Cyber Risk Resilience®

Im heutigen Cyber-Umfeld schützen konventionelle Abwehrmechanismen nur mehr unzureichend. Unternehmen stehen vor der Herausforderung, dass Angriffe auf ihre Daten und Systeme nicht nur permanent stattfinden, sondern mit grösster Wahrscheinlichkeit auch erfolgreich sind. Aus diesem Grund ist die Widerstands- und Überlebensfähigkeit der IT-Systeme entlang des Angriffskontinuums – vor, während und nach einem Angriff – zur wichtigsten Funktion der Informationssicherheit geworden. Cyber Risk Resilience® beschreibt das Gesamtkonzept zur Erlangung dieser Widerstandsfähigkeit. Dazu gehören neben technischen Massnahmen auch prozessuale und organisatorische Elemente.

Der Ansatz der Resilienz

In den letzten Jahren hat ein Wandel in der Informationssicherheit stattgefunden. Die Denkweise, dass man sich gegen Angriffe schützen kann und muss, ist einem neuen Denkansatz gewichen. Die Bedrohungen im Cyber-Umfeld sind so vielschichtig und undurchsichtig geworden, dass man kaum mehr wissen kann, wer wie und wann angreifen wird. Unternehmen müssen sich mit der Tatsache abfinden, dass ein erfolgreicher Angriff lediglich eine Frage der Zeit ist. Es ist deshalb überlebenswichtig, dass die Geschäftsprozesse so gebaut werden, dass sie trotz eines erfolgreichen Angriffes, ein für die Unternehmung akzeptables Leistungserbringungsniveau erhalten - also widerstandsfähig (resilient) gegenüber bekannten und unbekannten Angriffen werden.

Die vier Disziplinen der Cyber Risk Resilience®

Um resilient gegenüber von Cyber-Angriffen zu werden, müssen Unternehmen folgende vier Disziplinen in ihren Geschäftsprozessen, ihrer IT-Systemlandschaft und in ihrer Unternehmenskultur verankern:

Resilience Level 1 - Protect: Es müssen Schutzmassnahmen implementiert werden, um die Unternehmung gegen bekannte Angriffe zu schützen. Diese sollen verhindern, dass ein Angriff erfolgreich ist und die Geschäftsprozesse unbeeinflusst weiterlaufen. Je besser und effektiver die Schutzmassnahmen sind, desto seltener sinkt das Niveau ihrer Leistungserbringung aufgrund eines Cyber-Angriffes.

Resilience Level 2 - Detect: Sensoren und Warnsysteme müssen implementiert werden, um Alarm zu schlagen, falls ein Angriff erfolgreich ist und sich unbefugte User oder Programme in der Unternehmung befinden. Je besser diese Warnsysteme sind, desto schneller können die Analyse- und Gegenmassnahmen beginnen und desto weniger fällt das Leistungserbringungsniveau der Geschäftsprozesse, bevor Korrekturmassahmen eingeleitet werden.

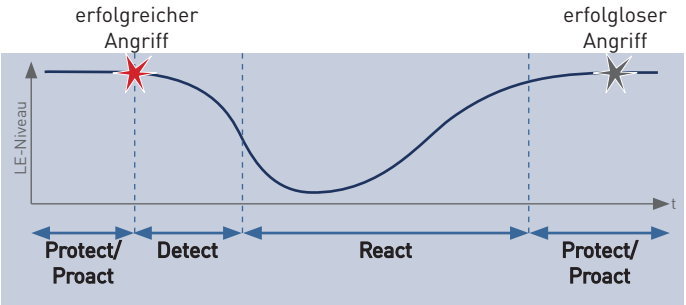
> Unternehmen, welche sich nur auf den Schutz gegen Cyberbedrohungen fokussieren, verschliessen ihre Augen vor der Tatsache, dass es nicht die Frage ist, "ob" man, sondern "wann" man angegriffen wird.

Resilience Level 3 - React: Nachdem erkannt wurde, dass ein Cyber-Angriff erfolgreich war, müssen die Analyse-, Eingrenzungs- und Korrekturmassnahmen eingeleitet werden. Primäres Ziel ist es, die Geschäftsprozesse so schnell wie möglich auf ein akzeptables Leistungserbringungsniveau zu bringen. Je besser die React-Disziplin in einer Unternehmung umgesetzt ist, desto schneller kann wieder ein akzeptabler Normalzustand erreicht werden.

Resilience Level 4 - Proact: Bei der vierten Stufe der Resilienz geht es darum, dass sich die Unternehmung automatisch an die Bedrohungslage anpasst und auch unbekannte Angriffe abwehren kann. Durch Zuhilfenahme von Threat Intelligence kann somit ein Abwehrdispositiv eingerichtet werden, bevor der Angriff auf die Unternehmung trifft. Dies stellt die höchste Stufe der Resilienz dar.

> Bauen Sie Ihre Geschäftsprozesse so, dass sie widerstandsfähig gegenüber Cyberangriffen werden.

Die folgende Grafik zeigt, wie sich das Leistungserbringungs-Niveau (LE-Niveau) bei einem erfolgreichen Angriff verhält und welche Resi–lienz-Disziplinen in welchem Stadium greifen.



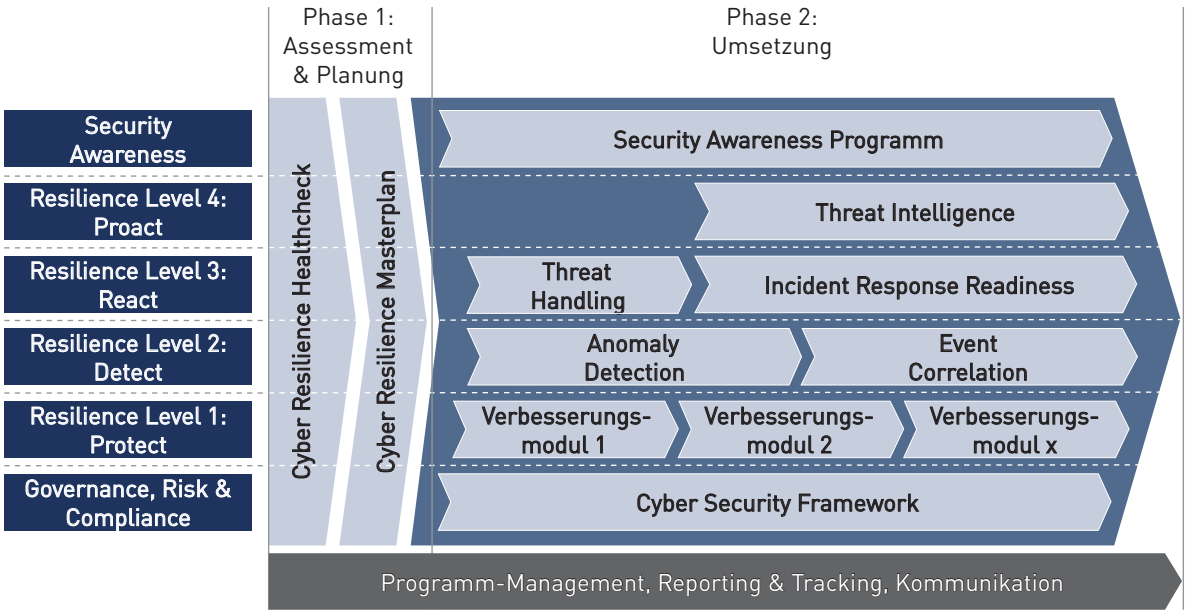
ISPIN AG ZURICH
swiss made security.®

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). 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 Cyber Resilience Healthcheck durchgeführt. Hierbei assessieren wir alle Bereiche Ihres Unternehmens in Bezug auf Cyber Risk Resilience®. 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.

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 für Cyber Risk Resilience®

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

- Das Cyber Risk Resilience® Programm ist 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