APP Unternehmensberatung AG

Praxisleitfaden:
Informationssicherheit für Führungskräfte



Informationssicherheit ist Aufgabe der gesamten Organisation. Sie strategisch zu steuern, taktisch zu planen und operativ zu leben ist jedoch in der Verantwortung der Führungskräfte. Es braucht dazu klare Prinzipien, abgestimmte Prozesse und ein gemeinsames Verständnis, damit Organisationen sicher und handlungsfähig bleiben.

Nachfolgend stellen wir konkrete Handlungsempfehlungen der Informationssicherheit für Führungskräfte vor und zeigen, wie diese strategisch, taktisch und operativ wirksam verankert werden können.



Strategische Ebene

Die strategische Ebene legt den Fokus auf die langfristigen, richtungsgebenden Aspekte der Informationssicherheit (IS), denn ohne diese grundlegenden Beschlüsse scheitern auch die nachfolgenden Ebenen.



Leitprinzipien & Kultur

Übernehmen Sie die IS-Leitprinzipien und verankern Sie diese in Ihrer Organisationskultur.

Beispiele

- Verankern Sie *Security by Design* und integrieren Sie Sicherheitsaspekte von Anfang an in die Entwicklung von Produkten und Services.
- Fördern Sie eine lernende Organisation und stärken Sie eine offene Meldekultur.



Strategie & Rahmenbedingungen

Berücksichtigen Sie die IS in der langfristigen Strategie und setzen Sie den Rahmen für Partner-, Risiko- und Ressourcenmanagement.

Beispiele

- Gestalten Sie Partnerschaften bewusst, sowohl technologisch (Cloud vs. On-Prem) als auch organisatorisch (Standard vs. Innovation).
- Legen Sie Vorgaben für Partner klar fest, definieren Sie, welche Vorgaben und Standards von Partnern eingehalten und regelmässig nachgewiesen werden müssen (z. B. ISO 27001 Nachweis).
- Steuern Sie den Umgang mit sensiblen Informationen und Personendaten gezielt. Ein Datenverlust kann erhebliche Reputationsschäden verursachen und soll daher als strategisches Risiko gesteuert werden.



Investitionsentscheidungen

Treffen Sie grundlegende Investitionsentscheidungen hinsichtlich der (zu beschaffenden) Technologien und Ressourcen.

Beispiele

- Müssen sensible Informationen und Personendaten bewirtschaftet werden, entscheiden Sie sich für einen Partner mit Datencenter mit Standort Schweiz.
- Entscheiden Sie, ob ein *Security Operation Center* selbst aufgebaut und betrieben oder extern bezogen wird (*Make or Buy*).



Schutzobjekte & Schutzziele

Bestimmen Sie die wichtigsten Schutzobjekte (IT- als auch nicht IT-basierte Informations-Assets) und legen Sie die Schutzziele innerhalb der Wertschöpfungskette fest.

Beispiel

- Definieren Sie Informationssammlungen zu Kundendaten oder geistigem Eigentum als Schutzobjekte und legen Sie damit Schutzziele CIA *(Confidentiality (C), Integrity (I), Availability (A))* fest.



Taktische Ebene

Die taktische Ebene übersetzt die strategischen Vorgaben in konkrete Strukturen und Prozesse in der Organisation. Diese Ebene sorgt dafür, dass Informationssicherheit nicht nur geplant, sondern auch umgesetzt werden kann.



Beschaffungsdesign & Lieferanten

Integrieren Sie IS von Anfang an in das Beschaffungsdesign und das Lieferantenmanagement.

Beispiele

- Integrieren Sie für die Informationssicherheit spezialisierte Rollen (ISBO, CISO) in Ihr Beschaffungsteam.
- Übernehmen Sie die strategischen Vorgaben und ergänzen diese um beschaffungsspezifische IS-Anforderungen und verankern Sie sie in den Verträgen (Zertifizierungen oder Sicherheitsvorkehrungen).



Verantwortlichkeiten & Berechtigungen

Richten Sie die Verantwortlichkeiten nach bestehenden Vorgaben und Rechtsgrundlagen aus und setzen Sie diese gezielt in den Berechtigungskonzepten um (Need-to-Know Prinzip).

Beispiele

- Legen Sie die Verantwortlichen für Schutzobjekte und Risikoeigner in der Abwicklung eines Projektes und im späteren Betrieb von Anfang an fest.
- Berücksichtigen Sie das 4-Augen-Prinzip im Prozess zur Vergabe von Zugriffsberechtigungen auf sensible Informationen.
- Planen Sie bewusst periodisch Überprüfungen ein, z. B. die Überprüfung von Zugriffsrechten. Sie vermeiden damit, dass ehemalige Mitarbeitende, Partner oder spezielle Testaccounts über längere Zeit noch Zugriff auf Ihre Systeme besitzen.



Kompetenzen, Lücken & Weiterbildung

Stellen Sie sicher, dass die richtigen Kompetenzen vorhanden sind, Lücken frühzeitig erkannt und Zeit sowie (monetäre) Ressourcen für Weiterbildungen bereitgestellt werden.

Beispiele

- Schulen Sie rollen- und stufenbasiert. Mitarbeitende benötigen eine regelmässige Auffrischung zum Thema «Verhalten im Umgang mit Informationen». Für Risikoeigner stehen Themen wie «Aktuelle Bedrohungslage» oder «Risikobewertung und –behandlung» im Vordergrund.
- Überprüfen Sie individuell die Fähigkeiten (Skill-Matrix) und Schulungsinhalte zu den neuesten Entwicklungen.



Bereichsübergreifende Zusammenarbeit

Koordinieren Sie bereichsübergreifend Zusammenarbeit bei der Umsetzung der IS-Strategie.

Beispiele

- Halten Sie regelmässige Meetings und Schnittstellenanalysen zwischen IT, Informationssicherheit und Fachbereichen und fördern Sie so die interdisziplinäre Zusammenarbeit in den Teams.
- Fördern Sie *Communities of Practice* (z. B. sämtliche Schutzprojektverantwortliche tauschen sich über Vorgehen und aktuelle Problemstellungen aus).

Operative Ebene

Die operative Ebene beinhaltet die tägliche Anwendung und kontinuierliche Verbesserung der Informationssicherheit.

Kommunikation & Vorbildlichkeit

Leben Sie die Sicherheitskultur im Alltag vor und fördern Sie offene Kommunikation im Team.

Beispiele

- Gehen Sie als Führungskraft mit gutem Beispiel voran und sprechen Sie offen über Sicherheitsrisiken im Team.
- Setzen Sie bewusst eine offene Fehlerkultur um, indem Sie *Lessons Learned* regelmässig und transparent behandeln.

Handlungsfähigkeit & Verbesserung

Sichern Sie die stetige Handlungsfähigkeit und streben Sie eine kontinuierliche Verbesserung an.

Beispiele

- Definieren und arbeiten Sie für alle sicherheitsrelevanten Rollen Stellvertretungen ein.
- Leiten Sie aus *Lessons Learned* Massnahmen ab und setzen Sie diese zeitnah um. Beantragen Sie z. B. zusätzliche personelle Ressourcen, wenn sie feststellen, dass die Stellvertreterregelung nicht konsequent umgesetzt werden kann.

Risikomanagement & -minderung

Führen Sie ein kontinuierliches Risikomanagement bei den zu schützenden Objekten durch und leiten Sie entsprechend risikominimierende Massnahmen ein.

Beispiele

- Führen Sie eine als dringend und wichtig erachtete Multi-Faktor-Authentifizierung ein statt kosmetischer Updates der Benutzeroberfläche.
- Prüfen Sie regelmässig, insbesondere wenn sicherheitsrelevante Änderungen vorliegen, ob der Schutzbedarf Ihrer Schutzobjekte noch aktuell ist oder angepasst werden muss, zum Beispiel wenn Sie neu besonders schützenswerte Personendaten verarbeiten.

Umweltänderungen

Beobachten Sie proaktiv externe Veränderungen im (Lieferanten-)Umfeld.

Beispiele

- Führen Sie ein Monitoring hinsichtlich Gesetzesänderungen, Technologietrends sowie neuen Bedrohungen ein, analysieren Sie die Auswirkungen und definieren Sie die zu ergreifenden Massnahmen.
- Stellen Sie sicher, dass Sie die Supply Chain Ihrer Schutzobjekte kennen und reagieren können, falls Sie Änderungen in dieser feststellen. Wird z. B. ein Lieferant von einem grösseren Konzern aufgekauft, kann dies zu Änderungen der Vertragsbedingungen bzw. Einhaltung von Vorgaben führen.

Unsere Expertinnen und Experten

Gerne unterstützen wir Sie dabei, Informationssicherheit in Ihrer Organisation wirksam zu verankern – von der Strategie bis zur Umsetzung im Alltag. Nehmen Sie mit uns Kontakt auf und erfahren Sie, wie wir Sie auf diesem Weg begleiten können.

www.app.ch/infosec



Tel. +41 58 320 30 25
E-Mail andreas.steiner@app.ch



Tel. +41 58 320 30 38
E-Mail jana.papritz@app.ch