Dialog für Cybersicherheit

Ergebnisbericht

Workstream Cyberdome

Dialog für Cybersicherheit

Stand: Oktober 2026

Creative Commons CC-BY-SA-Lizenz 4.0 International

Dieser Bericht dokumentiert den Workstream Cyberdome, der von November 2025 bis Oktober 2026 im Rahmen des Dialogs für Cybersicherheit durchgeführt wurde. Die Idee hinter dem Workstream war der Aufbau eines niederschwelligen Schutzschirms durch Nutzung des BSI-Wissens, automatisierte Sicherheitslösungen und transparente, bidirektionale Kommunikation zwischen dem BSI sowie Stakeholdern aus Staat, Wirtschaft und Zivilgesellschaft. Die drei Skizzen „BSI git", „BSI Softwareprüfung“ und „Intelligence to Action“ wurden miteinander besprochen und Möglichkeiten erster Umsetzungspunkte gesucht. Die bis zum Abschluss des Workstreams erarbeiteten Ansätze und Lösungsvorschläge sind in diesem Bericht aufgeführt.

Ideengeber:innen des Workstreams: Jens Bitterer (Zivilgesellschaft), Anke Domscheid-Berg, Markus Drenger (Zivilgesellschaft), Manuel HonkHase Atug (Zivilgesellschaft), Martin Tschirsich (Zivilgesellschaft).

Beteiligte Mitwirkende des Workstreams: Frank Bindrich (BSI), Jens Bitterer (Zivilgesellschaft), Markus Drenger (Zivilgesellschaft), Manuel HonkHase Atug (Zivilgesellschaft), Franzi Ehret (Zivilgesellschaft), Martin Tschirsich (Zivilgesellschaft), Andreas Rohr (Zivilgesellschaft), Peter Schoo (Wissenschaft), Thilo Roschel

Der Dialog für Cybersicherheit des Bundesamtes für Sicherheit in der Informationstechnik ist ein partizipativ ausgerichteter gesamtgesellschaftlicher Dialog, um die Vielschichtigkeit der Perspektiven auf das Thema Cybersicherheit möglichst breit und realitätsnah abzubilden und allen Beteiligten einen Austausch bzw. eine Mitwirkung auf Augenhöhe zu ermöglichen.

Der Dialog für Cybersicherheit soll daher ausdrücklich den verschiedenen Meinungen und Ansätzen zur Annäherung an das Thema Cybersicherheit aus Sicht der Zivilgesellschaft Raum und die Möglichkeit zum Austausch geben, ohne dies durch eine engmaschige Steuerung des BSI zu beschränken.

Der vorliegende Bericht wurde von der BSI-Geschäftsstelle und den Workstream-Teilnehmer:innen eigenständig erarbeitet. Die dort wiedergegebenen Ansichten spiegeln nicht zwangsläufig die Ansicht des BSI bzw. aller Teilnehmenden wider.

Weitere Informationen zum Dialog für Cybersicherheit:

http://www.dialog-cybersicherheit.de

Kontakt Geschäftsstelle: projekt-digitalegesellschaft@bsi.bund.de

Lizenz: Dieser Bericht steht unter der Lizenz Creative Commons CC-BY-SA-Lizenz 4.0 International.

Dialog für Cybersicherheit

Inhalt

1. Einleitung 2
Überblick 2
Die drei ursprünglichen Use Cases 2
Konsolidierung zum Cyberdome-Konzept / Finale Ideenskizze 2
Die drei Bausteine des Cyberdome 2
Zusammenfassung der Konsolidierung 3
2. Baustein 1: BSI Git Vorschlag 3
Problemstellung 4
Ansatz 4
Vorteile für IT-Sicherheitsvorgaben und Architekturrichtlinien 5
Umfang 5
Inhaltliche Umsetzungsvorschläge 6
Offene Fragen und mögliche nächste Schritte 8
Bewertung 9
3. Baustein 2: „Intelligence to Action“ (DNS Angebot des BSI) 9
Problemstellung 9
Ansatz 10
Vorteile des Ansatzes 10
Umfang 11
Datenschutz, Transparenz und Resilienz 11
Mögliche Umsetzung 12
Bewertung 12
4. Baustein 3: Software Checks: 13
Problemstellung 13
Ansatz 13
Vorteile für IT-Sicherheitsvorgaben und Architekturrichtlinien 14
Umfang 14
Umsetzungsvorschlag 15
Bewertung 15
5. Schnittstelle zu ähnlichen/verwandten Projekten 16
Grundschutz ++ 16
BSI-Cyberdome 16
CyberGovSecure 19
6. Ergebnis 20
7. Literatur 22

1. Einleitung

Überblick

Der Cyberdome Workstream entstand aus drei eigenständigen Use Cases, die im Rahmen des Dialogs für Cybersicherheit entwickelt und am 15. November 2025 während der Denkwerkstatt „Sichere Informationsgesellschaft“ in Berlin zu einem integrierten Konzept konsolidiert wurden.

Die drei ursprünglichen Use Cases

1. Threat Intelligence to Action (DiCySi_Ideen_Skizzen_2025_Cyberdome.pdf)

Threat Intelligence Informationen zu Cyberangriffen sind in Expertenkreisen und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) bekannt, werden aber von anderen öffentlichen Stellen und Unternehmen nicht automatisiert zum Schutz ihrer IT-Infrastruktur übernommen. Behörden und Unternehmen werden unnötig Opfer von Cyberangriffen, da seit Tagen/Stunden bekannte C2-Domains[1] und C2-IP-Adressen weder gefiltert noch blockiert wurden.

2. BSI-GIT: Versionierte Informationsbasis (DiCySi_Ideen_Skizze_2025_BSI_git.pdf)

Das BSI veröffentlicht viele Standards, Paper und Empfehlungen unstrukturiert und vereinzelt auf der Homepage. Kaum jemand liest diese, sie sind versteckt und URLs gehen bei jedem Webseitenupdate kaputt. Es fehlt die Möglichkeit, Veröffentlichungen zu abonnieren, Veränderungen leicht zu erkennen und automatisiert weiterzuverarbeiten (RSS, git, etc.).

3. Software-Check: Systeme zur Angriffserkennung (DiCySi_Ideen_Skizze_2025_Bundes_Softwarecheck.pdf)

Kaum eine kleinere öffentliche Stelle implementiert sinnvolle Systeme zur Angriffserkennung oder hat funktionierende Alarmierungs- und Warnfunktionen. Die Vielzahl an Papieren, Ratgebern und Hinweisen des BSI bilden keine entlastende, praktische Hilfe für die tausenden IT-Abteilungen in öffentlichen Stellen.

Konsolidierung zum Cyberdome-Konzept / Finale Ideenskizze

Kerngedanke: Eine "Cyberschale" (Cyberdome), um Entwicklung und Betrieb bei der öffentlichen Hand automatisiert mit niedrigschwelligen Maßnahmen zu schützen. KMUs und ISPs können das optional mitnutzen.

Zentrale Herausforderung: Infos wie IoCs[2] müssen automatisiert und möglichst schnell verarbeitet werden. Bei ca. 11.500 Kommunen und ca. 300 Landkreisen mit Ressourcendefizit. 3,2 Millionen KMUs haben die gleiche Herausforderung.

Die drei Bausteine des Cyberdome

Baustein 1: BSI git - Versionierte Informationsbasis

- Strukturierte Kommunikation durch Git-Repository
- Förderung von Automation (Empfehlungen in CICDs[3] einbetten)
- Fachdiskussionen über Empfehlungen in entsprechenden Change-Prozessen

[1] Command & Control
[2] Indicators of Compromise
[3] Continuous Integration / Continuous Deployment

Baustein 2: Verwaltungs-Traffic (DNS, IP[4]) / "Intelligence to Action“

- DNS-Resolver/Filter für öffentliche Stellen basierend auf BSI-Wissen über C2-Infrastrukturen
- Monitoring & Alerting niederschwellig für kleine Einrichtungen ohne eigenes MISP[5]
- Erweiterung für private Stellen in Dialog mit ISPs[6] & DNS-Services

Baustein 3: SupplyChain / Software-Check

- Prüfung von Verletzung von Best Practices, Standards, Architektur und Security Properties von Software in der Beschaffung
- Prozess / Vergabeklausel / EVB-IT[7]
- Integration in bestehende CICDs (Zendis, SupplyChain)

Zusammenfassung der Konsolidierung

Aspekt	**Ursprüngliche Use Cases**	**Konsolidiertes Cyberdome-Konzept**
Fokus	Drei separate Lösungen	Integriertes Schutzkonzept ("Cyberschale")
Zielgruppe	Öffentliche Hand (Softwarecheck) Wirtschaft, Zivilgesellschaft, öffentliche Hand (BSI-Git) Kleinere öffentliche Stellen	Öffentliche Hand + optional KMUs/ISPs
Kernelemente	NS-Filter[8], Git-Repo, Software-Check	Drei Bausteine unter einem Dach
Philosophie	Einzelmaßnahmen	"Defence in depth" – verbesserter Schutz in Schichten
Kommunikation	Getrennte Kanäle	Git als zentrale Kommunikationsbasis

2. Baustein 1: BSI Git Vorschlag

IT-Sicherheitsvorgaben, Standards und Richtlinien des BSI werden heute überwiegend als statische Dokumente bereitgestellt, die nur eingeschränkt versionierbar, automatisierbar und für Beteiligung geeignet sind. Mit dem vorgeschlagenen BSI Git werden diese Inhalte als zentrale, versionierte und maschinenlesbare Wissensbasis bereitgestellt und transparenter sowie effizienter nutzbar. Gleichzeitig entsteht ein strukturierter Rückkanal für Verwaltung, Wirtschaft und Zivilgesellschaft, um Erfahrungen, Verbesserungsvorschläge und neue Anforderungen einzubringen. Der Ansatz stärkt Automatisierung, Standardisierung und Cyberresilienz und unterstützt eine schnellere und konsistentere Umsetzung von Sicherheits- und Architekturvorgaben.

[4] Domain Name System, Internet Protocol
[5] Malware Information Sharing Platform
[6] Internet Service Provider
[7] Europäische Vergabeverordnung – Informationstechnik
[8] Name Server-Filter

Problemstellung

Die adressierte Problemstellung besteht darin, dass vom BSI IT-Sicherheitsvorgaben, Architekturrichtlinien, technische Standards, Mindeststandards und Empfehlungen heute häufig in Form von PDF-Dokumenten, Webseiten oder einzelnen Veröffentlichungen bereitgestellt werden. Diese Informationen sind zwar verfügbar, lassen sich jedoch nur eingeschränkt automatisiert verarbeiten, versionieren, kommentieren oder in technische Prozesse integrieren.

Für Anwender:innen in Behörden, Kommunen und Unternehmen ist oft nicht eindeutig erkennbar, welche Version eines Dokuments aktuell gültig ist, welche Änderungen vorgenommen wurden und welche fachlichen Überlegungen zu einer Anpassung geführt haben. Gleichzeitig existieren nur begrenzte Möglichkeiten, Rückmeldungen strukturiert einzubringen oder Unklarheiten direkt mit den BSI Herausgebern zu klären. Dadurch entstehen Interpretationsspielräume, Medienbrüche und ein höherer, oft manueller Aufwand bei der Umsetzung von Sicherheitsanforderungen.

Die Folge ist, dass Sicherheitsvorgaben und Architekturrichtlinien häufig zeitverzögert, uneinheitlich oder unvollständig umgesetzt werden. Zudem gehen wertvolle Erfahrungen aus der praktischen Anwendung nur eingeschränkt in die Weiterentwicklung der Vorgaben ein.

Die *Gitification* adressiert dieses Problem, indem in einem BSI Git Standards und Richtlinien wie Quellcode von Software behandelt werden: versioniert, transparent, maschinenlesbar, nachvollziehbar und mit einem strukturierten Beteiligungsprozess versehen. Dadurch werden Anforderungen einfacher konsumierbar, automatisierbar und kontinuierlich weiterentwickelbar.

Beispiel

Eine Kommune betreibt ein Fachverfahren und orientiert sich dabei an einer Technischen Richtlinie des BSI zur Absicherung von Webanwendungen. Die Richtlinie liegt als PDF vor und wird lokal abgelegt. Einige Monate später veröffentlicht das BSI eine aktualisierte Version mit verschärften Anforderungen an die TLS-Konfiguration[9].

In der heutigen Situation erfährt die Kommune möglicherweise erst spät von der Änderung. Zudem muss sie die neue Version manuell mit der bisherigen vergleichen, um die relevanten Anpassungen zu identifizieren. Warum eine Änderung vorgenommen wurde und welche Auswirkungen sie hat, ist häufig nur mit zusätzlichem Rechercheaufwand nachvollziehbar.

Im *Gitification*-Ansatz wäre die Richtlinie in einem Repository veröffentlicht. Die Kommune könnte die Richtlinie abonnieren und würde automatisch über Änderungen informiert. Die konkreten Unterschiede zwischen den Versionen wären unmittelbar sichtbar. Die Diskussion und Begründung der Änderung wären dokumentiert und nachvollziehbar. Darüber hinaus könnten Werkzeuge die neue Vorgabe automatisiert auswerten und darauf prüfen, ob die bestehende Infrastruktur und ihre Konfiguration weiterhin den aktuellen Anforderungen entspricht.

Dadurch werden Transparenz, Nachvollziehbarkeit, Standardisierung und Automatisierung verbessert und die Wahrscheinlichkeit erhöht, dass neue Sicherheitsanforderungen zeitnah und korrekt umgesetzt werden. Dies stärkt letztlich die Cyberresilienz der öffentlichen Verwaltung und ihrer Dienstleister.

Ansatz

Im Rahmen der *Gitification* stellt das BSI ein Git-Repository als zentrale Plattform für die Veröffentlichung, Pflege und Weiterentwicklung von (Mindest-)Standards, Richtlinien und

[9] Transport Layer Security-Konfiguration

Empfehlungen. Statt statischer PDF Dokumente werden Inhalte strukturiert, maschinenlesbar und langfristig versioniert in einem Repository bereitgestellt.

Das Repository fungiert als digitaler Aktenschrank mit API[10] und bildet die zentrale Referenzquelle für Staat, Wirtschaft und Zivilgesellschaft mit den folgenden Kernprinzipien:

- Single Source of Truth für geltende (Mindest-)Standards, Richtlinien und Empfehlungen
- Digitaler Aktenschrank mit API für automatisierte Nutzung und Integration
- Strukturierter Rückkanal für Feedback, Fehlerkorrekturen und Weiterentwicklungen
- Transparenz und Nachvollziehbarkeit durch öffentliche Historie, Diskussionen und Entscheidungsprozesse

Durch die Nutzung etablierter Git-Workflows werden Änderungen nachvollziehbar, Beteiligung erleichtert und die Weiterverarbeitung der Inhalte durch Dritte ermöglicht.

Vorteile für IT-Sicherheitsvorgaben und Architekturrichtlinien

Die *Gitification* von Standards und Richtlinien schafft die Grundlage für eine stärkere Automatisierung von IT-Sicherheits- und Architekturvorgaben. Anforderungen können direkt in CI/CD-, DevSecOps[11]- und Compliance-Prozesse integriert und automatisiert überprüft werden.

Durch die vollständige Versionshistorie entsteht hohe Nachvollziehbarkeit. Änderungen, Entscheidungen und gültige Anforderungen sind jederzeit transparent dokumentiert und auditierbar.

Die zentrale Bereitstellung fördert die Standardisierung von BSI Sicherheitsvorgaben, Architekturrichtlinien, Referenzkonfigurationen und Mindeststandards. Dies reduziert Interpretationsspielräume und verbessert die Interoperabilität zwischen Behörden, Projekten und Dienstleistern.

Ein strukturierter Feedbackprozess ermöglicht die aktive Beteiligung von Verwaltung, Wirtschaft und Zivilgesellschaft. Erfahrungen aus der Praxis können frühzeitig in die Weiterentwicklung von Standards einfließen und deren Qualität sowie Akzeptanz erhöhen.

Insgesamt stärkt der Ansatz die Cyberresilienz, da Sicherheitsanforderungen des BSI schneller verbreitet, konsistent umgesetzt und technisch überprüft werden können. Richtlinien werden dadurch von statischen Dokumenten zu einem aktiven Bestandteil moderner IT- und Sicherheitsprozesse.

Umfang

Ein BSI Git kann als Brücke zwischen dem BSI und den operativen IT-Bereichen in Bund, Ländern und Kommunen dienen. Ein strukturierter Rückkanal ermöglicht die Meldung von Fehlern, Unklarheiten und Verbesserungsvorschlägen sowie die Einbringung neuer Anforderungen und Standards. Dadurch entsteht ein kontinuierlicher fachlicher Austausch mit den Menschen, die diese Vorgaben anwenden.

Technische Diskussionen, Änderungsentscheidungen und Normungsaktivitäten werden transparent dokumentiert. Die Beteiligung relevanter Interessengruppen wird erleichtert und nachvollziehbar gestaltet.

Mögliche Anwendungsbereiche können umfassen:

- Förderung von Automatisierung und Maschinenlesbarkeit
- Strukturierte Bereitstellung von Standards und Richtlinien

[10] Application Programming Interface
[11] Development, Security and Operations

- Historie und Änderungsverfolgung mittels standardisierter Änderungsdeltas (Diffs)
- Abonnierbare Informationskanäle und globale Feeds
- Integration in CI/CD- und DevSecOps-Prozesse
- Unterstützung von Compliance- und Audit-Anforderungen
- Bereitstellung sicherer Referenzkonfigurationen für die öffentliche Verwaltung

Dabei ist ein mögliches Zukunftsszenario die direkte Kopplung von Standards an Entwicklungs- und Betriebsprozesse. Änderungen an Vorgaben könnten automatisiert Builds, Tests oder Compliance-Prüfungen in öffentlichen Softwareprojekten auslösen. Dienstleister wären verpflichtet, notwendige Anpassungen innerhalb definierter Fristen umzusetzen.

Inhaltliche Umsetzungsvorschläge

Ziel ist die Einführung eines strukturierten „Aktenplans“ für Standards, Richtlinien und Empfehlungen des BSI, der wesentliche Anforderungen erfüllt:

- Klare Trennung zwischen gültigen und historischen Versionen
- Schnelle Identifikation aktueller Dokumente
- Einheitliche Dokumentationsstandards
- Verpflichtende Kurzfassung („TL;DR“)[12] zu Beginn jedes Dokuments

Eine beispielhafte Struktur ist

/grundschutz++	IT-Grundschutz-Kataloge und Bausteine
/sbom	SBOM- und Software-Lieferkettenvorgaben
/tr	Technische Richtlinien
/lagebilder	IT-Sicherheitslagebilder
/secops	Sicherheitsvorgaben für IT-Projekte
/mindeststandards	Mindeststandards des BSI nach § 44 Abs. 1 Satz 1 BSIG

Format und Standards

Für die Dokumentation sollten offene und versionierbare Formate genutzt werden, beispielsweise:

- Markdown
- AsciiDoc

Dabei sind einheitliche Vorgaben für Tabellen, Grafiken, Metadaten und Verlinkungen zu definieren.

Versionierung und Branching

Empfohlen wird ein praxistaugliches, standardisiertes Versionsmodell:

- main für veröffentlichte und gültige Inhalte
- draft für Entwürfe und laufende Bearbeitung
- nachvollziehbare Freigabeprozesse
- optionale Nutzung von *Semantic Versioning* als Major.Minor.Patch.Build[13]

[12] Steht für „Too long, didn‘t read“ – Zu lange, hab‘s nicht gelesen
[13] Major.Minor.Patch.Build stellt eine Namenskonvention für die Versionierung ein Versionsformat dar: Hauptversionen (Major), Unterrevisionen (Minor), Korrekturen (Patch) und Builds (fertiges Anwendungsprogramm).

Technischer Repository-Aufbau und Struktur

Als primäre Plattform für das Repository bietet sich eine bestehende GitLab-Infrastruktur bereitgestellt beim BSI z.B. unter gitlab.bsi.bund.de in Verbindung mit OpenCode an. Damit können die Inhalte innerhalb der bestehenden Infrastruktur gepflegt, versioniert und veröffentlicht werden. Für eine möglichst breite Zugänglichkeit und zusätzliche Ausfallsicherheit kann das Repository ergänzend auf externen Plattformen wie GitHub oder GitLab.com gespiegelt werden. Dabei bleibt die BSI-Infrastruktur die maßgebliche Quelle, während die externen Repositories als öffentlich zugängliche Mirrors dienen.

Für die Repository-Struktur sind verschiedene Optionen zu untersuchen und zu bewerten. Dabei ist insbesondere zu prüfen, ob ein zentrales Monorepo oder mehrere themenspezifische Repositories für die unterschiedlichen Inhalte und Anwendungsbereiche geeigneter sind. Unabhängig von der gewählten Struktur sollten einheitliche Namenskonventionen und Verzeichnisstandards definiert werden, um eine einfache Auffindbarkeit und konsistente Nutzung zu gewährleisten. Zudem ist zu bewerten, welche Variante langfristig eine gute Skalierbarkeit bei wachsendem Umfang und steigender Zahl an Nutzern und Inhalten ermöglicht.

Nutzergruppen und Use Cases

Das System des BSI Git kann unterschiedliche Zielgruppen unterstützen:

- BSI: Pflege und Veröffentlichung von Standards
- DevOps-Teams: Integration in Entwicklungs- und Betriebsprozesse
- Compliance- und Audit-Teams: Nachvollziehbare Dokumentation und Prüfpfade
- Softwarehersteller: Umsetzung regulatorischer Anforderungen
- Wissenschaft und Zivilgesellschaft: Transparente Beteiligung und Kommentierung

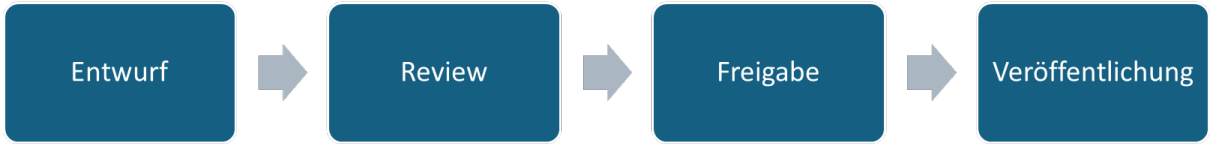
Ferner ist der Ansatz darüber hinaus geeignet für:

- branchenspezifische Sicherheitsstandards (B3S)
- Protection Profiles und CC[14] Informationen
- Normen und Richtlinien
- Sicherheitsanforderungen für Software-Lieferketten

Auch externe Standards, beispielsweise die erwähnten B3S, könnten nach fachlicher Freigabe durch das BSI zentral bereitgestellt werden.

Workflows und Benachrichtigungen

Ein standardisierter Workflow könnte folgende Schritte umfassen



und ergänzend können Automatisierungsmechanismen integriert werden mittels

- API-Zugriffe
- Webhooks

[14] Common Criteria

- automatische Prüfungen
- Build- und Testprozesse
- Benachrichtigungen bei Änderungen

die sowohl konventionelle Nachrichtenverbreitung als auch CI/CD- und DevSecOps-Prozesse unterstützen.

Nutzer können Änderungen über verschiedene Kanäle verfolgen:

- RSS-Feeds
- E-Mail-Benachrichtigungen
- Watch-Funktionen
- Alerts für relevante Dokumente oder Themenbereiche

Rückkanal und Community-Feedback

Ein wesentlicher Bestandteil des Ansatzes ist die Möglichkeit für Anwender:innen, Fachverbände, Unternehmen, Wissenschaft und Zivilgesellschaft, sich aktiv an der Weiterentwicklung von Standards und Richtlinien zu beteiligen. Hierzu werden etablierte Git-Mechanismen genutzt, die einen transparenten, nachvollziehbaren und niedrigschwelligen Austausch zwischen Herausgebern und Anwendern:innen ermöglichen.

Wesentliche Voraussetzung dafür ist allerdings, dass Anwender:innen Git bedienen können.

Mögliche Beteiligungsformen sind:

- *Issues* zur Meldung von Fehlern, Unklarheiten und Verbesserungsvorschlägen
- *Pull Requests* für konkrete Änderungs- oder Ergänzungsvorschläge
- *Feature Requests* zur Einbringung neuer Anforderungen, Themen oder Standards
- *Discussions* für den allgemeinen fachlichen Austausch und die Diskussion von Lösungsansätzen

Alle Beiträge, Diskussionen und Entscheidungen werden nachvollziehbar dokumentiert und schaffen so einen transparenten Beteiligungsprozess. Gleichzeitig sollte geprüft werden, in welchem Umfang eine anonyme oder pseudonyme Beteiligung ermöglicht werden kann.

Dies kann insbesondere für Einzelpersonen, Sicherheitsforschende oder andere externe Stakeholder relevant sein, die sich fachlich einbringen möchten, ohne öffentlich mit ihrem Namen oder ihrer Organisation in Erscheinung zu treten. Dadurch kann die Beteiligungshürde weiter gesenkt und die Vielfalt der eingebrachten Perspektiven erhöht werden.

Offene Fragen und mögliche nächste Schritte

Vor einer Umsetzung sind sowohl organisatorische und technische Fragestellungen, als auch konkrete Anforderungen der beteiligten Stakeholder zu klären. Gleichzeitig bietet sich die Möglichkeit, den Ansatz schrittweise zu validieren und weiterzuentwickeln.

Offene Fragen

- Wer übernimmt Moderation und Bearbeitung eingehender Beiträge?
- Welche Reaktionszeiten und Zuständigkeiten gelten?
- Wie erfolgt Priorisierung und Entscheidungsfindung?
- Welche Qualitäts- und Freigabeprozesse sind erforderlich?
- Welche Themen gehören in den öffentlichen Feedbackprozess, welche Art Rückmeldungen auf die vom BSI bereitgestellten Informationen können Qualität verbessern, und welche nicht?
- Wie werden Datenschutz- und Löschanforderungen umgesetzt?
- Wie kann die Beteiligung von Interessenvertretern transparent gestaltet werden?
- Soll eine anonyme oder pseudonyme Beteiligung möglich sein?

Mögliche nächste Schritte

- Identifikation von Bedarfen durch Gespräche mit Stakeholdern
- Analyse bestehender Git-basierter Beteiligungsverfahren
- Abstimmung mit bestehenden BSI-Initiativen wie z. B. CyberGovSecure
- Erhebung von Anforderungen aus Bund, Ländern und Kommunen
- Bewertung technischer und organisatorischer Umsetzungsoptionen
- Entwicklung eines Pilotprojekts auf OpenCode

Die Ergebnisse dieser Schritte können dann als Grundlage für die Einordnung und Priorisierung einer möglichen weiterführenden Umsetzung dienen.

Bewertung

Die *Gitification* von Standards und Richtlinien eröffnet einen modernen, transparenten und kollaborativen Kommunikationskanal zwischen dem BSI und den Menschen, die diese Vorgaben anwenden.

Der Ansatz erhöht die Nachvollziehbarkeit von Entscheidungen, verbessert die Qualität von Richtlinien[15] durch frühzeitiges Feedback und erleichtert die technische Integration von Anforderungen in Entwicklungs- und Betriebsprozesse. Gleichzeitig stärkt er die Wiederverwendbarkeit, Automatisierung und Verständlichkeit von Sicherheitsvorgaben.

Die Umsetzung wird zusätzliche organisatorische und personelle Ressourcen erfordern. Dem gegenüber stehen jedoch langfristige Vorteile durch höhere Transparenz, bessere Beteiligungsmöglichkeiten und eine nachhaltige Stärkung der Cyberresilienz im öffentlichen Sektor.

3. Baustein 2: „Intelligence to Action“ (DNS Angebot des BSI)

Mit „Intelligence to Action“ schlägt der Workstream einen niedrigschwelligen, DNS-basierten Schutzmechanismus für öffentliche Stellen vor. Ziel ist es, vorhandenes Wissen des BSI über bekannte Command-and-Control-Infrastrukturen unmittelbar für den Schutz von IT-Systemen nutzbar zu machen. Ein hierfür bereitgestellter DNS-Resolver könnte Zugriffe auf bekannte schädliche Domains blockieren oder umleiten und betroffene Einrichtungen automatisiert alarmieren. Der Vorschlag richtet sich insbesondere an Einrichtungen, die nicht über eigene Threat-Intelligence-Plattformen oder umfangreiche Cybersecurity-Ressourcen verfügen.

Der nachfolgend beschriebene Ansatz ist ein Konzeptvorschlag des Workstreams. Er beschreibt kein bereits vorhandenes oder durch das BSI verbindlich zugesagtes Angebot.

Problemstellung

Threat-Intelligence-Informationen zu aktuellen Cyberangriffen sind häufig bereits in Fachkreisen vorhanden, erreichen jedoch nicht immer rechtzeitig die zuständigen Stellen in der öffentlichen Verwaltung, in Unternehmen oder in der Zivilgesellschaft. In der Folge werden bekannte C2-Domains und andere schädliche Infrastrukturen nicht oder erst verspätet blockiert. Organisationen können dadurch Opfer von Angriffen werden, obwohl verwertbare Informationen über die verwendete Angriffsinfrastruktur bereits vorliegen.

Besonders kleinere öffentliche Einrichtungen verfügen häufig weder über eine eigene MISP-Infrastruktur noch über ausreichende personelle Ressourcen, um verschiedene Threat-Intelligence-Quellen kontinuierlich auszuwerten und daraus technische Schutzmaßnahmen

[15] z.B. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/Liste-TR-nach-Aenderungsdatum/traenderungen_node.html

abzuleiten. Die Herausforderung besteht deshalb weniger in der grundsätzlichen Verfügbarkeit von Informationen als in deren zeitnaher, automatisierter und skalierbarer Umsetzung.

DNS bietet hierfür einen geeigneten Ansatzpunkt. Der überwiegende Teil der Kommunikation mit internetbasierten Diensten setzt eine Namensauflösung voraus. Werden bekannte schädliche Domains bereits bei der DNS-Auflösung erkannt, können Verbindungen zu diesen Systemen verhindert oder für weitere Analysen durch BSI-Fachkräfte kontrolliert umgeleitet werden.

Ansatz

Der Workstream schlägt vor, dass das BSI einen besonders geschützten DNS-Resolver für die öffentliche Verwaltung bereitstellt oder den Aufbau eines solchen Angebots gemeinsam mit geeigneten staatlichen oder privaten Partnern orchestriert. Der Resolver soll aktuelle, fachlich kuratierte Informationen über bekannte schädliche Domains und C2-Infrastrukturen verarbeiten und diese Informationen automatisiert in konkrete Schutzmaßnahmen überführen.

Die Nutzung soll zunächst freiwillig und niedrigschwellig möglich sein. Öffentliche Einrichtungen könnten den Resolver als DNS-Dienst einbinden und eine zuständige Kontaktstelle für sicherheitsrelevante Meldungen hinterlegen. Wird aus dem Netz einer teilnehmenden Einrichtung eine bekannte schädliche Domain angefragt, könnte der Zugriff blockiert oder an ein geeignetes Sinkhole vom BSI umgeleitet werden. Gleichzeitig könnte die registrierte Kontaktstelle über das Ereignis informiert werden.

Das Konzept verbindet damit drei Funktionen:

- Nutzung eines kuratierten Threat-Intelligence-Feeds für bekannte schädliche Domains und gegebenenfalls IP-Adressen
- DNS-basierte Blockierung oder kontrollierte Umleitung von Zugriffen
- Niedrigschwelliges Monitoring und Alerting für die teilnehmenden Einrichtungen

Ob der Dienst zentral durch das BSI, gemeinsam mit dem ITZBund, durch eine andere öffentliche Stelle oder in einer verteilten Struktur betrieben wird, wurde durch den Workstream nicht abschließend festgelegt. Entscheidend ist aus Sicht des Workstreams, dass das Wissen und die fachliche Autorität des BSI in die Auswahl und Pflege der verwendeten Informationen einfließen.

Beispiel

Eine öffentliche Einrichtung nutzt den vorgeschlagenen DNS-Resolver. Ein kompromittierter Arbeitsplatz versucht, eine bereits bekannte C2-Domain aufzulösen. Der Resolver erkennt die Domain anhand des kuratierten Threat-Intelligence-Feeds und verhindert die reguläre Namensauflösung. Alternativ kann die Anfrage an ein Sinkhole des BSI weitergeleitet werden.

Die Verbindung zur bekannten Angriffsinfrastruktur wird dadurch unterbrochen. Zusätzlich erhält die für die Einrichtung registrierte Kontaktstelle eine Meldung, sodass der betroffene Arbeitsplatz untersucht und weitere Maßnahmen eingeleitet werden können. Die Einrichtung profitiert damit von aktuellen Threat-Intelligence-Informationen, ohne selbst eine entsprechende Plattform betreiben und kontinuierlich pflegen zu müssen.

Vorteile des Ansatzes

Der wesentliche Vorteil liegt in der unmittelbaren Überführung vorhandener Erkenntnisse in eine technische Schutzwirkung. Informationen über bekannte Angriffsstrukturen werden nicht ausschließlich veröffentlicht oder an einzelne Fachstellen weitergegeben, sondern automatisiert für präventive Maßnahmen genutzt.

Für öffentliche Einrichtungen ergeben sich insbesondere folgende Vorteile:

- Niedrigschwellige Nutzung von BSI-Wissen über bekannte C2-Infrastrukturen

- Schutz ohne Aufbau einer eigenen Threat-Intelligence-Infrastruktur
- Zentrale und kontinuierliche Pflege relevanter Informationen
- Automatisierte Blockierung bekannter schädlicher Domains
- Frühzeitige Alarmierung bei verdächtigen DNS-Anfragen
- Unterstützung kleiner Einrichtungen mit begrenzten personellen und technischen Ressourcen
- Skalierbare Bereitstellung für eine größere Zahl öffentlicher Stellen

Durch die Verbindung von Filterung und Alarmierung entsteht nicht nur eine präventive Schutzmaßnahme. Verdächtige Aktivitäten können gleichzeitig als Anlass für eine Untersuchung innerhalb der betroffenen Einrichtung dienen.

Umfang

Als Minimum Viable Product (MVP) schlagen wir vor:

1. Ein MVP für öffentliche Nutzung (KMUs, ISPs etc.) als kuratierter Feed bekannter schädlicher Domains, der eine grundlegende Blockierungsfunktion bereitstellt und über eine sichere Quelle sämtlichen Interessenten zur Verfügung gestellt wird. Dieses sollte im Format DNS-Blocklist für Pihole[16] und ähnliche Lösungen passieren.

   Dieser Ansatz stellt eine Vorstufe zum DNS-Resolver-Ansatz dar und zeichnet sich durch höhere Nachvollziehbarkeit, höhere Redundanz und geringere Angreifbarkeit durch mögliche staatliche Zensur aus.

   Nachteil ist, dass Informationen höherer Vertraulichkeitsstufen nicht in den Feed einbezogen werden dürfen.

2. Ein MVP zur Nutzung als DNS-Resolver für Behörden (Bund, Länder, Kommunen), der einen kuratierten Feed bekannter schädlicher Domains nutzt und eine grundlegende Blockierungs- und Alarmierungsfunktion bereitstellt. Erweiterte Analysefunktionen sollen den Einstieg nicht unnötig erschweren. Der Kern des Vorschlags bleibt ein einfach nutzbarer DNS-Dienst, der vom Wissen des BSI profitiert.

In weiteren Ausbaustufen könnten zusätzliche Funktionen geprüft werden:

- Bereitstellung der kuratierten Informationen in unterschiedlichen technischen Formaten
- Einbindung weiterer qualifizierter Threat-Intelligence-Quellen
- Ergänzung um IP-basierte Filtermechanismen
- Unterstützung dezentral oder lokal betriebener DNS-Filter
- Dokumentierte Verfahren zur Aufnahme, Korrektur und Entfernung von Einträgen
- Nutzung von Sinkhole-Funktionen für passives Monitoring
- Kooperation mit Internet Service Providern für freiwillige Schutzangebote
- Prüfung möglicher Kooperationen mit europäischen Partnern und bestehenden Angeboten wie DNS4EU

Eine Erweiterung auf Unternehmen und weitere gesellschaftliche Akteure kann perspektivisch im Dialog mit Internet Service Providern und DNS-Dienstleistern betrachtet werden. Der primäre Fokus des vorgeschlagenen MVP liegt jedoch auf öffentlichen Stellen.

Datenschutz, Transparenz und Resilienz

DNS-Daten können abhängig von der technischen und organisatorischen Ausgestaltung einen Personenbezug aufweisen. Dies kann beispielsweise der Fall sein, wenn Anfragen statischen internen IP-Adressen oder einzelnen Nutzer:innen zugeordnet werden können. Vor einer

16 Pihole ist ein quelloffener DNS-Server für das listenbasierte Blocken unerwünschter Verbindungen

Umsetzung müssen deshalb die datenschutzrechtliche Zulässigkeit, die erforderliche Datenminimierung, Speicherfristen, Zugriffsberechtigungen und die zulässigen Verwendungszwecke geklärt werden.

Die für den Betrieb erhobenen Daten sollten ausschließlich für den definierten Schutzzweck verwendet werden. Eine darüber hinausgehende Zweitverwendung wurde im Workstream als sehr kritisch bewertet. Ebenso sind eine nachvollziehbare Trennung von Sicherheitsaufgaben und anderen staatlichen Aufgaben sowie transparente und öffentlich einsehbare Regeln für Auswertung und Weitergabe erforderlich.

Für die Akzeptanz eines solchen Angebots ist zudem ein nachvollziehbarer Umgang mit fehlerhaften oder veralteten Einträgen erforderlich. Es sollte klar geregelt sein, wie Domains in die Filterung aufgenommen, überprüft, korrigiert und wieder entfernt werden. Die Herkunft und Qualität der verwendeten Informationen müssen bewertet werden, soweit dies unter Berücksichtigung bestehender Vertraulichkeitsanforderungen möglich ist.

Da der vorgeschlagene DNS-Dienst zu einer sicherheitsrelevanten Infrastruktur werden kann, sind mögliche Missbrauchs- und Abhängigkeitsrisiken ebenfalls zu berücksichtigen. Dazu gehören insbesondere die Verfügbarkeit des Dienstes, die Vermeidung einer unkontrollierten Zentralisierung, der Schutz vor Manipulation sowie geeignete Fallbackmöglichkeiten bei technischen Störungen. Die konkrete Lösung dieser Betriebsfragen war nicht Gegenstand des Workstreams, wurde jedoch als notwendiger Bestandteil einer möglichen Umsetzung identifiziert.

Mögliche Umsetzung

Für die weitere Bewertung des Konzeptvorschlags sollten insbesondere folgende Punkte durch das BSI und mögliche Umsetzungspartner geprüft werden:

- Rechtliche und datenschutzrechtliche Rahmenbedingungen für die freiwillige Nutzung durch öffentliche Stellen
- Geeignetes Betriebsmodell und mögliche Rollen von BSI, ITZBund und weiteren Partnern
- Anforderungen an Verfügbarkeit, Skalierbarkeit und technische Resilienz
- Auswahl, Bewertung und Aktualisierung geeigneter Threat-Intelligence-Quellen
- Prozesse zur Aufnahme, Freigabe, Korrektur und Entfernung von Filtereinträgen
- Verfahren zur Registrierung und Alarmierung teilnehmender Einrichtungen
- Umgang mit vertraulichen Informationen und unterschiedlichen TLP[17]-Einstufungen
- Transparenzanforderungen und Schutz vor einer zweckfremden Verwendung der anfallenden Daten
- Anschlussfähigkeit an bestehende nationale und europäische DNS-Sicherheitsangebote

Auf dieser Grundlage könnte ein begrenztes MVP für freiwillig teilnehmende öffentliche Einrichtungen bewertet werden. Die dabei gewonnenen Erfahrungen könnten anschließend für die Entscheidung über eine mögliche Weiterentwicklung und Ausweitung des Ansatzes genutzt werden.

Bewertung

Der vorgeschlagene DNS-Resolver bietet einen konkreten und vergleichsweise niedrigschwelligen Ansatz, um vorhandenes Wissen über bekannte Angriffsinfrastrukturen in unmittelbar wirksame Schutzmaßnahmen zu überführen. Besonders kleinere öffentliche

[17] Traffic Light Protocol, Standard zur Klassifizierung der Vertraulichkeit von Sicherheitsinformationen

Einrichtungen könnten davon profitieren, da sie keine eigene Threat-Intelligence-Infrastruktur aufbauen und betreiben müssten.

Eine fachliche Einbindung des BSI kann zur Qualität und Vertrauenswürdigkeit der verwendeten Informationen beitragen. Gleichzeitig erfordert ein solches Angebot dauerhaft verfügbare Betriebsstrukturen, verlässliche Prozesse zur Pflege der Filterinformationen und eine eindeutige rechtliche sowie datenschutzrechtliche Ausgestaltung.

Der Workstream empfiehlt deshalb, den Ansatz als möglichen Baustein eines Cyberdome weiter zu prüfen. Der Vorschlag stellt weder eine Festlegung auf ein bestimmtes Betriebsmodell noch eine Aussage über eine bereits beschlossene oder zugesagte Umsetzung durch das BSI dar.

4. Baustein 3: Software Checks:

Mit standardisierten Software Checks können Sicherheits-, Qualitäts- und Compliance-Anforderungen bereits vor der Inbetriebnahme von IT-Systemen effizient überprüft werden. Mit diesem Thema unterstützt der Workstream insbesondere Verwaltungen mit begrenzten Ressourcen und schafft einheitliche, nachvollziehbare Prüfmaßstäbe für Beschaffung und Abnahme. Gleichzeitig stärkt der Ansatz die Umsetzung von Sicherheitsvorgaben und fördert die nachhaltige Verbesserung der Cyberresilienz im öffentlichen Sektor.

Problemstellung

Mit diesem Vorschlag richtet sich der Workstream insbesondere an kleinere Kommunen, Bundesbehörden und andere öffentliche Stellen, die Software beschaffen, einführen und betreiben.

In der Praxis stehen bei Beschaffungsvorhaben häufig fachlich und organisatorisch ausgebildete Mitarbeitende den erfahrenen Softwareanbietern gegenüber. Insbesondere bei der Abnahme und Inbetriebnahme von Software fehlen oft die Ressourcen, das technische Know-how oder die geeigneten Werkzeuge, um die Qualität und Sicherheit der gelieferten Systeme angemessen zu bewerten.

Gerade im föderalen Umfeld existieren zahlreiche kleine und große Verwaltungseinheiten, die eigenständig Software beschaffen und IT-Systeme betreiben. Bei der Abnahme dieser Systeme müssen jedoch vielfältige Anforderungen an Qualität, IT-Sicherheit und Compliance geprüft werden. Für kleinere Stellen ist dies häufig nur eingeschränkt leistbar.

Hinzu kommt, dass übergreifende Sicherheitsstandards und Architekturrichtlinien in Ausschreibungen oftmals nicht verbindlich festgelegt oder später nicht konsequent überprüft werden. Gleichzeitig fehlt bislang ein organisatorischer Rahmen, um die Expertise des BSI systematisch, standardisiert und für viele Stellen nutzbar einzubinden.

Hier setzt die Idee der „Software-Checks“ an. Ziel ist es, Verwaltungen bei der Prüfung und Abnahme von Software zu unterstützen und sicherzustellen, dass wesentliche Sicherheitsanforderungen vor der Inbetriebnahme zuverlässig überprüft werden können.

Ansatz

Bundesverwaltungen wird ein standardisierter Software-Check als SaaS- bzw. Security-Angebot in Anlehnung an § 19 BSIG (Bereitstellung von IT-Sicherheitsprodukten) bereitgestellt. In Ausschreibungen können Auftraggeber auf den BSI-Software-Check verweisen. Softwareanbieter weisen im Rahmen der Lieferung die Einhaltung definierter Mindestanforderungen nach. „Das BSI stellt Einrichtungen der Bundesverwaltung einen standardisierten Software-Check als IT-Sicherheitsprodukt bereit (§ 3 Abs. 1 S. 2 Nr. 15 i. V. m. § 19 BSIG). Länder und kommunale Einrichtungen (per Anfrage über die Länder) können das Angebot auf Ersuchen nach § 3 Abs. 2 BSIG nutzen.“ ODER: „Das BSI sollte einen

standardisierten Software-Check als SaaS-Angebot bereitstellen, der neben der Bundesverwaltung auch Ländern und Kommunen offensteht. Hierfür wäre eine Erweiterung des BSIG erforderlich, da § 19 BSIG bislang nur die Bundesverwaltung erfasst und § 3 Abs. 2 BSIG eine Unterstützung nur auf Ersuchen der Länder vorsieht."

Der Workstream dient als Katalysator für die Etablierung eines bundesweit nutzbaren Basischecks für Software und IT-Systeme. Unter Schirmherrschaft des BSI soll ein moderierter Prozess entstehen, der standardisierte Prüfungen definiert und soweit möglich automatisiert durchführt. Ziel ist die frühzeitige Erkennung von Sicherheitsmängeln, Qualitätsproblemen und Compliance-Verstößen.

Als Proof of Concept kann die Build- und Prüfplattform OpenCode[18] der ZENDIS GmbH genutzt werden. Gemeinsam mit den zuständigen Stellen für EVB-IT-Verträge kann ein Verfahren etabliert werden, bei dem Softwarelieferanten die sichere Implementierung ihrer Lösungen in Testumgebungen nachweisen müssen.

Viele Sicherheitsprobleme sind bereits bei der Auslieferung einer Software vorhanden und können vor der Inbetriebnahme erkannt werden. Beispiele sind Standardzugänge wie „admin/admin", fest hinterlegte Passwörter oder unsichere Konfigurationen. Solche Schwachstellen lassen sich mit geringem Aufwand automatisiert identifizieren.

Kern der Idee ist eine Sammlung standardisierter Softwareprüfungen. Das BSI bringt dabei seine fachliche Expertise ein. Ergänzt wird die Sammlung durch geeignete Prüfwerkzeuge, praxisnahe Anleitungen sowie Ausschreibungstexte, die bereits bei der Vergabe klare Anforderungen an Abnahmetests und Sicherheitsprüfungen definieren. Erweitert werden kann diese Sammlung durch freiwillige Beteiligung von Wirtschaft, Verwaltung und Zivilgesellschaft.

Vorteile für IT-Sicherheitsvorgaben und Architekturrichtlinien

Automatisierte Software-Checks ermöglichen die Überprüfung von Sicherheitsanforderungen und die Einhaltung architektonischer Vorgaben.

Unter anderem können folgende Aspekte validiert werden:

- Umsetzung von IT-Sicherheitsvorgaben
- Konformität mit Architekturstandards
- APIs bzw. Schnittstellen
- CBOMs und SBOMs[19]
- Anforderungen aus Zero-Trust-Architekturen
- Integrations- und Systemtests
- Grundkonfigurationen von IT-Systemen
- Nachweis sicherer Betriebs- und Deploymentprozesse

Dadurch werden Sicherheitsanforderungen frühzeitig überprüfbar und die Qualität der gelieferten Lösungen nachhaltig verbessert.

Umfang

Der Einstieg kann bewusst niedrigschwellig erfolgen. Bereits vorhandene Prüfungen, beispielsweise aus dem Umfeld von DevGuard[20], können als erste Grundlage dienen.

Mögliche Prüfbereiche sind:

- Hard-coded Secrets und Zugangsdaten
- Automatisierter Build-, Installations- und Konfigurationsprozess

[18] https://www.opencode.de
[19] Cryptography Bill of Materials, Software Bill of Materials
[20] https://docs.devguard.org/explanations/core-concepts/what-is-devguard/

- Sichere SSH- und HTTPS-Konfigurationen
- PQC-Checks (Post-Quantum Cryptography)
- Dependency-Checks inklusive CVE-Management
- CBOM- und SBOM-Prüfungen
- Minimale erforderliche Rechte und Netzwerkfreigaben
- Telemetrie- und Datenübertragungsanalysen
- API- und Formatprüfungen
- Validierung von Datenfeldern und Eingabeformaten
- OWASP[21] Top 10
- Automatisierte Backup-, Restore-, Upgrade- und Rollback-Verfahren
- Autoscaling-Tests
- Betrieb in dokumentierten IT-Grundschutz-konformen Umgebungen
- Prüfung von Quellcode, Docker-Images, VMDK-, QCOW2- und VHDX-Images[22] sowie Helm-Charts
- Analyse von Tracking- und Analysediensten

Nicht Bestandteil der ersten Ausbaustufe sind Prüfungen zur Erkennung oder Bewertung KI-generierten Quellcodes. Eine spätere Erweiterung bleibt möglich.

Die Liste ist grundsätzlich offen und kann kontinuierlich erweitert werden.

Umsetzungsvorschlag

Nachfolgend ist ein Umsetzungsvorschlag aufgeführt, ohne dafür an dieser Stelle eine rechtliche Prüfung durchgeführt zu haben, die über die Kompetenzen des Workstreams hinausgehen würde.

- Die ZENDIS GmbH nutzt OpenCode als bestehende Plattform mit integrierten Software-Checks.
- Ergänzung der EVB-IT-Verträge um entsprechende Prüf- und Nachweisklauseln.
- Das BSI unterstützt die Weiterentwicklung der Sicherheitsprüfungen im DevSecOps-Prozess.
- Das BSI bewirbt und begleitet die Einführung des Konzepts.
- IT-Planungsrat und FITKO ergänzen den Ansatz um Architektur- und Standardisierungsvorgaben.
- Die oben aufgeführten Werkzeuge, Software und Prozessvorgaben für die Prüfungen werden idealerweise zentral, z.B. vom BSI, gepflegt und versioniert bereitgestellt, idealerweise soll dieses Produkt neutral erwirkt werden.[23]

Bewertung

Der Ansatz bietet insbesondere kleineren Auftraggebern in Bund, Ländern und Kommunen eine konkrete Unterstützung bei der Abnahme und Bewertung von Software.

Die standardisierten Prüfungen erhöhen die Vergleichbarkeit von Lösungen, verbessern die Einhaltung von Sicherheitsanforderungen und reduzieren typische Fehler bereits vor der Inbetriebnahme. Dadurch steigt das allgemeine Sicherheitsniveau und die Widerstandsfähigkeit gegenüber Cyberangriffen.

Eine Beteiligung und fachliche Begleitung durch das BSI ist für Akzeptanz, Qualitätssicherung und Weiterentwicklung des Ansatzes wesentlich. Gleichzeitig bleibt eine Schulung der Anwender erforderlich, um Prüfergebnisse korrekt einordnen und bewerten zu können.

---

[21] Open Worldwide Application Security Project
[22] Virtuelle Festplatten Formate
[23] ein Beispiel hierfür ist DevGuard

Der Ansatz ist technisch gut skalierbar, lässt sich zentral pflegen und kann über Git-basierte Prozesse sowie bestehende DevSecOps-Plattformen effizient ausgerollt und weiterentwickelt werden.

5. Schnittstelle zu ähnlichen/verwandten Projekten

Die vom Workstream erarbeiteten drei Skizzen wurden dem BSI übergeben mit der Zielstellung, Austausche zu entsprechenden BSI-Fachreferaten und BSI-Projekten zu initiieren, die Berührungspunkte haben. In einem zweiten Schritt sollte geprüft werden, ob weitere externe Stakeholder angesprochen werden, um die Ideen und Inhalte der drei Skizzen auf Umsetzungsmöglichkeiten zu prüfen und ggfls. erste Umsetzungsschritte zu gehen. Dieses Vernetzen mit dem BSI und weiteren Stakeholdern zahlt auf die Idee des Dialogs für Cybersicherheit ein, gemeinsam Themen der Cybersicherheit zu bearbeiten.

Grundschutz ++

Am 22. April 2026 wurde dem Workstream vom BSI eine Einführung in den Grundschutz++ gegeben. Grundschutz++ ist die Neuentwicklung des IT-Grundschutzes durch das BSI. Es markiert den Übergang von der bisherigen PDF-basierten Dokumentation zu einem vollständig digitalen, maschinenlesbaren Regelwerk mit Automatisierungspotenzial technisch umgesetzt durch den OSCAL[24]-Standard. Der Anwenderkatalog Grundschutz ++ ist Teil der „Stand-der-Technik-Bibliothek“, einer Plattform, auf der alle Anforderungen und Maßnahmen zentral bereitgestellt werden, und löst das IT-Grundschutz-Kompendium ab. Die Bibliothek wird über ein öffentliches GitHub-Repository bereitgestellt, sodass laufende Updates und Beteiligung der Community möglich sind.

Das Konzept der eigenständigen technischen Richtlinien soll in dieser Form auslaufen. Perspektivisch ist geplant, entsprechende Vorgaben ebenfalls in das durch den Grundschutz++ etablierte Format (OSCAL) zu überführen. Durch gegenseitige Referenzierung sollen somit die Anforderungen vereinheitlicht, das Regelwerk entschlackt und die Aktualität sichergestellt werden. Da aber der Grundschutz++ sich aktuell in seiner Einführungs-/Pilotierungsphase befindet, sind entsprechende Vorgaben und Prozesse noch in der Entwicklung.

BSI-Cyberdome

In Deutschland läuft aktuell der Aufbau des Cyberdomes, ein von der Bundesregierung geplantes nationales Schutz- und Frühwarnsystem zur Abwehr von Cyberangriffen in Deutschland. Das BSI ist hieran beteiligt. Da Schnittmengen aus den drei Workstream-Skizzen und dem BSI-Cyberdome identifiziert wurden, erfolgte die Initiierung von zwei Austauschtreffen.

Diese Austauschtreffen zwischen Teilnehmenden des Workstream Cyberdome und Projektbeteiligten des BSI-Cyberdome fanden am 1. Juni 2026 und am 13. Juli 2026 statt. An den Gesprächen nahmen sowohl Mitarbeitende des BSI als auch externe, durch das BSI beauftragte Berater teil.

Zum Zeitpunkt der Treffen befanden sich beide Vorhaben in unterschiedlichen Projektphasen. Der Workstream Cyberdome war als einjähriges Projekt angelegt, mit dem Ziel, Impulse aus der Zivilgesellschaft zur Stärkung der Cyberresilienz in Deutschland zu entwickeln. Zum Zeitpunkt der Gespräche war etwa die Hälfte der Projektlaufzeit abgeschlossen. Das BSI-

[24] Open Security Control Assessment Language

Cyberdome hingegen ist als mehrjähriges Vorhaben angelegt und hatte kurz zuvor durch einen Kabinettsbeschluss erstmals finanzielle Mittel über das BMI erhalten.

Die Treffen dienten dazu, Adressaten, Aufgaben und Zielsetzungen der beiden Initiativen besser zu verstehen und voneinander abzugrenzen. Im Mittelpunkt stand der Austausch über die Rolle der Zivilgesellschaft, ihre Erwartungen an das BSI-Cyberdome sowie das grundsätzliche Verständnis des Vorhabens. Als gemeinsamer Tenor wurde festgehalten, dass der BSI-Cyberdome das Potenzial besitzt, einen erkennbaren Mehrwert für die Cyberresilienz in Deutschland zu schaffen, der über allgemeine Schutzmaßnahmen hinausgeht.

Dabei wurde die Erwartung formuliert, dass der Servicegedanke des BSI-Cyberdome im Vordergrund stehen sollte und eine Zweckentfremdung des Vorhabens – insbesondere für Überwachungszwecke – ausgeschlossen bleibt.

Zugleich wurde grundsätzlich klargestellt, dass die Teilnehmenden des Workstreams zwar der Zivilgesellschaft angehören, jedoch nicht für die gesamte Zivilgesellschaft sprechen können.

Konzepte und Ausrichtungen der Projekte

Eine wesentliche Erkenntnis aus den Gesprächen war die unterschiedliche Ausrichtung der beiden Vorhaben zu verstehen. Obwohl beide Projekte einen Beitrag zur Verbesserung der Cyberresilienz leisten möchten, adressieren sie unterschiedliche Phasen entlang derselben Wirkungskette.

Der Workstream Cyberdome verfolgt einen eher konzeptionellen und gestaltenden Ansatz. Er beschäftigt sich mit Fragestellungen vor der technischen Umsetzung und entwickelt Impulse, Anforderungen, Konzepte und Rahmenbedingungen für eine resilientere digitale Gesellschaft. Der Fokus liegt auf der Frage, welche Maßnahmen, Strukturen und Prozesse erforderlich sind, um Cyberresilienz nachhaltig zu stärken.

Der BSI-Cyberdome setzt dagegen stärker auf technische Beobachtung und operative Erkenntnisgewinnung. Er soll Informationen aus Sensorik, Datenquellen und Analysen zusammenführen, Bedrohungen erkennen und daraus konkretere Handlungsempfehlungen oder Unterstützungsleistungen ableiten.

Der Unterschied lässt sich vereinfacht entlang einer gemeinsamen Wirkungskette darstellen:

Innerhalb dieser Kette wirkt der Workstream Cyberdome überwiegend auf den linken Stufen, insbesondere bei Vorhaben, Entwurf, Prüfung und der Vorbereitung von Umsetzungsmaßnahmen.

Der BSI-Cyberdome wirkt hingegen schwerpunktmäßig auf den rechten Stufen der Kette, wo technische Beobachtung, Lagebilder, Threat Intelligence und die Ableitung konkreter Analyse-Ergebnisse für Teilnehmer eines Analyseverbunds im Vordergrund stehen.

Merkmal	**Workstream Cyberdome**	**BSI-Cyberdome**
Kernidee	Informationen aus Vorhaben-/Entwurfsdokumenten operational nutzbar machen.	Technische Sensorik zur Gewinnung und Ableitung von Threat Intelligence.
Ausgangs-punkt	Dokumente, Vorhaben, geplante Infrastruktur/Änderungen.	Netzwerk-/System-/Sicherheitsdaten, Beobachtungen und Events.
Fokus	„Was ist geplant bzw. soll vermieden werden?"	„Was passiert bzw. welche Bedrohung lässt sich daraus ableiten?"
Operations-bezug	DNS, C2-IP-Adressen, Vermeidung unerwünschter C2-Domains.	Erkennung, Bewertung und Ableitung von TI (Threat Intelligence).
Output	Vorgaben, Prüfungen, Warnungen, Ausschluss-/Vermeidungskriterien.	Indicators, Erkenntnisse, Priorisierungen und später Aktionen.
Zeitperspekt-ive	Eher präventiv / vor Umsetzung.	Zunächst detektiv, später reaktiv / adaptiv.
Automatisier-ung	Prüfung gegen bekannte Regeln/Vorgaben.	Erkennung, → Analyse → TI (Threat Intelligence) → Entscheidung → Aktion.
Zielbild	Fehler und Konflikte bereits im Entwurf verhindern.	Bedrohungen erkennen (Lagebild) und auf Erkenntnisse (im Analyseverbund) reagieren.

Tabelle 1 Gegenüberstellung der Cyberdome Konzepte

Werden die beiden Projekte nicht nach ihrer technischen Umsetzung, sondern entlang dieser Wertschöpfungskette betrachtet, zeigt sich, dass sie unterschiedliche Ebenen adressieren und keine konkurrierenden Ansätze darstellen. Vielmehr können sie sich gegenseitig ergänzen: Der Workstream Cyberdome kann Impulse, Anforderungen und Perspektiven für die Ausgestaltung des BSI-Cyberdome beitragen, während die Erkenntnisse des BSI-Cyberdome wiederum Hinweise auf neue Handlungsbedarfe und Weiterentwicklungen für die Arbeit des Workstream Cyberdome geben können.

Die im Workstream Cyberdome behandelten Themen oder Vorschläge wurden zu Beginn des Projektes bestimmt. Seitens des BSI-Cyberdome wurde signalisiert, dass einzelne

Anregungen aus den Gesprächen geprüft werden, beispielsweise die Nutzung von DNS-Informationen für Analyse- und Lagebildzwecke.

In den Gesprächen wurde zudem klargestellt, dass der Austausch mit den Teilnehmenden des DiCy Workstreams nicht als umfassender Dialog mit der Zivilgesellschaft verstanden werden kann und darf. Aus Sicht des Workstream Cyberdome wird dem BSI empfohlen, den Austausch mit zivilgesellschaftlichen Akteuren breiter anzulegen, um Verständnis, Transparenz und Akzeptanz für das BSI-Cyberdome zu fördern. Dies kann dazu beitragen, Zielsetzung und Nutzen des Vorhabens frühzeitig zu vermitteln und Wahrnehmungen, insbesondere hinsichtlich möglicher Überwachungsabsichten, zu vermeiden.

CyberGovSecure

Mit der Umsetzung der NIS2-Directive der EU in deutsches Recht wurde das „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ geschaffen. Darin wurden nach einigen Diskussionen auch die Bundesverwaltung, die IT-Dienstleister der Bundesverwaltung, sowie ausgewählte Dritte (siehe § 29 (1) S.3 BSIG) inkludiert. Die sogenannten Einrichtungen der Bundesverwaltung werden als besonders wichtige Einrichtungen eingestuft, siehe § 29 (2) BSIG und unterliegen damit in wesentlichen Teilen den NIS2-Regelungen. Mit dem Programm CyberGovSecure sollen nun die in der NIS2 geforderten Maßnahmen zur Stärkung der Cybersicherheit in der Bundesverwaltung umgesetzt werden.[25]

Es berücksichtigt dabei die unterschiedlichen Ausgangslagen und Umsetzungsstände der Behörden. Innerhalb des Programms sind priorisierte Maßnahmen vorgesehen, die in definierten Zeiträumen durchgeführt werden sollen. Dabei hat Vorrang, diese zügig und pragmatisch umzusetzen. Zu den Maßnahmen gehören etwa ein zeitgemäßes Schwachstellenmanagement, verbesserte Angriffserkennung oder die Härtung zentraler IT-Systeme. Die Ideen des Workstreams Cyberdome könnten hier als Arbeitspakete weitergeführt werden. So könnten bspw. der DNS-Resolver an geeigneter Stelle bei den IT-Dienstleistern platziert, Softwarechecks als übergeordnete Anforderung ebenfalls bei den IT-Dienstleistern überhaupt etabliert und die Gitification als Grundanforderung zur Umsetzung von Richtlinien, Regeln und Standards gesetzt werden. Insbesondere die Gitifcation würde den ohnehin durch das BSI angestrebten Weg mit BSI IT-Grundschutz++ unterstützen. Nicht nur IT-Richtlinien, sondern auch ISMS Richtlinien, als zentrale Vorgaben für einen IT-Betrieb sollten im Git abgebildet werden, mit allen aus den Richtlinien abgeleiteten Maßnahmen, Arbeitsanweisungen usw.

Dokumente in Form von Word und Excel versauern im Explorer, während der IT-Betrieb seine eigenen Regeln macht. Hier kann eine wirkliche Chance entstehen. Gleichfalls wird die Bundesverwaltung an die Nutzung und die Funktionsweise des Git gewöhnt und es kann eine wirkliche Schnittstelle zwischen Governance und Betrieb entstehen.

Der Workstream Cyberdome wünscht sich (debattieren und abstimmen) eine Weiterführung der Ideen nach dem Ende des eigentlichen Workstreams. Im Rahmen des CyberGovSecure wäre diese Fortführung eine Möglichkeit. Einen Austausch mit dem BSI zum CyberGovSecure erfolgte am 11. August 2026.

Die Ideen des Workstreams müssten dann auch auf VS-NfD[26]-Tauglichkeit ausgerichtet werden, weil das die Mindestanforderung ist und die VSA[27] nicht nur für Teil-Segmente gilt, sondern sowohl für die Netze des Bundes als zentrales Netz der Bundesverwaltung als auch

[25] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Sicherheitsberatung/Bund/CyberGovSecure/CyberGovSecure.html
[26] Verschlusssache - Nur für Dienstgebrauch
[27] Verschlusssachenanweisung

für die angeschlossenen Dienststellen. Da hier zentrale Dienste in der Bundescloud angeboten werden, könnte die zentrale Git-Instanz hier ebenfalls mit einem entsprechenden Berechtigungskonzept bereitgestellt werden. Die Verwaltung der Berechtigungen übernehmen die einzelnen Behörden.

6. Ergebnis

Der Workstream Cyberdome hat seine Idee ausgearbeitet, den IT-Schutzschirm für die öffentliche Verwaltung durch drei Bausteine aufzuspannen.

Erstens soll durch die sogenannte Gitification von Standards und Richtlinien erstmalig eine Verknüpfung von Governance und Betrieb erfolgen. Damit würde eine Grundlage geschaffen für eine stärkere Automatisierung von IT-Sicherheits- und Architekturvorgaben. Anforderungen könnten direkt in CI/CD-, DevSecOps- und Compliance-Prozesse integriert und automatisiert überprüft werden. Der Auditor prüfte dann nicht mehr auf die vorhandene PDF- oder Word-Richtlinie, sondern das entsprechende Repository im Git. Auditoren erhielten zur Vorbereitung weiterhin Informationen, nun aber als entsprechende Auszüge aus den Repositories. Sämtliche Stakeholder im ISMS arbeiteten mit dem Repository, sodass keine anderen Informationssenken mit Duplikaten existierten. Durch die vollständige Versionshistorie entstünde eine hohe Nachvollziehbarkeit. Änderungen, Entscheidungen und gültige Anforderungen wären jederzeit transparent dokumentiert und auditierbar. Die zentrale Bereitstellung förderte die Standardisierung von BSI Sicherheitsvorgaben.

Im Bereich der Detektion von Angriffen soll eine weitere Ressource die Verteidigung unterstützen, welche den zweiten Baustein des IT-Schutzschirms darstellt. Mit dem vom BSI bereitgestellten DNS-Resolver existierte ein kuratierter Feed bekannter schädlicher Domains mit einer grundlegende Blockierungs- und Alarmierungsfunktion. Der DNS-Resolver würde so aufgebaut, dass er sich einfach in eine bestehende Monitoringinfrastruktur einfügen lässt. Die Betreuung durch das BSI stellte sicher, dass die aktuellsten Informationen direkt im DNS-Resolver zur Verfügung stünden. Die Auswertung oder Analyse der Informationen, sowie Interpretationsabhängigkeiten durch Drittanbieter-Software entfielen damit.

Der dritte Baustein betrifft die Beschaffung von Software. Mit einem standardisierten Softwarecheck sollen insbesondere Verwaltungen bei der Beschaffung dahingehend unterstützt werden, dass zu beschaffende Software im Hinblick auf Sicherheits-, Qualitäts- und Compliance-Anforderungen bereits vor der Inbetriebnahme effizient überprüft werden kann. Anbieter von Software könnten/ müssten den Softwarecheck positiv bestehen, als Kriterium für die Vergabe. Dadurch sollte verhindert werden, dass Software eingesetzt wird, die grundlegende Schwächen aufweist. Anbieter würden somit von vorneherein zur Einhaltung grundlegender Qualitätsstandards angehalten.

Das BSI schätzt die drei Skizzen und den wertvollen fachlichen Impuls der Zivilgesellschaft sehr. Der Workstream hat mit seinen drei Skizzen fachliche Impulse aus zivilgesellschaftlicher Perspektive eingebracht. Nach Rückmeldung des BSI werden die Vorschläge positiv aufgenommen und derzeit in mehreren Referaten betrachtet.

Die Skizze „BSI Softwareprüfung“ wurde an den BSI Open Source Circle weitergegeben. Dieser bildet eine Schnittstelle innerhalb des BSI und zu externen Stakeholdern, darunter das Zentrum für Digitale Souveränität (ZenDiS). Als Open-Source-Arbeitsgruppe des BSI befasst sich der Open Source Circle insbesondere mit drei Aufgaben:

- Cybersicherheit im Bereich Open-Source-Software und -Hardware gestalten,
- Vernetzung und Community Building fördern,
- Als Anlaufstelle für Fragen rund um Open Source dienen.

In einer ersten Rückmeldung wurden inhaltliche Überschneidungen zwischen den Überlegungen der Zivilgesellschaft und den bestehenden Aktivitäten des BSI sichtbar. Weitere Schritte sind vorgesehen; über deren Entwicklung sollen die Teilnehmenden des Workstreams informiert werden.

Der Austausch soll auch über das Ende der Workstream-Laufzeit hinaus fortgeführt werden. Damit bleibt die Möglichkeit bestehen, die eingebrachten Impulse weiterzuverfolgen und an geeignete laufende Aktivitäten des BSI anzuknüpfen.

Mit der Skizze BSI-GIT hat der Workstream einen Vorschlag eingebracht, um BSI-Anforderungen und technische Maßnahmen strukturierter, transparenter und besser maschinell nutzbar zu machen. In der Rückmeldung aus dem Team Grundschutz++ / Stand der Technik (SdT) wurde deutlich, dass es hierzu bereits Arbeiten gibt, die bestehende Anforderungen durch konkrete und möglichst technisch überprüfbare Maßnahmen ergänzen. Beispiele dafür sind Lieferkettensicherheit, Netzarchitektur, Passwortrichtlinien und Keycloak. Auch an einer Visualisierung von Themen und Trends sowie an weiteren Maßnahmen wird gearbeitet.

Darüber hinaus verfolgt das BSI die Perspektive, den SdT als kontinuierlichen Kreislauf weiterzuentwickeln: Erkenntnisse über Schwachstellen sollen zur systematischen Ableitung von Risiken genutzt werden, aus denen sich wiederum Anforderungen und konkrete Maßnahmen ergeben. Neue Erkenntnisse sollen damit nicht nur dokumentiert werden, sondern auch in die Überprüfung und Weiterentwicklung bestehender Anforderungen einfließen.

Für die technische Umsetzung baut das BSI unter anderem auf GitLab, Datenbanken, Skripte, CI/CD-Pipelines und Codex. Damit sollen Anforderungen, Risiken und Maßnahmen strukturiert, nachvollziehbar, versionierbar und maschinenlesbar abgebildet sowie perspektivisch automatisiert verarbeitet werden können.

Die Rückmeldung zeigt damit Anknüpfungspunkte zwischen dem Vorschlag des Workstreams und den laufenden Arbeiten des BSI. Insbesondere die strukturierte, versionierte Bereitstellung von Anforderungen und die Rückführung neuer Erkenntnisse in deren Weiterentwicklung bieten Ansatzpunkte, um die Ideen der BSI-GIT-Skizze mit den bestehenden Vorhaben zu verbinden. Das BSI sieht hier eine wichtige Schnittstelle zum Workstream Cyberdome.

Auch nach Abschluss des Workstreams werden die Teilnehmenden über weitere Schritte des BSI in Bezug auf die drei Skizzen und mögliche Umsetzungen informiert bzw. für weiteren Austausch angefragt werden.

7. Literatur

BSI Publikation: Maßnahmenkatalog Ransomware
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.pdf?__blob=publicationFile&v=3

BSI Publikation: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall, Arbeitspapier – Version 1.2 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.pdf?__blob=publicationFile&v=3

BSI Webseite - Checkliste Technik:
https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Unternehmen/Ich-habe-einen-IT-Sicherheitsvorfall-Checkliste-Technik/ich-habe-einen-it-sicherheitsvorfall-checkliste-technik_node.html

BSI-Webseite: Liste zertifizierter IT-Sicherheitsdienstleister in den Geltungsbereichen IS-Revision und IS-Penetrationstests

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Anerkennung-von-Stellen-und-Zertifizierung-IT-Sicherheitsdienstleister/IS-Rev/Liste-IT-Sicherheitsdienstleister/liste-is-revi-is-pentester_node.html

BSI-Veröffentlichung: Liste der qualifizierten APT-Response-Dienstleister; Stand: 01.08.2024

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.html