Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Interne Revision VBS

22. Dezember 2022

Prüfbericht «Betrieb Security Operations Center (SOC)»

IT-Prüfung I 2022-03

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 2022

Prüfbericht «Betrieb Security Operations Center (SOC)»

Sehr geehrte Frau Bundesrätin Amherd

Gerne lassen wir Ihnen unseren Prüfbericht «Betrieb Security Operations Center (SOC)» zukommen. Unsere Prüfarbeiten fanden zwischen August und September 2022 statt. Den vorliegenden Bericht haben wir mit unseren Ansprechpartnern besprochen. Die Stellungnahme der Gruppe Verteidigung zu unserem Bericht ist in Kapitel 7 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

Interne Revision VBS
Schauplatzgasse 11
3003 Bern

1 Entstehung des Security Operations Center (SOC)

Im Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) der Schweiz kommt der Prävention und Bewältigung von Cyberrisiken eine wichtige Rolle zu. Aufgrund der Zunahme der Cyberrisiken und Erfahrungen mit konkreten Angriffen wird im VBS das Dispositiv zum Schutz vor Cyberangriffen laufend überprüft und verfeinert. Infolge des Cyberangriffs auf die RUAG im Jahr 2016 erteilte der damalige Chef VBS den Auftrag, einen «Aktionsplan Cyberdefence VBS» (APCD) für die Periode 2017–2020 zu erstellen, welcher übergreifend die Aufgaben, Kompetenzen und Prozesse der Verwaltungseinheiten des VBS im Umgang mit Cyberdefence definierte. Nicht zuletzt wegen der Lageentwicklung wurde für die Periode 2021–2024 eine «Strategie Cyber VBS» erarbeitet, welche auf dem Aktionsplan aufbaut. Der Aktionsplan wie auch die «Strategie Cyber VBS» sind mit der übergeordneten «Nationale(n) Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) für die Jahre 2018–2022» abgestimmt.

Mit der Umsetzung der vom APCD gesetzten Ziele wurden im Bereich Cyberschutz massgebliche Fortschritte erzielt. Dazu zählt z. B. die Schaffung einer permanenten Überwachung der Netzwerke und Systeme unter der Leitung des Chief Information Security Officer (CISO) bei der Führungsunterstützungsbasis (FUB). Ihm unterstellt ist das Cyber Fusion Center (CFC), welches u. a. aus dem Security Operations Center (SOC), dem militärischen Computer Emergency Response Team (milCERT), Infrastruktur und Weiterentwicklung (INWE) und dem Cyber Operations Center (CyOC) besteht.[1]

Bedrohungen und Angriffe auf die Informations- und Kommunikationstechnologie (IKT)-Systeme und -infrastrukturen, welche die Aufgabenerfüllung der Gruppe Verteidigung (Gruppe V) beeinträchtigen, gilt es frühzeitig zu erkennen und im Idealfall gänzlich zu verhindern. Das SOC ist seit 2020 in Betrieb und stellt mit seiner Überwachungsfunktion eine wichtige Verteidigungslinie gegen Cyberangriffe und Datendiebstähle dar.

[1] «Strategie Cyber VBS» vom März 2021, Seite 20

2 Auftrag, Methodik und Abgrenzung

Die Chefin VBS erteilte der Internen Revision VBS (IR VBS) am 18. Mai 2022 den Auftrag zu prüfen, ob sich das durch die FUB (bzw. Projekt Kommando Cyber) betriebene Security Operations Center (SOC) als zentrale Sicherheitsleitstelle angemessen um den Schutz der IKT-Infrastruktur des Departements kümmert. Dabei prüften wir auch, ob im VBS die bestehenden Firewall- sowie generellen Sicherheitskonzepte den heutigen Standards entsprechen und angemessen ausgestaltet sind.

Für die Beurteilung von Mindestanforderungen an Sicherheitskontrollen zur Bewältigung und Abwehr von Cyberangriffen stützt sich die IR VBS auf das allgemein anerkannte CIS Critical Security Controls (CIS Controls) Framework[2] des «Center for Internet Security» ab. Im Rahmen dieser IT-Prüfung haben wir aus dem CIS Controls Framework folgende Bereiche herangezogen, um risikoorientiert das Kontrolldesign zu beurteilen:

– Sichere Konfiguration von Infrastruktur und Software (Fokus auf Firewalls): «*Control 04 - Secure Configuration of Enterprise Assets and Software*»;
– Netzwerküberwachung: «*Control 13 - Network Monitoring and Defense*»;
– Vorfallreaktionsmanagement: «*Control 17 - Incident Response Management*».

Im Rahmen dieses Prüfauftrages führten wir strukturierte Befragungen mit den Verantwortlichen im SOC und bei Network IT Services durch. Ergänzend befragten wir die Sicherheitsverantwortlichen innerhalb der FUB sowie beim Projekt Kommando Cyber und analysierten Dokumente. Dabei wählten wir ein risikoorientiertes Vorgehen.

3 Unterlagen und Auskunftserteilung

Die Gruppe V hat der IR VBS die notwendigen Auskünfte umfassend und zuvorkommend erteilt. Die gewünschten Unterlagen standen dem Prüfteam vollumfänglich zur Verfügung. Die IR VBS dankt für die gewährte Unterstützung.

[2] Center for Internet Security: CIS Critical Security Controls (cisecurity.org)

4 Betrieb des SOC

4.1 Aufgaben

Das SOC stellt mit gezielten Detektionsmethoden die frühzeitige Erkennung von Anomalien und Cyberangriffen fest. Zudem stellt es mit einem effizienten Security Information & Event Management (SIEM[3]) Prozess die Behandlung von Security-Events und die Triage von Security Incidents sicher. Des Weiteren gewährleistet das SOC mit einer effektiven und effizienten Abwicklung der Sicherheitsvorfälle die Bewältigung und Abwehr von Cyberangriffen.

Feststellung: Im Rahmen des «Aktionsplan Cyberdefence VBS» (APCD) wurde der generelle Auftrag «Cyberdefence» in vier Funktionen (Steuerung, Cyberschutz, Abwehr und Aktion im Cyberraum sowie Unterstützung) unterteilt. Das SOC verantwortet mit gezielten Detektionsmethoden (d. h. Sensorik) die frühzeitige Erkennung von Anomalien und Cyberangriffen und stellt zusammen mit dem milCERT sowie CyOC den Incident Response-Prozess sicher. Mit dem SIEM-Prozess werden sicherheitsrelevante Vorfälle und Ereignisse identifiziert, kategorisiert und analysiert sowie bei Bedarf an das milCERT eskaliert. Das milCERT ist u. a. für die vertiefte Analyse von Angriffsvektoren und die gerichtsverwertbare Sicherung von Beweismitteln verantwortlich. Für die Erstellung des militärischen Cyber-Lagebildes zeichnet sich das CyOC verantwortlich und stellt die Kommunikationsflüsse bei Cybervorfällen sicher. Die Verantwortlichkeiten für die militärische Cyberabwehr sind in der Verordnung des Bundesrates über die militärische Cyberabwehr (MCAV[4]) noch nicht auf die aktuelle Organisationstruktur angepasst worden.

Im SOC werden neue Verfahren zur verbesserten Erkennung von Anomalien und Cyberangriffen entwickelt und bereitgestellt. Ein etablierter Security Incident Response-Prozess im SOC stellt die Bewältigung und Abwehr von Cyberangriffen sicher. Die Aufgaben, Kompetenzen und Verantwortlichkeiten (AKV) primär gegenüber dem milCERT, aber auch dem CyOC, sind jedoch nicht klar abgegrenzt und schriftlich festgehalten worden.

Beurteilung: Die organisatorische Einbettung des SOC beim CFC innerhalb des Projektes Kommando Cyber erachten wir als angemessen. Die zugewiesenen Aufgabenbereiche und die dazugehörigen AKV des SOC, vor allem gegenüber dem milCERT sowie dem CyOC, bedürfen einer Präzisierung. Aufgrund der Neuorganisation (Kommando Cyber) müssen die Verantwortlichkeiten für die militärische Cyberabwehr in der MCAV noch angepasst werden.

---

[3] Deutsche Übersetzung: Sicherheitsinformations- und Vorfallmanagement; SIEM ist ein Ansatz des Sicherheitsmanagements, der darauf abzielt, eine ganzheitliche Sicht auf die Sicherheit der Informationstechnologie einer Organisation zu haben und den Cybersecurity-Fachkräften einen Einblick in die Aktivitäten in ihrer IKT-Umgebung zu verschaffen.

[4] SR **510.921** - Verordnung vom 30. Januar 2019 über die militärische Cyberabwehr (MCAV) (admin.ch)

4.2 Ressourcen

Gemäss «Gesamtkonzeption Cyber»[5] der Schweizer Armee aus dem Jahr 2022 soll die Resilienz der Operationszentralen CER[6]-Eigenschutz verbessert werden. Weiter muss die personelle Durchhaltefähigkeit so weit ausgebaut werden, dass die Armee gleichzeitig mehrere Cyberangriffe bewältigen kann.

Feststellung: Das SOC wird aktuell während den normalen Geschäftszeiten (5/12[7]) betrieben und durch die Miliz des neu gegründeten Cyber Bataillon 42 unterstützt. Im Rahmen von dedizierten temporären Einsätzen kann der Betrieb 7/24 bedarfsgerecht sichergestellt werden. Aufgrund der knappen Ressourcenlage muss sich das SOC aktuell allerdings auf den Grundauftrag der frühzeitigen Erkennung von Anomalien und Cyberangriffen sowie deren Bewältigung und Abwehr fokussieren.

Für die Unterstützungsleistung zur Härtung von bestehenden Systemen oder zur Sicherstellung eines durchgängigen 7/24-Betriebs, die vertiefte Zusammenarbeit mit Partnern auf internationaler Ebene sowie die Aus- und Weiterbildung von Mitarbeitenden und der Miliz fehlen aktuell die Ressourcen. Die Rekrutierung von gut ausgebildetem Fachpersonal für die Besetzung der offenen Stellen hat diverse Gründe (u. a. hohe Anforderungen, angespannte Arbeitsmarktverhältnisse) und kommt nur schleppend voran.

Zudem haben wir festgestellt, dass es bei der FUB im Bereich des Firewall Managements aktuell einen überdurchschnittlich hohen Anteil an externen Fachkräften gibt. Auch die Eidgenössische Finanzkontrolle (EFK) hat in ihrem Bericht über die Prüfung der Ressourcensteuerung (EFK-22125) vom 5.10.2022 auf das Problem der Ressourcenverfügbarkeit in der FUB aufmerksam gemacht.

Beurteilung: Unter der angespannten Ressourcensituation leiden sämtliche vorerwähnten Arbeiten bezüglich des weiteren Ausbaus der Sensorik, dem Ausbau der Sicherheitsvorkehrungen, der internationalen Zusammenarbeit und der Aus- sowie Weiterbildung der Mitarbeitenden und der Miliz. Damit das SOC aktuell seiner Verantwortung nachkommen und zu einem höheren Reifegrad bei der Betriebssicherheit beitragen kann, müssen die vakanten Positionen schnellstmöglich besetzt werden. Für einen permanenten 7/24-Betrieb des SOC ab Anfang 2025 müssen die notwendigen personellen Ressourcen zugunsten des Fähigkeitsaufwuchses «Gesamtkonzeption Cyber» im Kommando Cyber bald möglichst alimentiert werden. Gut ausgebildete und qualifizierte Arbeitskräfte im Cyber-Bereich sind auf dem hart umkämpften Arbeitsmarkt Mangelware. Das (Projekt) Kommando Cyber steht dabei in direktem Konkurrenzkampf mit der Privatwirtschaft. Dies sehen wir als grosse Herausforderung, um die gesteckten Ziele termingerecht zu realisieren.

---

5 Gesamtkonzeption Cyber - Konzeption der Weiterentwicklung der Fähigkeiten der Schweizer Armee im Cyber- und elektromagnetischen Raum bis Mitte der 2030er-Jahre, Gesamtkonzeption Cyber (admin.ch)

6 CER - Cyber- und elektromagnetischer Raum

7 Bereitschaft 12 Stunden am Tag, 5 Tage die Woche

Der hohe Anteil an externen Mitarbeitenden im Bereich des Firewall Managements ist als kritisch zu betrachten. Es besteht das latente Risiko, dass diese Fachkräfte in einer ausserordentlichen Lage unter Umständen nicht mehr zur Verfügung stehen. Zudem läuft die FUB Gefahr, dass das Know-how von Externen nicht gehalten bzw. das Gruppe V-spezifische Wissen nicht längerfristig aufgebaut werden kann.

4.3 Zusammenarbeit mit internen und externen Partnern

Das SOC hat zur Erfüllung seiner Aufgaben verschiedenste Schnittstellen zu Partnern innerhalb und ausserhalb des VBS.

Feststellung: Das SOC arbeitet mehrheitlich mit operativen Bereichen der FUB zusammen. Ergänzend werden wichtige Informationen aus dem Umfeld des BIT/CSIRT[8], govCERT, CNO[9] und dem Nachrichtendienst des Bundes (NDB) eingeholt. Diese departementsübergreifende Zusammenarbeit stellt den Informationsaustausch über die aktuellsten Cyberbedrohungen sicher.

Auch auf internationaler Ebene ist das SOC präsent. Das SOC pflegt Kontakte zu den Cybersicherheitsexpertinnen und -experten der NATO (z. B. beim «Cooperative Cyber Defence Centre of Excellence» (CCDCOE) in Tallinn), den DACH-Nachbarstaaten[10] und diversen internationalen CERT[11] und ist bestrebt, die Zusammenarbeit kontinuierlich zu vertiefen. Zusätzlich finden im Bereich Cyber Defence regelmässige Übungen statt, an denen Vertreterinnen und Vertreter der Gruppe V und der Armee teilnehmen (z. B. «Cyber Coalition» und «Locked Shields»). Das Ziel besteht darin, die eigenen Kompetenzen und Prozesse fortlaufend zu überprüfen und zu verbessern sowie die internationale Kooperation zu stärken.

Beurteilung: Kooperationen sind zeitaufwändig. Doch ist die Zusammenarbeit mit Partnern für die Einschätzung von Bedrohungen und Herausforderungen im Cyberbereich sowie im Hinblick auf Aufdeckung und Verhinderung von Cyberangriffen unverzichtbar. Aufgrund der knappen Ressourcenlage im SOC kann aktuell aber nur ein begrenzter Nutzen aus der Zusammenarbeit mit internen und externen Partnern gezogen werden.

4.4 Firewall Management

Gemäss dem CIS Controls Framework müssen Netzwerkinfrastruktur, Server und Endgeräte geschützt und die Sicherheitskonfiguration mit einer aktiven Verwaltung aktuell gehalten werden. Weiter müssen die gemeldeten bzw. die öffentlich bekannt gewordenen Schwachstellen mit Hilfe von Werkzeugen analysiert, überwacht und dokumentiert werden bis eine wirksame Fehlerkorrektur ins System eingespeist wurde. Werden diese Anforderungen nicht oder nur

[8] CSIRT - Computer Security Incident Response Team

[9] CNO - Computer Network Operation

[10] DACH - Akronym für Deutschland, Österreich und die Schweiz

[11] CERT - Computer Emergency Response Team

ungenügend mittels zielgerichteter Werkzeuge und Verfahren umgesetzt, besteht das Risiko einer Gefährdung der Netzwerkinfrastruktur.

Feststellung: Die Anforderungen an die Sicherheit im Netzwerk der Gruppe V werden folgendermassen umgesetzt: Einerseits wird Sensorik eingesetzt, welche Anomalien und Anzeichen eines Cyberangriffs frühzeitig erkennen und an das SOC melden. Andererseits werden die Systemkonfigurationen und Parameter regelmässig den aktuellen Bedürfnissen und Anforderungen entsprechend angepasst.

Erkenntnisse aus öffentlich bekannt gewordenen Sicherheitsvorfällen oder Anpassungen an neue Bedürfnisse werden mittels systematischen Änderungsprozessen vorgenommen. Auf sämtlichen Firewalls der Gruppe V werden laufend die notwendigen Software-Releases installiert.

Beurteilung: Durch das zentrale und einheitliche Management der Firewalls wird eine effiziente Überwachung der Netzwerkaktivitäten durch das SOC ermöglicht. In den vergangenen Monaten wurde der aktuelle Software-Release gemäss Prozess installiert. Die Mindestanforderungen des CIS Controls Framework an das Firewall Management werden erfüllt.

4.5 Netzwerküberwachung

Die gesamte Netzwerkumgebung sowie Server und Endgeräte müssen gemäss CIS Controls Framework mit Hilfe von Sicherheitssystemen (u. a. SIEM, Intrusion Detection System) überwacht werden, damit Anomalien und Cyberangriffe frühzeitig identifiziert werden können.

Feststellung: Das SOC baut seine Überwachungsfunktion laufend aus. Einige Systeme konnten noch nicht in die Gesamtüberwachung einbezogen werden. Bei diesen Systemen handelt es sich mehrheitlich um ältere, eigenständige Systeme der Armee, welche nicht ohne erheblichen Aufwand integriert werden können. Bei neu zu beschaffenden Systemen wird das SOC bereits frühzeitig im Prozess involviert, damit die Systeme von Beginn weg in die Überwachung eingebunden werden können.

Das Erkennen fremder oder unbekannter Systeme im Netzwerk der Gruppe V gestaltet sich heute noch schwierig. Sobald ein fremdes Gerät mit dem internen Netzwerk verbunden ist, greifen die meisten bestehenden Sicherheitsmechanismen wie externe Firewalls, Virenscanner oder Proxy-Server[12] nicht mehr.

Im Rahmen des Projektes «Integrierte IKT Management Plattform (IIMP)» wurde im Oktober 2022 eine neue Softwarelösung eingeführt. Sicherheitsvorfälle können damit effizienter bearbeitet und behoben werden. Dabei handelt es sich aber nicht um eine umfassende, proaktive Netzwerkzugangskontrolle (NAP/NAC[13]).

[12] Definition Proxy-Server: Was ist ein Proxy? – Definition im IT-Lexikon (it-service.network)

[13] Network Access Protection (NAP) / Network Access Control (NAC)

Beurteilung: Eine zentrale Netzwerküberwachung existiert. Aktuell gibt es aber noch vereinzelte Systeme, welche nicht in die zentrale Überwachung durch das SOC eingebunden sind. Es ist daher unabdingbar, dass diese Systeme einer kritischen Prüfung unterzogen werden. Daraus abgeleitet müssen diese Systeme zeitnah ins Inventar der Überwachung aufgenommen oder risikomindernde Massnahmen definiert werden.

Wir sind der Ansicht, dass fremde oder unbekannte Systeme im Netzwerk der Gruppe V proaktiv erkannt und überwacht werden müssen. Mit NAP/NAC Netzwerkzugangskontrollen könnte eine solche Überwachung umgesetzt werden. Dies würde zudem den Analyseaufwand beim SOC reduzieren.

4.6 Abwicklung von Sicherheitsvorfällen

Das CIS Controls Framework empfiehlt, dass die gemeldeten Vorfälle mit einem etablierten Prozess zeitnah zu bearbeiten sind und entsprechende Massnahmen zur Behebung eingeleitet werden sollen. Werden diese nicht oder nur ungenügend umgesetzt besteht das Risiko, dass die Vorfälle einen erheblichen Reputationsschaden für das Departement verursachen und/oder ein Datenleck begünstigen.

Feststellung: Im SOC bestehen detaillierte Prozessabläufe zur Bewältigung von Sicherheitsvorfällen (d. h. Security Event und Security Incident Management). Mit deren Hilfe werden die Vorfälle systematisch erkannt, bewertet, fachgerecht analysiert und den korrekten Folgeprozessen bis zur Lösungsfindung zugewiesen. Es findet auch ein regelmässiger Austausch mit Schlüsselpersonen des CFC sowie dem Fachpersonal der FUB statt, um die Prozesse kontinuierlich zu verbessern und Vorfälle effizienter zu adressieren.

Beurteilung: Die Abwicklung von Sicherheitsvorfällen basiert auf klar definierten Prozessabläufen. Diese Prozesse haben sich bewährt und sind eingespielt. Aufgrund der knappen Ressourcen kann das SOC das Personal des Informatikbetriebs bei der Umsetzung von Sicherheitsmassnahmen aktuell jedoch nicht optimal unterstützen.

5 Fazit

Wir sind der Ansicht, dass die IKT-Infrastruktur des Departements durch das SOC – im Rahmen des Grundauftrages – zielführend überwacht und geschützt wird. Die Verantwortlichkeiten für die militärische Cyberabwehr sind in der entsprechenden Verordnung jedoch noch nicht auf die aktuelle Organisationstruktur angepasst worden (Kommando Cyber, MCAV).

Die ergänzend beurteilten Sicherheitskontrollen bei den Firewalls erfüllen die Mindestanforderungen des CIS Controls Framework. Für die Abwicklung von Sicherheitsvorfällen liegen etablierte und eingespielte Prozesse vor.

Bezüglich der Ressourcen haben wir einen durchzogenen Gesamteindruck gewonnen. Im Bereich des Firewall Managements gibt es aktuell einen überdurchschnittlich hohen Anteil an externen Fachkräften, welche bei einer ausserordentlichen Lage unter Umständen nicht mehr zur Verfügung stehen.

Weiter ist das SOC ressourcenmässig knapp ausgestattet. Aktuell ist ein Betrieb während den normalen Geschäftszeiten (5/12) gewährleistet. Dabei wird das SOC durch die Miliz des neu gegründeten Cyber Bataillon 42 unterstützt. Im Rahmen von dedizierten temporären Einsätzen kann auch ein 7/24-Betrieb sichergestellt werden. Für einen permanenten 7/24-Betrieb des SOC ab Anfang 2025 müssen die notwendigen personellen Ressourcen zugunsten des Fähigkeitsaufwuchses «Gesamtkonzeption Cyber» im Kommando Cyber bald möglichst alimentiert werden.

Die angespannte Ressourcenlage wirkt sich auch ungünstig auf die Aus- und Weiterbildung wie auch auf die Kooperationen mit internen und externen Partnern aus. Des Weiteren kommt die Rekrutierung von geeigneten Fachkräften nur sehr schleppend voran.

Bei der Netzwerküberwachung sind wir der Ansicht, dass fremde oder unbekannte Systeme im Netzwerk der Gruppe V durch eine rasche Einführung von NAP/NAC-Schutzmassnahmen besser und effizienter erkannt und überwacht werden müssen. Dies würde den Analyseaufwand beim SOC reduzieren.

6 Empfehlungen

Aufgrund unseres Fazits empfehlen wir der Gruppe V,

1) den hohen Anteil an externen Fachkräften im Bereich des Firewall Managements zu reduzieren. Damit ein permanenter 7/24-Betrieb des SOC ab Anfang 2025 sichergestellt werden kann, sollten die dafür notwendigen Stellen im SOC rasch möglichst besetzt werden.

2) geeignete Schutzmechanismen im Bereich der Netzwerkzugangskontrolle (NAP/NAC) zu implementieren.

7 Stellungnahme

Gruppe Verteidigung
Die Gruppe Verteidigung dankt der IR VBS für die transparente und sachliche Analyse im vorliegenden Prüfbericht und ist mit den Empfehlungen der IR VBS einverstanden. Betreffend die Empfehlung 1) wird das Security Operations Center (SOC) erst mit der Genehmigung des Fähigkeitsaufwuchses «Gesamtkonzeption Cyber» in die Lage versetzt, einen 7/24 Betrieb sicher zu stellen. Eine Internalisierung des Firewall-Managements muss im Rahmen der Entflechtung ausgearbeitet werden. Hinsichtlich der Empfehlung 2) ist die Umsetzung von geeigneten Schutzmechanismen im Bereich der Netzwerkzugangskontrolle (NAP/NAC) im Führungsnetz Schweiz geplant und in schrittweiser Umsetzung.