Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Interne Revision VBS

22. Dezember 2021 [redacted]

Prüfbericht «Einhaltung Grundschutz Bund bei externen IT-Partnern: Domotiksysteme»

IT-Prüfung I 2021-06

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Interne Revision VBS

Frau
Bundesrätin Viola Amherd
Chefin VBS
Bundeshaus Ost
3003 Bern

Bern, 22. Dezember 2021

Prüfbericht «Einhaltung Grundschutz Bund bei externen IT-Partnern: Domotiksysteme»

Sehr geehrte Frau Bundesrätin Amherd

Gerne lassen wir Ihnen unseren Prüfbericht «Einhaltung Grundschutz Bund bei externen IT-Partnern: Domotiksysteme» zukommen. Unsere Prüfarbeiten bezüglich der Domotiksysteme fanden zwischen August und Oktober 2021 bei der Firma RUAG Real Estate AG in Bern und Thun statt. Den vorliegenden Bericht haben wir mit unseren Ansprechpartnern in der Gruppe Verteidigung sowie der armasuisse besprochen und den Verantwortlichen der RUAG Real Estate AG abgestimmt. Die Stellungnahmen zu diesem Bericht sind in Kapitel 8 ersichtlich.

Diese Prüfung wurde in Übereinstimmung mit den internationalen Standards für die berufliche Praxis der internen Revision durchgeführt.

Sollten Sie Fragen zu unserem Bericht haben, stehen wir Ihnen gerne zur Verfügung.

Freundliche Grüsse

Interne Revision VBS

[redacted]

Verteiler
- Generalsekretär VBS
- Chef der Armee
- Chef Armeestab
- Rüstungschef
- RUAG Real Estate AG

Interne Revision VBS
Schauplatzgasse 11
3003 Bern

1 Einleitung / Kurzüberblick

IKT-Grundschutz in der Bundesverwaltung[1]

Informatiksicherheit ist für alle Verwaltungseinheiten (VE) der Bundesverwaltung (BV) unverzichtbar. Durch den laufenden Ausbau der digitalen Vernetzung und die Anwendung von neuen virtuellen Konzepten (z. B. das Cloud-Computing) nehmen die Risiken und Bedrohungen aus der Cyberwelt immer mehr zu. Daher kommt dem Schutz der Informatikinfrastruktur eine besondere Bedeutung zu.

Um diesen Sicherheitsanforderungen nachzukommen, hat das Nationale Zentrum für Cybersicherheit (NCSC) die minimalen Sicherheitsvorgaben im Bereich Informatiksicherheit verbindlich festgelegt.[2] Diese Vorgaben sind im Dokument «IKT-Grundschutz in der Bundesverwaltung» (kurz: Grundschutz Bund) festgehalten.[3] Dieser Grundschutz Bund ist ein Tailoring des Standards ISO/IEC 27002:2013, erweitert mit spezifischen Massnahmen der Bundesverwaltung. Die Umsetzung der Sicherheitsvorgaben und -massnahmen sind durch die verpflichtete VE zu dokumentieren und zu überprüfen.[4]

Da verschiedene VE im VBS Informatiksysteme mit Unterstützung von externen Dienstleistern aufbauen und betreiben, gelten die Sicherheitsvorgaben des Grundschutzes Bund auch bei diesen Partnern.

Intelligente Gebäudetechnik – Ein Kurzüberblick

Die intelligente und vernetzte Gebäudetechnik (auch als Domotik bezeichnet) hat in Geschäfts- und Arbeitsräumen Einzug gehalten. Heute werden mittels intelligenter Technologie verschiedenste Gebäudefunktionen über das Netzwerk gesteuert und zentral überwacht. Neben Heizung, Lüftung und Klimatechnik gehören auch die Zutrittskontrolle sowie die Raum- und Aussenbereichsüberwachung zur Domotik.

Diese Technologien bergen jedoch nicht unerhebliche Cyberrisiken in sich. Verwaltungsgebäude mit erhöhten Schutzbedürfnissen, wie zum Beispiel die Infrastruktur der Armee, müssen mit adäquaten Sicherheitsmassnahmen versehen werden. Sollte es unbefugten Dritten gelingen, sich virtuellen Zutritt zur vernetzten Gebäudetechnik zu verschaffen, eröffnet dies ihnen eine Vielzahl von Angriffsmöglichkeiten. Denn Gebäudetechnologien sind mit dem IT-Netzwerk verbunden. Auf diesem Wege bieten Domotiksysteme Angreifern eine Vielzahl von

1 Nationales Zentrum für Cybersicherheit (NCSC) - IKT-Grundschutz in der Bundesverwaltung: Grundschutz (admin.ch) (22.12.2021)

2 SR **120.73** - Verordnung vom 27. Mai 2020 über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV) (admin.ch) (22.12.2021)

3 Nationales Zentrum für Cybersicherheit (NCSC) - IKT-Grundschutz in der Bundesverwaltung: Grundschutz (admin.ch) (22.12.2021)

4 BBl **2019 1303** - Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung (admin.ch), Ziff. 2.2 Abs. 2, Ziff. 2.3 Abs. 2 und Ziff. 3.2 Abs. 3 (22.12.2021)

Einstiegsmöglichkeiten, um Schaden anzurichten. Daher muss die Sicherheit jedes einzelnen internetfähigen Gerätes, sei es die Gebäudeleittechnik mit den dazugehörigen Systemen zur Steuerung von Heizung, Lüftung, Klima, Elektroanlagen oder Zutrittskontrollsysteme sowie generell die Sicherheitssysteme, auf dessen Relevanz analysiert werden.

2 Auftrag, Methodik und Abgrenzung

Die Chefin VBS beauftragte am 25. Januar 2021 die Interne Revision VBS bei ausgewählten externen Dienstleistern zu prüfen, ob die einschlägigen Sicherheitsbestimmungen der BV eingehalten werden. Für die Auswahl dieser Prüfungen wählten wir ein risikoorientiertes Vorgehen und fokussierten uns auf relevante Informatiksysteme, welche von externen Partnern entwickelt oder betrieben werden. Das Auswahlverfahren stimmten wir mit unseren Ansprechpersonen in den Departementsbereichen ab. Ebenfalls wurde die Abteilung Digitalisierung und Cybersicherheit VBS in unsere Planungsarbeiten miteinbezogen. Dabei führten wir auch eine umfassende Dokumentenanalyse (z. B. Verträge und Auditberichte) durch.

Im Rahmen dieses Prüfauftrags beurteilten wir die Einhaltung des Grundschutzes Bund bei der Bewirtschaftung der Domotiksysteme an zwei Standorten in Bern und Thun. An beiden Standorten vermietet die RUAG Real Estate AG (nachfolgend RUAG RE) Immobilien an die Gruppe Verteidigung (Gruppe V). Die Prüfung umfasste die RUAG als Leistungserbringerin, die Gruppe V als Leistungsbezügerin und armasuisse als Beschaffungsstelle, wobei nur die Umsetzung des Grundschutzes Bund im Verantwortungsbereich von RUAG RE geprüft wurde.

In einem ersten Schritt liessen wir RUAG RE die Umsetzung des Grundschutzes Bund in Bezug auf die Domotiksysteme an den Standorten in Bern und Thun im Rahmen einer Selbsteinschätzung beurteilen.

Anschliessend erfolgte eine Beurteilung durch Dokumentenanalyse sowie durch strukturierte Befragungen der Schlüsselpersonen, stichprobenweise Einsicht in die Systeme und durch eine Begehung der Immobilien vor Ort. Unsere Ergebnisse spiegelten wir im Anschluss mit RUAG RE, der Gruppe V sowie der armasuisse.

Diese Prüfung hat ausschliesslich die Einhaltung der Vorgaben des Grundschutzes Bund bei den eingesetzten Domotiksystemen zum Gegenstand. Das Vergabeverfahren, welches zum Vertragsverhältnis führte und Domotiksysteme an weiteren Standorten waren nicht Teil unserer Prüfung.

3 Würdigung

Während unserer Prüfung trafen wir bei RUAG RE, der Gruppe V und der armasuisse ausnahmslos auf engagierte Ansprechpersonen, die uns unterstützt und Informationen transparent zur Verfügung gestellt haben. Zudem gewannen wir den Eindruck, dass all unseren Ansprechpersonen die Umsetzung der Anforderungen aus dem Grundschutz Bund ein wichtiges Anliegen ist und der sichere Betrieb der Domotiksysteme bei allen Fachexperten eine hohe Bedeutung hat. Wir bedanken uns bei allen Beteiligten für die zielführende Zusammenarbeit während der Prüfung.

4 RUAG Real Estate AG

RUAG Real Estate AG wurde im Jahre 2009 als privatrechtliche Aktiengesellschaft (AG) gegründet. Die Sparte Immobilien bietet Mieterinnen und Mietern an 15 Standorten in der Schweiz massgeschneiderte Immobilienlösungen und -services an.

Die Sparte Immobilien beschäftigt über 100 Mitarbeiterinnen und Mitarbeiter. Bei den von RUAG RE vermieteten Immobilien werden die Räume nach den Bedürfnissen der Mieter ausgestaltet und zur Nutzung überlassen. Als Eigentümerin von insgesamt fünf Industrie- und Businessarealen in der ganzen Schweiz werden neben der Immobilienbewirtschaftung u. a. auch Baudienstleistungen und ein Facility Management angeboten.[5]

Basierend auf dem Bundesratsentscheid vom 27. Juni 2018 wurde RUAG in zwei Einheiten aufgespalten, die vom Bund über eine Beteiligungsgesellschaft (BGRB Holding AG) gehalten werden. Die RUAG MRO Holding AG (nachfolgend RUAG MRO) erbringt in erster Linie Leistungen für die Schweizer Armee. Die RUAG International Holding AG (nachfolgend RUAG International) hat die Geschäftstätigkeit im Raumfahrtbereich übernommen.

Durch die Aufspaltung in die RUAG MRO und RUAG International befindet sich die RUAG RE in einem Entflechtungsprozess. Die Umstellungen im Netzbereich der Domotik wurden im September 2021 abgeschlossen und die IT-Infrastruktur wird seither vollständig in den Räumlichkeiten von und durch RUAG RE betrieben. Einige Prozesse und Dokumente müssen in Folge der Entflechtung noch erstellt bzw. überarbeitet werden, um das neue IT-Umfeld abzubilden.

[5] RUAG Real Estate - Unternehmensbroschüre: Übersicht zum Unternehmen RUAG Real Estate AG | RUAG (22.12.2021)

5 Domotiksysteme im Einsatz

Im Rahmen unserer Prüfhandlungen wurden für die beiden Standorte in Bern und Thun folgende Domotiksysteme identifiziert, welche durch die RUAG RE bewirtschaftet werden:

Systeme / Standorte	Bern (G37)	Thun (G655)
Gebäude-/ Sicherheitsleitsystem (GLS / SLS)	Ja	Nein
Zutrittssysteme (SAC)	Ja	Ja
Brandmeldeanlage (BMA)	Ja (*)	Ja (*)
Heizung, Lüftung, Klima (HLK)	Ja	Nein
(*) = durch externe Sicherheitsspezialisten bewirtschaftet		

Das **GLS / SLS Gebäude-/ Sicherheitsleitsystem** am Standort in Bern wurde bis September 2021 in einem logischen Netzwerk im Verbund von RUAG International, losgelöst von Arbeitsrechnern, betrieben. Seit Oktober 2021 befindet sich dieses im entflochtenen Netzwerk der RUAG RE. Das Leitsystem am Standort Bern wird aktuell lediglich für die Visualisierung von Informationen zu Heizung, Lüftung, Klima eingesetzt, wobei letztere aufgrund des Gebäudeausbaus resp. der -verwendung nicht zum Einsatz kommen.

Das **Zutrittssystem (SAC)** wurde an beiden Standorten bis September 2021 von RUAG International auf dem GLS-Netzwerk, losgelöst von Arbeitsrechnern, bewirtschaftet und gemäss Vorgaben der Nutzerinnen und Nutzer mit den entsprechenden Berechtigungen aufgesetzt. Seit Oktober 2021 befindet sich dieses im entflochtenen Netzwerk der RUAG RE.

Die **Brandmeldeanlagen (BMA)** an beiden Standorten sind mit der Leitzentrale (Loge) der jeweiligen Areale verbunden. Sensoren detektieren in den Gebäuden und melden allfällige Brände an die Einsatzkräfte vor Ort. Diese BMA kann durch RUAG RE nicht gesteuert werden und wird vollständig durch externe Sicherheitsspezialisten bewirtschaftet.

Die **Heizung, Lüftung, Klima (HLK)** werden mittels manuellen Einstellungen (d. h. Steuerung der Ventile) direkt in den geprüften Gebäuden kontrolliert. Die HLK kann in diesem Fall nicht zentral von aussen gesteuert werden, der Zugriff beschränkt sich via Gebäudeleitsystem auf die Visualisierung der Raumtemperatur.

Die Hardware für weitere Domotiksysteme, z. B. die **Einbruchmeldeanlagen (EMA)**, die **Gegensprechanlagen (GSA)** oder die **Videoüberwachung (CCTV)** wird an den beiden Standorten (sofern eingesetzt) durch RUAG RE zur Verfügung gestellt. Für den vollständigen Unterhalt und Betrieb dieser Systeme zeichnet sich jedoch der Mieter verantwortlich.

6 Feststellungen und Beurteilung

Unsere Prüfung ergab, dass teilweise Grundlagen, die zum zielführenden und sicheren Betrieb von Domotiksystemen benötigt werden, noch nicht vollständig erarbeitet wurden.

6.1 Domotikstrategie ausarbeiten und Domotiksysteme inventarisieren

Feststellung: Die RUAG RE hat keine formalisierte übergreifende Domotikstrategie, die als Basis für die eingesetzten Systeme dient. Eine solche Strategie soll den Ansprüchen des Leistungsbezügers an die Sicherheit und Funktionalität sowie den Betrieb und die Standardisierung genügen. Gleichzeitig werden damit auch die betriebswirtschaftlichen Interessen der RUAG RE abgedeckt. Zudem haben wir festgestellt, dass keine zentral geführte Übersicht bezüglich der eingesetzten Domotiksysteme existiert und ein solches Inventar im Rahmen der Entflechtung noch nicht aufgesetzt resp. aktualisiert wurde. Dies gilt sowohl für Netzwerk- als auch für Softwarekomponenten.

Beurteilung: Unsere Prüfung ergab, dass im Bereich Strategie der Domotiksysteme noch Handlungsbedarf besteht. Für einen sicheren Einsatz von Domotiksystemen, unter Einhaltung des Grundschutzes Bund, erachten wir eine übergreifende Domotikstrategie als zentral. Weiter vertreten wir die Haltung, dass ein vollständiges Domotikinventar für eine zielführende Bewirtschaftung der Gebäudetechnik unumgänglich ist.

6.2 Prozesse unvollständig dokumentiert bzw. im Aufbau

Feststellung: Die Ausgestaltung sowie Umsetzung der Prozesse zur vollständigen Adressierung der Anforderungen des Grundschutzes Bund für die aktuell eingesetzten Domotiksysteme sind teilweise noch lückenhaft. Einige Prozesse sind erst im Aufbau oder müssen noch an die Bedürfnisse des neuen Kontrollumfelds nach der Entflechtung angepasst werden. Wir zählen hierzu die wesentlichen Prozesse und Kontrollbereiche mit Bezug auf die Domotiksysteme auf:

1) **Berechtigungs- und Änderungswesen:** Die aktuellen Prozesse des Berechtigungswesens basieren z. T. noch auf Vorschriften (u. a. Konzernregelungen) vor der Entflechtung. Diese werden noch überarbeitet und der neuen Situation entsprechend umgesetzt. Des Weiteren wird die Dokumentation mit den Prozessschritten für den neuen Änderungsprozess erst noch ausgearbeitet und formalisiert.
2) **Netzwerkarchitektur und Systemüberwachung**: Die Umsetzung der geplanten System-/Netzwerkarchitektur wurde per Ende September 2021 vollständig abgeschlossen. Die entsprechenden Netzwerkdokumentationen werden noch konsolidiert und finalisiert. Zudem befindet sich ein eigenes Security Operation Center zur Sicherstellung der Betriebssicherheit momentan im Aufbau.
3) **Business Continuity Management (BCM)**: Ein formell dokumentiertes BCM für die Domotiksysteme ist aktuell nicht vorhanden.

Beurteilung: Die Einhaltung des Grundschutzes Bund konnte aufgrund der unvollständigen Dokumentationen und der laufenden Arbeiten im Rahmen der Entflechtung nicht abschliessend beurteilt werden.

6.3 Life-Cycle-Management weiterentwickeln

Feststellung: Heute werden Gebäude und Anlagen nicht mehr einmalig dem Nutzenden übergeben. Sie verstehen sich als dynamische «Produkte». Die laufenden technologischen Herausforderungen, insbesondere im noch wenig gefestigtem Domotikumfeld, verlangen eine fortlaufende Risikobeurteilung und Weiterentwicklung bzw. Optimierung der Systeme. Für den zielführenden Betrieb der eingesetzten Systeme besteht noch kein übergeordnetes und formalisiertes Life-Cycle Management.

Beurteilung: Unsere Prüfung ergab im Bereich Life-Cycle Management, dass noch kein formalisierter Prozess vorhanden ist. Wir erachten es als elementar, dass die Herausforderungen im Umfeld der Domotiksysteme angesichts der Komplexität und veränderten Bedürfnissen strukturiert angegangen werden.

7 Empfehlungen

Aufgrund unsere Feststellungen empfehlen wir der Gruppe Verteidigung, zusammen mit den Verantwortlichen der RUAG Real Estate AG:

zu 6.1 eine Domotikstrategie für den zielführenden Betrieb auszuarbeiten und die Domotiksysteme zu inventarisieren.

zu 6.2 Prozesse für die Domotiksysteme zu erstellen bzw. an das neue IT-Umfeld anzupassen sowie die dazugehörigen Kontrollen zu definieren und anschliessend zu implementieren.

zu 6.3 ein formalisiertes Life-Cycle Management für die Domotiksysteme auszuarbeiten.

8 Stellungnahmen

armasuisse
armasuisse begrüsst den Bericht und hat dazu folgende Bemerkungen: Die zu erarbeitenden Strategien, Prozesse und Vorgaben müssen mit den bestehenden Vorgaben abgeglichen werden. Es sind dies insbesondere die Empfehlungen der KBOB[6] zur MSRL-Technik[7], die technischen Vorgaben MSRL von armasuisse Immobilien und die fachtechnischen Vorgaben der Führungsunterstützungsbasis (FUB) in diesem Bereich.

Gruppe Verteidigung
Die Gruppe Verteidigung trägt die drei genannten Empfehlungen mit und begrüsst eine rasche Umsetzung.

RUAG Real Estate AG
Der vorliegende Prüfbericht gibt einen guten und objektiven Einblick in die Domotiksysteme. Die erst kürzlich erfolgte IT-Entflechtung wurde in der Beurteilung berücksichtigt. Die Systeme im Bereich Zutritt sind gut dokumentiert und zentral geführt. Die anderen Systeme sind dezentral geführt und somit unterschiedlich dokumentiert. Mit der neuen IT-Umgebung wurde die Basis geschaffen, um die restlichen Systeme zu dokumentieren. Die Brandmelde- und Einbruchanlagen sind an den Standorten unterschiedlich ausgeführt (Konzept und Komponenten). Über die Zeit (Ende der Nutzungsdauer des Systems) ist eine Harmonisierung, sowohl bei den Systemlieferanten als auch bei den Wartungsverträgen anzustreben. Die Anlagen sind anders als bei üblichen IT-Komponenten sehr langlebig, weshalb die Umsetzung einige Zeit in Anspruch nehmen wird. Mittels Inventarisierung, Analyse und Bewertung der Domotiksysteme kann schrittweise die Domotikstrategie entwickelt und implementiert werden. **Aktionsplan**: zu 6.1 Domotikstrategie für den zielführenden Betrieb ausarbeiten und die Domotiksysteme inventarisieren: - Inventarisierung bis Ende Q2-2022 - Analyse der Systeme bis Ende Q2-2022 - Entwicklung der Domotikstrategie bis Ende Q3-2022 - Umsetzung der Domotikstrategie ab Q1-2023

[6] KBOB = Koordinationskonferenz der Bau- und Liegenschaftsorgane der öffentlichen Bauherren

[7] MSRL = Mess-, Steuer-, Regel- und Leittechnik

zu 6.2

Prozesse für die Domotiksysteme zu erstellen bzw. an das neue IT-Umfeld anzupassen sowie die dazugehörigen Kontrollen zu definieren und anschliessend zu implementieren:

- Aufbau Fachgruppe Leitsysteme (AVK) bis Ende Q1-2022
- Harmonisierung der Prozesse für Leitsysteme inkl. Berücksichtigung IT-Umfeld und Umsetzung der Kontrollen. bis Ende Q3-2022

zu 6.3

Ein formalisiertes Life-Cycle Management für die Domotiksysteme auszuarbeiten:

- Life Cycle Management der Leitsysteme ausarbeiten bis Ende Q3-2022