Redguard

Security Survey

2023

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 sieht das aktuelle Sicherheitsniveau in der Schweiz aus?

Seit fünf Jahren bitten wir Schweizer Organisationen und Unternehmen eine Selbsteinschätzung zu ihrem aktuellen Sicherheitsniveau abzugeben. Dazu haben wir, basierend auf dem IKT-Minimalstandard, einen Quick-Test entwickelt (www.ikt-redguard.ch). Wie die Resultate ausgefallen sind und welche Trends sich über die letzten Jahre zeigen, erfahren Sie in diesem Bericht.

Redguards Security Survey zum fünften Jahr in Folge

Bereits zum fünften Mal publiziert die Redguard AG die Resultate ihrer Umfrage zum IKT-Minimalstandard: Zeit für ein Résumé.

Die gute Nachricht zuerst: Unternehmen sind heute sensibilisierter für das Thema Cyber Security als noch vor einigen Jahren. Dies zeigen nicht nur die Umfragewerte der letzten Jahre, sondern auch unsere alltäglichen Gespräche mit Kunden und Unternehmen, die Unterstützung suchen.

Die schlechte Nachricht: Das ist vor allem den steigenden Meldungen von erfolgreichen Angriffen mittels Ransomware, Phishings und Co. zu verdanken. Diese häufen sich und kommen näher, was viele Unternehmen zu Gegenmassnahmen bewogen hat.

Fokus Kontinuierliche Überwachung

Trotz des Bewusstseins für Cyber Security und dem Bemühen, diese sicherzustellen, erreichen die meisten Unternehmen nicht den Minimalsicherheitslevel – und das über fünf Jahre hinweg.

Viele Sicherheitsvorfälle, die unserem Incident Response Team gemeldet wurden, hätten mit einer systematischen Überwachung vermieden werden können.

Dies hat uns dazu bewogen, während eines Jahres ein zeitgemässes Security Operations Center (SOC) mit Microsoft-Security-Technologien in der Cloud und einem dazugehörigen Team aufzubauen. Nach erfolgreicher Pilotbetriebs-Phase haben wir das SOC in unsere Schwesterfirma FusionOne ausgelagert. Mit dem SOC as a Service kann eine frühzeitige Erkennung von und Reaktion auf Cybergefahren sichergestellt werden – auch mit dem Budget eines KMUs.

Der Trend sollte zu mehr proaktiver, kontinuierlicher Überwachung gehen. Denn die Angreifer schlafen nie. Regelmässige Penetration Tests zeigen Schwachstellen – die gängigen und die, welche spezifisch Ihr Unternehmen angreifbar machen.

Um das aktuelle Sicherheitsniveau zwischen den Penetration Tests zu überwachen, bietet sich ein Continuous Security Scanning an, regelmässige und automatisierte Schwachstellen-Scans. Basierend auf über zehn Jahren Erfahrung im Auffinden von Schwachstellen hat Redguard dafür eine Schweizer Plattform entwickelt, die intuitiv bedienbar sowie verständlich ist.

Gefahren der Zukunft

Auch wenn viele neue Tools und Services entwickelt und verbessert werden, die der Cyber Security dienlich sind, werden diese einerseits noch zu wenig von Unternehmen genutzt und andererseits verändern bzw. verhärten sich auch die Cyber-Gefahren laufend.

Neue Technologien wie ChatGPT können beispielsweise Malware-Codes und Phishing-Mails schreiben, was deren Menge vervielfachen und die Ausführung perfektionieren kann. Mit diesen «Helfern» ausgestattet könnten auch bisher Unerfahrene ihre fehlenden Skills wettmachen und zu der ohnehin bereits hohen Anzahl an Angreifenden dazukommen.

[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

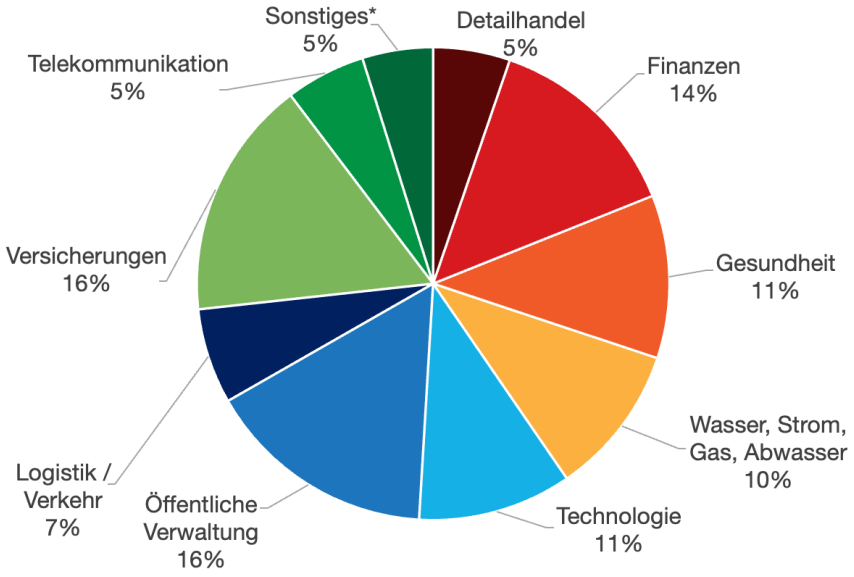
Mit Blick in die Vergangenheit, lässt sich manchmal ein Stück Zukunft erahnen. So lassen die Ergebnisse der letzten fünf Jahren darauf schliessen, dass Organisationen (insbesondere KMU) den IKT-Minimalstandard nur bedingt selbständig umsetzen können und auf externe Unterstützung, beispielsweise durch Redguard, angewiesen sind. Unser Ziel ist es seit über zehn Jahren, für Ihre Cyber-Sicherheit zu sorgen und Ihre Werte zu schützen – lieber heute als morgen.

Für Ihre Unterstützung bedanken wir uns herzlichst
Ihr Redguard Team

Redguards Quick-Test-Assessment

Die Ergebnisse der Redguard Security Surveys basieren auf einer Selbsteinschätzung der teilnehmenden Unternehmen und Organisationen. Diese 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:	
Industrie	50.0%
Beratung	16.7%
Bildung	16.7%
Ingenieursbüro	8.3%
Softwareentwicklung	8.3%

Abbildung 1: Befragte Unternehmen nach Branche (%)

An der Umfrage teilnehmende Organisationen

Redguard hat rund 2'000 Schweizer Organisationen eingeladen, ihr Sicherheitsniveau mittels Quick-Test zum IKT-Minimalstandard einzuschätzen. Auch dieses Jahr haben sich über 100 Organisationen aus verschiedenen Branchen für den Standard interessiert und ihre Selbsteinschätzung abgegeben.

Abbildung 1 zeigt, dass die Ergebnisse des Security Surveys wieder einmal breit abgestützt sind. Die teilnehmenden Unternehmen und Organisationen stammen aus den unterschiedlichsten Branchen, wobei die Ausprägung sehr ausgewogen ist. Gleichzeitig haben Unternehmen unterschiedlichster Grösse zur Security Survey beigetragen, wie wir in der Abbildung 2 sehen. Bei 41% handelt es sich nach Angaben der Teilnehmenden um grosse Unternehmen mit über 500 Mitarbeitenden. Den grösseren Anteil machen KMUs aus mit 25% Kleinunternehmen (1-50 MA) und 22% mittelgrossen Unternehmen (50-200 MA).

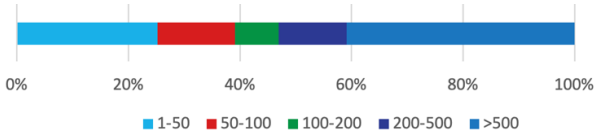


Abbildung 1: Befragte Unternehmen nach Anzahl Mitarbeitenden

IKT-Minimalstandard bei den meisten nicht erfüllt

Obwohl Unternehmen ihr Sicherheitsniveau 2023 im Vergleich zu den Vorjahren in allen Punkten besser oder gleichbleibend einschätzen, liegt auch der aktuelle Wert deutlich unter dem von Bund und Verbänden empfohlenen Minimalniveau.

Dennoch freuen uns auch die kleinen Schritte in die richtige Richtung, welche wir auch in den steigenden Anfragen von KMUs wahrnehmen. Diese sind zunehmend sensibilisiert und wissen, dass sie ein besonders beliebtes Ziel für Angreifende sind. Letztere erwarten nämlich, dass KMUs nur wenige bis keine Sicherheitsvorkehrungen treffen, was ihnen einen Angriff erleichtert. Deswegen ist es für KMUs unumgehbar, ihr Sicherheitsniveau zumindest auf das Minimum anzuheben. Hilfe dazu finden Sie unter dem Punkt Massnahmen.

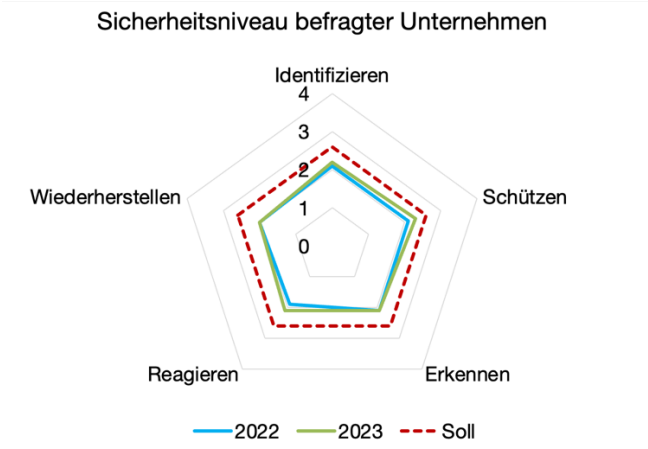


Abbildung 2: Ergebnisse der Redguard Security Survey

	2019	2020	2021	2022	2023	Soll
Identifizieren	2.0	2.0	2.0	2.1	2.2	2.6
Schützen	2.3	2.3	2.1	2.1	2.3	2.6
Erkennen	2.2	1.9	1.9	2.1	2.1	2.6
Reagieren	2.2	1.8	1.7	1.9	2.1	2.6
Wiederherstellen	1.7	1.7	1.8	2.0	2.0	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.

	2022		2023	
Funktion	**Fail**	**Pass**	**Fail**	**Pass**
Identifizieren	66%	34%	60%	40%
Schützen	57%	43%	54%	46%
Erkennen	63%	37%	59%	41%
Reagieren	61%	39%	58%	42%
Wiederherstellen	66%	34%	63%	37%
Total	**63%**	**37%**	**59%**	**41%**

Tabelle 1: Survey-Ergebnisse bezüglich der fünf Funktionen und Vergleich zum Vorjahr

Wir sehen eine Stagnation in den Bereichen *Identifizieren*, *Erkennen* und *Wiederherstellen*. Eine leichte Verbesserung wird hingegen bei den Funktionen *Schützen* und *Reagieren* angegeben.

Ein Blick auf die Antworten (Tabelle 1), aufgeteilt in die fünf Funktionen des IKT-Minimalstandards, verdeutlicht, dass nur 41% der Organisationen der Ansicht sind, das vom IKT-Minimalstandard geforderte Sicherheitsniveau zu erreichen.

In der Tabelle 2 gewinnen wir einen interessanten Überblick über die Selbsteinschätzungen der letzten fünf Jahre, die Redguard jeweils ausgewertet hat. Durchweg die besten Punkte erzielt die Funktion *Schützen*. Ein Grund könnte sein, dass besonders in der Software-Entwicklung immer öfter die Sicherheit von Beginn an miteinbezogen wird. Mit dem DevSecOps-Ansatz wird für ein reibungsloses Zusammenspiel

zwischen den Bereichen Software-Entwicklung (Dev), Sicherheit (Sec) und Betrieb (Ops) gesorgt.

Redguard empfiehlt dieses Vorgehen schon lange, da es effizienter und kostengünstiger ist. Ein besonders wichtiger Aspekt ist die Sicherheit von Containern und die Konfiguration der Orchestrierung-Tools wie z. B. Kubernetes. Etwas schlechter schneiden die Funktionen *Identifizieren* und *Erkennen* ab. Das deutet darauf hin, dass viele Sicherheitsvorfälle zu spät erkannt werden, weil die Systeme zu wenig kontinuierlich überwacht werden und nicht rechtzeitig Alarm geschlagen werden kann. Auch hier empfehlen wir Gegenmassnahmen, z. B. in Form von Continuous Security Scanning, regelmässige Schwachstellen-Scans, die das Sicherheitsniveau eines Unternehmens zwischen periodisch angesetzten Penetration Tests abbildet und böse Überraschungen verhindert. Zur frühzeitigen Erkennung von und Reaktion auf Cybergefahren in der Cloud bietet sich z. B. ein Security Operations Center (SOC) an. Dies kann zu einer erheblichen Entlastung des internen IT-Teams und einem massiven Anstieg der Sicherheit führen.

Mit Blick zurück auf die Tabelle 2 erkennen wir deutlich, dass Firmen sich über alle Jahre hinweg in den Funktionen *Reagieren* und *Wiederherstellen* am schlechtesten bewertet haben. Redguard hat diesen Bedarf erkannt und betreut Kunden bereits seit vielen Jahren als Incident-Partner im Rahmen von CISO-Mandaten. Seit über einem Jahr nutzen Kunden nun auch unser Incident Response Team als eigenständigen Service. Auch hier erkennen wir eine steigende Sensibilisierung für das Thema Cyber Security und Incidents. Gemäss Selbsteinschätzung der teilnehmenden Unternehmen, beurteilen sich jedoch die meisten als zu wenig vorbereitet, um einen Sicherheitsvorfall zu managen.

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 ist fundiertes Fachwissen sowie eine pragmatische Handhabung für eine erfolgreiche Umsetzung des IKT-Minimalstandards essenziell. 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 – Schulen Sie Ihre Mitarbeitenden und schützen Sie Ihre Systeme

- 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 mit E-Learning-Einheiten, klassischen Schulungsangeboten, 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

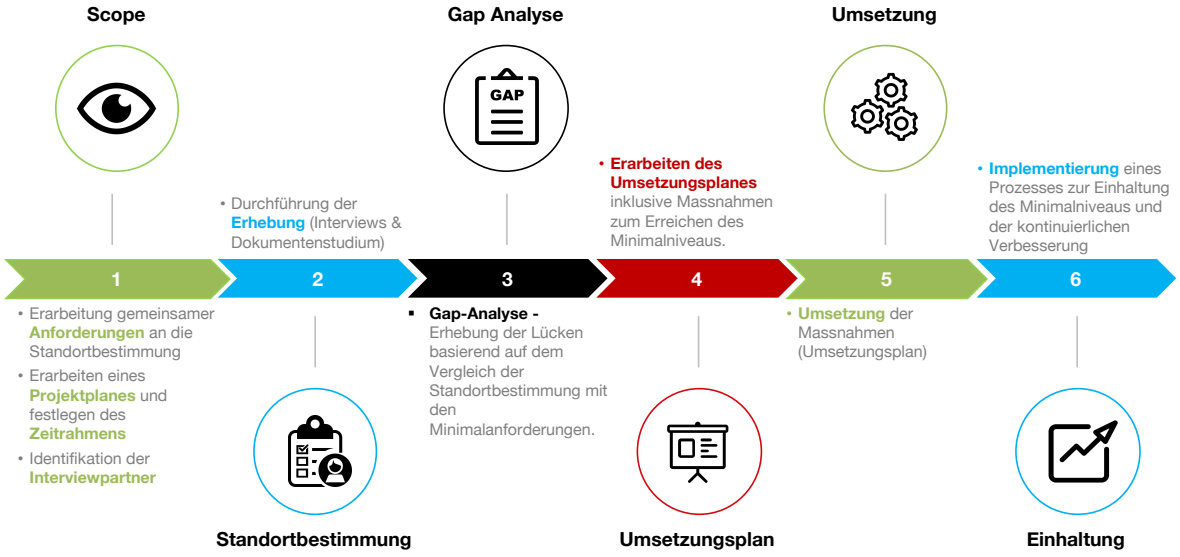
- Reaktionspläne helfen Ihnen, um im Ernstfall richtig zu reagieren und Zeit zu gewinnen. Mit einem Reaktionsplan haben Sie viele Fragen bereits im Vorfeld beantwortet: Wer ist in Ihrer Organisation zuständig bei einem Cyber Security-Vorfall? Wie informieren Sie Ihre Mitarbeitenden und Kunden? Stellen 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, indem wir gemeinsam mit Ihnen Wiederherstellungspläne erarbeiten.

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 80 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 bei einem Incident

Sollten Sie aller Massnahmen zum Trotz von einem Cyber Security-Vorfall betroffen sein, so steht Ihnen unser Incident Response Team jederzeit zur Verfügung. Garantierte Verfügbarkeit mit vorgängigem Agreement.

Massnahmen

1.1 Massnahmen – Security Operations Center (SOC)

Security Operations bezieht sich auf den Prozess des Überwachens, Überprüfens und Reagierens auf Sicherheitsereignisse und Bedrohungen in einer IT-Infrastruktur. Durch Security Operations wird die Cybersicherheit eines Unternehmens massgeblich verbessert. Hierbei geht es vor allem darum, ungewöhnliche und potenziell schadhafte Aktivitäten frühzeitig zu erkennen und aufzuhalten.

SOC as a Service

Mit unserem cloud-basierten Security Operations Center lagern Sie Ihre Cybersicherheit an Redguard-Experten unserer Schwesterfirma FusionOne aus. Das Serviceangebot ist für alle Organisationen und Unternehmen zugänglich, die Microsoft 365 nutzen. Das SOC wurde auch mit KMUs entwickelt und getestet und erfüllt deren Bedürfnisse an ihren Alltag und ihr Budget.

Weitere Informationen: https://www.fusionone.ch

1.2 Massnahmen – Continuous Security Scanning

Mit permanenten, automatisierten Schwachstellen-Scans sorgen Sie für ein stets ausreichendes Sicherheitsniveau Ihres Unternehmens. Das Continuous Security Scanning eignet sich als Überbrückung zwischen den regelmässigen Penetration Tests.

Automatisierte Schwachstellen-Überprüfung

Die von Redguard entwickelte Schweizer Plattform Vulnerability Guard bietet Ihnen eine optimale Einschätzung Ihres Sicherheitsniveaus und die Einordnung der Daten in einen historischen Kontext. So ist für Sie klar ersichtlich, welche Schwachstellen neu identifiziert oder geschlossen wurden und damit auch, wie sich der Schutz Ihrer Infrastruktur mit der Zeit verändert. Sie entlarven damit nicht nur generische Schwachstellen, sondern auch solche, welche spezifisch in Ihren Applikationen enthalten sind.

In die Entwicklung flossen zehn Jahre Erfahrung in Cyber Security ein. Dennoch ist sie im Gegensatz zu anderen Schwachstellenscannern auch ohne IT-Sicherheitsexperten und mit begrenztem Budget bedienbar.

1.3 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 allein

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/

1.4 Massnahmen – DevSecOps

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

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.

Anhang

1.5 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.

1.6 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 – Beschränkt 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:

- IKT (Informations- und Kommunikationstechnologie) -Minimalstandard des Bundesamtes für wirtschaftliche Landesversorgung (BWL):
  https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html
- Factsheet IKT-Minimalstandard von Redguard
  https://www.redguard.ch/downloads/factsheet_ikt_minimalstandard_de.pdf
- Redguards Quick-Test zum IKT-Minimalstandard
  DE: http://ikt.redguard.ch
  FR: http://ikt-fr.redguard.ch
- Website von Redguard
  https://www.redguard.ch