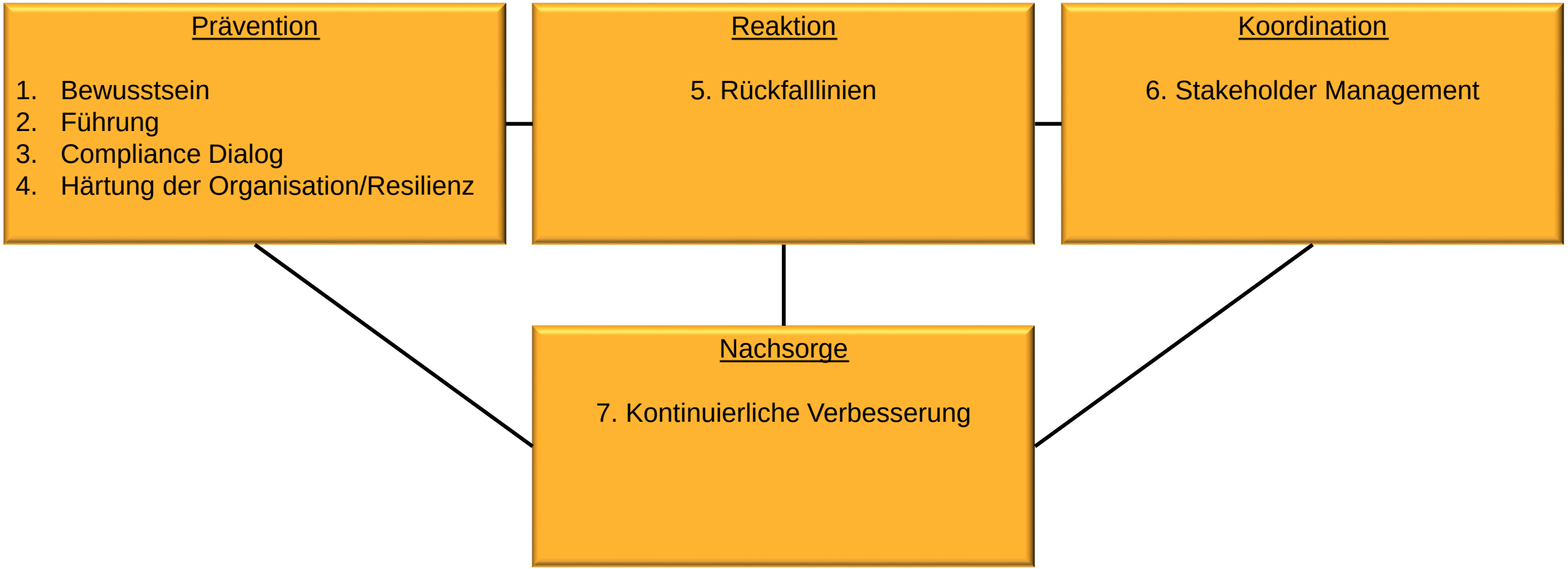
7 Punkte für die erfolgreiche Cyberabwehr im Mittelstand

CDV Consulting

COMPLIANCE · DATENSCHUTZ · VERGABESERVICE

Roland Kemper LL.M., MSc.

Hauptbegriffe, unter die die 7 Punkte gefasst werden können:



Prävention

1. Bewusstsein
Regelmäßig wiederkehrende Sensibilisierungsmaßnahmen und simulierte Situationen müssen die Mitarbeiter für mögliche Einfallstore von IT-Sicherheitsrisiken vorbereiten („***Awareness***“) von eher technisch geprägten „Phishing E-Mails“ bis zum Vortäuschen vermeintlich vertrauenswürdiger Kontakte („CEO Fraud“, „Social Engineering“).

2. Führung
IT-Sicherheit muss in Anbetracht der sich exponentiell vervielfältigenden Angriffe und Schäden „Sache der Unternehmensleitung“ sein („***Leadership***“). Ein Mitglied der Geschäftsleitung muss direkt verantwortlich sein für die Steuerung von Cyber-Risiken. Ein Informationssicherheitsverantwortlicher muss jederzeit an die Geschäftsleitung über relevante Entwicklungen und notwendige Maßnahmen berichten dürfen. Der Informationssicherheitsverantwortlicher muss einschlägige Richtlinien pflegen und ihre Befolgung nachhalten.

3. Compliance Dialog
Dass das Befolgen der Sensibilisierungsmaßnahmen wichtig ist, muss die Geschäftsleitung den Mitarbeiter vorleben („***tone from the top***“). Sinnvoll sind wiederkehrende Gesprächsformen zu Themen wie Geheimnisschutz, Arbeitsschutz und eben Informationssicherheit („***Compliance Dialog***“). Die Geschäftsleitung muss nicht nur „Ansagen“ machen, sondern diese auch sinnvoll mit den Kernwerten des Unternehmens verknüpfen. Mitarbeiter müssen das Gefühl haben, dass ihre Nachfragen, auch bei der Geschäftsleitung, in Ordnung sind. All dies steigert die Akzeptanz und die Wirksamkeit von Maßnahmen.

menschliche Verteidigungs-linien

4. Härtung der Organisation / Resilienz
Entsprechend dem Konzept der Verteidigungslinien müssen die menschlichen Verteidigungslinien („Bewusstsein“, „Führung“, „Compliance Dialog“) durch planende Elemente verstärkt werden. => **Notfallreaktionsplan**.

planende Elemente

Prävention

4. Härtung der Organisation / Resilienz (planende Elemente)

Notfallreaktionsplan:
Hier geht es insbesondere darum, unter Berücksichtigung bekannter Standards wie ISO 27001 einen auf das Unternehmen passenden Notfallreaktionsplan („***Incident Response Plan***“) zu entwerfen und jederzeit umsetzbar im Alltag der Organisation zu verankern. Dieser Plan berücksichtigt insbesondere die folgenden Aspekte:

Szenarios: Wie und mit welcher Wahrscheinlichkeit können bestimmte Angriffe die IT-Systeme und die Leistungsprozesse beeinträchtigen?

Prognose von Schäden: Was sind die wahrscheinlichen Schäden (z.B. Vermögen durch Produktionsausfall? Vertragsstrafen wegen Lieferunterbrechungen? Reputation, etwa durch Datenverlust?)?

Wer ist betroffen? Wer ist intern und extern betroffen und mit wem muss wie kommuniziert werden („***Stakeholder***“)? So enthalten die Einkaufsbedingungen von Kunden häufig Benachrichtigungspflichten.

Lieferkette: Kurzsichtig ist es, nur Angriffe auf die eigene IT-Landschaft als Risiken zu begreifen. Genauso müssen Unternehmen die Risiken für die IT-Landschaft ihrer Lieferkette steuern („***supply chain risks***“). Dies schließt insbesondere ein, dass die Lieferanten durchgehend zur Einhaltung bestimmter Standards (etwa „***TISAX***“ für die Automobilindustrie) verpflichtet werden.

Krisenstab: Wer macht was und welche Abläufe gelten grundsätzlich? Der Krisenstab sollte nicht erst im Krisenfall zusammentreten und Krisen bereits simuliert haben. Gerade in den ersten 72 Stunden nach Entdecken eines Angriffs müssen Weichen gestellt werden.

Standardisierte Reaktionsmuster („templates“): Antworten an Betroffene sollten schon „in der Schublade“ liegen und im Krisenfall möglichst nur angepasst werden müssen.

Einbindung der Geschäftsleitung: Besonderes Augenmerk ist zu richten auf die Einbindung der Geschäftsleitung in das Krisenmanagement.

Einbindung der staatlichen Ermittlungsbehörden: „Cyber Attacken“ sind keine Privatsache. Die staatlichen Ermittlungsbehörden verfolgen bestimmte Angriffe im öffentlichen Interesse. Es muss sichergestellt werden, dass das private Unternehmensinteresse und die öffentlichen Interessen nicht in Widerstreit treten. Deswegen muss der Krisenstab darauf vorbereitet sein, wie er die Kontakte zu den Ermittlungsbehörden pflegt.

Datenschutzbehörden: Angriffe auf die IT-Landschaft können Datenschutzvorfälle darstellen. Dies kann Meldepflichten gegenüber Datenschutzbehörden und individuell Betroffenen zur Folge haben. Wenn das angegriffene Unternehmen eines der „kritischen Infrastruktur“ ist, kann eine Benachrichtigung des Bundesamtes für Sicherheit in der Informationstechnik erforderlich sein („BSI Gesetz“). Vergleichbare Pflichten können Unternehmen der Finanzwirtschaft treffen gemäß Zahlungsdienstaufsichts- und Kapitalmarktgesetzen.

Versicherung: Versicherer müssen rechtzeitig eingebunden werden. Wenn sich das Unternehmen organisatorisch nachweislich so aufstellt, dass mögliche Risiken aus Angriffen auf die IT-Landschaft offensiv angegangen werden, dann besteht die Chance, sich gegen solche Angriffe zu versichern.

Umgang mit Kriminellen: Leider werden Angriffe auf die IT-Landschaft von Unternehmen häufig mit Forderungen seitens der kriminellen Angreifer verbunden. Hier stellt sich die Frage, wer die Expertise hat, mit diesen Forderungen umzugehen und zu verhandeln. Zu beachten ist, dass Versicherungen immer weniger bereit sind, die Schäden aus der Zahlung von Lösegeldforderungen zu versichern.

Forensiker: Um das Einfallstor des Angriffs, den Umfang des Schadens und empfehlenswerte Gegen- und Nachsorgemaßnahmen zu bestimmen, müssen regelmäßig private oder polizeiliche Forensiker in den Einsatz. Ob und inwieweit Forensiker tätig werden sollen, muss so früh wie möglich entschieden werden. Der Krisenstab muss also die Fähigkeiten von Forensikern kennen und den Kontakt zu einsatzbereiten Forensikern pflegen.

Techniker: Techniker müssen befallene Systeme und Datenbestände gegebenenfalls reinigen oder aus anderen Quellen („***back-ups***“) wiederherstellen. Gegebenenfalls müssen sie Hardware- und Datenumgebung komplett ersetzen. Dies sollte in Wiederherstellungsplänen („***disaster recovery***“) vorausschauend geplant sein.

Separierung des Notfallreaktionsplan: Der beste Notfallreaktionsplan hilft nicht, wenn der Cyber-Angriff die Datengrundlage des Notfallreaktionsplans korrumpiert. Der Notfallreaktionsplan (einschließlich der Kontaktdaten des Krisenteams, der Forensiker, des Versicherers, der Techniker etc.) sollte also in IT-technisch völlig getrennten Systemen bereitliegen.

Kommunikationskonzept: Das Vorstehende zeigt, dass mit Vielen gezielt gesprochen werden muss. Liegt ein Kommunikationskonzept vor? Passt dieses zur Unternehmenskultur? Welche Botschaft erhalten Belegschaft, Kunden und Lieferanten?

Reaktion

5. Rückfalllinien

Ein wichtiges Mittel hierfür sind „Kontinuitäts- und Wiederherstellungs-Pläne“ („business continuity & disaster recovery“

Koordination

6. Stakeholder Management

Im Fall eines Cyber-Angriffs muss das Unternehmen die Interessen verschiedener Betroffener koordinieren (Krisenteam, Ermittlungsbehörden, Forensiker, Versicherung, Techniker, Lieferanten, Kunden etc.). Geschieht dies zu spät oder fehlerhaft, kann dies empfindliche rechtliche Folgen haben. Die rechtlichen Spielräume und Folgen muss das Unternehmen deshalb im Blick haben. Die internen oder externen Rechtsberater des Unternehmens müssen deshalb mir dem Notfallreaktionsplan, dem Kontinuitätsplan und dem Wiederherstellungsplan des Unternehmens vertraut sein und wissen, wie sie diesen im Krisenfall zu Gunsten des Unternehmens einsetzen.

Nachsorge

7. Kontinuierliche Verbesserung

Nicht zuletzt mit Rücksicht auf eine Wiederversicherbarkeit muss das Unternehmen Lehren aus erfolgten Angriffen ziehen und in Verbesserungsmaßnahmen einbringen.