FINMA RS 2008/21

Die IT Welt ist im Umbruch und mit ihr auch die Art und Weise, wie Unternehmen mit den daraus resultierenden Cyberbedrohungen umgehen müssen. Diesen Umstand hat die FINMA erkannt und am 22. September 2016 eine revidierte Version des Rundschreibens 2008/21 "Operationelle Risiken - Banken" veröffentlicht. Im Abschnitt IV des aktualisierten Rundschreibens konkretisiert sie Anforderungen, welche sich auf das Management der Technologieinfrastruktur und dem Umgang mit Cyber-Risiken beziehen.

Was ist neu?

Das revidierte Rundschreiben fokussiert seine Anforderungen an die Informationstechnologie auf die folgenden zwei Bereiche:

- IT Risikomanagement Konzept
- Risikomanagement Konzept für den Umgang mit Cyber-Risiken

Die starke Abhängigkeit der Bankenwelt auf Technologieinfrastruktur hat dazu geführt, dass der Umgang mit Cyber-Risiken zur Verantwortung der Geschäftsleitung geworden ist.

IT-Risikomanagement Konzept

Die Geschäftsleitung hat ein IT-Risikomanagement Konzept in Übereinstimmung mit der IT Strategie und der definierten Risikotoleranz zu implementieren. Dieses muss die folgenden minimalen Aspekte beinhalten:

- **Inventar:** Übersicht über die Bestandteile der Netzwerkinfrastruktur und Inventar aller kritischen Applikationen und damit verbundenen IT-Infrastruktur.
- **Rollen und Verantwortlichkeiten:** Eindeutige Festlegung von Rollen, Aufgaben und Verantwortlichkeiten in Bezug auf kritische Applikationen, IT-Infrastruktur und sensiblen Daten und Prozessen.
- **IT-Risikomanagement Prozess:** Systematischer Prozess zur Identifikation und Beurteilung von IT-Risiken.
- **Awareness:** Massnahmen zur Stärkung des Bewusstseins der Mitarbeiter im Hinblick auf IT-Risiken und IT-Informationssicherheit.

Risikomanagement Konzept für den Umgang mit Cyber-Risiken

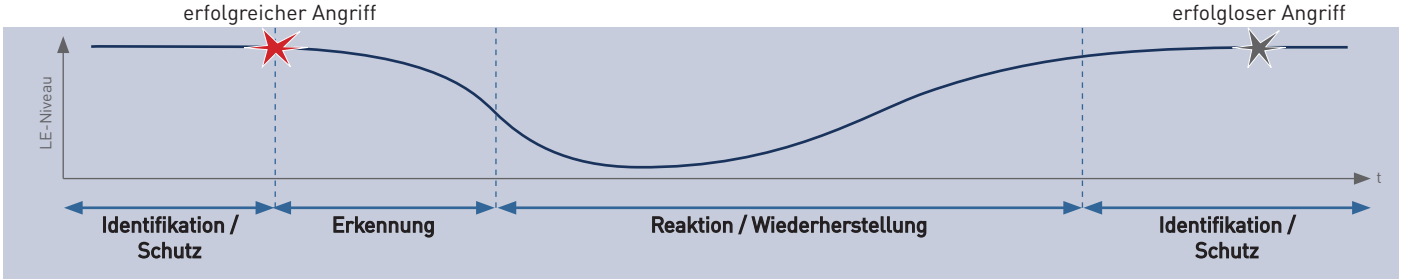
Die Geschäftsleitung hat ein Risikomanagement-Konzept für den Umgang mit Cyber-Risiken zu implementieren. Dieses Konzept muss sowohl die folgenden minimalen Aspekte abzudecken, als auch durch geeignete Prozesse und eindeutiger Festlegung von Aufgaben, Rollen und Verantwortlichkeiten umgesetzt werden:

- **Identifikation von Bedrohungen:** Institutsspezifische Bedrohungspotentiale durch Cyber-Attacken, insbesondere in Bezug auf kritische und/oder sensitive Daten sind zu identifizieren.
- **Schutz vor Cyber-Attacken:** Die Geschäftsprozesse und Technologieinfrastruktur sind gegen Cyber-Attacken zu schützen.
- **Erkennung von Cyber-Attacken:** Die IT Infrastruktur muss systematisch überwacht und Attacken müssen zeitnah erkannt und aufgezeichnet werden.
- **Reaktion auf Cyber-Attacken:** zeitnahe und geziehlte Massnahmen mit dem Ziel der Aufrechterhaltung des normalen Geschäftsbetriebes.
- **Wiederherstellung des normalen Geschäftsbetriebes:** zeitnahe Wiederherstellung des normalen Geschäftsbetriebes durch geeignete Massnahmen.
- **Regelmässige Verwundbarkeitsanalysen:** Durchführung von regelmässigen Verwundbarkeitsanalysen und Penetration Testings zur Identifkation von Lücken und Schwachstellen.

Der ISPIN Cyber Risk Resilience® Ansatz ist compliant mit dem angepassten Rundschreiben und gibt Ihnen einen Security Masterplan für die nächsten Jahre vor.

Interpretation der ISPIN AG

Die FINMA hat mit ihrer Anpassung genau den Zeitgeist getroffen und eine sehr moderne Sicht der Informationssicherheit eingenommen. Diese Denkweise ist stark an das NIST Cyber Security Framework angelehnt und widerspiegelt den von ISPIN AG seit einigen Jahren verfolgten "Cyber Risk Resilience®"-Ansatz. Hierbei geht es darum, eine erfolgreiche Attacke nicht als Möglichkeit, sondern als Fakt anzusehen und seine Geschäftsprozesse und darunterliegende IT konsequent darauf einzurichten, trotz erfolgreicher Attacke möglichst widerstandsfähig zu bleiben.



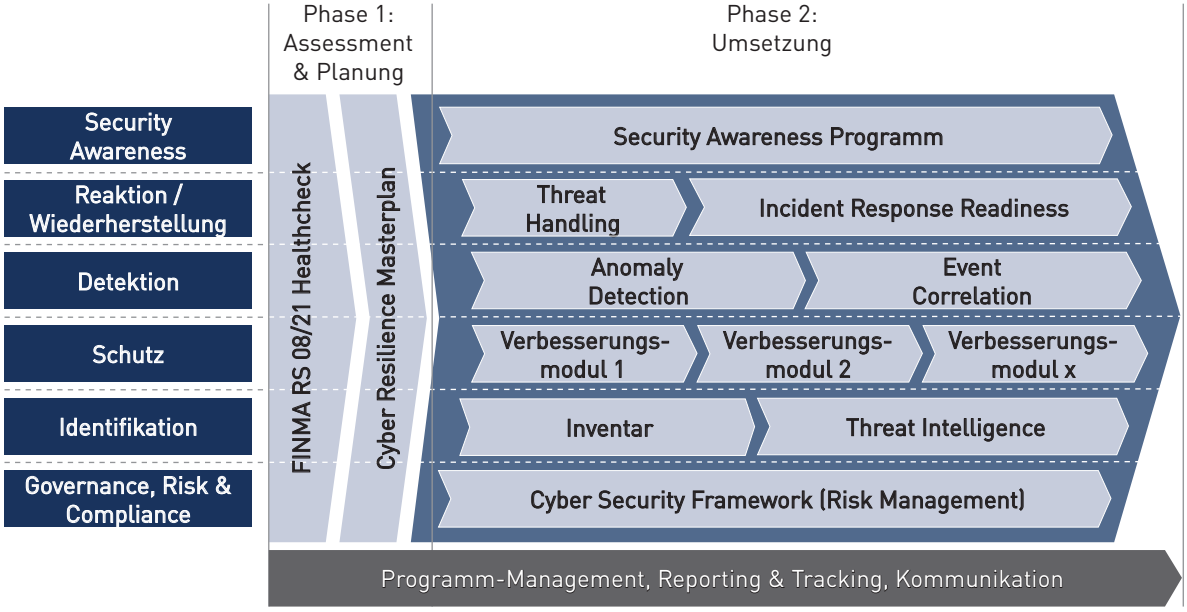
ISPIN AG ZURICH
swiss made security.

Das Cyber Risk Resilience® Programm von ISPIN

Das Cyber Risk Resilience® Programm basiert auf **modernsten Erkenntnissen** der Informationssicherheit und **global anerkannten Standards** wie NIST, NERC, SANS, ISO 27k, NSSKI (VBS). Für Unternehmen, welche mit dem neuen **FINMA RS 2008/21 compliant** sein müssen, bietet ISPIN ein auf dieses Rundschreiben massgeschneidertes Vorgehen an. Es positioniert Ihr Unternehmen so, dass Sie den aktuellen und zukünftigen Bedrohungen aus der Cyberwelt trotzen können.

In der **Phase 1**, der **Assessment & Planungsphase** wird ein FINMA RS 08/21 Healthcheck durchgeführt. Hierbei assessieren wir alle Bereiche Ihres Unternehmens in Bezug auf Cyber Risk Resilience® und den spezifisch im Rundschreiben formulierten Aspekte. Um ein ganzheitliches Bild zu erhalten, fokussieren wir auf Prozesse, Menschen, Organisation und Technolgie. Zusammen mit Ihnen definieren wir das akzeptable Leistungserbringungsniveau Ihrer Unternehmung und leiten daraus den Sollwert der Informationssicherheit ab, welcher erreicht werden sollte. Das Resultat ist ein Cyber Resilience Masterplan, welcher Ihnen eine Umsetzungsplanung mit Priorisierung und Kostenprojektionen für die nächsten eins bis drei Jahre aufzeigt. Dieser Masterplan positioniert sie optimal, auch für zukünftige verschärfungen des Rundschreibens.

In der **Phase 2**, der **Umsetzungsphase** unterstützen wir Sie bei der Implementation der Cyber Resilience Massnahmen gemäss Ihrem persönlichen Masterplan. Als Programm-Manager koordinieren wir Ihre Umsetzungsaktivitäten und stellen adäquates Reporting, Tracking und Kommunikation sicher. Unsere Security-Spezialisten stehen Ihnen für die verschiedenen Thematiken zur Seite.



ISPIN, Ihr kompetenter Partner

Das Cyber Risk Resilience® Programm von ISPIN hat folgende Vorteile für Sie:

- Das Cyber Risk Resilience® Programm ist compliant mit dem angepassten FINMA RS 2008/21 und angelehnt an global anerkannte Standards und Frameworks.
- Wir erarbeiten für Sie eine Security Strategie für die nächsten eins bis drei Jahre.
- Der Cyber Resilience Masterplan ist voll auf Sie abgestimmt und basiert auf Ihrem Bedrohungsumfeld und Ihrem benötigtem/gewünschten Sicherheitsniveau.
- ISPIN übernimmt die Gesamtkoordination des Programmes und steht Ihnen mit über 50 Spezialisten aus diversen Bereichen stets zur Seite.
- Wir unterstützen Sie beim gesamten Transformationsprozess - von der Unterstützung bei technischen Fragestellungen bis hin zu Kommunikationsstrategien.
- Der Cyber Resilience Masterplan macht die Ausgaben für Sie plan- und budgetierbar.
- User Cyber Risk Resilience® Programm basiert auf den bei Ihnen bereits umgesetzten Securitymassnahmen und führt sie nahtlos weiter.

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