Cyber Security First Cut

Mit der Digitalisierung steigt auch die Abhängigkeit zu Ihrer Informationstechnologie. Und Ihre Geschäftsprozesse werden angreifbar. Die heutige Cyber Bedrohungslage zwingt Sie zu handeln. Unser Lösungansatz gibt Ihnen ein klares Bild Ihrer Cyber Security, liefert Ihnen einen umfassenden Masterplan, um auf das gewünschte Sicherheitsniveau zu kommen und macht das Thema Ihrer Unternehmensführung verständlich.

Die Herausforderungen

Um der heutigen Bedrohungslage im Cyber-Umfeld gerecht zu werden, ist eine gefestigte IT-Landschaft unabdingbar. Dies verlangt eine Analyse der bestehenden Infrastruktur und die Definition der nötigen Massnahmen, um eine grundlegende **Cyber Resilience** zu schaffen.

Mit dem Aufbau einer stabilen und sicheren Cyber-Infrastruktur wird die Plattform zur Verfügung gestellt, damit das Unternehmen mit seinen Aussenstellen, Partnern, Lieferanten und Kunden sicher und zuverlässig kommunizieren kann.

Eine Organisation kann sich mit Massnahmen in der Informationssicherheit gut schützen und für die Integrität der eigenen IT grossen Nutzen stiften. Aber gerade der Humanfaktor wird oft stiefmütterlich behandelt: Es wird ihm in den meisten Unternehmungen bis heute nicht genügend Aufmerksamkeit geschenkt.

Informationssicherheits- und Cyber Security-Programme tragen wesentlich dazu bei, sensitive Daten, die auf IT-Systemen liegen, vor IP-Diebstahl, Penetration, Kompromittierung oder Sabotage zu schützen.

Nur wenn man die Unternehmung als Ganzes anschaut, kann man eine solide Aussage über den Stand der Informationssicherheit machen.

Ihr Nutzen

Der Cyber Security First Cut zeigt die Risiken und den Stand der Cyber Security hinsichtlich der aktuellen **Bedrohungslage** im Unternehmen auf. Es bildet somit eine hervorragende Grundlage für eine zukünftige **Cyber-Sicherheitsstrategie**.

Der Cyber Security First Cut von ISPIN legt Ihnen die nötigen Instrumente und Kommunikationsmittel in die Hände, um Ihre Security-Strategie effizient vorwärts treiben zu können.

Dank des im Cyber Security First Cut mitgelieferten **Massnahmenplans** mit Massnahmenpriorisierung, einem Dashboard als Monitoringtool, einer Roadmap und Angaben zu Budgetbedarf wird optimale Planungssicherheit gewonnen.

Das zusätzliche **Kommunikationspaket,** welches genau auf die Stufe Geschäftsleitung und Verwaltungsrat abgestimmt ist, unterstützt Sie bei der Kommunikation der Analyse-Resultate.

Mensch, Technologie und Prozesse

Moderne Informationssicherheitsansätze erweitern den klassischen Fokus auf Technologie um die Aspekte „Mensch“ und „Prozesse“. Unternehmen, welche den Schutzbedarf auf ihre IT-Infrastruktur und Netzwerke beschränken, begeben sich in eine Schein-Sicherheit. Mensch, Prozesse und Organisation können oft unerwartete Verwundbarkeiten aufweisen, welchen mit einer technischen Sicherung nicht beizukommen ist.

Cyber Security First Cut-Ansatz

Analyse Status Quo

- Interviews und Reviews Ihrer Dokumentation und Ihres Status Quo der Sicherheit im Vergleich zu relevanten Standards
- Interviews und Reviews von Dokumenten betreffend Geschäftsziele

GAP-Analyse

- Identifikation von fehlenden Elementen im Vergleich zu Standard Security Frameworks und der damit verbundenen Risiken
- Abgleich und Festlegung der GAPs mit Projektteam

Ausarbeitung Masterplan

- Definition Scope, Umfang und Service Level basierend auf der Analyse
- Erarbeitung Cyber Security Masterplan für die nächsten 2-5 Jahre
- Zeit und Ressourcen-Planung

Realisierung

- Operative Umsetzung
- Etablierung von Projekten
- Koordination mit Geschäftszielen
- Koordination mit Security-relevanten Projekten

Betrieb & Qualitätskontrolle

- Regelmässige Überwachung und Auditierung der Informations- und IT-Sicherheit
- Qualitätssicherung des Service Levels

ISPIN AG ZURICH
swiss made security.

Modulare Anpassungsfähigkeit

Unser modularer Ansatz erlaubt es Ihnen, die Sicherheitsanalyse Ihres Unternehmens so zu fokussieren, damit die Resultate **genau Ihren Bedürfnissen entsprechen**.

ISPIN führt Sie durch einen **etablierten Prozess**, in welchem die nötigen Informationen gesammelt werden, um ein erfolgreiches Assessment durchzuführen. Dieses beinhaltet eine Kombination von Interviews, Dokumentenanalyse und auch technische Analysen durch unsere Fachspezialisten.

Wir dokumentieren unsere Erkenntnisse und identifizierten Schwachstellen. Ein Massnahmenplan wird definiert und mit Ihnen besprochen. Zudem stellen wir ein Kommunikationspaket für Sie zusammen, welches Ihnen ermöglicht, die nötige **Akzeptanz und Verständnis** auf Stufe Geschäftsleitung und Verwaltungsrat zu erreichen.

Cyber Security First Cut Module

1 Physische Sicherheit	☐	**1.1 Physical Security** Inspektion der Gebäude und Büros bezüglich der physischen Zugänge, Platzierung von Sicherheitsausstattung, Platzierung der Infrastruktur sowie Umgebungsbedingungen, Review der Sicherheitspläne und Mechanismen für Notfälle.
	☐	**1.2 Social Engineering Risks** Begleitetes Social Engineering Audit.
2 Awareness	☐	**2.1 Wirkungsanalyse der Sicherheitskultur** Interviews mit Schlüsselpersonen, mit welchen das Sicherheitsbewusstsein bzw. die damit zusammenhängende Sicherheitskultur erhoben wird. Briefing der für die interne Kommunikation zuständigen Verantwortlichen zur Entwicklung der Sicherheitskultur.
3 Organisation und Prozesse	☐	**3.1 Sicherheitsvorgaben und Risikomanagement** Prüfung der Sicherheitsvorgaben anhand des Outputs aus dem Risiko-Management.
	☐	**3.2 Sicherheitsvorgaben und deren organisatorische Umsetzung** Auf Fragebögen basierende Interviews mit Schlüsselpersonen aus (üblicherweise) IT-, HRM- und Legal-Abteilungen. Weitere können hinzugefügt werden. Review von Policy-Dokumentationen und Recherche von relevanten Regulatorien.
4 IT Architektur	☐	**4.1 Technische Kommunikations- und Sicherheitskonzepte** Review von ausgewählten Architektur-Themen basierend auf Dokumentationen und Diskussionen. Üblicherweise ein netzspezifisches und/oder ein applikationsspezifisches Thema. z.B.: Perimeter-Schutz, Middleware-Infrastruktur, best. Online-Applikation.
5 IT System-sicherheit	☐	**5.1 Technischer Schwachstellen-Scan** Stark automatisierter Schwachstellen-Scan basierend auf Datenbanken mit bekannten Schwachstellen.
	☐	**5.2 Prüfung der System-Konfigurationen / Hardening** Manuelle Hardening- und Baseline-Prüfungen der System- und OS-Konfigurationen.
	☐	**5.3 Penetration Test** Manuelle und werkzeuggestützte Penetration-Tests mit spezifischen Hacker- und Test-Tools basierend auf einem Whitebox-Ansatz.
6 Projekt	☑	**6.1 Projekt-Managemement und Berichterstattung** Kickoff- und Resultat-Workshop, Projektorganisation/-Koordination. Informationskorrelation und Abgleich der gesammelten Eindrücke (Soft Facts) zur generellen Beurteilung der Situation.
	☑	**6.2 Lieferobjekt Schlussbericht** Abschlussbereicht mit kritischen Risiken und Lücke zu einem wirtschaftlichen Information Security Farmework nach ISO27001 sowie Vorgehensvorschlag. Detaillierter und auf Kunde zugeschnittener Massnahmenkatalog, zusammengefasst in einzelne Arbeitspakete (Budget, Zeit und Ressourcen).
	☐	**6.3 Lieferobjekt Security Management Cockpit** Erstellen des Security Management Cockpits mit den Dimensionen "Distance to Compliance and Standards" (angepasst an Ihre Unternehmung). Darstellung der Findings und Massnahmen.

Kontaktieren Sie uns.

Gerne stellen wir eine massgeschneiderte Offerte für Sie zusammen.
Kontaktieren Sie uns für mehr Informationen und Referenzauskünfte.

Craig Fletcher, CCO
+41 44 838 31 11
craig.fletcher@ispin.ch