ISPIN AG ZURICH
swiss made security.®

Member of CymbiQ Group

persistent security in a changing world

Cyber Risk Resilience®

Erfolgs- und Überlebensfaktor: Erwarten Sie das Unbekannte.

Neue Cyberangriffe. Neue Denkweise.

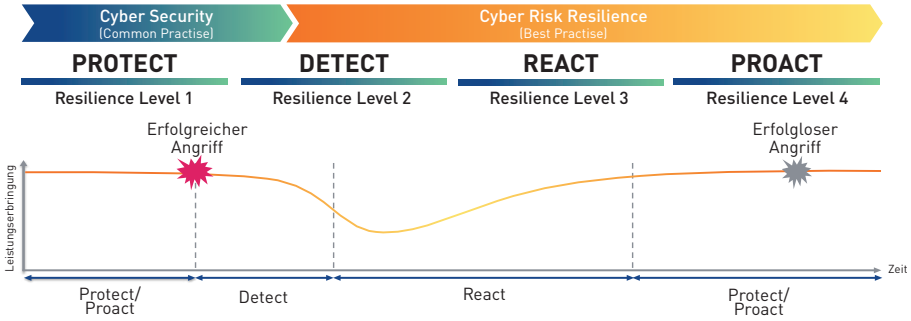
Die Frage, die sich jedes Unternehmen heute stellen muss, lautet nicht länger: «Gibt es je einen Cyberangriff auf unsere Firma?», sondern vielmehr: «Wie und wann findet der Angriff statt?» Ein Unternehmen muss auch bislang unbekannte Bedrohungen abwehren können und widerstandsfähig werden – oder eben resilient. Das verlangt weit mehr, als herkömmliche IT-Security leisten kann. Cyber Risk Resilience® befähigt Firmen, einen erfolgreichen Angriff so unbeschadet wie möglich zu überstehen, das Niveau der eigenen Leistungserbringung zu erhalten und aus dem Angriff zu lernen.

Erfolgreiche Cyberangriffe sind im heutigen vernetzten IT-Umfeld lediglich eine Frage der Zeit – sie sind nicht länger der Sonderfall, sondern der Normalfall. Die Bedrohungen sind dabei so vielschichtig geworden, dass die klassischen Risikomodelle und IT-Security-Massnahmen wie Firewalls etc. an ihre Grenzen stossen, denn sie schützen nur vor bekannten Angriffen und Verhaltensmustern. Mit ihnen alleine lassen sich Cyberbedrohungen von heute nicht mehr entschärfen. Neue Modelle und Denkweisen sind gefordert, um sie abzuwehren.

Vorausschauend handeln statt reagieren

Beim Denkansatz der Cyber Risk Resilience® von ISPIN geht es nicht länger darum, auf Bedrohungen nur zu reagieren. Vielmehr gestalten Unternehmen mit ihm sämtliche Geschäftsprozesse so, dass sie bekannten und unbekannten Angriffen standhalten. Sie werden resilient gemacht. So können sie auch bei einem erfolgreichen Angriff das Niveau ihrer Leistungserbringung weitgehend halten, ihre Geschäftstätigkeit mit möglichst geringen Einschränkungen fortführen – und trotz eines Angriffs überleben.

Damit Ihr Unternehmen resilient wird, muss es vier Disziplinen verankern – in seiner IT-Landschaft ebenso wie in den Geschäftsprozessen und der Unternehmenskultur.



Level 1: Protect

Ihr Unternehmen muss Schutzmassnahmen implementieren, damit es gegen bekannte Angriffe geschützt ist. Je besser diese Schutzmassnahmen sind, desto unbeschadeter übersteht Ihr Unternehmen einen Angriff und kann seine Leistungen weiter erbringen.

Level 2: Detect

Ihr Unternehmen benötigt Sensoren und Warnsysteme, die Alarm schlagen, wenn ein Angriff erfolgreich war. Dank ihnen erkennen Sie, wann Ihre Schutzmassnahmen auf dem Level Protect nicht gewirkt haben. So wird Ihre Geschäftstätigkeit so gering wie möglich beeinträchtigt – Sie können mit der Analyse beginnen und Korrekturmassnahmen einleiten.

Level 3: React

Wurde ein erfolgreicher Cyberangriff erkannt, müssen Sie rasch reagieren – mit Analyse-, Eingrenzungs- und Korrekturmassnahmen. Oberstes Ziel: die Geschäftsprozesse so schnell wie möglich auf ein akzeptables Niveau der Leistungserbringung zu führen. Je besser ein Unternehmen die React-Disziplin umsetzt, desto schneller erreichen betroffene Bereiche wieder den Normalzustand.

Level 4: Proact

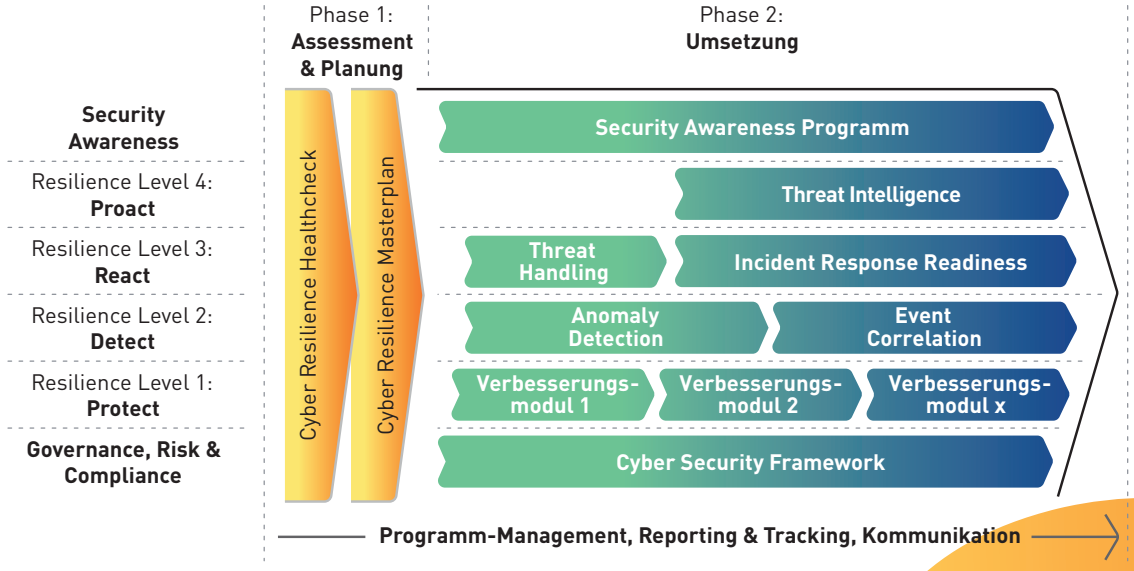
Proact stellt die höchste Stufe der Resilienz dar: Ihr Unternehmen passt seine Schutzmassnahmen automatisch der Bedrohungslage an, erkennt auch unbekannte Angriffe frühzeitig und wehrt sie ab, bevor sie Schaden anrichten können. Das Abwehrdispositiv von ISPIN basiert auf den Erkenntnissen unserer leistungsfähigen Threat Intelligence.

«Unternehmen, die sich nur auf den Schutz gegen Cyberbedrohungen fokussieren, verschliessen ihre Augen vor der Tatsache, dass es nicht die Frage ist, OB sondern WANN man angegriffen wird.»

Craig Fletcher,
CEO ISPIN AG

Das Cyber Risk Resilience® Programm von ISPIN

Das Cyber Risk Resilience® Programm von ISPIN basiert auf modernsten Erkenntnissen der Informationssicherheit, der Threat Intelligence und global anerkannten Standards wie NIST, NERC, SANS, ISO 27k, NSSKI (VBS). Es etabliert die vier Disziplinen in Ihrem Unternehmen und befähigt es dadurch, aktuelle Cyberbedrohungen genauso wirksam zu entschärfen wie zukünftige. ISPIN implementiert das Programm in zwei Phasen.



Phase 1: Planung

In der Assessment- und Planungsphase führt ISPIN einen Cyber-Resilience-Healthcheck durch. Dieser prüft sämtliche Unternehmensbereiche auf ihre Cyber Risk Resilience®. Dabei beziehen wir alle Faktoren ein: Prozesse, Menschen, Organisation und Technologie. So erhalten Sie ein ganzheitliches Bild der Widerstandsfähigkeit Ihres Unternehmens.

Anschliessend definieren wir zusammen mit Ihnen das Niveau der Leistungserbringung Ihres Unternehmens, das nie unterschritten werden darf. Daraus leitet sich der angestrebte Grad der Informationssicherheit ab. Wir erarbeiten einen Cyber-Resilience-Masterplan, der die Umsetzungsschritte mit Priorisierung und Kostenprojektionen für die nächsten ein bis drei Jahre aufzeigt.

Phase 2: Umsetzung

In der Umsetzungsphase implementiert ISPIN zusammen mit Ihnen die Cyber-Resilience-Massnahmen gemäss Ihrem individuellen Masterplan. Als Programm-Manager koordinieren wir Ihre Umsetzungsaktivitäten und stellen Reporting, Tracking und Kommunikation sicher. Unsere Security-Spezialisten begleiten Sie bei allen Themen mit Fachwissen und Engagement.

Ihre Vorteile auf einen Blick

- Auf Ihr Unternehmen, Bedrohungsumfeld und gewünschtes Sicherheitsniveau abgestimmter Masterplan
- Reduktion finanzieller Verluste dank frühzeitiger Erkennung, Schwächung und Abwehr von Angriffen
- Messbare Erhöhung der Widerstandsfähigkeit Ihres Unternehmens
- Stärkung von Image und Vertrauen bei Lieferanten und Kunden
- Kosteneinsparung dank gezielter Investitionen in die Sicherheit
- Erfüllung regulatorischer und rechtlicher Anforderungen
- Verbesserung der Unternehmenskultur und Prozesse dank Steigerung der Security Awareness aller Mitarbeitenden
- Reduktion der Wiederherstellungszeiten bei Angriffen um bis zu 80 %
- Angelehnt an internationale Standards und Frameworks wie NIST, NERC, SANS, ISO 27k, NSSKI (VBS)

Cyber-Security – Swiss made und auf Ihre Bedürfnisse zugeschnitten.

ISPIN ist ein führender Schweizer Anbieter für Lösungen in Cyber Security und Cyber Risk Resilience®.

Kunden profitieren von einem lückenlosen Spektrum an Beratungs- und Lösungskompetenz: Security Awareness & Culture, Governance, Risk & Compliance (GRC) gehören ebenso dazu wie Cyber Defense Services, Cloud Workload Protection und Sicherheitsinfrastrukturen.

Mehr als 150 Kunden aus allen Segmenten der Privatwirtschaft und der öffentlichen Hand vertrauen ISPIN. Im modernsten Cyber Defense Center der Schweiz betreibt und überwacht ISPIN rund um die Uhr die Infrastrukturen von namhaften Unternehmen, Organisationen und Behörden.

Cyber-Resilienz sicherstellen. Vorausschauend handeln.

ISPIN ist die Pionierin des proaktiven Konzepts der Cyber Risk Resilience (CRR)®. Mit Cyber Risk Resilience stellen Sie sicher, dass Ihre Geschäftsprozesse Angriffe so unbeschadet wie möglich überstehen und nahtlos weiterlaufen.

Sprechen Sie jetzt mit uns über alle Möglichkeiten, die Resilienz Ihres Unternehmens gegenüber Cyberbedrohungen zu stärken. Wir beraten Sie mit Freude und Kompetenz.

ISPIN AG
Grindelstrasse 6
CH-8303 Bassersdorf
Tel.: +41 44 838 31 11
www.ispin.ch