

Nutzungsrichtlinie für Softwareentwicklungs-Dienstleistende

Fremdfirmeneinwahl Softwareentwicklungs-Service-Infrastruktur des Bundesverwaltungsamtes

Stand Datum:	25. Juni 2025
Version:	0.9
Status:	<input type="checkbox"/> in Bearbeitung <input checked="" type="checkbox"/> vorgelegt <input type="checkbox"/> abgenommen

Inhaltsverzeichnis

1.	Geltungsbereich und Vertraulichkeit.....	3
1.1.	Zielgruppe	3
1.2.	Geltungsbereich.....	3
1.3.	Einstufung	3
1.4.	Zuständigkeit und Revision.....	3
2.	Einleitung	4
3.	Überblick	5
4.	Quellen grundlegender Anforderungen und Empfehlungen	6
5.	Sicherheitsanforderungen an die SWE-DL	8
6.	Anhang.....	17
6.1.	Anlagen	17
6.2.	Referenzierte Dokumente	17
6.3.	Referenzen aus den Einzelanforderungen	19

1. Geltungsbereich und Vertraulichkeit

1.1. Zielgruppe

Dieses Dokument ist ein Auszug aus der Richtlinie zur Informationssicherheit des BVA zur Bereitstellung und Nutzung der Fremdfirmeneinwahl. Mit der Fremdfirmeneinwahl (FFE) soll Softwareentwicklungs-Dienstleistenden (SWE-DL) ein sicherer Zugang zum FFE-Netzwerk / Netzwerk der Softwareentwicklungs-Service-Infrastruktur (ZSSI) des BVA gewährt werden, der den Anforderungen an eine effiziente Softwareentwicklung und an die Informationssicherheit gleichermaßen genügt.

Dieses Dokument richtet sich an Softwareentwicklungs-Dienstleistende, die für ihre Tätigkeiten die Fremdfirmeneinwahl nutzen möchten.

1.2. Geltungsbereich

Dieses Dokument ist für den Gebrauch durch SWE-DL bestimmt.

Eine Vervielfältigung, Speicherung, Umformatierung, Übertragung und/oder Weitergabe bzw. Verteilung in elektronischer und/oder physikalischer Form, auch von Auszügen, außerhalb des BVA bedarf der vorherigen Genehmigung der/des Informationssicherheitsbeauftragten (ISB) des BVA.

1.3. Einstufung

Für das vorliegende Dokument wird keine Einstufung nach der VS-Anweisung des Bundes (VSA) vorgenommen.

1.4. Zuständigkeit und Revision

Die Zuständigkeit für die Inhalte dieses Dokumentes obliegt der/dem ISB BVA. Das Dokument ist entsprechend der jeweiligen IT-Sicherheitslage und Entwicklung fortzuschreiben. Die diesem Dokument zugrunde liegende Richtlinie ist spätestens nach zwei Jahren einer Revision zu unterziehen.

Die Freigabe der diesem Dokument zugrunde liegende Richtlinie erfolgt durch die Behördenleitung im BVA.

2. Einleitung

Die Durchführung großer, komplexer Softwareentwicklungs-Projekte beim BVA ist ohne die Unterstützung durch externe Softwareentwicklungs-Dienstleistende (SWE-DL) nicht leistbar.

Der Zweck der Fremdfirmeneinwahl (FFE) besteht darin, die Zusammenarbeit und den Informationsaustausch zwischen den SWE-Referaten beim BVA und den externen Entwicklerinnen und Entwicklern der SWE-DL zu fördern, ohne dass physische Präsenz vor Ort erforderlich ist.

Denn ein effizienter Softwareentwicklungsprozess erfordert, dass die SWE-DL aus eigenen Räumlichkeiten mit eigenen Werkzeugen selbstorganisiert arbeiten. Das ermöglicht die für eine moderne Softwareentwicklung mit agilem Vorgehen und kurzen Entwicklungszyklen erforderliche Flexibilität, beschleunigt die Fehlerbearbeitung und -behebung und spart Kosten.

Auf der anderen Seite ist es eine grundlegende Anforderung der Informationssicherheit, dass der Quellcode BVA-Eigentum ist und das BVA sich auch im unmittelbaren Besitz des Quellcodes befindet. Vertraulichkeit, Integrität und Verfügbarkeit aller Sourcen und Informationen müssen behördenintern ohne Abhängigkeiten zu externen Firmen kontrolliert werden.

Mit der Fremdfirmeneinwahl soll einem SWE-DL ein sicherer Zugang zum FFE-Netzwerk / Netzwerk der Softwareentwicklungs-Service-Infrastruktur (ZSSI) des BVA gewährt werden, der den Anforderungen an eine effiziente Softwareentwicklung und an die Informationssicherheit gleichermaßen genügt.

Mit der Fremdfirmeneinwahl ist jedoch ein spezifisches Gefährdungspotential verbunden. Tätigkeiten und Zugriffe auf Seiten der SWE-DL stehen außerhalb der dienstrechtlichen, eine Kontrolle seitens BVA ist nur im begrenzten Umfang möglich. Dabei steht das Bundesverwaltungsamt als beauftragende Behörde weiterhin in der Verantwortung für die Vertraulichkeit, Integrität und Verfügbarkeit der Anwendungen, Daten und Informationen im Zugriff der SWE-DL.

Der vorliegende Auszug formuliert Anforderungen und Maßnahmen sicheren Nutzung der Fremdfirmeneinwahl durch die SWE-DL. Sie adressiert ausschließlich die Informationssicherheit. Die inhaltliche Steuerung der Softwareentwicklung, die Kontrolle der Arbeitsergebnisse oder die Ahndung von Minderleistungen werden nicht betrachtet.

Die Schlüsselworte (Modalverben) „MUSS“, „KANN“, „SOLLTE“, „SOLLTE NICHT“, „DARF NUR“ und „DARF NICHT“ haben, wie im IT-Grundschutz-Kompendium des BSI, die in RFC-2119 definierte Bedeutung.

3. Überblick

Die Fremdfirmeneinwahl realisiert mit jedem SWE-DL ein eigenes Site-to-Site-VPN. Als IPsec-VPN-Gateways kommen SINA Boxen der secunet Security Networks AG zum Einsatz. Die Bereitstellung der SINA Hardware¹, deren Verwaltung, Konfiguration und Administration erfolgen durch das ITZBund.

Die Fremdfirmeneinwahl ermöglicht den SWE-DL, aus eigenen Netzen (und damit aus eigenen Räumlichkeiten inkl. Home Office und mobilem Arbeiten) mit eigenen Entwicklungs-Arbeitsplätzen² über einen sicheren Kommunikationskanal auf die Werkzeuge der zentralen Softwareentwicklungs-Service-Infrastruktur (ZSSI) in den Netzen des BVA und damit auf das FFE/ZSSI-Netzwerk beim BVA³ zuzugreifen.

Die folgende Abbildung stellt typische Zugriffe dar, die im Rahmen der Softwareentwicklung durch SWE-DL erfolgen. Wesentlichen Anforderungen dieses Dokumentes liegt dieses Bild zugrunde.

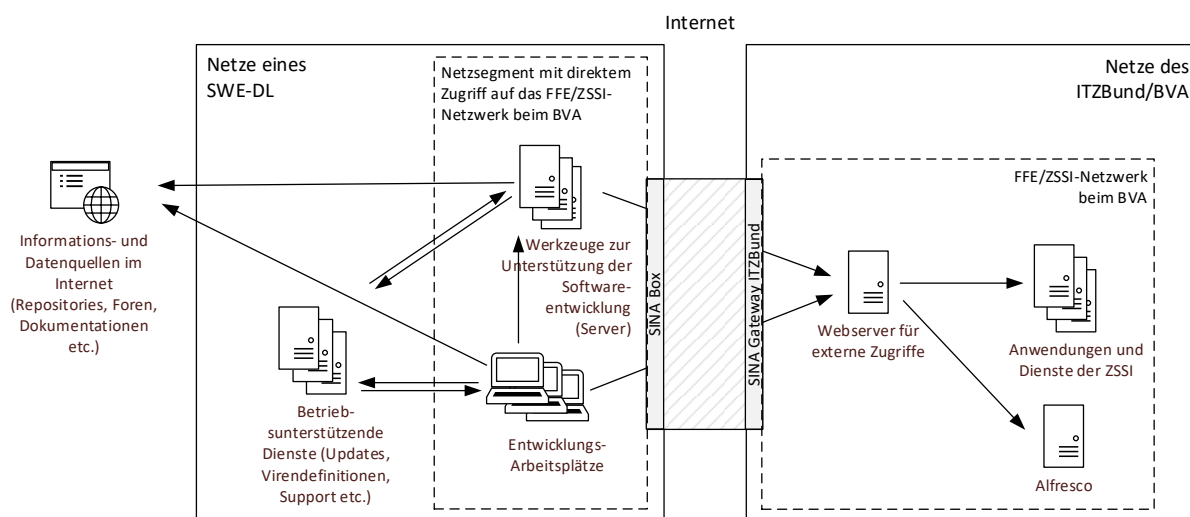


Abbildung 1: Modell Softwareentwicklung unter Nutzung der Fremdfirmeneinwahl

¹ Da SINA Workstations für ihre Zugriffe auf die Netze des BVA eine eigene, von der Fremdfirmeneinwahl unabhängige Infrastruktur nutzen, werden diese im vorliegenden Dokument nicht betrachtet.

² Neben den eigentlichen Entwicklerinnen und Entwicklern (Personen, die Software-Quellcode erstellen) benötigen und erhalten weitere Personen der SWE-DL u. a. aus der Projektleitung, der Qualitätssicherung oder dem Architektur- oder Testteam Zugriff auf das FFE/ZSSI-Netzwerk beim BVA. Alle Arbeitsplätze bei einer/einem SWE-DL, die im Rahmen eines SWE-Projektes Zugriffe auf Netzbereiche des BVA benötigen und erhalten, werden unter dem Begriff „Entwicklungs-Arbeitsplatz“ zusammengefasst.

³ Der Begriff FFE/ZSSI-Netzwerk beim BVA bezeichnet die logische Zusammenfassung aller Netze/Netzsegmente beim ITZBund und beim BVA, über die die Kommunikation der SWE-DL vom SINA Gateway des ITZBund zu den Systemen der ZSSI geführt wird.

4. Quellen grundlegender Anforderungen und Empfehlungen

In diesem Kapitel werden die Quellen grundlegender Anforderungen und Empfehlungen an die Sicherheit der Fremdfirmeneinwahl dargestellt.

IT-Grundschutz Kompendium [BSI-GSK]

Im IT-Grundschutz-Kompendium hat das BSI standardisierte Sicherheitsanforderungen für typische Geschäftsprozesse, Anwendungen, IT-Systeme, Kommunikationsverbindungen, Gebäude und Räume in IT-Grundschutz-Bausteinen beschrieben. Für die Fremdfirmeneinwahl sind insbesondere die Themen Identitäts- und Berechtigungsmanagement, Detektion von sicherheitsrelevanten Ereignissen und Notfallmanagement, Netzarchitektur und -design, Firewalls und VPN sowie physische Sicherheit relevant. Diese wurden in einem Fach-Sicherheitskonzept für die Fremdfirmeneinwahl betrachtet. Im Wesentlichen wurden die Anforderungen dieser Richtlinie aus dem Sicherheitskonzept abgeleitet, ergänzt um weitere Aspekte aus den nachfolgenden Quellen.

Mindeststandards des BSI nach § 8 Abs. 1 Satz 1 BSIG [BSI-MST]

Als gesetzliche Vorgabe definieren Mindeststandards ein verbindliches Mindestniveau für die Informationssicherheit. Für die Fremdfirmeneinwahl ist insbesondere der Mindeststandard des BSI zur Nutzung der ressortübergreifenden Kommunikationsnetze des Bundes („Nutzerpflichten NdB“) in der aktuell gültigen Version relevant. Diese Nutzerpflichten richten sich an die Nutzer der NdB und legen die umzusetzenden Sicherheitsanforderungen und -maßnahmen fest, um an den NdB als Nutzer teilnehmen zu können.

Verschlusssachenanweisung [[VSA]]

Die Verschlusssachenanweisung richtet sich an Bundesbehörden und bundesunmittelbare öffentlich-rechtliche Einrichtungen (Dienststellen), die mit Verschlusssachen arbeiten, sowie an dort tätige Personen, die Zugang zu Verschlusssachen haben oder eine Tätigkeit ausüben, bei der sie sich Zugang zu Verschlusssachen verschaffen können. In der ZSSI kann es erforderlich sein, auch Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH vorzuhalten.

GeheimSchutzhandbuch [GSH]

Die Grundlage für das GeheimSchutzverfahren in der Wirtschaft sind im GeheimSchutzhandbuch, herausgegeben für nichtöffentliche Stellen durch das Bundesministerium für Wirtschaft und Klimaschutz (BMWK), festgelegt.

Einsatz- und Betriebsbedingungen der SINA Hardware [SINA]

Die Fremdfirmeneinwahl wird über SINA Hardware realisiert. Die Einsatz- und Betriebsbedingungen (Security Operating Procedures, SecOPs) der SINA Hardware werden vom BSI herausgegeben und sind integraler Bestandteil deren Zulassungsdokumentation. Die Beachtung und Umsetzung der Anforderungen dieser Dokumente ist verbindlich für den Betrieb der jeweiligen Hardware.

BSI-Standards zur Internet-Sicherheit - ISi-Reihe [BSI -ISi]

Die ISi-Reihe (BSI-Standards zur Internet-Sicherheit) gibt konkrete technische Empfehlungen zu verschiedenen Themenbereichen der IT-Sicherheit. Für die Fremdfirmeneinwahl sind insbesondere die Module *Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)*, *Sicherer Fernzugriff auf das interne Netz (ISi-Fern)* sowie *Virtuelles Privates Netz (ISi-VPN)*⁴ relevant.

Empfehlungen zum Aufbau von VPN und Integration in Sicherheitsgateways [BSI-VPN]

Gegenstand der Veröffentlichung des BSI aus dem Jahre 2006 ist die sichere Integration von VPN-Komponenten in Sicherheitsgateways.

Benutzerdefinierte Bausteine (aus der Praxis für die Praxis) [BSI-bB]

IT-Grundschutz-Anwender und das BSI stellen regelmäßig neue Hilfsmittel zur Verfügung, um die einzelnen Angebote des IT-Grundschutzes noch besser nutzen zu können. Für die Fremdfirmeneinwahl sind insbesondere die von der secunet Security Networks AG erstellten benutzerdefinierten Bausteine *NET.bd.2 SINA Box* und *NET.bd.x: SINA Management* relevant.

⁴ Dieses ISi-Modul ist nach Aussage des BSI veraltet und wird zurzeit nicht aktualisiert.

5. Sicherheitsanforderungen an die SWE-DL

Für die Nutzung der SWE durch die SWE-DL gelten die folgenden Sicherheitsanforderungen.

Anforderung	Beschreibung und Quelle
SWE-DL.01 Anforderungen an den Empfang, die Lagerung und den Weiter-/Rücktransport von SINA Boxen	<p>Die SINA Box wird den SWE-DL vom ITZBund bereitgestellt.</p> <p>Beim Empfang MUSS der SWE-DL die Unversehrtheit der Verpackung sowie des Gerätes (Gerätesiegelbruch) prüfen. Jede vermutete Manipulation oder externe Beschädigung MUSS unverzüglich dem/der ISB des BVA gemeldet werden.</p> <p>Bei (Zwischen-)Lagerung, (Weiter-)Transport und Rückversand MUSS die SINA Box gegen unautorisierten Zugriff geschützt werden, um eine Verletzung deren Integrität zu verhindern. ALLE für den Betrieb des Geräts erforderlichen Smartcards MÜSSEN entfernt werden.</p> <p>—</p> <p>Quelle _Ref1_ aus Kapitel 6.3</p>
SWE-DL.02 Regelmäßige Durchführung von Sichtprüfungen der SINA Boxen und Meldung vermuteter Manipulationen	<p>Die SINA Box MUSS in regelmäßigen Intervallen, die ein Jahr nicht überschreiten sollten, einer Sichtprüfung unterzogen werden. Jede vermutete Manipulation oder externe Beschädigung MUSS unverzüglich der/dem ISB beim BVA gemeldet werden.</p> <p>Die SINA Box DARF ausschließlich vom Hersteller zum Zwecke der Wartung / Reparatur / Instandsetzung geöffnet werden.</p> <p>—</p> <p>Quelle _ Ref 2_ aus Kapitel 6.3</p>
SWE-DL.03 Betrieb der SINA Boxen in Deutschland	<p>Die SINA Box MUSS in Deutschland betrieben werden. Ein erforderlicher Betrieb im Ausland KANN nach Abstimmung mit der/des ISB des BVA nur dann erfolgen, wenn mit dem Land ein Geheimschutzabkommen besteht.</p> <p>—</p> <p>Quelle _ Ref 3_ aus Kapitel 6.3</p>

Anforderung	Beschreibung und Quelle
SWE-DL.04 Räumliche Sicherheit des Betriebsorts der SINA Boxen bei den SWE-DL	<p>Die SINA Box bei den SWE-DL MUSS in einer geeigneten, verschlossenen Umgebung/ in einem geeigneten Sicherheitsbereich betrieben werden (Rechenzentrum, Serverraum, Technikschränk).</p> <p>Der Betriebsort MUSS vor Einbruch geschützt werden.</p> <p>Die SWE-DL MÜSSEN die Hülle der Räumlichkeit/des Sicherheitsbereichs mindestens in RC2-Qualität gemäß DIN EN 1627 ausbilden. Die Qualität der Schlösser, Schließzylinder und Schutzbeschläge SOLLTE der Widerstandsklasse der Tür entsprechen.</p> <p>Es SOLLTEN Räumlichkeiten ohne Außenfester genutzt werden.</p> <p>Der SWE-DL MUSS sämtliche Türen, Fenster und sonstige Öffnungen der Räumlichkeit / des Sicherheitsbereichs durch eine Einbruchmeldeanlage (EMA) auf Öffnung, Verriegelung und Durchbruch überwachen. Die Alarmempfangsstelle MUSS jederzeit erreichbar sein. Sie MUSS technisch sowie personell in der Lage sein, geeignet auf die gemeldete Gefährdung zu reagieren.</p> <p>—</p> <p>Quelle _ Ref 4_ aus Kapitel 6.3</p>
SWE-DL.05 Zutrittsschutz zum Betriebsort der SINA-Box beim SWE-DL	<p>Alle Zutrittsmöglichkeiten zum Betriebsort der SINA Box beim SWE-DL MÜSSEN mit Zutrittskontrollenrichtungen⁵ ausgestattet sein.</p> <p>Die Zahl der Zutrittsberechtigten zur Räumlichkeit/zum Sicherheitsbereich MUSS auf das unabdingbare Minimum begrenzt sein. Sämtliche Zutrittsberechtigten MÜSSEN dem SWE-DL namentlich benannt werden und SOLLTEN sicherheitsüberprüft (einfache Sicherheitsüberprüfung gemäß Sicherheitsüberprüfungsgesetz) sein.</p> <p>Personen ohne Zutrittsberechtigung MÜSSEN sich beim Zutritt zum Betriebsort der SINA Box in ständiger Begleitung von zugriffsberechtigtem Personal befinden.</p> <p>Vergebene Zutrittsberechtigungen MÜSSEN mindestens jährlich auf Notwendigkeit geprüft werden. Berechtigungen, die als entbehrlich erkannt werden, MÜSSEN umgehend entzogen werden, Schlüssel MÜSSEN eingezogen werden. Bei Personalwechsel MÜSSEN diese Überprüfungen umgehend erfolgen.</p> <p>—</p> <p>Quelle _ Ref 5_ aus Kapitel 6.3</p>

⁵ Eine Zutrittskontrollenrichtung ist eine Einrichtung, die eine Zutrittskontrolle wirksam umsetzt. Eine Zutrittskontrollenrichtung steuert den Zutritt zu einem bestimmten, abgegrenzten räumlichen Bereich über ein festgelegtes Regelwerk, damit nur berechtigte Personen Zutritt zu den für sie freigegebenen Bereichen erhalten. Eine

Anforderung	Beschreibung und Quelle
SWE-DL.06 Netztrennung beim SWE-DL	<p>Bei der Konzeptionierung und Implementierung der Entwicklungs-Netze auf Seiten der SWE-DL (Netzbereiche/Netzsegmente mit direktem Zugriff auf das FFE/ZSSI-Netzwerk beim BVA, vgl. Abbildung 1) MÜSSEN die übrigen Netze der SWE-DL als nicht vertrauenswürdig eingestuft und entsprechend behandelt werden.</p> <p>Das Netzsegment auf Seiten eines SWE-DL, aus dem die Zugriffe in die Netzinfrastruktur des BVA erfolgen, MUSS von anderen Netzen des SWE-DL (z. B. vom produktiven, internen Netz des SWE-DL) getrennt werden. Dies SOLLTE durch physische Netztrennung oder Sicherheitsgateways⁶ realisiert werden.</p> <p>Entwicklungs-Arbeitsplätze und IT-Systeme mit direktem Zugriff auf das FFE/ZSSI-Netzwerk beim BVA über die Fremdfirmeneinwahl DÜRFEN NICHT ungeschützt (z. B. durch direkte Nutzung eines DSL-Routers) aus dem Internet erreichbar sein. Direkte Zugriffe auf diese Entwicklungs-Arbeitsplätze und IT-Systeme aus SWE-DL-fremden Netzen (z. B. im Rahmen von Fernwartung) DÜRFEN NICHT erfolgen.</p> <p>Bei erforderlichen Zugriffen auf das Internet MÜSSEN Entwicklungs-Arbeitsplätze und IT-Systeme der SWE-DL die SWE-DL-eigene Netzwerkstruktur nutzen. Dies ist nur zulässig, wenn die Netzwerkinfrastruktur der SWE-DL mindestens durch eine zweistufige Firewall-Struktur, bestehend aus zustandsbehafteten Paketfiltern (Firewall), vom Internet getrennt ist und der Internetverkehr über diese Firewall-Struktur geführt wird. Zusätzlich MUSS ausgehende Kommunikation zum Internet an einem Sicherheits-Proxy entkoppelt werden.</p> <p>_____</p> <p>Quelle _ Ref 6_ aus Kapitel 6.3</p>

Zutrittskontrollereinrichtung ist typischerweise eine technische Vorrichtung, sie kann jedoch auch organisatorisch/personell z. B. durch einen Sicherheitsdienst umgesetzt oder unterstützt werden.

⁶ Am Übergang zwischen vertrauenswürdigen und nicht-vertrauenswürdigen Netzen werden typischerweise Sicherheitsgateways installiert. Ein Sicherheitsgateway ist ein System aus soft- und hardwaretechnischen Komponenten. Es gewährleistet die sichere Kopplung von IP-Netzen durch Einschränkung der technisch möglichen auf die in einer IT-Sicherheitsrichtlinie ordnungsgemäß definierten Kommunikation. Sicherheit bei der Netzkopplung bedeutet hierbei, dass ausschließlich erwünschte Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen werden. Zudem können mit Sicherheitsgateways die übertragenen Daten kontrolliert werden.

Anforderung	Beschreibung und Quelle
SWE-DL.07 Keine Nutzung der Entwicklungs-Arbeitsplätze für SWE anderer Kunden	<p>Entwicklungs-Arbeitsplätze des SWE-DL mit direktem Zugang zum FFE/ZSSI-Netzwerk beim BVA über die Fremdfirmeneinwahl SOLLTEN NICHT für die Softwareentwicklung für andere Kunden verwendet werden.</p> <p>Ist dies nicht möglich, MUSS der SWE-DL ein Mandantentrennungskonzept⁷ erstellen und umsetzen. Das Mandantentrennungskonzept und dessen Umsetzung MUSS sicherstellen, dass Daten und Verarbeitungskontexte verschiedener Kunden des SWE-DL ausreichend sicher getrennt werden. Dabei MUSS zwischen mandantenabhängigen und mandantenübergreifenden Daten und Objekten unterschieden werden.</p> <p>Das Mandantentrennungskonzept MUSS vor der Freischaltung des Zugangs über die Fremdfirmeneinwahl der/dem ISB des BVA vorgestellt werden. Bei ungeeigneter Trennung KANN die/der ISB des BVA die Freischaltung der Fremdfirmeneinwahl verwehren.</p> <p>—</p> <p>Quelle _ Ref 7_ aus Kapitel 6.3</p>
SWE-DL.08 Trennung der Entwicklung für das BVA von der Entwicklung für andere Kunden	<p>Systeme der SWE-DL mit direktem Zugang zum FFE/ZSSI-Netzwerk beim BVA über die Fremdfirmeneinwahl (Entwicklungs-Rechner und Server mit Werkzeugen zur Unterstützung der Softwareentwicklung, vgl. Abbildung 1) DÜRFEN KEINEN direkten Zugang zu Netzen anderer Kunden haben.</p> <p>—</p> <p>Quelle _ Ref 8_ aus Kapitel 6.3</p>
SWE-DL.09 Identitäts- und Berechtigungsmanagement für SWE-Umgebung beim SWE-DL	<p>Durch ein geeignetes Identitäts- und Berechtigungsmanagement MÜSSEN die SWE-DL sicherstellen, dass nur Personen, die an Softwareentwicklungsprojekten für das BVA beteiligt sind und dafür Zugriff auf Anwendungen oder Systeme im FFE/ZSSI-Netzwerk beim BVA benötigen, für die Entwicklungs-Arbeitsplätze und IT-Systeme mit direktem Zugriff auf das FFE/ZSSI-Netzwerk beim BVA über die Fremdfirmeneinwahl berechtigt werden.</p> <p>—</p> <p>Quelle _ Ref 10_ aus Kapitel 6.3</p>

⁷ Diese Anforderung geht davon aus, dass ein SWE-DL für mehrere Kunden tätig ist. Durch Mandantentrennung soll sichergestellt werden, dass die Informationen eines Kunden zu keinem Zeitpunkt von einem anderen Kunden eingesehen oder beeinflusst werden können.

Anforderung	Beschreibung und Quelle
SWE-DL.10 Sichere Authentisierung an den Entwicklungs-Arbeitsplätzen	<p>Die Nutzung der Entwicklungs-Arbeitsplätze MUSS durch ein starkes, personalisiertes Authentisierungsverfahren geschützt sein. Es SOLLTE eine sichere Mehr-Faktor-Authentisierung unter Einbeziehung unterschiedlicher Faktoren (Wissen, Besitz, Eigenschaft) für die lokale Anmeldung an Entwicklungs-Arbeitsplätzen eingerichtet werden, z. B. Passwort mit Chipkarte oder Token.</p> <p>—</p> <p>Quelle _ Ref 11_ aus Kapitel 6.3</p>
SWE-DL.11 Schutz der Entwicklungs-Arbeitsplätze mit Zugriff auf das FFE/ZSSI-Netzwerk beim BVA	<p>Die Entwicklungs-Arbeitsplätze bei den SWE-DL mit Zugriff auf das FFE/ZSSI-Netzwerk beim BVA MÜSSEN gehärtet sein. Das automatische Übermitteln von Telemetrie-Daten und Diagnose-Daten an Softwarehersteller MUSS unterbunden werden.</p> <p>Auf externe Schnittstellen SOLLTE nur restriktiv zugegriffen werden können.</p> <p>Es MUSS untersagt werden, dass nicht zugelassene Geräte oder Wechsel-datenträger mit den Clients verbunden werden. Es MUSS verhindert werden, dass über Wechselaufwerke oder externe Schnittstellen unberechtigt Daten von den Clients kopiert werden können.</p> <p>Wenn vertrauliche Informationen auf den Entwicklungs-Arbeitsplätzen gespeichert werden, SOLLTEN mindestens die schutzbedürftigen Dateien sowie ausgewählte Dateisystembereiche oder besser die gesamten Datenträger verschlüsselt werden.</p> <p>—</p> <p>Quelle _ Ref 12_ aus Kapitel 6.3</p>

Anforderung	Beschreibung und Quelle
<p>SWE-DL.12 Schutz der IT-Systeme (SWE-Werkzeuge) mit Zugriff auf das FFE/ZSSI-Netzwerk beim BVA</p>	<p>IT-Systeme bei den SWE-DL mit Zugriff auf das FFE/ZSSI-Netzwerk beim BVA MÜSSEN gehärtet sein. Updates und (Sicherheits-)patches MÜSSEN zeitnah eingespielt werden (z.B. über einen kontrollierten Autoupdate-Mechanismus).</p> <p>Nicht benötigte Anwendungen MÜSSEN auf den Servern entfernt werden. Ist das nicht möglich, MUSS deren Ausführung unterbunden werden.</p> <p>Vorhandene lokale Paketfilter MÜSSEN über ein Regelwerk so ausgestaltet werden, dass die eingehende und ausgehende Kommunikation auf die erforderlichen Kommunikationspartner, Kommunikationsprotokolle sowie Ports und Schnittstellen beschränkt wird. Die Identität von Remote-Systemen und die Integrität der Verbindungen mit diesen SOLLTE kryptografisch abgesichert sein.</p> <p>IT-Systeme bei den SWE-DL mit Zugriff auf das FFE/ZSSI-Netzwerk beim BVA SOLLTEN regelmäßigen Sicherheitstests unterzogen werden, die überprüfen, ob alle Sicherheitsvorgaben eingehalten werden und gegebenenfalls vorhandene Schwachstellen identifizieren.</p> <p>—</p> <p>Quelle _ Ref 13_ aus Kapitel 6.3</p>
<p>SWE-DL.13 Einsatz von Schutzprogrammen gegen Schadsoftware</p>	<p>Auf allen IT-Systemen eines SWE-DL, die über die Fremdfirmeneinwahl auf das FFE/ZSSI-Netzwerk beim BVA zugreifen können, MÜSSEN Schutzprogramme gegen Schadsoftware eingesetzt werden.</p> <p>Der gesamte Datenbestand auf diesen Systemen MUSS regelmäßig auf Schadsoftware geprüft werden. Das Schutzprogramm MUSS nach Schadsoftware suchen, wenn Dateien ausgetauscht oder übertragen werden.</p> <p>—</p> <p>Quelle _ Ref 14_ aus Kapitel 6.3</p>

Anforderung	Beschreibung und Quelle
<p>SWE-DL.14 Erstellen eines Sicherheitskonzeptes zum Schutz des Entwicklungsnetzes und der SINA Boxen beim SWE-DL</p>	<p>Laut BSI Standard 200-2 umfasst ein Informationsverbund „die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen.“</p> <p>Demnach gehören die vom SWE-DL für die Softwareentwicklung verwendeten IT-Systeme mit Zugriff auf das FFE/ZSSI-Netzwerk beim BVA und die Räumlichkeiten, in denen die SINA-Box betrieben wird, zum Informationsverbund der Fremdfirmeneinwahl.</p> <p>SWE-DL MÜSSEN Sicherheitsmaßnahmen planen und umsetzen, die geeignet sind, die Anforderungen des IT-Grundschutzes oder einer Zertifizierung nach ISO 27001 zu erfüllen. Sicherheitsmaßnahmen und Risiken MÜSSEN in einem Sicherheitskonzept gemäß obiger Standards betrachtet werden. Insbesondere die Themen Identitäts- und Berechtigungsmanagement, Patch- und Änderungsmanagement, Schutz vor Schadprogrammen, Detektion von sicherheitsrelevanten Ereignissen sowie Netzarchitektur und -design und Sicherheit von Gebäude-Infrastrukturen MÜSSEN im Sicherheitskonzept betrachtet werden.</p> <p>Beim Einsatz von Sub-Dienstleistenden MÜSSEN diese in der Sicherheitskonzeption ebenfalls berücksichtigt werden.</p> <p>Der/dem ISB des BVA MUSS auf Anfrage Einsicht in das Sicherheitskonzept gewährt werden.</p> <p>—</p> <p>Quelle _ Ref 15_ aus Kapitel 6.3</p>
<p>SWE-DL.15 Einhalten der Vorgaben der VSA inklusive VS-NfD-Merkblatt</p>	<p>Im Rahmen der Softwareentwicklung über die Fremdfirmeneinwahl zugängliche Daten können Verschlusssachen des Geheimhaltungsgrades VS-NUR-FÜR DEN DIENSTGEBRAUCH enthalten.</p> <p>Zudem läuft auf den bei den DWE-DL betriebenen SINA Boxen die "governmental" Version der Software, die als VS-NfD eingestuft ist.</p> <p>Beim Zugriff auf/ bei der Verarbeitung von Verschlusssachen MÜSSEN die Vorgaben der VSA beachtet werden. Dies gilt insbesondere für die an der Verarbeitung beteiligten IT-Systeme (VS-IT).</p> <p>Der SWE-DL MUSS die Bestimmungen des Merkblattes zur Behandlung von Verschlusssachen (VS) des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH befolgen.</p> <p>—</p> <p>Quelle _ Ref 16_ aus Kapitel 6.3</p>

Anforderung	Beschreibung und Quelle
SWE-DL.16 Benachrichtigung der/des ISB des BVA bei Sicherheitsvorfällen	<p>SWE-DL MÜSSEN die/den ISB des BVA über Sicherheitsvorfälle, die unmittelbar oder mittelbar die Sicherheit des BVA gefährden können, unverzüglich informieren. Dies betrifft erkannte Schwachstellen in Systemen mit unmittelbarem Zugriff auf das FFE/ZSSI-Netzwerk beim BVA ebenso wie Angriffe auf zentrale Dienste (Identitätsverwaltung, Authentisierung und Autorisierung) oder die IT-Infrastruktur des SWE-DL.</p> <p>Werden keine abweichenden Vereinbarungen oder Absprachen getroffen, MUSS der im Vertrag festgelegte Meldeweg eingehalten werden.</p> <p>—</p> <p>Quelle _ Ref 17_ aus Kapitel 6.3</p>
SWE-DL.17 Eindämmen der Auswirkung von Sicherheitsvorfällen	<p>Können Sicherheitsvorfälle beim SWE-DL die Sicherheit des BVA unmittelbar oder mittelbar gefährden, so MUSS der SWE-DL zeitnah geeignete Maßnahmen ergreifen, um das Ausbreiten in die Umgebung des BVA zu unterbinden.</p> <p>Im Zweifel MUSS der SWE-DL seinen VPN Zugang durch Herunterfahren der SINA Box oder Ziehen des Netzsteckers schließen.</p> <p>Die/der ISB des BVA ist umgehend über die festgelegten Meldewege zu kontaktieren.</p> <p>—</p> <p>Quelle _ Ref 18_ aus Kapitel 6.3</p>
SWE-DL.18 Mitwirkung bei IT-forensischen Untersuchungen des BVA und des BSI	<p>Wurden auf Seiten des BVA Angriffe oder Angriffsversuche über die Fremdfirmeneinwahl detektiert, so MUSS der SWE-DL auf Anfrage des BVA oder des BSI IT-forensischen Untersuchungen durch Überprüfungen im eigenen Netz unterstützen.</p> <p>—</p> <p>Quelle: _ Ref 19_ aus Kapitel 6.3</p>
SWE-DL.19 Erreichbarkeit für zeitnahe Reaktion auf Sicherheitsvorfälle	<p>Um zeitnah auf Sicherheitsvorfälle reagieren zu können, die durch das BVA detektiert wurden, MUSS der SWE-DL in der Lage sein, Meldungen und Hinweise der/des ISB beim BVA zu empfangen und zeitnah zu bearbeiten. Dazu gehört die Umsetzung / Veranlassung von Ad-Hoc-Maßnahmen zur Eindämmung des Angriffs.</p> <p>Werden keine abweichenden Vereinbarungen oder Absprachen getroffen, gelten die im Vertrag festgelegte Meldewege und -zeiten.</p> <p>—</p> <p>Quelle: _ Ref 20_ aus Kapitel 6.3</p>

Anforderung	Beschreibung und Quelle
SWE-DL.20 Weitergabe der Anforderungen an Sub-Dienstleistende	<p>Werden Tätigkeiten und Prozesse, die die Fremdfirmeneinwahl unmittelbar betreffen (z. B. der Betrieb der SINA-Box, der Betrieb der eigenen IT-Infrastruktur) von den SWE-DL an Sub-Dienstleistende ausgelagert, MUSS die Nutzungsrichtlinie an die Sub-Dienstleistenden weitergegeben werden. Die Sub-Dienstleistenden müssen von den SWE-DL vertraglich zur Einhaltung verpflichtet werden.</p> <p>Der SWE-DL MUSS die/den ISB des BVA über bestehende Zugriffsmöglichkeiten von Sub-Dienstleistende auf IT-Systeme des SWE-DL, die über die Fremdfirmeneinwahl auf das FFE/ZSSI-Netzwerk beim BVA zugreifen können (Entwicklungs-Arbeitsplätze, Server mit SWE-Tools), informieren. Gleiches gilt für Zutrittsmöglichkeiten von Sub-Dienstleistenden zum Betriebsort der SINA Box (IT-Betriebsdienstleister, Wachpersonal etc.).</p> <p>—</p> <p>Quelle _ Ref 21_ aus Kapitel 6.3</p>
SWE-DL.21 Dokumentation des Netzes	<p>Die SWE-DL MÜSSEN eine vollständige Dokumentation des Entwicklungs-Netzes inkl. Segmentierung und Abgrenzung zu anderen Netzen erstellen. Diese Dokumentation MUSS auch VLANs und virtualisierte Netze in Virtualisierungs-Hosts beinhalten.</p> <p>Die Dokumentation MUSS einen Netzplan beinhalten.</p> <p>Die Dokumentation des Netzes / der Netzplan MUSS der/dem ISB des BVA auf Anfrage vorgelegt werden.</p> <p>—</p> <p>Quelle _ Ref 22_ aus Kapitel 6.3</p>
SWE-DL.22 Einräumen von Kontrollrechten zur Überprüfung der Einhaltung der Nutzungsrichtlinie	<p>Die SWE-DL MÜSSEN dem BVA oder vom BVA beauftragten Dritten das Recht einräumen, im Rahmen von IS-Revisionen bei den SWE-DL die Einhaltung der Nutzungsrichtlinie zu kontrollieren. Details regelt der Vertrag zwischen den SWE-DL und dem BVA.</p> <p>—</p> <p>Quelle _ Ref 23_ aus Kapitel 6.3</p>

Tabelle 1 Sicherheitsanforderungen an die SWE-DL

6. Anhang

6.1. Anlagen

keine

6.2. Referenzierte Dokumente

Referenz	Dokument / Link / Quelle
BSI-GSK	IT-Grundschutzkompendium, Edition 2023 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html
BSI-MST	Mindeststandards des BSI nach § 8 Abs. 1 Satz 1 BSIG https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Mindeststandards_node.html
BSI -ISi	BSI-Standards zur Internet-Sicherheit (ISi-Reihe) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/ISI-Reihe/isi-reihe_node.html
BSI-VPN	BSI: Aufbau von Virtual Private Networks (VPN) und Integration in Sicherheitsgateways, Bundesanzeiger Verlag, 2007, ISBN 978-3-89817-617-0 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/vpn_pdf.html
BSI-bB	BSI/ secunet Security Networks AG: Benutzerdefinierter Baustein NET.bd.2 SINA Box https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Benutzerdefinierte_BS/SinaBox.html?nn=943082 BSI/ secunet Security Networks AG: Benutzerdefinierter Baustein NET.bd.x: SINA Management https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Benutzerdefinierte_BS/SinaManagement.html?nn=943082

Referenz	Dokument / Link / Quelle
[VSA]	<p>Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA) vom 13. März 2023.</p> <p>https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Geheim-schutz/Geheimschutzberatung/VorschriftenStandards/vorschriftenstandards_node.html</p>
[GSH]	<p>GeheimSchutzhandbuch, Stand: 23.08.2017</p> <p>https://www.bmwk-sicherheitsforum.de/handbuch/text/</p>
SINA	<p>Einsatz- und Betriebsbedingungen SINA Box</p> <p>https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Zulas-sung/Liste-zugelassener-Produkte/liste-zugelassener-produkte_node.html</p> <p>Bereitstellung erfolgt über das ITZBund.</p>
[ISR TLP]	<p>https://prod.office.bva.in.bund.de/cocoon/portal/portallink?doctype=Navknoten&id=16361</p>

Tabelle 2: Referenzierte Dokumente

6.3. Referenzen aus den Einzelanforderungen

Nr.	Anforderung aus ISR	Quelle
Ref1	SWE-DL.01 Anforderungen an den Empfang, die Lagerung und den Weiter-/Rücktransport von SINA Boxen	Aus [SINA]: „Vom Empfänger der Sendung ist die Unversehrtheit der Verpackung sowie des Gerätes (Gerätesiegelbruch) zu prüfen. (...) Bei Lagerung und beim Transport und Versand ist die SINA L2 Box H gegen unautorisierten Zugriff zu schützen, um eine Verletzung der Integrität von SINA L2 Box H zu verhindern. (...) Vor dem Versand der Geräte an den Hersteller sind vom Nutzer folgende Maßnahmen zu ergreifen: • Löschen der sicherheitskritischen Parameter (z.B. der Geräteklassen) • Entfernen aller für den Betrieb des Geräts erforderlichen Smartcards“
Ref 2	SWE-DL.02 Regelmäßige Durchführung von Sichtprüfungen der SINA Boxen und Meldung vermuteter Manipulationen	Aus [SINA]: „Die SINA L2 Box H ist in regelmäßigen Intervallen, die ein Jahr nicht überschreiten sollten, einer Sichtprüfung zu unterziehen. Jede vermutete Manipulation oder externe Beschädigung ist unverzüglich dem zuständigen IT-Sicherheitsbeauftragten zu melden (...) Die SINA L2 Box H darf ausschließlich vom Hersteller zum Zwecke der Wartung / Reparatur / Instandsetzung geöffnet werden.“
Ref 3	SWE-DL.03 Betrieb der SINA Boxen in Deutschland	Aus [VSA] § 34 Weitergabe von deutschen Verschlusssachen an nichtdeutsche Stellen und nichtöffentliche Stellen mit Sitz im Ausland (1) Die Weitergabe von deutschen Verschlusssachen an Dienststellen ausländischer Staaten sowie über- oder zwischenstaatlicher Organisationen (nichtdeutsche Stellen) setzt ein Regierungs- oder Ressortgeheimschutzabkommen oder ein entsprechendes internationales Abkommen voraus, welches die Bedingungen für die Weitergabe und weitere Handhabung regelt. Die Weitergabe von Verschlusssachen an nichtöffentliche Stellen mit Sitz im Ausland setzt entsprechende Regelungen in einem solchen Abkommen voraus.

_ Ref 4_	SWE-DL.04 Räumliche Sicherheit des Betriebsorts der SINA Boxen bei den SWE-DL	<p>Aus [BSI-GSK, INF.2.A13 Planung und Installation von Gefahrenmeldeanlagen (S)]: „Basierend auf dem Sicherheitskonzept des Gebäudes SOLLTE geplant werden, welche Gefahrenmeldeanlagen für welche Bereiche des Rechenzentrums benötigt und installiert werden. (...) Es SOLLTE eine zum jeweiligen Einsatzzweck passende Gefahrenmeldeanlage (GMA) installiert werden. Die Meldungen der GMA SOLLTEN unter Beachtung der dafür geltenden Technischen Anschlussbedingungen (TAB) auf eine Alarmempfangsstelle aufgeschaltet werden. Die ausgewählte Alarmempfangsstelle MUSS jederzeit erreichbar sein. Sie MUSS technisch sowie personell in der Lage sein, geeignet auf die gemeldete Gefährdung zu reagieren.“</p> <p>Aus [BSI-GSK, INF.5.A4 Schutz vor Einbruch]: „Der Raum MUSS vor Einbruch geschützt werden. Je nach erforderlichem Sicherheitsniveau des Raumes für technische Infrastruktur SOLLTEN geeignete raumbildende Teile wie Wände, Decken und Böden sowie Fenster und Türen mit entsprechenden Widerstandsklassen nach DIN EN 1627 ausgewählt werden.“</p> <p>Aus [BSI-GSK, INF.2.A7 Verschließen und Sichern (B)]: „Türen und Fenster MÜSSEN einen dem Sicherheitsniveau angemessenen Schutz gegen Angriffe und Umgebungseinflüsse bieten. (...)“</p> <p>Aus [SINA, 6.2 Anforderungen an die Materielle Sicherheit]: „Im Betrieb ist die SINA L2 Box H gegen unautorisierten Zugriff zu schützen, um einen Missbrauch und eine dadurch verursachte Kompromittierung der Vertraulichkeit oder eine Verletzung der Integrität oder der Authentizität geschützter Informationen zu verhindern. Dies wird in der Regel durch Lagerung, Installation und Betrieb in einem VS-Sicherheitsbereich, einem VS-Verwahrgeass, einem ähnlich gesicherten Behältnis oder Raum sichergestellt werden, zu denen ausschließlich autorisiertes, überprüftes und ermächtigt Personal Zugang hat.“</p> <p>Aus [BSI-MST, NdB.A1.0.0.06]: „Der Nutzer MUSS die Hülle des Technikraumes oder den Sicherheitsbereich, in dem sich der Technikraum befindet, in RC4-Qualität ausbilden. Der Nutzer KANN abweichend die Widerstandsklasse RC3 ausbilden, wenn nachhaltig und dokumentiert folgende Anforderungen erfüllt sind: (...). Der Nutzer MUSS sämtliche Türen und Fenster des Technikraumes durch eine Einbruchmeldeanlage (EMA) auf Öffnung, Verriegelung und Durchbruch überwachen.“</p>
----------	---	---

Nr.	Anforderung aus ISR	Quelle
_ Ref 5_	SWE-DL.05 Zutrittsschutz zum Betriebsort der SINA-Box beim SWE-DL	<p>Aus [BSI-GSK, INF.2.A6 Zutrittskontrolle (B)]: „Der Zutritt zum Rechenzentrum MUSS kontrolliert werden. Zutrittsrechte MÜSSEN gemäß der Vorgaben des Bausteins ORP.4 Identitäts- und Berechtigungsmanagement vergeben werden. Für im Rechenzentrum tätige Personen MUSS sichergestellt werden, dass diese keinen Zutritt zu IT-Systemen außerhalb ihres Tätigkeitsbereiches erhalten. (...)“</p> <p>Alle Zutrittsmöglichkeiten zum Rechenzentrum MÜSSEN mit Zutrittskontrollereinrichtungen ausgestattet sein. Jeder Zutritt zum Rechenzentrum MUSS von der Zutrittskontrolle individuell erfasst werden. Im Falle eines Serverraums SOLLTE geprüft werden, ob eine Überwachung aller Zutrittsmöglichkeiten sinnvoll ist.“</p> <p>Aus [BSI-GSK, INF.5.A3 Zutrittsregelung und -kontrolle]</p> <p>Aus [BSI-GSK, OPS.3.2.A17 Zutritts-, Zugangs- und Zugriffskontrolle]</p> <p>Aus [SINA, 7.3 Kenntnis nur, wenn nötig (Need-To-Know)]: „Der Zugang zu SINA L2 Box H ist gemäß dem Prinzip „Kenntnis nur, wenn nötig (Need-To-Know)“ zu begrenzen.“</p>

Nr.	Anforderung aus ISR	Quelle
_ Ref 6 _	SWE-DL.06 Netztrennung beim SWE-DL	<p>Aus [BSI-GSK, NET.1.1.A4 Netztrennung in Zonen]</p> <p>Aus [BSI-GSK, NET.1.1.A9 Grundlegende Absicherung der Kommunikation mit nicht vertrauenswürdigen Netzen]</p> <p>Aus [BSI-GSK, NET.1.1.A10 DMZ-Segmentierung für Zugriffe aus dem Internet]</p> <p>Aus [BSI-GSK, NET.1.1.A12 Absicherung ausgehender interner Kommunikation zum Internet]</p> <p>Aus [BSI-GSK, NET.1.1.A24 Sichere logische Trennung mittels VLAN]</p> <p>Aus [BSI-GSK, NET.1.1.A31 Physische Trennung von Netzsegmenten]: „Abhängig von Sicherheitsrichtlinie und Anforderungsspezifikation SOLLTEN Netzsegmente physisch durch separate Switches getrennt werden.“</p> <p>Aus [Handreichung des ITZBund: 4.1 Netztrennung]: „Das Netz auf Nutzerseite, aus dem die Zugriffe in die Netzinfrastruktur des BVA und das ITZBund RZ Köln erfolgen, ist von anderen beim Nutzer anliegenden Netzen, zum Beispiel dem produktiven, internen Netz des Nutzers, dem Internet, evtl. vorhandenen DMZ, etc. zu trennen. Dies kann durch physische Netztrennung oder Sicherheitsgateways realisiert werden.“</p>
_ Ref 7 _	SWE-DL.07 Keine Nutzung der Entwicklungs-Arbeitsplätze für SWE anderer Kunden	<p>Aus [BSI-GSK, NET.3.3.A11 Sichere Anbindung eines externen Netzes (S)]: Es SOLLTE sichergestellt werden, dass VPN-Verbindungen NUR zwischen den dafür vorgesehenen IT-Systemen und Diensten aufgebaut werden.</p> <p>Aus [BSI-GSK, OPS.3.2.A4 Erstellung eines Mandantentrennungskonzepts]</p>

Nr.	Anforderung aus ISR	Quelle
_ Ref 8_	SWE-DL.08 Trennung der Entwicklung für das BVA von der Entwicklung für andere Kunden	<p>Aus [BSI-GSK, NET.3.3.A11 Sichere Anbindung eines externen Netzes (S)]: Es SOLLTE sichergestellt werden, dass VPN-Verbindungen NUR zwischen den dafür vorgesehenen IT-Systemen und Diensten aufgebaut werden.</p> <p>Aus [BSI-VPN, Kapitel 2.2.3 LAN-LAN]: „Für die Realisierung einer LAN-LAN-Anbindung existieren die folgenden Rahmenbedingungen:</p> <p>Bei einer LAN-LAN-Verbindung sind grundsätzlich alle Systeme der verbundenen Netze erreichbar. Es ist sicherzustellen, dass Client-Systeme nur Verbindungen mit internen Systemen initiieren können, die für die durchzuführenden Tätigkeiten erforderlich sind.“</p>
_ Ref 10_	SWE-DL.09 Identitäts- und Berechtigungsmanagement für SWE-Umgebung beim SWE-DL	Aus [BSI-GSK, ORP.4.A1 Regelung für die Einrichtung und Löschung von Benutzenden und Benutzendengruppen (B)]
_ Ref 11_	SWE-DL.10 Sichere Authentisierung an den Entwicklungs-Arbeitsplätzen	<p>Aus [BSI-GSK, SYS.2.1.A1 Sichere Authentisierung von Benutzenden (B)]: „Um den Client zu nutzen, MÜSSEN sich die Benutzenden gegenüber dem IT-System authentisieren. Benutzende MÜSSEN eine Bildschirmsperre verwenden, wenn sie den Client unbeaufsichtigt betreiben. Die Bildschirmsperre SOLLTE automatisch aktiviert werden, wenn für eine festgelegte Zeitspanne keine Aktion durch Benutzende durchgeführt wurde. Die Bildschirmsperre DARF NUR durch eine erfolgreiche Authentisierung wieder deaktiviert werden können. Benutzende SOLLTEN verpflichtet werden, sich nach Aufgabenerfüllung vom IT-System bzw. von der IT-Anwendung abzumelden.“</p> <p>Aus [BSI-GSK, SYS.2.1.A37 Verwendung von Mehr-Faktor-Authentisierung (H)]: „Es SOLLTE eine sichere Mehr-Faktor-Authentisierung unter Einbeziehung unterschiedlicher Faktoren (Wissen, Besitz, Eigenschaft) für die lokale Anmeldung am Client eingerichtet werden, z. B. Passwort mit Chipkarte oder Token.“</p>

Nr.	Anforderung aus ISR	Quelle
_ Ref 12_	SWE-DL.11 Schutz der Entwicklungs-Arbeitsplätze mit Zugriff auf das FFE/ZSSI-Netzwerk beim BVA	<p>Aus [BSI-GSK, SYS.2.1.A42 Nutzung von Cloud- und Online-Funktionen (B)]: „Es DÜRFEN NUR zwingend notwendige Cloud- und Online-Funktionen des Betriebssystems genutzt werden.“</p> <p>Aus [BSI-GSK, SYS.2.1.A24 Umgang mit externen Medien und Wechseldatenträgern (S)]: „Auf externe Schnittstellen SOLLTE nur restriktiv zugegriffen werden können. Es SOLLTE untersagt werden, dass nicht zugelassene Geräte oder Wechseldatenträger mit den Clients verbunden werden. Es SOLLTE verhindert werden, dass von den Clients auf Wechseldatenträger aus nicht vertrauenswürdigen Quellen zugegriffen werden kann. Die unerlaubte Ausführung von Programmen auf bzw. von externen Datenträgern SOLLTE technisch unterbunden werden. Es SOLLTE verhindert werden, dass über Wechsellaufwerke oder externe Schnittstellen unberechtigt Daten von den Clients kopiert werden können.“</p> <p>Aus [BSI-GSK, SYS.2.1.A28 Verschlüsselung der Clients (H)]: „Wenn vertrauliche Informationen auf den Clients gespeichert werden, SOLLTEN mindestens die schutzbedürftigen Dateien sowie ausgewählte Dateisystembereiche oder besser die gesamten Datenträger verschlüsselt werden. (...)“</p> <p>Aus [Warnung des BSI „Cyberangriffe auf IT-Dienstleister und Hochwertziele aus Verwaltung und Wirtschaft - Angriffe über Confluence- und Jira-Systeme“, CSW-Nr. 2023-231459-12C7, Version 1.2, 28.05.202]: „Verpflichten Sie Ihre externen Partner für die Umsetzung von grundlegenden Sicherheitsmaßnahmen auf den zugreifenden Clients.“</p>

Nr.	Anforderung aus ISR	Quelle
_ Ref 13_	SWE-DL.12 Schutz der IT-Systeme (SWE-Werkzeuge) mit Zugriff auf das FFE/ZSSI-Netzwerk beim BVA	<p>Aus [BSI-GSK, SYS.1.1.A19 Einrichtung lokaler Paketfilter]</p> <p>Aus [BSI-GSK, SYS.1.1.A24 Sicherheitsprüfungen für Server (S)]</p> <p>Aus [BSI-GSK, SYS.2.1.A3 Aktivieren von Autoupdate-Mechanismen (B): „Automatische Update-Mechanismen (Autoupdate) MÜSSEN aktiviert werden, sofern nicht andere Mechanismen wie regelmäßige manuelle Wartung oder ein zentrales Softwareverteilungssystem für Updates eingesetzt werden.</p> <p>Aus [BSI-GSK, SYS.2.1.A15 Sichere Installation und Konfiguration von Clients (S)]: „Die Installation und Konfiguration der IT-Systeme SOLLTE nur von autorisierten Personen (Administrierende oder vertraglich gebundene Dienstleistende) nach einem definierten Prozess in einer Installationsumgebung durchgeführt werden.“</p>
_ Ref 14_	SWE-DL.13 Einsatz von Schutzprogrammen gegen Schadsoftware	<p>Aus [BSI-GSK, SYS.1.1.A9 Einsatz von Virenschutz-Programmen auf Servern (B)]</p> <p>Aus [BSI-GSK, SYS.2.1.A6 Einsatz von Schutzprogrammen gegen Schadsoftware (B)]</p>
_ Ref 15_	SWE-DL.14 Erstellen eines Sicherheitskonzeptes zum Schutz des Entwicklungsnetzes und der SINA Boxen beim SWE-DL	<p>Aus [BSI-GSK, OPS.3.2.A1 Einhaltung der Schutzziele der Informationssicherheit durch ein Informationssicherheitsmanagement]</p> <p>Aus [BSI-GSK, OPS.3.2.A5 Erstellung eines Sicherheitskonzepts für die Outsourcing-Dienstleistung]</p>
_ Ref 16_	SWE-DL.15 Einhalten der Vorgaben der VSA inklusive VS-NfD-Merkblatt	<p>Aus [VSA, Anlage V zur VSA: Merkblatt zur Behandlung von Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD-Merkblatt)]</p> <p>Aus [Nutzungsrichtlinien Fremdfirmeneinwahl Bundesverwaltungsamt, Version 1.2 vom 06.06.2019 (ITZ-Bund_Nutzungsrichtlinien_FFE_v12.pdf)]</p>

Nr.	Anforderung aus ISR	Quelle
_ Ref 17 _	SWE-DL.16 Benachrichtigung der/des ISB des BVA bei Sicherheitsvorfällen	<p>Aus [BSI-GSK, DER.2.1.A4 Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen (B)]; Von einem Sicherheitsvorfall MÜSSEN alle betroffenen internen und externen Stellen zeitnah informiert werden. Dabei MUSS geprüft werden, ob der oder die Datenschutzbeauftragte, der Betriebs- und Personalrat sowie Mitarbeitende aus der Rechtsabteilung einbezogen werden müssen. Ebenso MÜSSEN die Meldepflichten für Behörden und regulierte Branchen berücksichtigt werden. Außerdem MUSS gewährleistet sein, dass betroffene Stellen über die erforderlichen Maßnahmen informiert werden.</p> <p>Aus [BSI-GSK, DER.2.1.A9 Festlegung von Meldewegen für Sicherheitsvorfälle (S)]</p> <p>Aus [BSI-GSK, OPS.3.2.A13 Anbindung an die Netze der Outsourcing-Partner]: „Gibt es Sicherheitsprobleme auf einer der beiden Seiten, SOLLTE festgelegt sein, wer informiert und wie eskaliert wird.“</p> <p>Aus [Warnung des BSI „Cyberangriffe auf IT-Dienstleister und Hochwertziele aus Verwaltung und Wirtschaft - Angriffe über Confluence- und Jira-Systeme“, CSW-Nr. 2023-231459-12C7, Version 1.2, 28.05.202]: „Verpflichten Sie externe Partner mit Zugriff auf Ihre Systeme vertraglich dazu, eigene Vorfälle schnell und transparent an Sie, Ihren etwaig hinzugezogenen APT-Response-Dienstleister und das BSI zu kommunizieren. Hierbei sind im Besonderen Partner zu berücksichtigen, welche hohe administrative Rechte benötigen.“</p>
_ Ref 18 _	SWE-DL.17 Eindämmen der Auswirkung von Sicherheitsvorfällen	<p>Aus [BSI-GSK, DER.2.1.A10 Eindämmen der Auswirkung von Sicherheitsvorfällen (S)]: „Parallel zur Ursachenanalyse eines Sicherheitsvorfalls SOLLTE entschieden werden, ob es wichtiger ist, den entstandenen Schaden einzudämmen oder den Vorfall aufzuklären. Um die Auswirkung eines Sicherheitsvorfalls abschätzen zu können, SOLLTEN ausreichend Informationen vorliegen. Für ausgewählte Sicherheitsvorfallszenarien SOLLTEN bereits im Vorfeld Worst-Case-Betrachtungen durchgeführt werden.“</p> <p>Aus [BSI-GSK, DER.1.A17 Automatische Reaktion auf sicherheitsrelevante Ereignisse]</p>

Nr.	Anforderung aus ISR	Quelle
_ Ref 19_	SWE-DL.18 Mitwirkung bei IT-forensischen Untersuchungen des BVA und des BSI	Aus [Warnung des BSI „Cyberangriffe auf IT-Dienstleister und Hochwertziele aus Verwaltung und Wirtschaft - Angriffe über Confluence- und Jira-Systeme“, CSW-Nr. 2023-231459-12C7, Version 1.2, 28.05.202]: „Die entsprechenden Systeme sollten mit den vom BSI übermittelten Indicators of Compromise - IoCs (IPAdressen, YARA-, und SNORT-Signaturen) überprüft werden.“
_ Ref 21_	SWE-DL.20 Weitergabe der Anforderungen an Sub-Dienstleistende	Aus [BSI-GSK, OPS.3.2.A3 Weitergabe der vertraglich geregelten Bestimmungen mit Nutzenden von Outsourcing an Sub-Dienstleistende]
_ Ref 22_	SWE-DL.21 Dokumentation des Netzes	Aus [BSI-GSK, NET.1.1.A2 Dokumentation des Netzes] Aus [BSI-GSK, NET.1.1.A22 Spezifikation des Segmentierungskonzepts]
_ Ref 20_	SWE-DL.19 Erreichbarkeit für zeitnahe Reaktion auf Sicherheitsvorfälle	Aus [BSI-GSK, DER.2.1.A9 Festlegung von Meldewegen für Sicherheitsvorfälle]
_ Ref 23_	SWE-DL.22 Einräumen von Kontrollrechten zur Überprüfung der Einhaltung der Nutzungsrichtlinie	Aus [BSI-GSK, OPS.3.2.A2 Grundanforderungen an Verträge mit Nutzenden von Outsourcing]: „Einheitliche Grundanforderungen an Outsourcing-Verträge MÜSSEN entwickelt werden. (...)Die Grundanforderungen MÜSSEN beinhalten, dass die Nutzenden das Recht haben Prüfungen, Revisionen und Auditierungen durchzuführen, um sicherzustellen, dass die vertraglich geregelten Anforderungen an die Informationssicherheit eingehalten werden.“

Tabelle 3: Quellen der Anforderungen