Redguard

Security Survey

2022

REDGUARD
SECURING YOUR ASSETS

Inhaltsverzeichnis

Mit der Publikation des IKT-Minimalstandards[1] durch den Bund verfügt die Schweiz seit 2018 über eine einheitliche, branchenübergreifende Vorgabe zum Schutz vor Cyber-Risiken. Doch wie genau sieht das aktuelle Sicherheitsniveau in der Schweiz aus? Besteht noch Handlungsbedarf oder verfügen die Schweizer Organisationen und Unternehmen bereits über ein ausreichendes Sicherheitsniveau? Diese Fragen werden im Redguard Security Survey 2022 beantwortet.

Zum vierten Jahr infolge publiziert die Redguard AG die Resultate ihrer Umfrage zum IKT-Minimalstandard. Auch dieses Jahr haben wir wieder über 1'000 Organisationen angeschrieben und sie gebeten, eine Selbsteinschätzung zu ihrem aktuellen Sicherheitsniveau abzugeben. Um Letzteres zu erheben, haben wir basierend auf dem IKT-Minimalstandard einen Quick-Test entwickelt (http://ikt.redguard.ch/).

Neben dem IKT-Minimalstandard enthielt die diesjährige Umfrage auch Fragen betreffend DevSecOps sowie Cloud Security. Letztere beiden Themen stehen seit den vergangenen zwei Jahren wieder vermehrt im Fokus unserer Kunden – Insbesondere Cloud Security durch die verstärkte Konzentration Schweizer Organisationen auf ihre Cloud-Strategie.

Wie den Resultaten der Umfrage zu entnehmen ist, glaubt laut eigener Einschätzung ein Grossteil der Organisationen noch Handlungsbedarf aufzuweisen. Weder der IKT-Minimalstandard noch DevSecOps oder Cloud Security sind Themen, welche die Organisationen völlig umgesetzt haben.

Die Schweiz ist ein Land der KMU's, welche einen Anteil von 99% der Schweizer Organisationen darstellen (www.kmu.admin.ch). Auch ein grosser Teil der kritischen Infrastrukturen gehören zur Kategorie der kleinen und mittelgrossen Unternehmen, beispielsweise Strom- oder Wasserversorger aber auch Lebensmittelproduzenten und Abwasserreinigungs-anlagen.

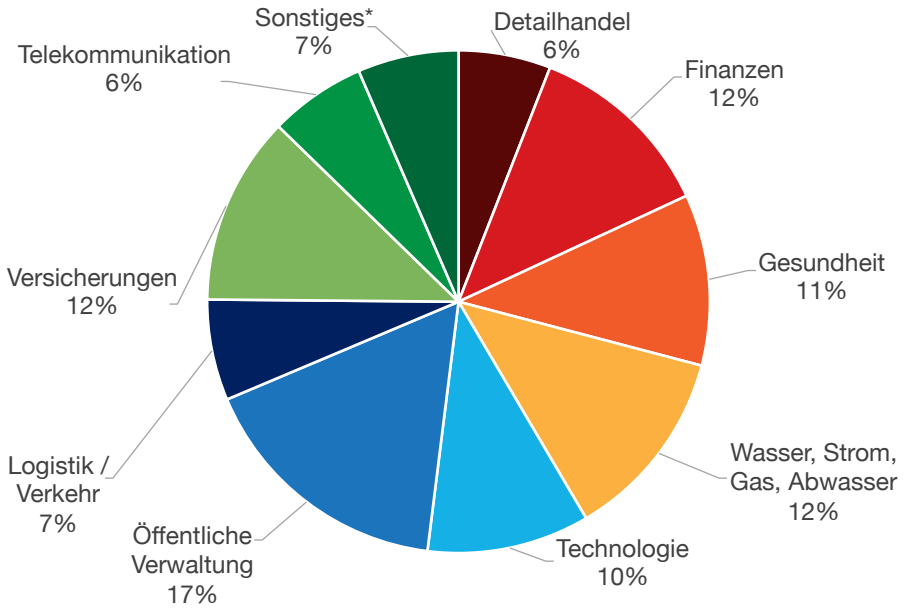
Das eigene Unternehmen im Bereich der Digitalisierung vorwärtszubringen ist bereits eine Herausforderung für sich. Dabei auch noch Informationssicherheit zu berücksichtigen, macht das Ganze auch für grosse Organisationen mit entsprechenden Fachexperten und ausreichend Ressourcen zu einer Knacknuss. Um genau diese Komplexität zu reduzieren und im Rahmen der Digitalisierung auch ein gesundes Mass an Sicherheit zu erzielen entwickelt Redguard ihre Dienstleistung kontinuierlich weiter. Ausführliche Informationen, welche Ansätze Sie in den Bereichen IKT-Minimalstandard, DevSecOps und Cloud Security in Ihrer Organisation angehen können finden Sie ab Seite 10.

Für Ihre Unterstützung bedanken wir uns herzlichst.
Ihr Redguard Team

[1] IKT (Informations- und Kommunikationstechnologie) – Minimalstandard des Bundesamtes für wirtschaftliche Landesversorgung (BWL): https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html

1. Rückmeldungen zur Umfrage

Die Ergebnisse des Redguard Security Survey basieren auf einer Selbsteinschätzung der teilnehmenden Unternehmen. Unternehmen und Organisationen erhalten mit dem Quick-Test die Chance, ihr Sicherheitsniveau in kurzer Zeit einzuschätzen und darauf basierend weitergehende Massnahmen abzuleiten. Auch dieses Jahr haben wir mit 178 Antworten einen sehr erfreulichen Rücklauf erlebt. Die von Redguard entwickelte Umfrage besteht aus insgesamt 16 Fragen zu den drei Themen. Damit werden Kernelemente des IKT-Minimalstandards, DevSecOps und Cloud Security abgedeckt[2].



*Sonstiges:	
Bau	30.4%
Dienstleister	30.4%
Ingenieurbüro	13.0%
Kommunikation	4.3%
Akademie	8.7%
Landwirtschaft	4.3%
Medien	4.3%

Abbildung 1: Befragte Unternehmen nach Branche (%)

Redguard hat über 1'000 Schweizer Organisationen eingeladen, ihr Sicherheitsniveau mittels Quick-Test zum IKT-Minimalstandard einzuschätzen. Auch dieses Jahr haben sich mit 178 Organisationen aus verschiedenen Branchen eine ansehnliche Anzahl für die Umfrage interessiert und ihre Selbsteinschätzung abgegeben. Abbildung 1 zeigt die breite Abstützung des Security Surveys. Die teilenehmenden Organisationen stammen aus allen Branchen der Schweiz, wobei auch der öffentliche Sektor angemessen vertreten ist. Gleichzeitig haben Unternehmen unterschiedlichster Grösse zum Security Survey beigetragen (vgl. Abbildung 2). Bei den Teilnehmenden handelt es sich bei 29.4% um grosse Unternehmen mit über 500 Mitarbeitenden. Die restlichen gut 70% der teilnehmenden Unternehmen und Organisationen verteilen sich auf 37% Kleinunternehmen (1-50 MA) und 33.6% mittelgrosse Unternehmen (50-500 MA).

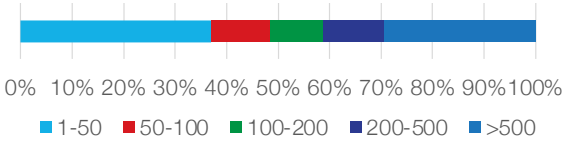


Abbildung 2: Befragte Unternehmen nach Anzahl Mitarbeitenden

[2] Der Fragekatalog befindet sich auf Seite 14 des vorliegenden Berichts.

2. Die Mehrheit der Organisationen hält den IKT-Minimalstandard nicht ein

Das von den insgesamt knapp 180 befragten Organisationen eingestufte Sicherheitsniveau liegt auch 2022 immer noch deutlich unter dem von Bund und Verbänden empfohlenen Minimalniveau. Im Vergleich zu den Vorjahren haben sich jedoch mehrere Werte leicht verbessert. Dies deutet darauf hin, dass sich die befragten Organisationen nur beschränkt verbessert haben.

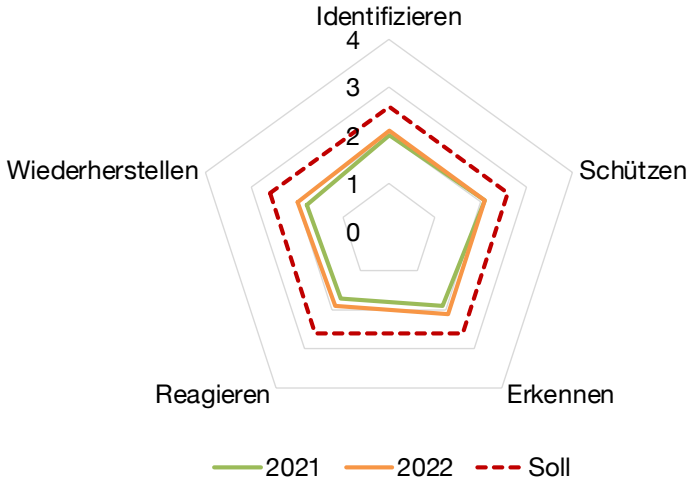


Abbildung 3: Ergebnisse der Redguard Security Survey

Error! Reference source not found. zeigt, dass laut e igener Einschätzung eine Mehrheit der befragten Organisationen das minimale Sicherheitsniveau des IKT-Minimalstandards auch 2022 noch nicht erreicht haben. Ein Blick auf die Antworten (Tabelle 2), aufgeteilt in die fünf Funktionen des IKT-Minimalstandards, verdeutlicht, dass gerade 37% der Organisationen der Ansicht sind, das vom IKT-Minimalstandard geforderte Sicherheitsniveau zu erreichen (dies ist eine Zunahme um einen Punkt im Vergleich zu 2021).

Trotz dem ernüchternden Resultat ist es doch erfreulich, dass gesamtheitlich betrachtet eine geringe Verbesserung festgestellt werden kann. Während im letzten Jahr (2021) noch lediglich 36% der befragten

	2020	2021	2022	Soll
Identifizieren	2.0	2.0	2.1	2.6
Schützen	2.3	2.1	2.1	2.6
Erkennen	1.9	1.9	2.1	2.6
Reagieren	1.8	1.7	1.9	2.6
Wiederherstellen	1.7	1.8	2.0	2.6

Tabelle 1: Ergebnisse pro Funktion im Jahresvergleich

Organisationen angaben, die Anforderungen des IKT-Minimalstandards zu erfüllen, sind es dieses Jahr 37%.

Betrachtet man die einzelnen Funktionen (Tabelle 1), wird ersichtlich, dass der erhöhte Erfüllungsgrad durch eine Verbesserung in vier der fünf Funktionen erzielt worden ist. Das beste Resultat wurde im Bereich «Schützen» erzielt. Organisationen schätzen ihre Massnahmen im präventiven Bereich (z. B. Antivirus, Firewall, Zonenkonzept, Awareness) als besser umgesetzt ein, als die restlichen Funktionen.

Funktion	Nicht-Erfüllt	Erfüllt
Identifizieren	66%	34%
Schützen	57%	43%
Erkennen	63%	37%
Reagieren	61%	39%
Wiederherstellen	66%	34%
Total	**63%**	**37%**

Tabelle 2: Survey-Ergebnisse nach fünf Funktionen

Die Arbeiten zur Verbesserung des Sicherheitsniveaus Schweizer Organisationen schreiten voran. Trotzdem muss konstatiert werden, dass die Schweiz in keinem der fünf Funktionen aktuell ausreichend geschützt ist. Wollen wir uns auch gegen kompetente Angreifer (z. B. Advanced Persistent Threats) und vor gezielten Ransomware-Angriffen schützen können, reicht das aktuelle Niveau noch nicht aus. Trotz gewissen Fortschritten steht noch ein weiter Weg vor uns, bevor wir uns als ausreichend gesichert wähnen können.

3. Resultate DevSecOps

DevSecOps ist die Verschmelzung von ursprünglich drei separat geführten Organisationsbereichen: Entwicklung (Development – Dev), Sicherheit (Security – Sec) und Betrieb (Operations – Ops). Hauptaspekt von DevSecOps ist dabei, dass nicht nur Entwicklung und Betrieb näher rücken, sondern gleichermassen auch die Sicherheit berücksichtigt werden soll. Grundsätzlich handelt es sich um einen Ansatz hinsichtlich Unternehmenskultur, Automatisierung und Plattformdesign bei welchem die Sicherheit als gemeinsame Verantwortung im gesamten IT-Lifecycle integriert ist.

In einem optimierten DevOps-Prozess ist im Idealfall schon ein Grossteil automatisiert. Sprich, neuer oder angepasster Programmcode wird durch die Entwickler in eine CI/CD Pipeline eingecheckt (Continuous Integration/Continuous Deployment). Der Code wird beispielsweise automatisch kompiliert und verschiedenen Tests unterzogen, anschliessend durch (idealerweise automatisierte) Review- und Genehmigungsprozesse geschickt und, wenn alles gut verläuft, wird die neu erstellte Version in die Produktiv-Umgebung übertragen.

Entsprechend unserer Umfrage haben lediglich knapp 25% der befragten Organisationen angegeben, ihr komplettes Change Management in einer CI/CD Pipeline abzubilden und auch Prüf- und Freigabe-prozesse darin zu berücksichtigen. Damit fehlt der Mehrheit der Organisationen eine kontinuierliche und automatisierte Überwachung über den gesamten Lifecycle der Applikation.

Angenommen ein Change durchläuft die klassische CI/CD Pipeline und ist grundsätzlich bereit für das Deployment. Dann steht noch eine letzte Hürde bevor – das Security Testing. Insbesondere bei öffentlich zugänglichen Applikationen (Banking Apps, Social Media Apps, E-Commerce-Plattformen, Cloud Services usw.) muss sichergestellt werden, dass keine Verwundbarkeiten mehr vorhanden sind. Das Testen durch ein Security Team kann jedoch Tage oder gar Wochen dauern. Durch die Integration von Security schon von Beginn an, kann der DevOps-Prozess deutlich effizienter und das Ergebnis sicherer gemacht werden. Die Integration von Security in die CI/CD Pipeline beinhaltet sowohl ein entsprechendes Coaching von Entwicklern durch das Security Team (Verantwortlichkeiten, Awareness, OWASP etc.), als auch den Einsatz von geeigneten Tools.

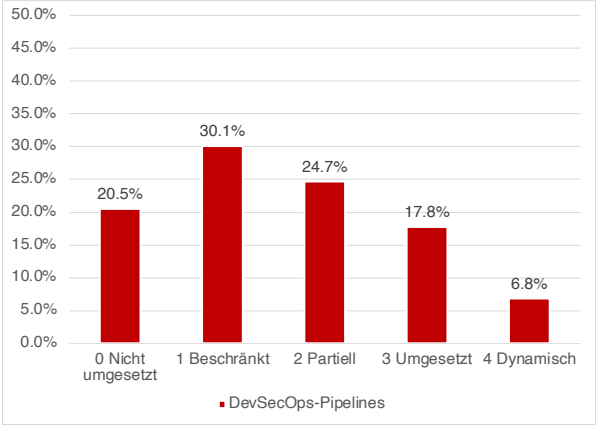


Abbildung 4: Ich bilde mein komplettes Change Management in CI/CD Pipelines ab und habe auch Prüf- und Freigabeprozesse darin integriert.

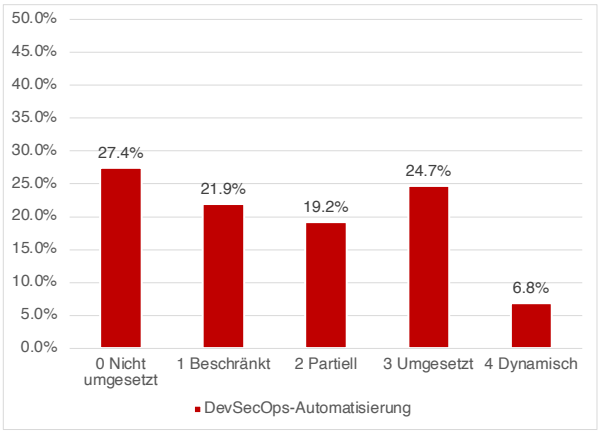


Abbildung 5: Ich nutze technische Werkzeuge, um meine Systeme und Applikationen regelmässig und vollautomatisiert auf Schwachstellen zu prüfen.

Über 68% der befragten Unternehmen geben an, nicht über die entsprechenden Tools zu verfügen, um ihr IT-System regelmässig von Anfang an auf Schwachstellen zu prüfen. Damit bleibt Security als notwendiges Übel sowie letzter Schritt vor Deployment bestehen und

verharrt in der Rolle als externer Überwacher des DevOps-Prozesses, anstatt eine Coaching-Rolle zu übernehmen und Security kooperativ mit den Entwicklern anzugehen.

Durch die Integration von Security in den DevOps-Prozess kann die Umsetzung von möglichst sicheren Applikationen adressiert werden. Im laufenden Betrieb wird jedoch zusätzlich eine Überwachung des Zustands und der Version der Systeme erforderlich (Security Monitoring). Damit soll eine rasche und effiziente Handhabung von Sicherheitsrisiken, Schwachstellen oder Vorfällen sichergestellt werden. Die Log4j-Schwachstelle[3] hat die Wichtigkeit dieser Thematik ein weiteres Mal aufgezeigt. Um ein Verständnis über verwundbare Systeme und Komponenten betreffend Log4j zu erlangen, respektive das Deployment der Patches zu koordinieren und kontrollieren, ist eine entsprechende Visibilität unumgänglich.

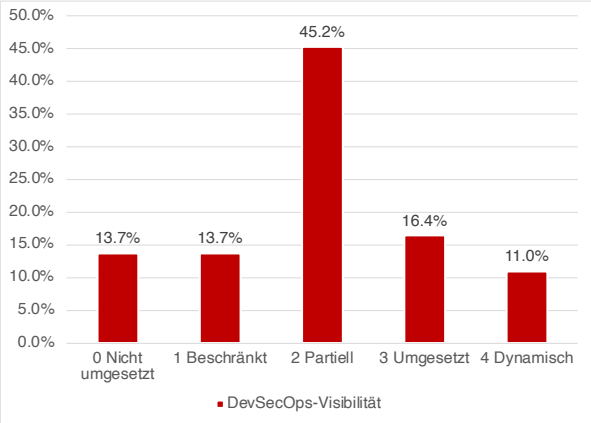


Abbildung 6: Ich kenne zu jedem Zeitpunkt den Status und die Version aller laufenden Systeme und deren Komponenten – insbesondere in Bezug auf deren Sicherheit.

Knapp 73% der befragten Organisationen geben an, dass sie über keine oder lediglich eine beschränkte Übersicht über den Status und die Version aller laufenden Systeme und damit verbunden deren Sicherheitszustand verfügt.

[3] Unter Log4J versteht man die kritische Schwachstelle CVE-2021-44228 [MIT2021] (Log4Shell) sowie zwei weitere Schwachstellen (CVE-2021-45046, CVE-2021-45105) in der weit verbreiteten Java-Bibliothek.

4. Resultate Cloud Security

Laut dem 2021 ISG Provider Lens™ Public Cloud – Services & Solutions Report for Switzerland gilt in der Geschäftsleitung von Schweizer Organisationen weiterhin ein wachsender Fokus auf die Cloud und ein entsprechendes Budget. Beim Gang in die Cloud (egal ob Microsoft Azure, Google Cloud, AWS oder eine sonstige Lösung) gilt, dass der Fokus auf Security nicht vergessen gehen darf. Wichtig ist dabei die Übersicht über die bezogenen Lösungen, die geteilte Zuständigkeit und auch die Notfallplanung.

Ein Unternehmen kann nur das schützen, was es auch effektiv sehen kann. Die Transparenz in der Cloud ist daher ein entscheidender Erfolgsfaktor für die Sicherheit. Mit der zunehmenden Beliebtheit der Cloud übernehmen die einzelnen Abteilungen einer Organisation jedoch zunehmend die Verantwortung für die Beschaffung der benötigten Ressourcen. Server und Rechenleistung online zu buchen, ist zunächst die einfachste und schnellste Lösung. Doch dieser Ansatz bringt auch Gefahren mit sich. Mit 55% behaupten über die Hälfte der befragten Organisationen, dass sie über eine unzureichende Übersicht (Transparenz) betreffend Verfügbarkeit, Nachvollziehbarkeit und Integrität ihrer in der Cloud verarbeiteten Dateien verfügen.

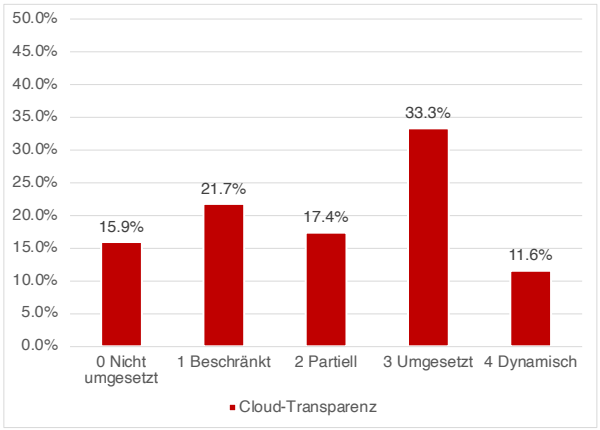


Abbildung 7: Ich habe einen Überblick bezüglich eingesetzten Cloud-Lösungen und die darin verarbeiteten Daten sowie deren Anforderungen bezüglich Verfügbarkeit, Nachvollziehbarkeit und Integrität.

Das Shared Responsibility-Modell ist das «Modell der geteilten Verantwortung». Es bildet eine wichtige Basis für jedes Cloud Security-Konzept. Es beschreibt die geteilte Verantwortung zwischen Leistungsbezüger und Cloud-Anbieter. Bei mangelnder Sorgfalt kann es beim Thema Sicherheit schnell zu Problemen kommen und Sicherheitsaspekte im gegenseitigen Missverständnis untergehen.

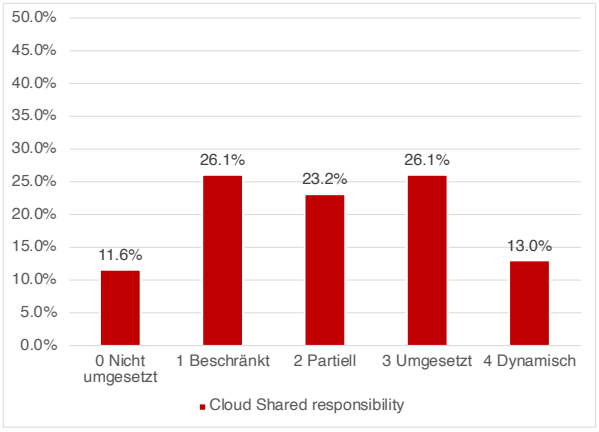


Abbildung 8: Ich stelle sicher, dass die Rollen und Zuständigkeiten zwischen Cloud-Anbieter, externen Dienstleistern und meinem Unternehmen für die cloudbasierten Lösungen klar definiert und organisatorisch implementiert sind.

Fast zwei Drittel (61%) der befragten Organisationen geben an, die Rollen und Verantwortlichkeiten zwischen Cloud-Anbieter und Leistungsbezügern nicht oder nur unzureichend zu definieren. «Der Mangel an Transparenz bezüglich Rollen und Zuständigkeiten ist einer der häufigsten Feststellungen bei unseren Cloud Security Assessments.», sagt Daniel Michel, Team Leader Cloud Security bei Redguard. In dieser Situation kann nicht sichergestellt werden, dass Sicherheitsaspekte in ausreichendem Masse

berücksichtigt werden, da noch nicht einmal deren Verantwortung ausreichend geklärt ist. Dies bildet laut unserer Erfahrung einen der klassischen Fallstricke hinsichtlich Umsetzung der Cloud-Strategie und sollte zwingend adressiert werden. Klar definierte Verantwortlichkeiten sind eine der Voraussetzungen, um Informationssicherheit in der Cloud erfolgreich umzusetzen.

Das Notfall-Management ist leider immer noch häufig ein unterrepräsentiertes Thema in Schweizer Organisationen. Die Notfallplanung im Cloud-Bereich bildet dabei keine Ausnahme. Es bestehen ausserdem neben dem BSI 100-4 Standard nur wenige praktische Leitfäden dazu. Das Vertrauen in den Dienstleister ist oftmals gross und dementsprechend auch die Überraschung bei einem Vorfall. So geben denn auch 62% der befragten Unternehmen an, nicht oder nur beschränkt über Notfallpläne betreffend ihrer bezogenen Cloud-Dienstleistungen zu verfügen. Wie in «klassischen Setups» gilt auch hier, dass Kosten-Nutzen berücksichtigend Entscheidungen betreffend Redundanzen und Kritikalität getroffen werden müssen.

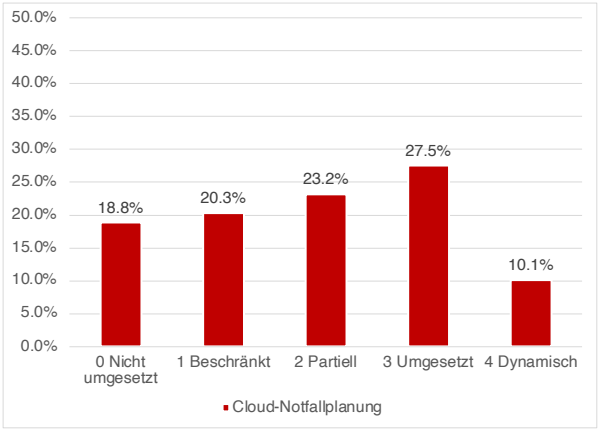


Abbildung 9: Ich stelle sicher, dass bei einem Ausfall der Cloud-Lösung der Geschäftsbetrieb weitergeführt werden kann und die Wiederherstellungspläne vorhanden sind. Die Backup- und Restore-Vorgehen sind definiert und werden regelmässig geprüft.

5. Drei Ansätze um Cyber Security als Organisation anzugehen

Zur Umsetzung des IKT-Minimalstandards (oder auch eines anderen Security-Rahmenwerks wie dem Cloud Controls Matrix (CCM) der Cloud Security Alliance oder dem ISO 27001 Cyber Security Standard aber auch beispielsweise der Einführung von DevSecOps) stehen jeder Organisation drei Wege zur Verfügung:

Independent – Selbstständige Umsetzung

Jeder Organisation steht es offen, Informationssicherheit eigenständig und mit vorhandenen Tools, Hilfestellungen und Fachwissen umzusetzen. Der IKT-Minimalstandard inklusive seinem Assessment-Tool steht auf der Website der Bundesverwaltung zur freien Verfügung. Ausserdem bietet Redguard eine Umsetzungshilfe mit den wichtigsten Massnahmen zur Einhaltung des IKT-Minimalstandard an, mit Hilfe dessen eine Organisation alle notwendigen Sicherheitsmassnahmen identifizieren und selbständig angehen kann. Eine weitere grosse Hilfe bei der Identifizierung von einfachen Massnahmen und ein guter Startpunkt für Organisationen bildet die Webseite des Nationalen Zentrums für Cybersicherheit. Dort finden Organisationen Informationen über aktuelle Bedrohungen, aber auch einige praktische Tipps und Tricks im Umgang mit den wichtigsten Risiken. Das NCSC hat zudem eine spezifische Hilfestellung für KMUs erstellt und stellt einen Link zum Cyber Security-Schnell-Check von digitalswitzerland zur Verfügung. KMUs welche sich ohne Schnell-Check direkt an die Umsetzung von Massnahmen wagen, können beispielsweise den 10-Punkte-Plan der Information Security Society Switzerland (ISSS) als Grundlage verwenden.

Ressource	Link
IKT-Minimalstandard	https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html
Umsetzungshilfe	https://www.redguard.ch/downloads/redguard_umsetzungshilfe_iktminimalstandard.pdf
NCSC	https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen.html
Hilfe für KMU	https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/schuetzen-sie-ihr-kmu.html
KMU Schnell-Check	https://digitalswitzerland.com/de/kmu-schnell-check/
ISSS 10-Punkte-Plan für KMU	https://www.kmu.admin.ch/dam/kmu/de/dokumente/savoir-pratique/Informatique-et-IT/InfoSurance_10_Points_Programme_FR.pdf.download.pdf/InfoSurance_10_Points_Programme_FR.pdf

Assisted – Umsetzung mit Unterstützung

Organisationen, welche Unterstützung bei der Umsetzung des IKT-Minimalstandards beanspruchen möchten und sich damit auf einen systematischen und effizienten Weg begeben, starten häufig mit einer Standortbestimmung. Mit einer Standortbestimmung durch einen externen Dienstleister wie Redguard erhält eine Organisation eine Übersicht über das aktuelle Sicherheitsniveau (wird beispielsweise der IKT-Minimalstandard bereits eingehalten oder nicht) und eine priorisierte Liste von Massnahmen, welche noch umgesetzt werden können.

Basierend auf den Resultaten der Standortbestimmung kann eine Organisation entscheiden, welche Massnahmen nun eigenständig weiterverfolgt und welche Massnahmen mit der Unterstützung von Redguard weitergetrieben werden. Somit lassen sich bestehende Ressourcen und Fachwissen optimal einsetzen und eine kostengünstige Umsetzungsvariante verfolgen. Dieser Ansatz eignet sich ausserdem, um interne Fachexperten durch gemeinsame Arbeiten mit Redguard zu «coachen» und dabei ihr Security Know-how noch weiter zu vertiefen.

Ressource	Link
Standortbestimmung	https://www.redguard.ch/consulting/risk-and-compliance/ https://www.redguard.ch/downloads/factsheet_ikt_minimalstandard_de.pdf

CISOaaS – Einen externen CISO beauftragen (Chief Information Security Officer as a Service)

Eine Organisation, welche aus Gründen des Ressourcen-Engpasses, fehlender Fachexpertise oder Personalfluktuation auf umfassende und kompetente Unterstützung im Bereich Informationssicherheit angewiesen ist, kann sich für kürzere oder längere Zeit einen CISO als Dienstleistung beziehen (CISOaaS). Der externe CISO (Informationssicherheits-verantwortliche) übernimmt dabei die Verantwortung für die Identifikation und Umsetzung jeglicher informationssicherheitsrelevanten Massnahmen und steht Fachexperten, Geschäftsleitung und allenfalls Verwaltungsrat als Hauptansprechperson zur Verfügung.

Gemeinsam mit dem zur Verfügung gestellten CISO werden die wichtigsten Massnahmen und der Umsetzungshorizont festgelegt. Entscheidet sich eine Organisation für die CISOaaS-Dienstleistung von Redguard, erhält diese nicht nur eine erfahrene und kompetente Person mit den notwendigen Fachkenntnissen, sondern auch Zugriff auf das gesamte Redguard-Netzwerk mit seiner gesamten Fachexpertise. So stehen einem CISOaaS von Redguard all seine rund 60 Kolleginnen und Kollegen mit all ihren dedizierten Fachkenntnissen zur Verfügung und können je nach Anforderung und in Absprache für spezifische Massnahmen eingesetzt werden.

Ressource	Link
CISOaaS	https://www.redguard.ch/consulting/security-officer-and-architect/ https://www.redguard.ch/downloads/redguard_success_story_coop_mineraloel_de.pdf

6. Massnahmen

6.1. Massnahmen DevSecOps

DevSecOps fühlt sich für die Beteiligten oft wie ein Puzzle mit noch nicht zusammengefügten Teilen an. Ein ganzheitlicher Partner wie die Redguard unterstützt Sie dabei, diese optimal miteinander zu verbinden und alle Stakeholder einzubinden.

Leistungsübersicht DevSecOps

Organisation

Der Erfolg von DevSecOps bedingt ein organisationsweites einheitliches Verständnis und entsprechende Prozesse. Mit unserem DevSecOps Assessment erheben wir den aktuellen Maturitätsgrad und unterstützen Sie bei der Ausarbeitung von DevSecOps-Prozessen und -Konzepten unter Berücksichtigung aller Stakeholder.

Technik

Gut aufeinander abgestimmte Systeme und Werkzeuge setzen die vorab definierten Prozesse um, schaffen einheitliche Abläufe und erreichen einen möglichst hohen Automatisierungsgrad. Wir unterstützen Sie beim Aufbau einer neuen Pipeline (Architektur, Evaluation und Umsetzung) oder erweitern Ihre bestehende Pipeline um weitere Sicherheitselemente.

Mensch

Um den Erfolg von DevSecOps nachhaltig sicherzustellen, muss auch internes Know-how aufgebaut werden. Wir bieten hierfür sowohl grundlegende Einführungsworkshops ins Thema DevSecOps aber auch tiefgehende Trainings für Fachspezialisten an, beispielsweise im Bereich Container- und Kubernetes-Sicherheit.

6.2. Massnahmen – Cloud Security

Der Trend «weg vom on-prem-Betrieb und hin zur Cloud-Lösung» ist aktuell sehr stark. Bei anhaltender Tendenz werden sich in naher Zukunft ein Grossteil der Schweizer Unternehmen mit der Cloud und mit seinen Security-Aspekten auseinandersetzen. Haben auch Sie vor, eine Cloud-Strategie anzugehen oder haben Sie diese bereits umgesetzt und möchten nun auch noch die Sicherheit Ihrer neuen Lösung sicherstellen? Dann unterstützen wir Sie gerne bei Ihrem Cloud-Ansatz, z. B. mit einem Cloud Security Assessment.

Cloud Security Assessment

In unserem Cloud Security Assessment prüfen wir das Sicherheitsniveau Ihrer Organisation mit Fokus auf Cloud Security. Wir beurteilen die Prozesse zur Unterstützung und Aufrechterhaltung der Informationssicherheit in diesem Bereich. Die Beurteilung erfolgt unter Berücksichtigung von branchenspezifischen gesetzlichen Vorgaben sowie internationalen Best Practices wie beispielsweise der Cloud Security Alliance (CSA) oder C5 des BSI. Anhand unserer Interviews und Stichproben stufen wir die Maturität Ihres Sicherheitsniveaus ein und liefern Ihnen einen Gesamtbericht sowie konkrete Verbesserungsempfehlungen.

Weitere Informationen: https://www.redguard.ch/consulting/risk-and-compliance/

6.3. Massnahmen – Incident Response

Auch wenn Sie sich vorbereiten und Ihre Mitarbeitenden schulen, kann es zu einem Sicherheitsvorfall kommen. Bei einem Angriff ist es von zentraler Bedeutung, dass Sie unmittelbar und zielgerichtet reagieren. Unsere Security-Spezialisten unterstützen Sie bei der optimalen Vorbereitung. Während einem Vorfall können Sie zudem auf die Unterstützung unseres Incident Response Teams zählen. Wir stellen sicher, dass keine wertvolle Zeit verloren geht und der Schaden für Ihr Unternehmen möglichst gering bleibt.

Incident Response Team – Im Notfall nicht alleine

Wir unterstützen Sie rund um die Uhr bei der Eindämmung und der Analyse von Cyber-Vorfällen und bei der Wiederherstellung Ihres Geschäftsbetriebs. Ihr Incident Response Team deckt alle notwendigen Expertisen ab (Technologie, regulatorische Vorgaben usw.) und ist mit Behörden und anderen IR-Teams im ständigen Kontakt. Wir sorgen für einen strukturierten Ablauf und kühle Köpfe.

Weitere Informationen: https://www.redguard.ch/consulting/cyber-security-incident/

7. Anhang

7.1. Anhang 1: Vorstellung Quick-Test

Umfrage zum IKT-Minimalstandard

Der für diese Studie entwickelte Quick-Test lehnt sich an die fünf Funktionen des IKT-Minimalstandards an und besteht aus zehn spezifischen Fragen. Dies erlaubt eine Aussage über das Maturitätsniveau der befragten Organisationen. Den Quick-Test finden Sie unter:

(DE) http://ikt.redguard.ch (FR) http://ikt-fr.redguard.ch

Nr.	Frage
1	**Risiken und Verwundbarkeiten (Identifizieren)** Ich erhebe Risiken sowie Verwundbarkeiten und identifiziere kritische Systeme.
2	**Cyber Security-Strategie (Identifizieren)** Ich habe Vorgaben zur Cyber Security in meinem Unternehmen erlassen, zum Beispiel in Form einer Strategie und Richtlinien/Vorgaben.
3	**Richtlinien & Prozesse (Schützen)** Ich erstelle Richtlinien zum Schutz von Informationssystemen und Betriebsmitteln, inklusive Prozess zur kontinuierlichen Verbesserung und Weiterentwicklung der Informationssicherheit.
4	**Awareness & Training (Schützen)** Ich stelle sicher, dass alle Mitarbeitenden unserer Organisation bezüglich Informationssicherheit stufen- und funktionsgerecht geschult sind und ihre Verantwortung sowie das korrekte Verhalten kennen.
5	**Erkennen/Monitoring (Erkennen)** Ich etabliere ein kontinuierliches System- und Netzwerkmonitoring, um potenzielle Cyber Security-Vorfälle zu entdecken.
6	**Erkennen/Eingrenzen (Erkennen)** Ich unterhalte einen Prozess, durch welchen ich sicherstelle, dass Auffälligkeiten sowie sicherheitsrelevante Ereignisse zeitgerecht erkannt und Auswirkungen des potenziellen Vorfalls verstanden werden.
7	**Meine Organisation ist für wichtige Eventualitäten gerüstet (Reagieren)** Ich habe einen Prozess zur Reaktion auf eingetretene Vorfälle – zum Beispiel Business Continuity Management, Incident Response Planning, Disaster Recovery – erarbeitet und teste diesen regelmässig.
8	**Incident Management-Prozess (Reagieren)** Ich stelle sicher, dass Cyber Security-Vorfälle eingegrenzt werden können, die weitere Ausbreitung unterbrochen wird und dadurch die Auswirkungen eines Vorfalls gemindert werden können.
9	**Wiederherstellungsplanung (Wiederherstellen)** Ich stelle sicher, dass ich über einen Wiederherstellungsplan verfüge, welcher so durchgeführt werden kann, dass nach einem Vorfall eine zeitnahe Wiederherstellung der Systeme gewährleistet ist.
10	**Kommunikationsplan (Wiederherstellen)** Ich habe für einen Cyber Security-Vorfall einen Kommunikationsplan vorbereitet und stelle sicher, dass die öffentliche Wahrnehmung meiner Organisation im Ereignisfall aktiv angegangen wird.

Umfrage zu DevSecOps

Nr.	Frage
1	**Visibilität** Ich kenne zu jedem Zeitpunkt den Status und die Version aller laufenden Systeme und deren Komponenten – insbesondere in Bezug auf deren Sicherheit.
2	**Pipelines** Ich bilde mein komplettes Change Management in CI/CD Pipelines ab und habe auch Prüf- und Freigabeprozesse darin integriert.
3	**Automatisierte und wiederkehrende Sicherheitsüberprüfungen** Ich nutze technische Werkzeuge, um meine Systeme und Applikationen regelmässig und vollautomatisiert auf Schwachstellen zu prüfen.

Umfrage Cloud Security

Nr.	Frage
1	**Transparenz** Ich habe einen Überblick bezüglich eingesetzten Cloud-Lösungen und die darin verarbeiteten Daten sowie deren Anforderungen bezüglich Verfügbarkeit, Nachvollziehbarkeit und Integrität.
2	**Shared responsibility** Ich stelle sicher, dass die Rollen und Zuständigkeiten zwischen Cloud-Anbieter, externen Dienstleistern und meinem Unternehmen für die cloudbasierten Lösungen klar definiert und organisatorisch implementiert sind.
3	**Notfallplanung** Ich stelle sicher, dass bei einem Ausfall der Cloud-Lösung der Geschäftsbetrieb weitergeführt werden kann und die Wiederherstellungspläne vorhanden sind. Die Backup- und Restore-Vorgehen sind definiert und werden regelmässig geprüft.

7.2. Anhang 2: Vorstellung Maturitätsskala

Jede der zehn Fragen des Quick-Tests kann anhand einer Skala von 0–4 bewertet werden. Die Werte für die Fragen werden gemittelt, sodass für jede der fünf Funktionen (Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen) das Maturitätsniveau erhoben werden kann.

Niveau	Antwort
0 – Nicht umgesetzt	Dieser Punkt wäre für meine Organisation wichtig, bis anhin besteht dazu jedoch nur sehr beschränkt etwas.
1 – Partiell umgesetzt	Prozess/Vorgabe ist nicht vollständig definiert und nicht abgenommen.
2 – Partiell umgesetzt	Prozess/Vorgabe ist zwar mehr oder weniger vollständig definiert und abgenommen, aber mindestens teilweise schon etwas veraltet.
3 – Umgesetzt	Prozess/Vorgabe ist vollständig definiert und grösstenteils umgesetzt. Er/sie ist auch relativ neu und immer noch gültig und korrekt. Die Herangehensweise ist jedoch grösstenteils statisch.
4 – Dynamisch	Prozess/Vorgabe ist vollständig umgesetzt. Er/sie wird kontinuierlich überprüft, regelmässig verbessert und dessen Effizienz sichergestellt.

Mehr zum IKT-Minimalstandard:

- Website des Bundesamtes für wirtschaftliche Landesversorgung
  https://www.bwl.admin.ch/
- Factsheet IKT-Minimalstandard von Redguard
  https://www.redguard.ch/downloads/factsheet_ikt_minimalstandard_de.pdf
- Website von Redguard
  https://www.redguard.ch/