



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Interne Revision VBS

18. November 2020



Prüfbericht

«Bewirtschaftung von Domotiksystemen»

IT-Prüfung I 2020-05



Mitglied des Institute of
Internal Auditing Switzerland



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, 18. November 2020

Prüfbericht «Bewirtschaftung von Domotiksystemen»

Sehr geehrte Frau Bundesrätin

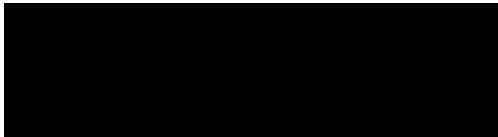
Gerne lassen wir Ihnen unseren Prüfbericht «Bewirtschaftung von Domotiksystemen» zu kommen. Unsere Prüfarbeiten fanden zwischen Juni und September 2020 statt. Das vorliegende Dokument haben wir mit unseren Ansprechpersonen abgestimmt. Die Stellungnahmen der Departementsbereiche zu unserem Bericht sind 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 jederzeit gerne zur Verfügung.

Freundliche Grüsse

Interne Revision VBS



Leiter Interne Revision VBS



Prüfleiter

Verteiler

- Generalsekretär VBS
- Chef der Armee
- Rüstungschef



1 Intelligente Gebäudetechnik: Ein Kurzüberblick

Die intelligente und vernetzte Gebäudetechnik (auch als **Domotik** bezeichnet) hat nicht nur in privaten Haushalten Einzug gehalten. Auch in Geschäfts- und Arbeitsräumen werden heute mittels intelligenter Technologie verschiedenste Gebäudefunktionen über Netzwerke gesteuert und zentral überwacht. Dabei wird oft der Begriff «Smart Building» verwendet. Darunter fallen z.B. Heizung, Lüftung, Klimatechnik sowie das effiziente Energiemanagement. Weiter gehören auch die Zutrittskontrolle sowie die Raum- und Aussenbereichsüberwachung zur Domotik. Immer mehr werden dabei auch mobile Datenübertragungen eingesetzt, um keine zusätzlichen und teuren Verkabelungen mehr einplanen zu müssen. Zudem sind Domotiksysteme aus Kosten- und Effizienzgründen oft nicht von den übrigen IT-Systemen entkoppelt.

Auch die öffentliche Verwaltung will heute von den Vorteilen einer vernetzten Gebäudetechnik profitieren und baut daher diese neuen, intelligenten Technologien immer öfter in ihren Gebäuden ein. Ebenfalls wird laufend renovationsbedürftige Infrastruktur mit intelligenter Technologie nachgerüstet. Dies alles erlaubt der öffentlichen Hand, ihre Objekte wirtschaftlicher und nachhaltiger zu verwalten. Zudem kann damit die Betriebssicherheit von Gebäuden und Anlagen erhöht werden.

Diese neuen Technologien bergen jedoch nicht unerhebliche **Cyberrisiken** in sich. Daher verlangen gerade auch Verwaltungsgebäude mit erhöhten Schutzbedürfnissen, wie zum Beispiel die Infrastruktur der Armee, nach adäquaten Sicherheitsmaßnahmen. Sollte es unbefugten Dritten gelingen, sich virtuellen Zutritt zur vernetzten Gebäudetechnik zu verschaffen, eröffnet dies ihnen eine Vielzahl von Angriffsmöglichkeiten. Denn, smarte Gebäudetechnologien sind notwendigerweise mit dem IT-Netzwerk der jeweiligen Organisationseinheit verbunden. Auf diesem Wege bieten Domotiksysteme Angreifern eine Vielzahl von Einstiegsmöglichkeiten, um Schaden anzurichten. Daher muss die Sicherheit jedes einzelnen internetfähigen Gerätes, sei es Heizungs-, Lüftungs- oder Zutrittssystem, auf dessen Relevanz analysiert werden. Diese Sicherheitsbeurteilung sollte sinnvollerweise durchgeführt werden, bevor die intelligente Technologie in Gebäuden eingesetzt wird.

2 Auftrag, Methodik und Abgrenzung

Die Chefin VBS erteilte der Internen Revision VBS am 15. Mai 2020 den Auftrag, die Bewirtschaftung von Domotiksystemen im VBS zu prüfen. Zudem soll das Life Cycle Management sowie die Sicherheit der Domotiksysteme beurteilt und allfälliger Handlungs- und Optimierungsbedarf aufgezeigt werden.

Wir wählten für diesen Auftrag ein risikoorientiertes Vorgehen. Dabei analysierten wir relevante Dokumente und führten mit Fachexperten bei der armasuisse Immobilien (ar Immo), Führungsunterstützungsbasis der Armee (FUB), Logistikbasis der Armee (LBA) sowie dem



Armeestab (A Stab) Befragungen durch. In diesen Gesprächen ging es primär darum, Aufgaben, Kompetenzen und Verantwortlichkeiten der einzelnen Rollen zu ermitteln. Zudem zogen wir Fachliteratur^{1 2} bei.

Es war nicht Ziel dieser Prüfung, eine vollständige Übersicht der im VBS eingesetzten Domotiksysteme zu erstellen. Den Fokus legten wir auf Domotiksysteme, die zur Steuerung von Gebäuden und Anlagen der Armee eingesetzt werden.

3 Würdigung

Während unserer Prüfung trafen wir ausnahmslos auf engagierte Interviewpartner³, die uns unterstützt und Informationen transparent zur Verfügung gestellt haben. Zudem gewannen wir den Eindruck, dass der sichere Betrieb der Domotiksysteme bei allen Fachexperten eine hohe Bedeutung hat. Wir bedanken uns bei allen Beteiligten für die zielführende Zusammenarbeit.

4 Domotiksysteme im VBS

Während den letzten ca. 20 Jahren wurden auch in Gebäuden und Anlagen des VBS immer mehr Domotiksysteme installiert. Nachfolgend erläutern wir kurz die wesentlichen Rollen und Aufgaben, die im VBS bei der Bewirtschaftung von Domotiksystemen bestehen.

4.1 Armeestab - Immobilien Verteidigung

Der Bereich Immobilien Verteidigung führt und steuert die Immobilienplanung Verteidigung. Er verantwortet die Ausrichtung des Immobilienmanagements auf die Kernaufgaben der Armee und verantwortet die Wirtschaftlichkeit, Zweckmässigkeit und Finanzierbarkeit des Immobilienportfolios. Dazu gehört die **Ermittlung und Einstreuierung der Immobilienbedürfnisse** der Armee.

4.2 armasuisse Immobilien

Als Immobilienkompetenzzentrum des VBS ist die ar Immo für das Management von rund 24 000 Hektaren Land und 7000 Gebäuden und Anlagen VBS zuständig. In ihrem Portfolio ist ar Immo verantwortlich für die Planung und Umsetzung bestehender und künftiger Kundenbedürfnisse, die Bewirtschaftung der militärisch genutzten Objekte, die Realisierung von

¹ J. Balow (2016), *Systeme der Gebäudeautomation*, Karlsruhe: cci Dialog GmbH

² S. Frank (2020), *Angriff auf die Radio-Fähigkeiten von IoT-Geräten eine Sicherheitsbedrohung?* Steinhausen: CyOne Security

³ Aus Gründen der Lesbarkeit wird bei Personenbezeichnungen die männliche Form gewählt; es ist jedoch immer auch die weibliche Form mitgemeint



Neu- und Umbauten sowie für die Veräusserung und den Rückbau von nicht mehr benötigten Infrastrukturen. Zu diesen Aufgaben gehört auch die bautechnische **Konzeption der Domotiksysteme im Rahmen von Neubau- und Renovationsprojekten**. Die ar Immo verfügt über mehrere Domotikfachexperten, die in den Immobilienprojekten des Departementes mitwirken.

4.3 Führungsunterstützungsbasis der Armee

Die FUB stellt u.a. Fachanwendungen sowie Informations- und Kommunikationssysteme für die Armee bereit. Ebenfalls sorgt die FUB mit einem unabhängig funktionierenden Kommunikationsnetz und geschützten Rechenzentren dafür, dass die Schweizer Armee in allen Lagen einsatzfähig ist. Zu diesen Aufgaben gehört auch der sichere und reibungslose **Betrieb und Unterhalt der Domotiksysteme**, die zur Steuerung der Gebäude und Anlagen verwendet werden. Hierzu verfügt auch die FUB über mehrere Domotikfachexperten. Momentan ist die FUB daran, die Domotik als integralen Service zu etablieren.

4.4 Logistikbasis der Armee

Die LBA betreibt u.a. die Infrastruktur für die Ausbildung und den Einsatz der Armee und hält die Objekte instand. Dazu gehört die **Nutzung der Domotiksysteme**, die zur Steuerung der Gebäude und Anlagen verwendet werden.

5 Herausforderungen im Bereich der Domotiksysteme

Nachfolgend legen wir in Kürze die aus unserer Sicht wesentlichsten Herausforderungen dar, die heute im VBS bei der Bewirtschaftung von Domotiksystemen bestehen. Wir gliedern diese Herausforderungen in die Themenbereiche «Grundlagen erarbeiten», «Entflechtung vorantreiben» sowie «Domotiksysteme sicher und robust betreiben». Diese drei Bereiche sollten – wenn möglich – aufbauend bearbeitet werden.

5.1 Grundlagen erarbeiten

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

5.1.1 Unterschiedliche Perspektiven verstehen und Begrifflichkeiten festlegen

Feststellung: Nicht alle relevanten Anspruchsgruppen im VBS haben die gleiche Sichtweise auf die Domotik. Zum Beispiel steht aus der Perspektive der ar Immo primär die zielführende Funktionalität der Domotik im Vordergrund. Deren Anforderungen werden in verschiedenen technischen Weisungen beschrieben. Die FUB hingegen legt Wert auf die konsequente Einhaltung der Sicherheitsanforderungen der Systeme. Diese beiden Sichtweisen können zu



Zielkonflikten führen. Weiter kommt erschwerend hinzu, dass bis heute im VBS der Begriff der Domotik nie einheitlich definiert wurde.

Beurteilung: Diese unterschiedlichen Perspektiven führten gelegentlich zu Reibungsverlusten zwischen der ar Immo und der FUB. Wir begrüssen die Idee, dass im Rahmen von regelmässigen «Roundtables» die relevanten Fachexperten einen Austausch führen. Diese neue Kommunikationsplattform kann helfen, das Verständnis für die unterschiedlichen Sichtweisen zu fördern. Ebenfalls erachten wir es als wichtig, dass die relevanten Begrifflichkeiten einheitlich festgelegt werden.

5.1.2 Aufgaben, Kompetenzen und Verantwortlichkeiten regeln

Feststellung: Die heutigen Aufgaben, Kompetenzen und Verantwortlichkeiten (AKV) der FUB im Immobilienprozess sind nicht immer abschliessend geklärt. Im Grundsatz bestehen die Rollen, wie wir sie in Kapitel 4 beschrieben haben. Jedoch entstehen gerade in den Detailarbeiten zwischen ar Immo und der FUB (aber auch innerhalb der FUB) gelegentlich Unsicherheiten und auch Verzögerungen, deren Ursache in den unterschiedlichen Interessen (z.B. Ressourcenverfügbarkeiten) der Prozessbeteiligten liegt.

Beurteilung: Vor allem der Schnittstelle «ar Immo zu FUB» kommt eine enorm wichtige Bedeutung zu. Daher müssen die bestehenden Dokumente zur Zusammenarbeit, die Aufgaben, Kompetenzen und Verantwortlichkeiten regeln, noch verfeinert werden. Zudem sollte aus unserer Sicht eine Diskussion darüber geführt werden, ob ein «Domotikverantwortlicher» im Departement eingesetzt werden muss. Damit würde der Gebäudeautomation das nötige Gewicht beigemessen. Schliesslich könnten auch die im Abschnitt 5.1.1 erwähnten «Roundtables» helfen, Lösungen im Einzelfall zu finden.

5.1.3 Fachbereich «DCS» für Vorgaben und Koordination miteinbeziehen

Feststellung: Der Themenbereich «Domotik» stellt eine Herausforderung dar, welche die Grenzen der verschiedenen Departementsbereiche im VBS überschreitet und nicht unerhebliche Cyberrisiken in sich birgt. Daher kommt dem Generalsekretariat VBS (GS-VBS), das auch im Bereich der Informatik koordinierende Aufgaben innehat, eine wichtige Bedeutung zu. Bis heute hat sich dieses jedoch kaum zu Domotikthemen geäussert.

Beurteilung: Der neu im GS-VBS geschaffene Fachbereich «Digitalisierung und Cybersicherheit VBS» (DCS) ist dazu prädestiniert, im Themenbereich der Domotik eine koordinative Rolle zu übernehmen und gegebenenfalls Vorgaben zu erlassen. Daher scheint uns unabdingbar, dass sich dieser Fachbereich den Herausforderungen der Domotiksysteme annimmt.

5.2 Entflechtung vorantreiben

Der Betrieb der bestehenden Domotiksysteme ist stark von der laufenden Entflechtung der IKT-Basisleistungen der FUB betroffen.

5.2.1 Domotiksysteme der Armee dem Führungsnetz zuweisen

Feststellung: Die grosse Mehrheit der Domotiksysteme, die zur Steuerung von Gebäuden und Anlagen der Armee dienen, werden heute über das Bereitschaftsnetz betrieben. Dieses liegt im Kompetenzbereich des Bundesamtes für Informatik (BIT). Das Bereitschaftsnetz erfüllt nicht die gleichen Sicherheitsanforderungen wie das Führungsnetz.

Beurteilung: Grundsätzlich sollten Domotiksysteme für schutzwürdige Gebäude und Anlagen der Armee über das Führungsnetz betrieben werden. Dieses liegt im Kompetenzbereich der FUB. Aus historischen Gründen ist dies jedoch heute nicht der Fall. Es ist geplant, im Rahmen der laufenden Entflechtung, alle Domotiksysteme von schutzwürdigen Objekten der Armee auf das Führungsnetz zu migrieren. Die dafür notwendige Kategorisierung der Objekte/Systeme ist jedoch noch nicht abgeschlossen.

5.2.2 Domotiksysteme der Armee inventarisieren

Feststellung: Im VBS besteht keine abschliessende Übersicht bezüglich der eingesetzten Domotiksysteme. Heute existieren bereits mehrere hundert solcher Systeme, wie eine Teilerhebung der FUB zeigte.

Beurteilung: Wir erachten es als sinnvoll, ein vollständiges Domotikinventar zu erstellen. Dies sollte die Basis für eine zielführende Bewirtschaftung der Gebäudetechnik bilden.

5.3 Domotiksysteme sicher und robust betreiben

Schliesslich ergab unsere Prüfung, dass für das Erbringen von sicheren und robusten Domotiksolutions noch gewisse technische Voraussetzungen geschaffen werden müssen.

5.3.1 Heterogene Systemlandschaft vereinheitlichen

Feststellung: Über die vergangenen Jahre wurden eine Vielzahl unterschiedlicher Domotiksysteme für die Steuerung der verschiedenen Gebäude und Anlagen eingeführt. Dies führt dazu, dass heute die Domotiklandschaft im VBS sehr heterogen zusammengesetzt ist. Dadurch sind die bestehenden Steuerungssysteme wenig standardisiert und skalierbar.

Beurteilung: Wünschenswert wäre, dass in Zukunft eine einheitlichere Domotiklandschaft besteht. Standardisierte Systeme würden helfen, die bestehenden Cyberrisiken einzudämmen und Skaleneffekte zu nutzen.

5.3.2 Life-Cycle-Management weiterentwickeln

Feststellung: Heute werden Gebäude und Anlagen nicht mehr einmalig dem Nutzenden übergeben. Sie verstehen sich als dynamische «Produkte», die flexibel konzipiert und danach laufend optimiert werden müssen. In diese gesamtheitliche Sichtweise müssen auch die Domotiksysteme miteinbezogen werden, um die Zukunftsfähigkeit der Gebäude und Anlagen zu erhalten. Diese integrale Betrachtung ist heute noch nicht vollumfänglich vorhanden.

Beurteilung: Während unseren Arbeiten gewannen wir den Eindruck, dass diese integrale Sichtweise auf den Lebenszyklus der Gebäude, die nach dem Fachwissen von ar Immo und FUB verlangt, noch verfeinert werden kann. Eng damit verbunden sind unsere Erläuterungen in Abschnitt 5.1.1 und 5.1.2.

5.3.3 Test- und Migrationsplattformen etablieren

Feststellung: Wir stellten fest, dass für die Einführung von neuen Domotiksystemen noch nicht in ausreichender Form geschützte Test- und Migrationsplattformen verfügbar sind.

Beurteilung: Wir vertreten die Ansicht, dass Test- und Migrationsplattformen eine Grundanforderung für eine zielführende und sichere Integration von Systemen darstellen.

6 Fazit

Der zielführenden Bewirtschaftung und dem sicheren Betrieb von Domotiksystemen kommt im VBS eine bedeutende Rolle zu. Intelligente Gebäude und Anlagen des VBS verfügen heute über eine Vielzahl von Sensoren, Kontrollsystmen, Netzwerken und Applikationen. Die zugrundeliegenden Technologien sind in erster Linie eingeführt worden, um diese Objekte ökonomischer und ökologischer zu bewirtschaften. Die moderne intelligente Gebäudeautomation hat allerdings auch dafür gesorgt, dass sich die Angriffsfläche aus dem Cyberraum erheblich vergrössert hat. Daher kommt heute dem engen Zusammenspiel zwischen FUB, ar Immo sowie auch der Fachstelle DCS eine hohe Bedeutung zu. Die integrale Zusammenarbeit dieser Stellen muss jedoch noch verfeinert werden, damit den in diesem Bericht dargelegten Herausforderungen begegnet werden kann. Die Bearbeitung dieser Herausforderungen wird aus unserer Sicht Jahre in Anspruch nehmen. Allenfalls könnte es Sinn machen, einen «Domotikverantwortlichen» im Departement einzusetzen. Insgesamt muss das Ziel bestehen, alle relevanten Domotiksysteme des VBS als integralen Bestandteil der sicheren und robusten IT-Umgebung zu bewirtschaften.

7 Empfehlung

Basierend auf unseren Feststellungen und Beurteilungen empfehlen wir, unter der Leitung des Generalsekretariats VBS (Fachbereich DCS), zusammen mit der FUB sowie der ar Immo, eine detaillierte Auslegeordnung zur Bewirtschaftung der Domotiksysteme durchzuführen. Diese Auslegeordnung soll mit einem Grundlagenpapier abgeschlossen werden, welches das weitere Vorgehen auf der Zeitachse beschreibt und die Leitplanken für die zukünftigen Arbeiten festlegt.



8 Stellungnahmen

Generalsekretariat VBS

Das Generalsekretariat VBS dankt der IR VBS für die sorgfältige Prüfung des sicheren Betriebs von Domotiksystemen. Wir sind mit den grundsätzlichen Erkenntnissen einverstanden. Das Generalsekretariat VBS unterstützt zudem die Empfehlung der IR VBS, nach welcher unter der Leitung des Fachbereichs Digitalisierung und Cybersicherheit VBS (DCS), zusammen mit der Gruppe Verteidigung (FUB) sowie der armasuisse (Immobilien), eine detaillierte Auslegeordnung zur Bewirtschaftung der Domotiksysteme zu erstellen sei.

Gruppe Verteidigung

Die Gruppe Verteidigung dankt für die konsistente, gesamtheitliche und ausgewogene Analyse. Sie wiederspiegelt die bestehende Situation für den Einsatz von Domotiksystemen im V gut und die abgeleiteten Schlüsse aus dem Bericht sind nachvollziehbar. Wir stimmen der Empfehlung zu. Wir begrüssen eine detaillierte Auslegeordnung zur Bewirtschaftung der Domotiksysteme, damit zur Erhöhung der Cybersicherheit ein enges Zusammenspiel zwischen FUB, ar Immo und den Sicherheitsorganen gefestigt werden kann, mit dem Ziel einer hochsicheren und robusten Informatik. Eine OE-übergreifende Koordination zur Bearbeitung dieser Auslegeordnung erachten wir als sinnvoll, die Notwendigkeit sowie ein möglicher Aufgabenbereich eines «Domotikverantwortlichen» auf Stufe Department soll dagegen erst durch die detaillierte Auslegeordnung und Analyse aufgezeigt werden.

armasuisse

armasuisse ist mit dem Bericht und den Empfehlungen einverstanden. Wir möchten darauf hinweisen, dass mit der neu geschaffenen Rolle für die FUB als zentralen Leistungserbringer IKT V und dem Gremium Plattform IKT im Immobilienmanagement VBS bereits die ersten Schritte unternommen wurden, um den Austausch zu verbessern.