Die (goldenen) Grundregeln des Krisenmanagements

Dipl. – Ing. Dietrich Läpke
dietrich.laepke@cyber-akademie.de

Die am Häufigsten Verwendete Regel

- Es kommt, wie es kommt
- Es ist schon immer gut gegangen

Nachzulesen u.a. am Flughafen Köln/Bonn :

„Das Kölsche Grundgesetz“

Leider häufig nicht nur in Köln angewandt und ganz falsch

Regel 1:
Krisenmanagement ist ein Regelkreis

- Prävention / Vorbeugung
- Vorsorge / Vorbereitung / Erfahrungsaustausch
- Gefahrenabwehr
- Rehabilitation / Wiederherstellung
- Auswertung / Evaluation / Kommunikation

Regel 2

- **Risiko- und Gefährdungsanalysen** sind unverzichtbare Grundlagen von Prävention und Vorbeugung.
- Nur wer weiß, was ihn bedrohen könnte, kann sich entsprechend vorbereiten und schützen.
- Auch ungewöhnliche Szenarien müssen angedacht werden „***think the unthinkable*“ .**
- Im Cyberraum drohen u.a.
  - Spionage
  - Sabotage
  - Raub
  - Erpressung

Regel 3

- Krisen fallen selten überraschend vom Himmel
- Früherkennung -spätestens auf der Chefebene -entscheidet darüber, ob man sich auf die Krise vorbereiten kann.
- Bei Bedrohungen z.B. aus dem Cyberraum ist oft schon jede Stunde wertvoll.
- Daher ist ständiges screening in vielen Bereichen (z. B. social media) notwendig

Regel 4

Unangenehme Botschaften / Anzeichen müssen stets unverzüglich in Richtung ***worst case*** analysiert werden.

Abwarten kann schlimmste Folgen haben !

Die Frage ist nur, wer bei Ihnen dafür zuständig ist bzw. sich dafür zuständig fühlt ??

In Krisensituationen sind dafür übrigens nicht Andere zuständig, sondern zuerst einmal man selbst, die eigene Organisationseinheit, die eigene Firma, …

Regel 5

Man muss sich auf Krisen vorbereiten:

- Szenarien antizipieren
- Krisenmanagement planen und organisieren
- Diese Strukturen regelmäßig testen, **beüben**, optimieren und pflegen
- Krisensichere Informations- und Kommunikationssysteme und -strukturen (intern und extern) vorbereiten
- Ständige Schwachstellenanalysen durchführen
  (*z.B. white hacking*)
- Redundanzen (in jeder Hinsicht!) vorbereiten

Regel 6

Besonders in der Krise ist ein - sich ständig wiederholender - konsequenter Führungs- und Entscheidungsprozess stringent anzuwenden.

Krisenmanagement heißt : **Entscheiden + Handeln**

- Was ist passiert ?
  = Lagefeststellung
- Was kann das für Folgen haben ?
  = **Lagebeurteilung und Risikoanalyse** – ***worst case***
- Was können wir tun ?
  = **Optionen des Handelns**

REGEL 6 FORTSETZUNG

- Was werden wir tun ? Was hat die geringsten negativen Folgen ?
  = **Entscheidung** durch den Chef
- Wer tut was wann wie mit wem bis wann ?
  = **Aufträge**
- Ist alles geschehen, was wir angeordnet / veranlasst haben?
  = **Auftragskontrolle**
- Neue Lagefeststellung, Lagebeurteilung /, Risikoanalyse
  = **Regelkreis**

> *Das Alles funktioniert koordiniert nur in einem - eingeübten - **Krisenstab** auf Basis eines maßgeschneiderten **Krisenmanagementhandbuches***

Regel 7

- Krisenmanagement ist Gemeinschaftsaufgabe aller Beteiligten unter – vorher festgelegter bzw. vereinbarter – Leitung bzw. Koordinierung.

- Die Abteilungen, Bereiche, Niederlassungen etc. behalten aber in der Regel ihre Zuständigkeiten und Verantwortlichkeiten.

- Der Krisenstab koordiniert und gibt Vorgaben, Aufträge etc. Die Umsetzung sollte aber immer Aufgabe derjenigen Organisationseinheiten sein, die auch im alltäglichen Geschäft dafür zuständig sind (*„never change a winning team“*)

Regel 8

- Man bekommt eine Krise letztlich nur dann in den Griff, wenn man aus der Reaktion wieder in die ***Aktion*** kommt. D.h. : Man wird Herr des Handelns in seinem Bereich und nicht mehr von der Krise gesteuert

- Aus der prognostischen ständigen Lagebeurteilung so schnell wie möglich zu präventivem Handeln kommen, um die *business continuity* wieder herzustellen.

- SEHR schwierig! Daher Prävention und Vorsorge!!

Regel 9

- Krisen dauern so lange, wie man benötigt, sie in den Griff zu bekommen …
- … und die Medien, die sozialen Netzwerke, die Bürger bzw. die Kunden und die Mitarbeiter davon überzeugt sind, dass auch alle Folgen bewältigt sind.

Regel 10

Heute ist die **Krisenkommunikation** genauso wichtig – wenn nicht für das Vertrauen der Bürger bzw. Kunden noch wichtiger – wie die Maßnahmen der Krisenbewältigung selbst.

Regel 11

Es sind die Krisen bzw. Vorfälle am gefährlichsten :

- Die man nicht mit der Feuerwehr bewältigen kann
- Die gar keine sind, sondern durch Gerüchte / Panik entstehen
- Die in den sozialen Medien zeitnah kommuniziert werden
- Die in den (sozialen) Medien zu falschen Behauptungen etc. führen
- Bei denen die Betroffenen nicht zeit- oder sachgerecht intern und extern informieren
- Bei denen die Betroffenen nicht alsbald die Kommunikationshoheit erlangen

Regel 12

Auch Krisenstäbe können von Krisen erfasst werden

Das ist regelmäßig dann der Fall, wenn man nicht regelmäßig mit verschiedenen Szenarien geübt hat und / oder die handelnden Personen kein Vertrauensverhältnis zueinander haben

Regel 13

Die nächste Krise kommt bestimmt.

Sie hat aber nicht die gleiche Ursache und findet nicht in der gleichen Region oder Institution statt, wie die letzte .

P.S. Regel 13 A : Krisen / Katastrohen / Hackerangriffe finden Freitag Nachmittag, am Wochenende oder am Feiertag statt.

Regel 14

- Bei gleichartigen Vorfällen muss ein sofortiger Informations- und Meinungsaustausch zwischen den Betroffenen erfolgen.

  Daher: ***In Krisen Köpfe kennen***

- Insbesondere die Krisenkommunikation – auch und besonders in den sozialen Medien – muss abgestimmt und möglichst gleichlautend sein – one voice policy

- Auch kann eine Abstimmung mit betroffenen anderen Unternehmen etc. sinnvoll sein

Regel 15

- Die Einschaltung der (Sicherheits-) Behörden bei Cyber-Vorfällen ist notwendig
- BSI u.a. bzgl. Modus Operandi / Warnung der Anderen
- LKA bzgl. Täterermittlung und „Abschaltung“ – *es handelt sich stets um Straftaten!!*
- Ggf. Verfassungsschutz bzgl. Prävention

Auch hier gilt: Vor Krisen Köpfe kennenlernen

Nur wenn bisher nicht Betroffene erfahren, was Anderen widerfahren ist, kann man den Kriminellen die Arbeit erschweren und künftige Schäden reduzieren.

Regel 16

Nur eine ehrliche Auswertung und Schwachstellenanalyse nach einer Krise und die schnelle Umsetzung der Schlussfolgerungen und des Handlungsbedarfs verbessern das Krisenmanagement .

Für nicht Betroffene gilt : Lernen aus den Erfahrungen Betroffener, denn das kann einem ja auch mal passieren.

Es ist nicht die Frage, **ob** Sie von einem Ereignis erwischt werden.

Es ist nur die Frage **W A N N**.

Danke für Ihre Aufmerksamkeit

dietrich.laepke@cyber-akdemie.de