Risikoinformationen zu der KUCO-Cyberversicherung

1. Gesamtschadenszahlen

1.1 Statistiken Deutschland

- Die Zahlen divergieren sehr stark:
  - Laut der europäischen Polizeibehörde Europol soll es weltweit insgesamt Schäden von 450 Milliarden gegeben haben – davon 65 Milliarden allein in Deutschland.
  - Dagegen sind die dem Bundekriminalamt (= BKA) gemeldeten Schäden wesentlich niedriger (was aber auch damit zusammenhängen kann, dass das BKA nur die ihm gemeldeten Vorfälle statistisch erfasst, die aber wegen der hohen Dunkelziffer in diesem Bereich wesentlich niedriger sein werden).
    So soll nach einer Statistik des BKA aus 2019:
    - Der Gesamtschaden in Deutschland 2017 71,8 Milliarden betragen haben, was
    - Im Vergleich zum Jahr 2012 immerhin eine Steigerung von 70% ausmachen würde.
  - Bereits die BKA-Statistik aus 2012 wies 64.000 Fälle von Cyberkriminalität aus (Dunkelziffer wahrscheinlich wesentlich höher).
  - Dagegen liegt nach der „Vereinigung der bayrischen Wirtschaft“ der Gesamtschaden der Deutschen Wirtschaft für 2013 bereits bei ca. 50 Milliarden.
- Nach einer Untersuchung der „ACE European Group“ haben bereits:
  - 47% der Unternehmen in Deutschland und
  - 44% der Unternehmen in Europa

  unberechtigte Hackerangriffe gehabt.
- Einer Studie des Digitalverbandes Bitcom aus 2017 zufolge:
  - Ist in den letzten 12 Monaten jeder zweite Internetnutzer in Deutschland Opfer von Cyberangriffen geworden, davon
  - Haben ca. die Hälfte einen finanziellen Schaden erlitten.
- Das US-IT-Unternehmen „Norton by Symantec“ kommt zu ähnlichen Ergebnissen. Danach:
  - Sind 38% der deutschen Internetnutzer von Cyberangriffen betroffen;
  - Soll dadurch ein Schaden von 2,2 Milliarden entstanden sein.

1.2 Besonders cybergefährdete Unternehmen in Deutschland

Nach Erkenntnissen des Bundesamtes für Verfassungsschutz sind viele:

- Gerade kleinere und mittlere Unternehmen, die stark in Forschung und Entwicklung investieren, das bevorzugte Ziel von Spionageattacken fremder Nachrichtendienste bzw. Konkurrenten;
- Sog. „Hidden Champions“. Das sind Weltmarktführer auf einem Spezialgebiet.
  60% aller dieser Hidden Champions sollen ihren Sitz in Deutschland haben.

2. Risikobewusstsein in Deutschland

2.1 Angst vor Reputations- und sonstigen Schäden

- Kurios ist gem. einer Untersuchung von „Spiegel Online“, dass deutsche Unternehmen:
  - Sich zwar mehr öffentliche Aufmerksamkeit für dieses Thema wünschen;
  - Jedoch über die Erfahrung in dem eigenen Unternehmen keine Antwort geben wollen; hauptsächlicher Punkt: Angst vor Reputationsschäden.
- Imageschäden und Vertrauensverlust beim Kunden werden von den Unternehmen zunehmend befürchtet.

- Deshalb wird das Cyberrisiko mittlerweile auch als eines der Top Unternehmensrisken eingeschätzt.
- In diesem Rahmen sehen die Unternehmen die von Lieferanten ausgehenden Cyber Risiken immer kritischer.
  Einer der für Cyberversicherer arbeitende Sicherheitsdienstleister behauptet in seiner internen Studie, dass 80% der von ihm befragten Unternehmen die Geschäftsbeziehungen zu ihren Anbietern/Zulieferern wegen deren unzureichender Cybersicherheit bereits gekündigt hätten.

2.2 Allgemeines zur Risikobewusstsein/Risikovorsorge

2.2.1 Risikovorsorge

- Lt. einer Untersuchung des Bundeswirtschaftsministeriums sichern ein viertel der kleinen und mittleren Unternahmen in Deutschland ihre Daten nicht bzw. nur unregelmäßig.
- Lt. dem in 2014 zum 4. Mal von der „Initiative im Netz Sicherheitsmonitor Mittelstand ist:
  - Die digitale Vernetzung bei kleineren und mittleren Unternehmen (**KMUs**) erheblich angestiegen;
  - Der Schutz vor IT-Risiken jedoch rückläufig:
    - So nahmen Schutzmaßnahmen bei E-Mail Versand auf 43% ab und
    - Jedes 4. Unternehmen ergreift hier überhaupt keine Maßnahmen, obwohl Sicherheitsfragen „als wichtig empfunden werden".

2.2.2 Risikobewusstsein

- Lt. Allianz „Risk Barometer Unternehmensrisiken 2017 in Europa" werden als größte Risiken angesehen:
  - Betriebsunterbrechungen (inklusive Lieferkettenunterbrechungen): 35%;
  - Cyberkriminalität, IT-Ausfälle, Spionage und Datenmissbrauch: 32%;
  - Produkt-Märkteentwicklung: 32%
- Lt. KPMG aus 2015 schätzen 89% der Deutschen das Risiko, dass deutsche Unternehmen Opfer von Cyberattacken werden, als sehr hoch ein.

3. Angriffsformen

- Definitionen und Erscheinungsformen von Cyber-Crime
  Laut Bundekriminalamt umfasst Cyber Crime Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten bzw. die mittels dieser Informationstechniken begangen werden.
  Bereits in einer Veröffentlichung des Gesamtverbandes für die deutsche Versicherungswirtschaft (= **GVD**) wurden die Schadenprogramme weltweit auf 250 Millionen geschätzt. Seit dieser Zeit hat sich deren Zunahme bekanntlich dramatisch entwickelt.
- Fallgestaltungen von Cyberkriminalität:
  - Einsatz von Ransomware (Englisch: ransom = Lösegeld)
    Dabei werden kryptographische Verfahren verwendet, um Dateien und Dokumente auf infizierten Computern zu verschlüsseln, wobei für die Zugriffwiederherstellung ein Lösegeld verlangt wird.
    Mittlerweile soll es mehr als 10 Millionen Varianten davon geben.
    Aktueller Fall: Wohl die Juwelier Kette Wempe.
  - Ausnutzung von menschlichen Schwachstellen durch sog. „Social Engineering" – Sozialmanipulation durch Ausspähen von Informationen über (gutgläubige) Mitarbeiter, z.B. vertrauliche Infos weiterzugeben.

z.B.: Verifizierung des Online-Banking Accounts; Angebote zur EDV-Telefonbetreuung oder EDV-Reparaturen.

- „Botnet“ (= Netzwerk aus Computern; aus den englischen Begriffen „robot“ und „network“ zusammengesetzt).
  Technik: Eine Vielzahl von Rechensystemen wird von einer Schadsoftware infiziert und dann „auf Kommando“ (meist durch Fernsteuerung) zusammengeschlossen, um bestimmte Aktionen durchzuführen.
- „Denial-Of-Service“-Angriff (= Dos) – absichtlich herbeigeführte Serverüberlastung durch Hacker, um die EDV „zum Absturz zu bringen“, damit keine Geschäftsabwicklungen mehr möglich sind.
- Weiteres Cyber-Beispiel:
  Massenangriffe auf die EDV/IT mit „Wanna Cry oder Petja/Net Petja-„Schadensprogrammen , die weltweit Computer befielen und lahmlegten und erst gegen Zahlung von Lösegeld wieder freigegeben wurden.
  Lt. Europol waren 230.000 Unternehmen weltweit davon betroffen. Dabei ging es vor allem um Firmen, die noch mit dem Windows XP gearbeitet hatten, das 2001 auf den Markt kam und von Microsoft seit 2016 nicht mehr gepflegt wird.

4. Cyber-Versicherungsinteresse bzw. Versicherungsabschlüsse in Deutschland

4.1 Statistische Informationen

- Aktuelle Infos zur Cyberversicherung
  Lt. Bitcom ergibt sich aufgrund einer Befragung von über 500 Industrieunternehmen in 2018 folgendes:
  - Unternehmen ab 500 Mitarbeiter:
    - 32% haben eine Versicherung abgeschlossen;
    - 38% planen oder diskutieren einen Abschluss.
  - Unternehmen zwischen 100 bis 500 Mitarbeitern:
    - 23 % haben eine Versicherung abgeschlossen;
    - 50 % planen oder diskutieren den Abschluss.
  - Unternehmen zwischen 10 und 99 Mitarbeitern:
    - Abschlussquote nur 10%;
    - 42 % planen oder diskutieren den Abschluss.
- Die hauptsächlichen Gründe für einen Abschluss
  Das sind der Reihenfolge nach:
  - Befürchtete Kosten durch einen Cyberangriff: 45%
  - Sorge um die Sicherheit eigener Daten: 40%
  - Angst vor Haftungsansprüchen von Kunden und sonstigen Dritten: 28%
  - Versicherungsnotwendigkeit wegen neuer Datenschutzbestimmungen: 27%
  - Weil der Abschluss einer Cyberversicherung gesetzlich erforderlich sei: 20% (stimmt nicht!)
- Von welchen Cyber Szenarien fühlen sich die Unternehmen bedroht bzw. sind bei ihnen bereits eingetreten?
  Lt. Umfrage der Commerzbank aus 2019 sind für die Unternehmen reale oder denkbare Bedrohungen der Reihenfolge nach:
  - Schädigungen der IT durch „Trojaner oder Viren“: 73%
  - Ausnutzung von Sicherheitslücken durch Hackerangriffe: 78%
  - Digitale Betrüger, die sich bereichern wollen: 64%.
- Täterkreis von kriminellen Handlungen aus Sicht der Unternehmen

Gem. einer Bitcom Veröffentlichung aus 2019 sind in den letzten 2 Jahren durch Cyber-Kriminalität betroffene Unternehmen befragt worden, wer die Täter waren oder wen sie als Täter vermuten. Danach sind Täter:

- Derzeitige bzw. frühere Mitarbeiter: 63%
- Geschäftliches Umfeld (Wettbewerber, Kunden, Lieferanten, Dienstleister): 48 %
- „Hobby-Hacker“: 29%.

4.2 Fazit: Bewertung des KUCO-Konzeptes auf der Grundlage vorstehender Cyberstatistiken/-Informationen

Gem. dem KUCO Konzept 2019 sind Cyber Risiken automatisch in der D&O Basisdeckung versichert (=“Schadensersatzansprüche“ gegen D&O versicherte Personen) oder über die D&O Entity bzw. Multi optional versicherbar (im Hinblick auf den Einschluss der VN und aller ihrer Mitarbeiter für Cyber-Haftpflicht – sowie für Hacker-Risiken).

Im Einzelnen:

Im Rahmen der KUCO Multi ist versicherbar:

- Mitarbeiterkriminalität
  (63% der geschädigten Unternehmen sehen derzeitige bzw. frühere Mitarbeiter als Täter an),
  einschließlich:
  - EDV-Kriminalität und
  - Mitarbeitersabotage sowie
- Drittkriminalität in Form der:
  - Hackerdelikte mittels:
    - Bereicherung
    - Schädigung der EDV bzw. IT
  - Täuschung Dritter durch die Nutzung der EDV.
    (V*on den befragten Unternehmen sehen 29% Hobby-Hacker und 17% organisierte Kriminalität als Schadensursache an.)*

Desweiteren sind über die Entity Deckung Reputationsschäden versicherbar.
(Imageschäden und Vertrauensverlusten bei Kunden werden von den Unternehmen zunehmend befürchtet; die werden zwischenzeitlich als eines der Top-Unternehmensrisiken eingestuft.)

- Dagegen sieht eine marktübliche Cyber-Kriminalitätsdeckung vor:
  - Cyberhaftpflicht-Versicherung, wie bei KUCO auch;
  - Cyberkriminalität:
    - Meist ohne Mitarbeiterkriminalität;
    - Teils mit Mitarbeiterkriminalität (dann aber häufig ohne Mitarbeitersabotage);
  - Service- und Kostenbausteine, jedoch keine Reputationsschäden.