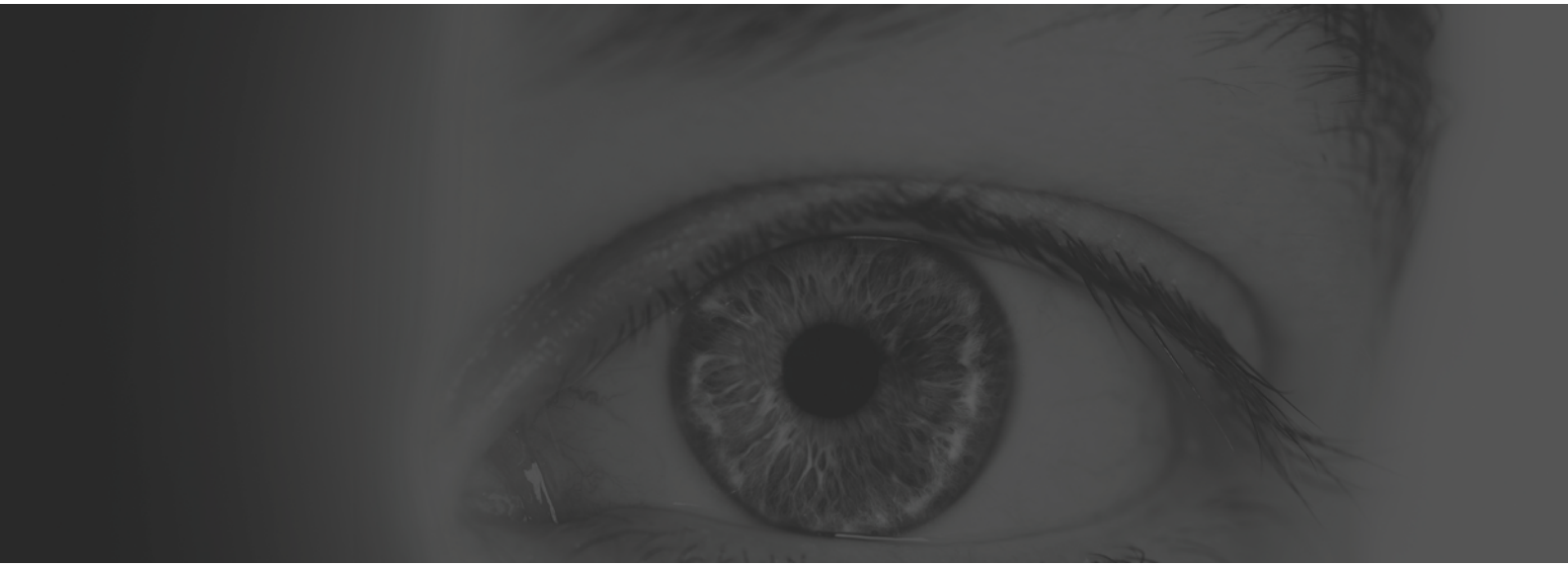


Redguard

Security Survey

2021

REDGUARD
SECURING YOUR ASSETS

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 überhaupt noch Handlungsbedarf oder verfügen die Schweizer Organisationen und Unternehmen bereits über ein ausreichendes Sicherheitsniveau? Diese Fragen werden im Redguard Security Survey 2021 beantwortet.

Zum dritten Jahr infolge publiziert die Redguard AG die Resultate ihrer Umfrage zum IKT-Minimalstandard. Auch dieses Jahr haben wir wieder weit 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 (www.ikt-redguard.ch).

Immer noch ist eine grosse Anzahl von Organisationen unzureichend vorbereitet für Cyber-Security-Vorfälle. Sowohl präventive Massnahmen aber insbesondere auch reaktive Aspekte werden laut Aussagen der Umfrageteilnehmenden nur unzureichend adressiert. So gaben beispielsweise knapp zwei Drittel der befragten Organisationen an, nur unzureichend auf einen Vorfall vorbereitet zu sein (z.B. mit einer Incident Management Planung oder einem Business Continuity Plan).

Informationssicherheit ist kein Zustand, welchen man endgültig erzielen kann, sondern ein Prozess, welchen man lebt, sowie ständig überprüft und weiterentwickelt. So muss man auch der Realität entgegentreten, dass eine Organisation nie hundertprozentig gegen Cyber-Risiken gewappnet ist und ein Vorfall trotz aller Massnahmen grundsätzlich jederzeit eintreten kann. Die Vorbereitung auf einen Vorfall mit einem entsprechenden Backup, dessen Wiederherstellung regelmässig getestet wird, ist ein erster Schritt in die richtige Richtung. Jedoch sollte sich jede Organisation auch Gedanken machen, wie konkret bei einem Vorfall reagiert werden kann (Incident Management) und welche Prozesse noch aufrechterhalten werden können (Business Continuity Management). Das letzte Jahr hat uns gezeigt, dass die unzureichende Vorbereitung auf einen Vorfall gar über die weitere Existenz einer Organisation mitentscheiden kann. Die Swiss Windows AG beispielsweise sah sich nach einem Ransomware-Angriff, welcher zu einem Produktionsausfall führte, gezwungen, Konkurs anzumelden.[2] Solche Produktionsausfälle müssen nicht sein und um diesen entgegenzuwirken, hat das Bundesamt für wirtschaftliche Landesversorgung den IKT-Minimalstandart publiziert. Mit dessen Hilfe kann sich eine Organisation sowohl präventiv vor Vorfällen schützen, aber auch eine Systematik entwickeln, durch welche die Organisation ihre Kernprozesse möglichst resilient gestaltet (BCM) und rasch betroffene Systeme wiederherstellen kann.

Für Ihre Unterstützung bedanken wir uns herzlichst
Ihr Redguard Team

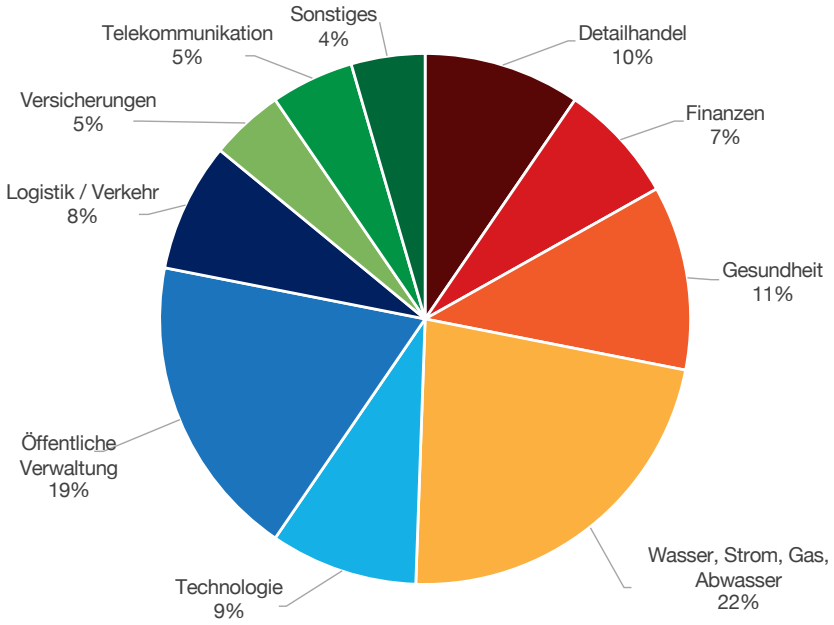
[1] IKT (Informations- und Kommunikationstechnologie) -Minimalstandard des Bundesamtes für wirtschaftliche Landesversorgung (BWL): https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html

[2] SRF: https://www.srf.ch/news/regional/ostschweiz/konkurs-fensterhersteller-offenbar-zwang-eine-cyberattacke-swisswindows-in-die-knie

Rückmeldungen zum Quick-Test IKT-Minimalstandard

Die Ergebnisse der 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.

Der von Redguard entwickelte Quick-Test zum IKT-Minimalstandard besteht aus zehn Fragen, welche auf die Kernelemente des IKT-Minimalstandards abzielen. Dabei werden die Themen Risikomanagement, Cyber-Security-Strategie, Awareness & Training, Überwachung von Systemen, Incident Management, Business Continuity Management, Disaster Recovery sowie Krisenkommunikation abgedeckt.



*Sonstiges:

Bau	42.9%
Ingenieurbüro	28.6%
Medien	14.3%
Kommunikation	14.3%
Einzelfirma	14.3%

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 179 Organisationen aus verschiedenen Branchen eine grosse Anzahl für den Standard interessiert und ihre Selbsteinschätzung abgegeben.

Abbildung 1 zeigt, dass die Security Survey breit abgestützt ist. Die teilenehmenden Unternehmen und Organisationen stammen aus den unterschiedlichsten Branchen, wobei auch der öffentliche Sektor angemessen vertreten ist. Gleichzeitig haben Unternehmen unterschiedlichster Grösse zur Security Survey beigetragen (vgl. Abbildung 1). Nach Angaben der Teilnehmenden handelt es sich bei 22% um grosse Unternehmen mit über 500 Mitarbeitenden. Die restlichen knapp 80% der teilnehmenden Unternehmen und Organisationen verteilen sich mit 40% Kleinunternehmen (1-50 MA) und 38% mittelgrossen Unternehmen (50-500 MA) etwa gleichmässig.

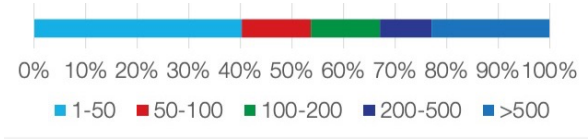


Abbildung 1: Befragte Unternehmen nach Anzahl Mitarbeitenden

Die Mehrheit der Organisationen hält den IKT-Minimalstandard nicht ein

Das von den knapp 180 befragten Organisationen eingestufte Sicherheitsniveau liegt auch 2021 noch deutlich unter dem von Bund und Verbänden empfohlenen Minimalniveau. Im vergleich zu den Vorjahren haben sich einige Werte noch weiter verschlechtert. Dies lässt darauf deuten, dass ein Grossteil der Unternehmen (insbesondere KMU) ohne Unterstützung durch externe Partner wie Redguard, nicht in der Lage sind den IKT-Minimalstandard umzusetzen.

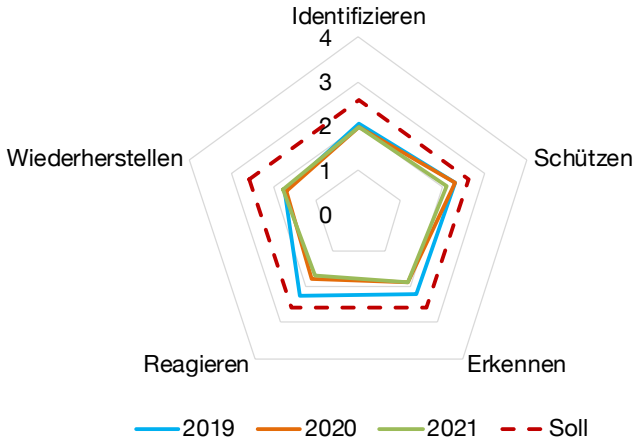


Abbildung 2: Ergebnisse der Redguard Security Survey

	2019	2020	2021	Soll
Identifizieren	2.0	2.0	2.0	2.6
Schützen	2.3	2.3	2.1	2.6
Erkennen	2.2	1.9	1.9	2.6
Reagieren	2.2	1.8	1.7	2.6
Wiederherstellen	1.7	1.7	1.8	2.6

Tabelle 2: Ergebnisse in Zahlen im Jahresvergleich

Abbildung 3 zeigt, dass laut eigener Einschätzung eine Mehrheit der befragten Organisationen das minimale Sicherheitsniveau des IKT-Minimalstandards noch nicht erreicht.

Funktion	Nicht-Erfüllt	Erfüllt
Identifizieren	62%	38%
Schützen	55%	45%
Erkennen	63%	37%
Reagieren	71%	29%
Wiederherstellen	70%	30%
Total	64%	36%

Tabelle 1: Survey Ergebnisse bezüglich der fünf Funktionen

Ein Blick auf die Antworten (Tabelle 1) aufgeteilt in die fünf Funktionen des IKT-Minimalstandards verdeutlicht, dass nur gerade 36% der Organisationen der Ansicht sind, das vom IKT-Minimalstandard geforderte Sicherheitsniveau zu erreichen.

Auffällig dabei ist, dass sich Unternehmen bei den Funktionen Identifizieren, Schützen und Erkennen deutlich besser bewerten als bei den zwei Funktionen Reagieren und Wiederherstellen.

Eine mögliche Erklärung dafür ist, dass Ransomware-Vorfälle erstens erhebliches Verbesserungspotential bei der korrekten Reaktion auf Cyber-Security-Vorfälle und zweitens die Wichtigkeit von Reaktions- und Wiederherstellungsplänen aufgezeigt haben.

Ausserdem fällt auf, dass sich das Sicherheitsniveau in den letzten beiden Jahren stagniert oder sich gar kontinuierlich verschlechtert hat. So haben sich, wie in Tabelle 2 ersichtlich, die Funktionen Schützen, Erkennen und Reagieren über die letzten beiden Jahre gesehen verschlechtert, währen sich die Wiederherstellungsfähigkeiten leicht verbessert haben und die Fähigkeiten im Bereich Identifizieren gleichgeblieben sind. Dies lässt darauf schliessen, dass Organisationen (insbesondere KMU) den IKT-Minimalstandard nur bedingt selbständig umsetzen können und auf externe Unterstützung, beispielsweise durch Redguard angewiesen sind.

Für den Ernstfall sind viele Unternehmen noch immer unzureichend vorbereitet

Die Redguard Security Survey zeigt, dass die Mehrheit der teilnehmenden Unternehmen nach wie vor unzureichend auf einen Cyber-Security-Vorfall vorbereitet sind. Ein Grossteil der teilnehmenden Unternehmen hat gemäss eigenen Angaben keinen vollständig umgesetzten Prozess für Cyber-Security-Vorfälle (65%).

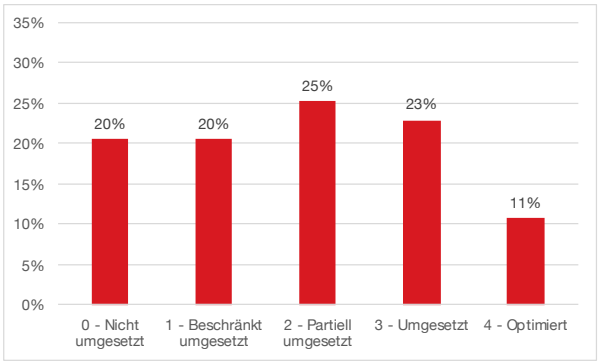


Abbildung 3: Incident Managent Prozess für Cyber-Security-Vorfälle

Ohne entsprechenden Prozess ist es unwahrscheinlich, dass Cyber-Security-Vorfälle rechtzeitig erkannt, eingegrenzt und der entstandene Schaden behoben werden kann. Bestätigt wird dieses Bild dadurch, dass wiederum einer Mehrheit der Organisationen angibt, für wichtige Eventualitäten nur unzureichend gerüstet zu sein (75%).

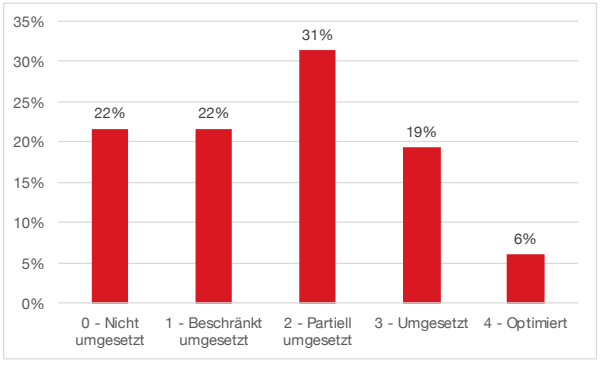


Abbildung 4: Definierte und getestete Disaster Recovery / Business Continuity Management

Nach deren Angaben fehlen Pläne für Disaster Recovery und Business Continuity Management entweder komplett oder sofern diese vorhanden sind, werden diese nicht regelmässig getestet. Im Ernstfall geht dadurch wichtige Zeit verloren, da Verantwortlichkeiten und Zuständigkeiten zuerst geklärt, die richtigen Personen alarmiert und mögliche Massnahmen erarbeitet werden müssen. Gleich verhält es sich bei der Krisenkommunikation. Nur weniger als ein Drittel der teilnehmenden Organisationen verfügt über einen Kommunikationsplan (28%).

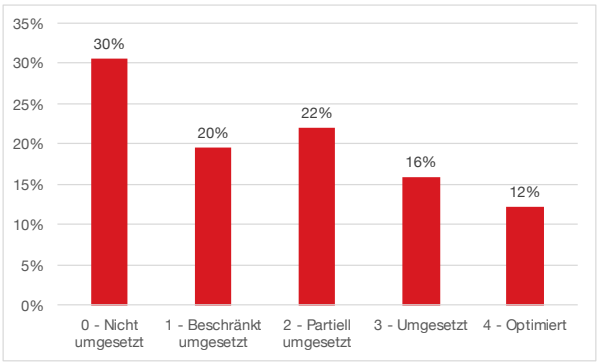


Abbildung 5: Vorhandensein eines Kommunikationsplans

Ein fehlender Kommunikationsplan kann dazu führen, dass ein Cyber-Security-Vorfall schnell zu einer Krise eskaliert. Keine Reaktion respektive Kommunikation impliziert oft Schuld und fördert die Verbreitung von Gerüchten (Stichwort: Social Media und Online-Medien).

Im Gegensatz dazu kann eine ehrliche, schnelle und sachliche Kommunikation in einer Krise deeskalierend wirken. Zudem kann damit die öffentliche Wahrnehmung der eigenen Organisation im Ereignisfall aktiv angegangen werden.

Ein definierter Prozess kombiniert mit vorbereiteten Disaster Recovery und Business Continuity Plänen ist Grundvoraussetzung für die erfolgreiche Bewältigung von Cyber-Security-Vorfällen. Wird dies zusätzlich durch eine aktive und ehrliche Kommunikation begleitet, so kann der entstandene Imageschaden begrenzt werden. Im Idealfall führt ein erfolgreich bewältigter Cyber-Security-Vorfall sogar dazu, dass die eigene Organisation durch Partner und Kunden positiv wahrgenommen wird, da die Krise kompetent gemanagt wurde.

Redguard hilft Ihnen, den IKT-Minimalstandard zu erfüllen

Der IKT-Minimalstandard ist so konzipiert, dass er von allen Unternehmen unabhängig von Branche und Grösse umgesetzt werden kann. Trotz Leitfaden und Assessment Tool des Bundesamts für wirtschaftliche Landesversorgung[3] ist fundiertes Fachwissen sowie eine pragmatische Handhabung für eine erfolgreiche Umsetzung des IKT-Minimalstandards essentiell. Redguard unterstützt Unternehmen bei der Umsetzung des IKT-Minimalstandards:

Identifizieren: Kennen Sie Ihre Risiken und gehen Sie Informationssicherheit strategisch an

- Redguard unterstützt Sie dabei, die Cyber-Risiken Ihrer Organisation zu identifizieren und systematisch zu erheben. Basierend auf Ihren Risiken erstellen Sie gemeinsam mit uns eine Informationssicherheitsstrategie, um diese Risiken zu behandeln sowie zu kontrollieren.

Schützen: Schützen Sie Ihre Systeme und schulen Sie Ihre Mitarbeitenden

- Erarbeiten Sie Vorgaben zum Schutz Ihrer Systeme und setzen Sie diese um. Redguard hilft Ihnen bei der Definition der richtigen Massnahmen in den Bereichen Zugriffsmanagement, Firewall und Netzwerkzonenkonzept sowie Schutz vor Malware.
- Technische Massnahmen allein reichen oftmals nicht: Schulen Sie Ihre Mitarbeitenden und zeigen Sie Ihnen, welchen Beitrag diese zur Informationssicherheit leisten können. Redguard unterstützt Sie entweder mit klassischen Schulungsangeboten oder mit Live Hackings und Phishing Kampagnen.

Erkennen: Kennen Sie Ihre Schwachstellen und testen Sie Ihre Verteidigung

- Richten Sie Ihre Systeme und Prozesses so ein, dass Sie in der Lage sind, mögliche Sicherheitsvorfälle zu erkennen.
- Stellen Sie Ihre Systeme und Informationssicherheit mit Penetration Tests oder einer Angriffssimulation auf die Probe. Die Spezialisten von Redguard führen in Ihrem Auftrag zielgerichtete Tests sowie Angriffe durch und zeigen Ihnen damit Verbesserungsmöglichkeiten auf.

Reagieren: Planen und üben Sie Ihre Reaktion auf Cyber-Security-Vorfälle

- Reaktionspläne helfen Ihnen, um im Ernstfall richtig zu reagieren und Zeit zu gewinnen. Mit einem Reaktionsplan haben Sie viele Fragen bereits im Vorfeld beantwortet: Wer ist in Ihrer Organisation zuständig bei einem Cyber-Security-Vorfall? Wie informieren Sie Ihre Mitarbeitenden und Kunden? Stellen Sie die Systeme komplett ab oder halten Sie einen Notbetrieb aufrecht?
- Bei Redguard können Sie den Ernstfall mittels einer Tabletop-Übung trainieren. Spielen Sie ein auf Ihre Organisation abgestimmtes Szenario Schritt für Schritt durch und leiten Sie daraus Verbesserungsmöglichkeiten und Massnahmen ab.

Wiederherstellen: Zurück zur Normalität

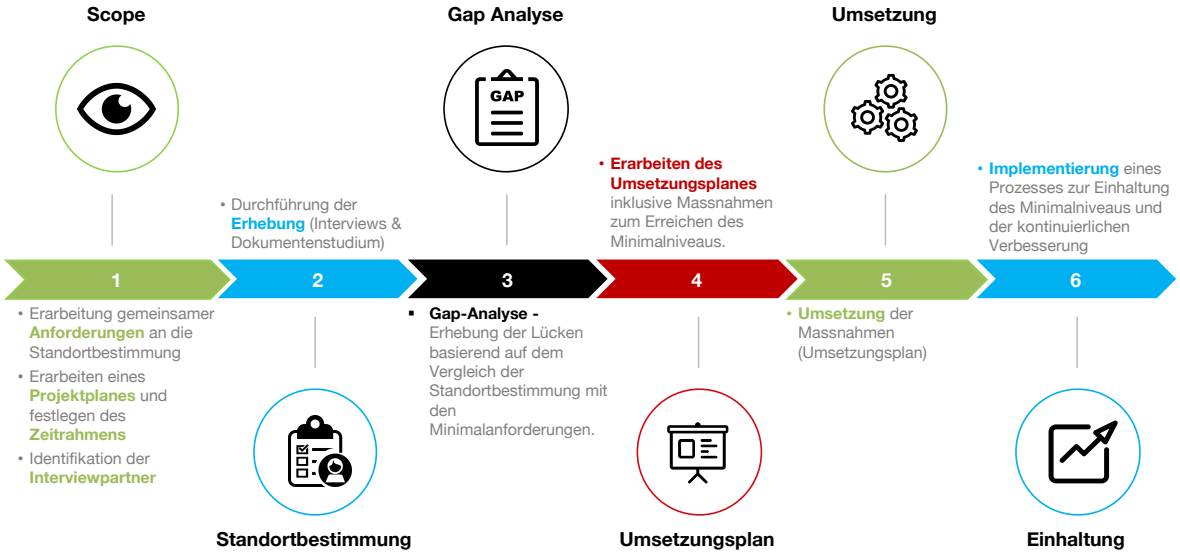
- Erstellen Sie einen Wiederherstellungsplan und setzten Sie sich konkrete Wiederherstellungsziele: Wie lange können Sie maximal ohne Ihre Systeme auskommen? Wie viel Datenverlust können Sie in Kauf nehmen?
- Redguard hilft Ihrer Organisation, das empfohlene minimale Sicherheitsniveau bei der Funktion «Wiederherstellen» zu erreichen, in den wir gemeinsam mit Ihnen Wiederherstellungspläne erarbeiten.

---

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

Ganzheitliche Umsetzung des IKT Minimalstandards

Konzentrieren Sie sich auf Ihr Kerngeschäft, während wir Ihre Informationssicherheit auf ein neues Level heben. Durch ein Team mit mehr als 50 Sicherheitsspezialisten bieten wir vollumfängliche Dienstleistungen aus einer Hand.



Standortbestimmung nach IKT Minimalstandard

Bestimmen Sie Ihre Maturität im Bereich Informationssicherheit durch eine unabhängige Stelle. Unsere Spezialisten prüfen Ihre Systeme, Dokumente und Prozesse. Daraus gewonnene Erkenntnisse werden in Interviews vertieft thematisiert. Als Lieferobjekt erhalten Sie einen Bericht mit den identifizierten Schwachstellen wie auch Massnahmen und konkreten Handlungsempfehlungen zu deren Behandlung und Verbesserung der Informationssicherheit.

CISOaaS – Umsetzung und Aufrechterhaltung des IKT-Minimalstandards

Mit der Dienstleistung «Security Officer as a Service» verfügen Sie über Ihren persönlichen Ansprechpartner, der Ihnen mit dem gesamten Know-how von Redguard zur Verfügung steht. Ihr Ansprechpartner setzt die Handlungsempfehlungen aus der Standortbestimmung als Projektleiter bei Ihrer Organisation um. Gleichzeitig sorgt er dafür, dass der IKT-Minimalstandard eingehalten und der Maturitätsgrad kontinuierlich verbessert wird.

Unterstützung im Worst-Case

Sollten Sie aller Massnahmen zum Trotz von einem Cyber-Security-Vorfall betroffen sein, so stehen Ihnen die Spezialisten der Redguard jederzeit zur Verfügung.

Anhang 1: Vorstellung Quick-Test

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:

http://ikt.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 potentielle 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 potentiellen 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)

Anhang 2: Vorstellung Maturitätsskala

Jede der zehn Fragen des Quick-Tests kann anhand einer Skala von 0–4 bewertet werden. Die Werte für beide 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:

- Quick-Test
  http://ikt.redguard.ch
- Website des Bundesamtes für wirtschaftliche Landesversorgung
  https://www.bwl.admin.ch/
- Tagesschau vom 27.08.2018
  https://www.srf.ch/news/schweiz/cyber-angriffe-auf-unternehmen-ein-minimalstandard-fuer-minimalen-schutz
- Factsheet Redguard
  https://www.redguard.ch/downloads/factsheet_ikt_minimalstandard_de.pdf
- Website von Redguard
  https://www.redguard.ch/