entscheidend, um persönliche und vertrauliche Daten der Bürgerinnen und Bürger, der Verwaltung sowie der Unternehmen vor Cyberangriffen zu schützen. Cybersicherheit ist Datenschutz.
- **Gewährleistung öffentlicher Dienste**: Die öffentliche Hand ist für die Bereitstellung zentraler Dienste verantwortlich, bei denen Ausfälle erhebliche wirtschaftliche und soziale Folgeeffekte mit sich bringen könnten. Cybersicherheit ist notwendig, um einen reibungslosen Betrieb dieser Dienste sicherzustellen und Ausfälle durch Cyberangriffe zu verhindern. Ein wirksamer Schutz ist zudem entscheidend, um lebenswichtige Infrastrukturen wie Energie, Wasser- und Lebensmittelversorgung sowie Transportnetze vor Angriffen zu schützen und deren kontinuierlichen Betrieb sicherzustellen.
- **Vertrauen in Regierung und Demokratie**: Ein hohes Schutzniveau fördert das Vertrauen der Bürgerinnen und Bürger in die Regierung und stärkt die demokratischen Prozesse, indem es die Integrität von Wahlen, politischen Institutionen und die Leistungsfähigkeit der öffentlichen Verwaltung schützt.
- **Wirtschaftliche Stabilität**: Ein hohes Sicherheitsniveau schützt die öffentliche Hand vor wirtschaftlichen Schäden durch Cyberangriffe, Datenverluste und Betriebsunterbrechungen. 67% des Gesamtschadens durch Industriespionage, Sabotage und Datendiebstahl können laut Bitkom Wirtschaftsschutzbericht 2024 in Deutschland auf Cyberattacken zurückgeführt werden (Summe: 178,6 Mrd. Euro).[1] Auch Unternehmen der öffentlichen Hand sind von diesem wirtschaftlichen Risiko betroffen.

[1] Siehe hierzu die Bitkom Studie Wirtschaftsschutz 2024 (Link).

- **Nationale Sicherheit**: Ein hohes Sicherheitsniveau ist unerlässlich, um Sicherheitssysteme vor Angriffen zu verteidigen und potenzielle Bedrohungen für die nationale Sicherheit abzuwehren.
- **Daseinsfürsorge des Staates**: Die Gewährleistung der Cybersicherheit im öffentlichen Raum dürfte inzwischen Teil der Verpflichtung zur Daseinsvorsorge des Staates (Art. 20 GG) sein. Eine Untätigkeit und damit einhergehende negative Auswirkung auf die Funktionsfähigkeit staatlicher Einrichtungen kann eine Verletzung der Daseinsvorsorgepflicht darstellen.
- **Vorbildwirkung**: Der Staat hat eine Vorbildwirkung gegenüber den Bürgerinnen und Bürgern sowie Unternehmen auch hinsichtlich des Themenfeldes Cybersicherheit.
- **Veränderte Bedrohungslage**: Entwicklungen der vergangenen Jahre in Bezug .auf Künstliche Intelligenz und im Kontext von Hybrid Work haben für neue Arbeitsrealitäten gesorgt, auf die der Public Sector bisher nicht vorbereitet ist.

Handlungsempfehlungen – Folgende Schritte sind aus Sicht der digitalen Wirtschaft jetzt erforderlich:

Sicherheitsanforderungen auf allen Ebenen

1. Gesetzliche Sicherheitsanforderungen müssen auf alle Ebenen und Institutionen der öffentlichen Hand ausgedehnt werden.

Eine reibungslos funktionierende öffentliche Verwaltung ist von entscheidender Bedeutung für unsere Gesellschaft und die Wirtschaft. Sicherheitsvorfälle können zu Ausfallzeiten führen, die sich finanziell auch in der Industrie und bei Privatpersonen bemerkbar machen. Dabei spielen nicht nur Bundesbehörden, sondern auch Kommunal- und Landesbehörden eine wichtige Rolle, beispielsweise im Zusammenhang mit Genehmigungs- und Überwachungsvorgängen. Daher ist es unerlässlich, auch diese Behörden, entgegen dem aktuellen Entwurf des NIS2-Umsetzungsgesetzes, als besonders wichtige Einrichtungen in den Anwendungsbereich von Sicherheitsvorgaben aufzunehmen, um ebenenunabhängig eine verlässliche und resiliente Verwaltung zu gewährleisten.[2] Zusätzlich müssen neben gesetzlichen Vorgaben wie NIS-2 auch allgemeingültige Sicherheitskonzepte wie Zero Trust auf alle Ebenen ausgeweitet werden. So fordern laut Wirtschaftsschutzbericht des Bitkom 84 %, dass die Meldung von Cyberangriffen für Unternehmen, aber auch Behörden oder öffentliche Einrichtungen verpflichtend sein sollte.[3] Insbesondere Kommunen müssen häufig sensible personenbezogene Daten verarbeiten. Dies ist beispielsweise bei Asylverfahren oder entsprechenden Anfragen im Kontext des Staatsschutzes der Fall. Um vollständige Datensicherheit zu gewährleisten, müssen daher alle Ebenen der Verwaltung in den Anwendungsbereich von relevanten Sicherheitsvorgaben einbezogen sein. Eine Ausnahme der Kommunen aufgrund des zu

84%

fordern eine verpflichtende Meldung von Cyberangriffen für den Public Sector.

[2] Siehe hierzu die Bitkom Stellungnahme zum NIS-2 Umsetzungs- und Cybersicherheitsstärkungsgesetz vom Mai 2024 (Link).
[3] Siehe hierzu die Bitkom Studie Wirtschaftsschutz 2023 (Link).

erwartenden Erfüllungsaufwands ist nicht rechtfertigbar, wenn man sich die Bedrohungen durch Cyberangriffe anschaut. Ein Lösungsansatz kann die Einrichtung von IT-Kompetenzzentren sein, die die IT-Infrastruktur von kleinen Kommunen übernehmen und so Synergien schaffen und Knowhow bündeln.

Moderne IT-Infrastruktur

2. Nur eine Implementierung und kontinuierliche Aktualisierung von moderner IT-Infrastruktur kann einen sicheren Betrieb der IT im Public Sector gewährleisten.

Die größten Schwachstellen für Cyberangriffe sind eine veraltete IT-Infrastruktur und der menschliche Faktor. Daher sollte im ersten Schritt eine strukturierte Bestandsaufnahme der IT-Landschaft in Deutschland erfolgen. Besonders kleinere Gemeinden und Landkreise verfügen oft nicht über die notwendigen Ressourcen und IT-Sicherheitssysteme, um Angriffe so wirksam abzuwehren wie spezialisierte Unternehmen. Ein Beispiel dafür ist der Angriff auf den Landkreis Anhalt-Bitterfeld, der vom BSI im Jahr 2021 als erster Cyber-Katastrophenfall Deutschlands eingestuft wurde.[4] Laut Bitkom Wirtschaftsschutzbericht stimmen 76 % der befragten Unternehmen der Aussage zu, dass die öffentliche Verwaltung in Deutschland viel schlechter auf Cyberangriffe vorbereitet ist als die deutsche Wirtschaft.[5]

76%

sehen die Verwaltung viel schlechter auf Cyberangriffe vorbereitet als die Wirtschaft.

Vergangene Krisen haben gezeigt, dass Verwaltungen einen sicheren, mobilen und leistungsfähigen Zugang zu Daten und Verwaltungsdiensten bereitstellen müssen. Um dies zu gewährleisten, ist eine moderne Verwaltung auf eine zuverlässige und moderne IT-Infrastruktur angewiesen.

> Der Cyberangriff auf den Landkreis Anhalt-Bitterfeld wurde vom BSI als erster Cyber-Katastrophenfall Deutschlands eingestuft. Solche Vorfälle dürfen nicht zum Alltag werden.

Die Ausweitung der Nutzung von (Multi-) Cloud-Lösungen ist dabei zentral, gepaart mit einer Konsolidierung der Cybersicherheitstechnologien, dem Einsatz künstlicher Intelligenz und verstärkter Automation, um schnell und professionell auf neue Gefahren reagieren zu können. Der Vorteil einer (Multi-)Cloud Infrastruktur liegt neben ihrer Zugänglichkeit in der dezentralen und sicheren Datenspeicherung. Außerdem hat sie den Vorteil, dass Sicherheitsupdates sofort bereitstehen und nicht erst auf den lokalen Systemen vor Ort aktualisiert werden müssen. Dies stellt sicher, dass die IT-Systeme der öffentlichen Hand stets auf dem neuesten Stand sind und vor bekannten Bedrohungen geschützt werden. Daher sind (Multi-)Cloud Lösungen nicht nur als Ersatz, sondern als hilfreicher Ansatz zu verstehen, um Security Dienste zu

[4] Siehe hierzu „Erster Cyber-Katastrophenfall in Deutschland“ (FAZ.net) (Link).
[5] Siehe hierzu die Bitkom Studie Wirtschaftsschutz 2024 (Link).

konsumieren und gleichzeitig den Aufwand für Wartung, Betrieb und Updates gering zu halten. Hinzu kommt, dass effektive Cybersicherheit nur durch das Zusammenführen und die automatisierte Analyse sehr großer Mengen an relevanten international zur Verfügung stehenden Gefahrendaten erfolgen kann. Dies kann nur durch Cloud Computing Leistung erbracht werden.

Die steigende Anzahl von Sicherheitsvorfällen lässt sich nicht mehr mit überkommener und angreifbarer IT-Infrastruktur in den Griff bekommen. Der technologische „Sanierungsstau“ hat in der Vergangenheit zu erheblichen Schäden geführt, darunter dem Verlust vertraulicher Informationen und einem sinkenden Vertrauen in die Resilienz öffentlicher Institutionen. Ausdrücklich zählen wir zu IT-Infrastruktur auch Endgeräte. Zu wenige Einrichtungen berücksichtigen deren Sicherheit, einschließlich der Firmware. Hardware, wie beispielsweise PCs und Drucker, sind kritische Elemente der Netzwerksicherheit, da jedes Gerät ein potenzielles Einfallstor für Cyberangriffe darstellt. Die Geräte sind vor allem dann einem erhöhten Gefährdungspotenzial ausgesetzt, wenn sie nicht nur im heimischen Umfeld, sondern auch mobil eingesetzt werden. Solche Angriffe gefährden die Vertraulichkeit, die Verfügbarkeit als auch die Integrität der mit den Geräten verarbeiteten und gespeicherten Daten sowie wie die Funktionsfähigkeit der Geräte selbst. Moderne Endgeräte können ab Werk mit integrierten Sicherheitsfunktionen ausgestattet werden, die bei der Einhaltung der Sicherheitsvorgaben unterstützen können.

Der öffentliche Sektor muss Cybersicherheit als kontinuierliche Aufgabe betrachten. Der Bitkom empfiehlt Unternehmen 20 % ihres IT-Budgets für Security auszugeben. An dieser Empfehlung kann sich auch die öffentliche Hand orientieren. Einrichtungen der öffentlichen Hand sollten einen festen Posten ihres Haushalts für Cybersicherheit einplanen.

20%

des IT-Budgets sollten für Security ausgegeben werden.

Definition von Schutzniveaus

3. Eine klare,realistische und individuelle Definition von Schutzniveaus ist essenziell, um Ressourcen effektiv zu verteilen und sicherzustellen, dass der Schutz dort verstärkt wird, wo er benötigt wird.

Bei der Erstellung von Anforderungen an IT-Infrastrukturen und Sicherheitsvorkehrungen sollte im Auge behalten werden, was als besonders schützenswert zu betrachten ist. Klar definierte, realistische und individuell für die Schutzziele festgelegte Schutzniveaus sorgen für eine effiziente Ressourcenverteilung und stellen sicher, dass dem Anspruch Daten bezogen auf ihre Verfügbarkeit, Vertraulichkeit oder Integrität besonders zu sichern, nachgekommen werden kann. Pauschale Anforderungsniveaus sorgen hingegen für hohe Aufwendungen, ohne eine tatsächlich resilientere IT-Infrastruktur zu schaffen. Allerdings sollten Einrichtungen der Zentralverwaltung das höchste Schutzniveau aufgrund ihrer kritischen Bedeutung für die Funktionsfähigkeit des Staates und das Vertrauen der Bürgerinnen und Bürger in die Demokratie erhalten.

Die Definition von Sicherheitsniveaus ist auch im Kontext der Vergabe relevant. Es ist von entscheidender Bedeutung, dass bei der Beschaffung von Endgeräten, Software und Dienstleistungen Sicherheitsanforderungen mitgedacht werden. Der Endgerät-sicherheit sollte als Teil von Cyber-Risikobewertungen im öffentlichen Sektor Priorität

eingeräumt werden, einschließlich der Fähigkeit zur Erkennung von Sicherheitsverletzungen und zur Erholung nach Attacken. Eine Organisation des öffentlichen Sektors sollte stets über ein klares Verständnis und eine aktuelle Formulierung von Mindestsicherheitsanforderungen und die bevorzugte Berücksichtigung des Standes der Technik verfügen. Sinnvollerweise sollten deshalb sowohl für die organisatorische als auch die technische Umsetzung Konzepte erarbeitet werden, die auch den Zugriff auf die entsprechenden Ressourcen je nach Sicherheitsniveau steuern. Dabei kann es beispielsweise helfen Netze zu segmentieren oder Rollenkonzepte mit unterschiedlichen Rechten zu etablieren. Systeme mit einem definierten hohen Schutzniveau sollten im Rahmen eines Sofortprogramms grundlegend geprüft und entsprechende Maßnahmen eingeleitet werden.

Investition von Verschlüsselungstechnologien

4. Die Umstellung auf zukunftsfähige Kryptographie, z. B. im Kontext von Quantencomputing, sollte bereits heute im Risikomanagement verankert und finanziell unterstützt werden.

Rasante Fortschritte im Quantencomputing stellen eine potenzielle Gefahr für die momentan noch genutzten Verschlüsselungsmechanismen in IT-Systemen dar. Es besteht die Möglichkeit, dass die heute gesammelten und gespeicherten Daten zu einem späteren Zeitpunkt entschlüsselt werden können, sobald entsprechende Quantencomputing-Algorithmen verfügbar sind. Angesichts dieser Entwicklungen gewinnt die quantensichere Kryptographie, die Methoden entwickelt, die auch den Fähigkeiten von Quantencomputern standhalten, zunehmend an Bedeutung. Empfehlungen für einen Umstieg auf quantensichere Kryptographie sind zwar bereits vorhanden, der Übergang ist jedoch komplex und zeitaufwändig. Daher ist ein frühzeitiges Handeln zur Migration zu quantensicheren Kryptographieverfahren insbesondere im öffentlichen Sektor von besonderer Bedeutung und muss in den nächsten fünf Jahren in den Fokus rücken.

Schulung des Personals

5. Um Cyberangriffe effektiv abwehren zu können, müssen alle Mitarbeitenden in Behörden umfassend im Bereich der IT-Sicherheit geschult und sensibilisiert werden.

Die größte Schwachstelle für Cyberangriffe ist neben veralteter IT-Infrastruktur der menschliche Faktor. Dieser darf nicht vernachlässigt werden. Dies gilt für die Privatwirtschaft, aber ebenso für öffentliche Einrichtungen. Grundlegendes Know-how im Bereich der IT-Sicherheit darf sich in den Behörden nicht auf die IT-Abteilungen beschränken. Sicherheitsvorfälle können ihre Ursprünge an den Arbeitsplätzen aller Mitarbeitenden in öffentlichen Einrichtungen haben. In einer digitalen Verwaltung müssen alle Mitarbeitenden für Sicherheitsrisiken in ihrem Arbeitsalltag sensibilisiert sein. Nur so kann ganzheitlich ein hohes Niveau von Cybersicherheit gewährleistet werden. Allerdings hat menschliches Handeln seine Grenzen. Gerade Künstliche Intelligenz stellt die Belegschaften vor Herausforderungen. Deswegen sind technische Lösungen entscheidend, um die Mitarbeitenden zu unterstützen und entlasten.

Integration von Threat Intelligence Services

6. Öffentliche Einrichtungen müssen in die Lage versetzt werden Bedrohungen frühzeitig zu erkennen und entsprechende Informationen zu teilen.

Die zunehmende Komplexität von Cyberbedrohungen erfordert die Integration fortschrittlicher Bedrohungserkennungs- (Threat Intelligence) und Reaktionsfähigkeiten in den IT-Infrastrukturen des öffentlichen Sektors. Die Nutzung von Bedrohungsinformationen und Echtzeitanalysen ist unerlässlich, um diese Gefahren proaktiv zu identifizieren und zu mildern. Wir setzen uns für die obligatorische Einführung von Bedrohungserkennungssystemen in allen öffentlichen Einrichtungen ein. Die Implementierung dieser Mechanismen ermöglicht es dem öffentlichen Sektor, der Komplexität moderner Cyberbedrohungen voraus zu sein und die Sicherheit und Kontinuität wesentlicher öffentlicher Dienstleistungen zu gewährleisten.

Schutz demokratischer Institutionen

7. Einrichtung einer gesonderten Task Force zur Sicherstellung der Integrität von Wahlen

Wir fordern die Einrichtung einer spezialisierten Taskforce, die sich auf die Identifizierung, Überwachung und Abwehr hybrider Bedrohungen für die Integrität von demokratischen Wahlen konzentriert. Diese Taskforce sollte die Fähigkeiten von öffentlichen Einrichtungen und privaten Cybersicherheitsfirmen bündeln, um umfassende Bedrohungsbewertungen und koordinierte Reaktionsstrategien vor, während und nach den Wahlperioden bereitzustellen. Angesichts der zunehmenden Komplexität dieser Bedrohungen wird eine dedizierte Taskforce sicherstellen, dass unsere demokratischen Prozesse sicher und widerstandsfähig bleiben und das Vertrauen der Öffentlichkeit in unsere Wahlsysteme erhalten bleibt.

Kooperationen bei der Vorbereitung auf Bedrohungslagen

8. Verbesserung der Zusammenarbeit zwischen Strafverfolgungsbehörden und privaten Cybersicherheitsunternehmen

Effektive Cybersicherheit im öffentlichen Sektor erfordert eine robuste Zusammenarbeit zwischen Strafverfolgungsbehörden und privaten Cybersicherheitsunternehmen. Diese Zusammenarbeit ist entscheidend für den Austausch von forensischen Beweisen und die Durchführung effektiver rechtlicher Schritte gegen böswillige Cyberakteure. Wir fordern die Einrichtung eines formalisierten Rahmens für die Zusammenarbeit zwischen öffentlichen Strafverfolgungsbehörden und privaten Cybersicherheitsfirmen. Dieser Rahmen sollte regelmäßige Informationsaustausche, gemeinsame Schulungsübungen und koordinierte Ermittlungsprotokolle bei Cybervorfällen ermöglichen. Durch die Förderung einer engeren Zusammenarbeit können wir die Ressourcen und Fachkenntnisse sowohl des öffentlichen als auch des privaten Sektors nutzen, um die nationale Cybersicherheitsresilienz zu stärken und rechtliche Maßnahmen gegen Cyberkriminalität effektiver zu gestalten.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner
Marc Danneberg | Leiter Public Sector
T 030 27576-526 | m.danneberg@bitkom.org

Felix Kuhlenkamp | Referent Sicherheitspolitik
T 030 27576-279 | f.kuhlenkamp@bitkom.org

Esther Steverding | Referentin Public Sector
T 030 27576-216 | e.steverding@bitkom.org

Sven Wagner | Referent Smart City
T 030 27576-314 | s.wagner@bitkom.org

Verantwortliches Bitkom-Gremium
AK Digitale Verwaltung

Titelbild
Gavin Hellier – stocksy.com