Cyber: Crime or Security?

- ND-Perspektive!
- Wie sind KMU betroffen?

70. Gewerbliche Winterkonferenz SGB / USAM
Klosters / 18.01.2019

Philipp Kronig, C NDBI

Haben wir ein Problem ?

Zur Bedrohungslage

- Zunahme der Bedeutung der Informationstechnologie für Geschäftsprozesse und Finanztransaktionen
- Zunahme der Teilnehmer an diesen Prozessen, zunehmende Vernetzung
- Zugang zu immer mehr wertvoller Information wird möglich
- Zunahme der Möglichkeiten für Betrug, Spionage, Erpressung, Sabotage
- Auftreten neuer Akteure (z.B. Organisierte Kriminalität, Staaten)
- Anpassung der Motive und Methoden bestehender Akteure: kommerzieller Gewinn, Know-how Transfer, politische Motive

Die zwei Hauptentwicklungen mit Blick auf die Bedrohungslage

Der Tabubruch

- Die Vorfälle in der Ukraine Ende 2015 und 2016, sowie die gezielten Angriffe mit "Ransomware" auf Spitäler Mitte 2016 zeigen, dass staatliche und kriminelle Akteure bewusst physische Effekte und Menschenleben in Kauf nehmen.

"Collaterals are the new Black"

- Die Schweiz läuft Gefahr zunehmend kollaterale Schäden durch Cyberangriffe zu erleiden und kommt im rauhen internationalen Klima vermehrt auch als Standort internationaler Organisationen unter Druck.

Haben wir eine Lösung ?

Haben wir eine Lösung ?

Die schlechte Nachricht: es gibt keine Lösung.

Die gute Nachricht: es gibt Erfolgsrezepte.

Erfolgsfaktor 1: risikobasiert und eigenverantwortlich agieren

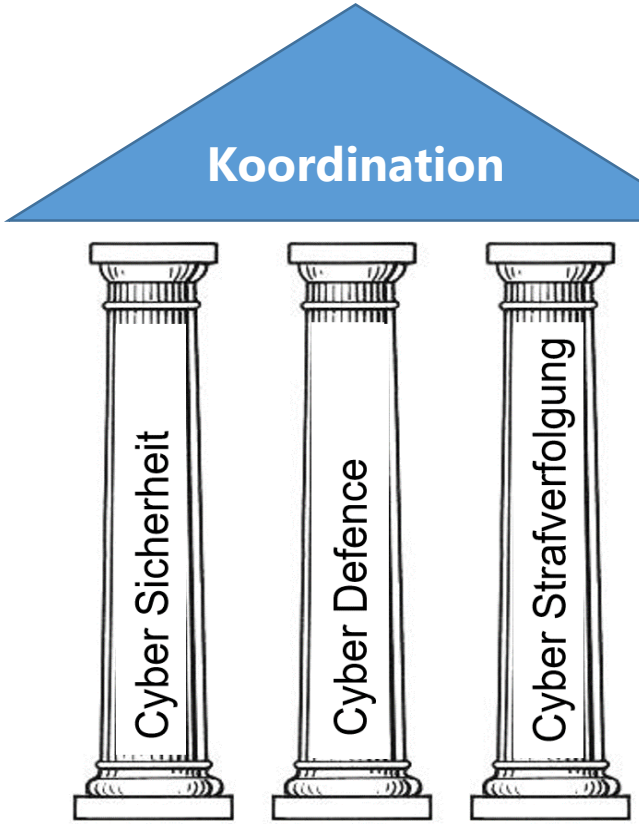
- Welche Prozesse / Daten müssen unbedingt geschützt werden? Welches Risiko bin ich bereit zu tragen?
- Risikomanagement ist Chefsache. Verantwortung kann letztlich nicht delegiert werden.
- Plan B für geschäftskritische Prozesse vorsehen.
- Der Schwächste wird angegriffen.

Erfolgsfaktor 2:
PPP / Staat nur subsidiär

- Schweiz hat breite Tradition der Zusammenarbeit Private / Staat in Sicherheitsfragen. Kleinheit fördert Vertrauen.

- Staat liefert originäre, vertrauenswürdige Informationen, Vernetzung der Konkurrenten , einheitliche Vorgaben.

Erfolgsfaktor 3: Kooperation statt Zentralisierung



- **Gemeinsames Lagebild**
- **Koordination bei Vorfällen / Krisenmanagement**
- **Zentrale Anlaufstelle für Dritte**

- **Cyber-Sicherheit:** Prävention, Vorfallbewältigung, Resilienzmanagement, Bildung und Forschung, internationale Zusammenarbeit
- **Cyber-Defence:** nachrichtendienstliche und militärische Massnahmen zur Abwehr von Cyber-Angriffen
- **Cyber-Strafverfolgung:** Massnahen der Polizei und Staatsanwaltschaft im Kampf gegen Cyber-Kriminalität

Erfolgsfaktor 4: Internationale Zusammenarbeit

- Jeder nennenswerter Cyberangriff weist internationale Bezüge (Infrastruktur, Täter, Opfer, Software, Geldflüsse) auf.
- Kein Staat verfügt selbst über alle wesentlichen Informationen.
- Gemeinsame Interessen, wechselnde Allianzen.
- Erfolgreiche internationale Übungen (EU, NATO, CERT).
- Auf diplomatischer / politischer Ebene ist kaum eine Bereitschaft für eine internationale Regelung spürbar.

Erfolgsfaktor 5: Integraler Ansatz

- Eine Strategie zum Schutz vor Cyberrisiken darf sich nicht mehr auf den Schutz kritischer Infrastrukturen beschränken.

- Staat, Gesellschaft und Wirtschaft sind gemeinsam gefordert. Die Verantwortungen und Zuständigkeiten müssen klar definiert und von allen Beteiligten gelebt werden.

- Cyber Sicherheit aus einer Hand ist eine Illusion und trägt der zunehmenden Durchdringung aller Lebenslagen nicht Rechnung.

Erfolgsfaktor 6: Notwendige Ressourcen bereitstellen

- Ausbildung von Experten zwingend notwendig (Cyber-RS, Masterlehrgänge).

- Investitionen in sichere Infrastrukturen (D: Agentur für Innovation in der Cybersicherheit mit 150 Millionen Euro Budget) und Personal (auch beim Bund).

Erfolgsfaktor 7: NDB

- Frühzeitiges Erkennen, Verhindern und Bekämpfen von sicherheitsrelevanten Angriffen gehören zum Kernbusiness des ND => first line of defence.
- Aussagen zur wahrscheinlichen Täterschaft (Attribution) ist eine Kernfähigkeit des ND.
- Gelebte internationale Vernetzung, originäre Quellen.
- Ermöglicht Massnahmen auf politischer und diplomatischer Ebene.
- In PPP-Modell MELANI eingebunden.

Erfolgsfaktoren auf Stufe KMU:

- Sensibilität der Angestellten für Cyberrisiken erhöhen (Umgang mit Mails, SMS, Soziale Medien).
- Konsequente Sicherung der geschäftsrelevanten Daten. Testen der Back-up Fähigkeit.
- Schutzsysteme für Hard- und Software aktuell halten.
- Password-Richtlinien durchsetzen.
- Sensible Daten und Prozesse besonders schützen (Verschlüsselung).
- Selbsttest: https://ictswitzerland.ch/themen/cyber-security/check/

… dann gibt es auch Erfolgsmeldungen…

Schweizer Erfolg gegen Cyber-Crime: Zwei Verhaftete in Niederlanden

Zwei Personen, die in der Schweiz E-Banking-Date international koordinierten Aktion verhaftet worc

Spiez-Spione sollen hinter Cyber-Angriff auf Anti-Doping-Agentur stecken

Zwei mutmassliche russische Spione sind im Frühjahr auf dem Weg zum Labor Spiez in den Niederlanden festgenommen und zurückgeschickt worden. Gegen die beiden Spione läuft zudem ein Cyberattacke auf die Welt-Anti- bekannt wird.

Erste Cyber-RS gestartet

Internet-Soldaten, vorwärts, Marsch!

Cyberattaque

La police valaisanne arrête les pirates informatiques du Groupe Mutuel

AL SWITZERLAND

chweiz will Vorkämpferin gegen Cybercrime werden

Remo Stoffel – Milliarden angelegt, Milliarden...

Home > Konjunktur > «WannaCry» verschont die Schweiz weitgehend

HACKERANGRIFF

«WannaCry» verschont die Schweiz weitgehend