BAKER & MCKENZIE

Cybersecurity

Rechtliche Risiken richtig erkennen, bewerten und reduzieren

RA Dr. Lukas Feiler, SSCP, CIPP/E

IT-LAW.AT Seminar
12. Juni 2015

TOPICS

- Cybersecurity – Eine Einleitung
- Daten- vs. Informations- vs. IT-Sicherheit
- Welche rechtlichen Risiken gibt es?
- Wie können Risiken sinnvoll bewertet werden?
- Möglichkeiten der Risiko-Behandlung
  - Risikominderung durch Zertifizierungen
  - Risikotransfer durch Cybersecurity-Insurance

Cybersecurity – Intro

Cybersecurity – Zentrale Herausforderungen

- Angreifer verfügen über professionelle Fähigkeiten
  - Typische Erscheinungsform der 1990er: Teenager
  - Typische Erscheinungsform der 2010er:
    - Organisierte Kriminalität
    - Hacktivists
    - Industriespionage durch ausländische Unternehmen und Nachrichtendienste (APTs)
- Die Angriffsfläche wird immer größer
  - Big Data, Internet of Things, …
- Weder Technologie noch Menschen sind perfekt

Daten- vs. Informations- vs. IT-Sicherheit

IT-Sicherheit vs. Info-Sicherheit vs. Datensicherheit (1/3)

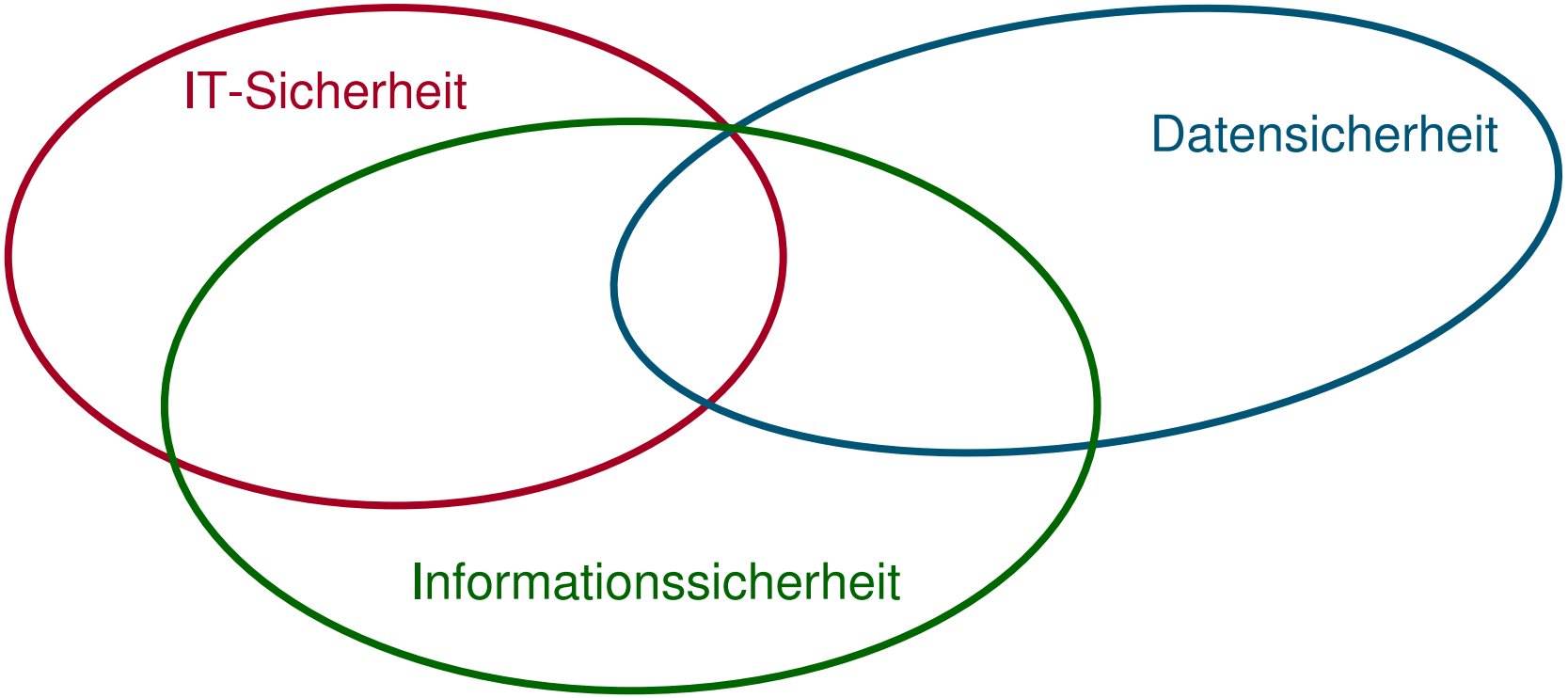
- Informationssicherheit:
  - Vertraulichkeit,
  - Integrität und
  - Verfügbarkeit

  von Informationen (unabhängig von ihrer Art und vom Träger)
- IT-Sicherheit
  - Informationssicherheit im Bereich der IT
  - Umfasst auch die Verfügbarkeit von IT-Infrastruktur

IT-Sicherheit vs. Info-Sicherheit vs. Datensicherheit (2/3)

- Datensicherheit
  - Personenbezogene Daten statt Informationen aller Art
  - Daten sind zu schützen vor (§ 14 DSG 2000):
  - Verlust
    → Verfügbarkeit (temporäre Nicht-Verfügbarkeit nicht erfasst)
  - zufälliger oder unrechtmäßiger Zerstörung
    → Integrität
  - Zugänglichkeit für Unbefugte
    → Vertraulichkeit
  - nicht ordnungsgemäß Verwendung
    → datenschutzrechtliche Rechtmäßigkeit

IT-Sicherheit vs. Info-Sicherheit vs. Datensicherheit (3/3)



Welche rechtlichen Cybersicherheits-Risiken gibt es?

Zentrale rechtliche Cybersecurity-Risiken

- Persönliche Haftung der Geschäftsleitung für IKS
- Verwaltungsstrafrechtliche Verantwortlichkeit
- Schadenersatzpflicht bei Datenschutzverletzungen
- Kosten einer Data-Breach-Notification
- Verlust der Patentfähigkeit von Erfindungen
- Schadenersatzpflichten gegenüber Kunden

Persönliche Haftung der Geschäftsleitung für das Interne Kontrollsystem

- Kapitalgesellschaften sind zur Führung eines IKS verpflichtet (§ 82 AktG, § 22 GmbHG)
- Geschäftsleitung haftet für unzulässiges IKS
- IKS: Methoden und Maßnahmen, die dazu dienen,
  - das Vermögen zu sichern,
    - → Vertraulichkeit von Geschäftsgeheimnissen
    - → Integrität von urheberrechtlich geschützten Werken (zB Software)
    - → Verfügbarkeit aller Digital Assets
  - die Genauigkeit und Zuverlässigkeit der Abrechnungsdaten zu gewährleisten und
    - → Integrität des Buchhaltungssystems
  - die Einhaltung der vorgeschriebenen Geschäftspolitik zu unterstützen

Verwaltungsstrafrechtliche Verantwortlichkeit für unzureichende Datensicherheit (1/2)

- Nach § 14 DSG 2000 verpflichtendes Sicherheitsniveau: Angemessen unter Berücksichtigung
  - der Art der verwendeten Daten
  - Umfang und Zweck der Verwendung

  } Risiko

  - des Standes der technischen Möglichkeiten
  - der wirtschaftlichen Vertretbarkeit

  } Kosten

- Um Angemessenheit zu beurteilen:
  - Risiko-Analyse
    - Wie quantifiziert man datenschutzrechtliche Risiken?
  - Kosten-Nutzen-Analyse
    - Kosten der Sicherheitsmaßnahmen vs. Höhe des Risikos

Verwaltungsstrafrechtliche Verantwortlichkeit für unzureichende Datensicherheit (2/2)

- Strafrahmen
  - Verwaltungsstrafen von bis zu EUR 10.000, wenn personenbezogene Daten nicht angemessen geschützt werden (§ 52 DSG 2000)
- Haftung
  - Geschäftsleitung oder gewerberechtlicher Geschäftsführer haftet für Verwaltungsstrafen – Gesellschaft haftet solidarisch (§ 9 VStG)
- Ausblick: Datenschutzgrundverordnung (Art 79 DS-GVO)
  - Strafe von bis zu
    - 100 Millionen EUR oder
    - 5% des weltweiten Jahresumsatzes des Unternehmens

    je nachdem, welcher der Beträge höher ist

Verwaltungsstrafen für Betreiber kritischer Infrastrukturen – Die NIS-Richtlinie der EU

- Ziel der Netzwerk- und Informationssicherheits-RL: Schutz kritischer Infrastrukturen
- Kontinuität der Dienste, die auf der IT beruhen, ist zu gewährleisten
  - → Infrastruktur-Sicherheit, keine Informationssicherheit
- Frühzeitige Umsetzung in Deutschland – und Österreich?
- Risiko-angemessene Maßnahmen erforderlich
  - Problem: Risiko-Analyse – wie bemisst man:
    - Ausfall der Bankomatdienste für 2 Tage
    - Eine Großstadt ohne Strom für 3 Tage
    - 100 Todesfälle durch Ausfall der medizinischen Versorgung

Verwaltungsstrafen für Betreiber kritischer Infrastrukturen – Die NIS-Richtlinie der EU

Welche Bereiche gehören zu den kritischen Infrastrukturen?

- Energie, insb.
  - Strom- und Gasversorger
  - Übertragungsnetzbetreiber (Strom), Erdöl-Fernleitungen und Erdöllager
  - Betreiber von Erdöl- und Erdgas-Produktions- und Behandlungsanlagen
- Verkehr
  - Eisenbahnen, Luftfahrtunternehmen, Flughäfen
  - Beförderungsunternehmen des Seeverkehrs, Häfen
  - Betreiber von Verkehrsmanagementsystemen & unterstützende Logistikdienste
- Banken: Kreditinstitute
- Börsen
- Gesundheit: Einrichtungen der medizinischen Versorgung

Schadenersatzpflicht bei Datenschutzverletzungen

- Bei schuldhafter Missachtung der Datensicherheitspflichten haftet ein Unternehmen (§ 33 DSG 2000)
  - für Vermögensschaden, der durch Sicherheitsverletzung entsteht
  - für immateriellen Schaden, wenn
    - Daten öffentlich zugänglich werden
    - zur Bloßstellung des Betroffenen geeignet (insb. bei sensiblen Daten)
- Unternehmen haftet auch für das Verschulden seiner Leute (§ 33 Abs 2)
- Unternehmen muss beweisen, dass es kein Verschulden trifft (§ 33 Abs 3)

Kosten einer verpflichtenden Breach-Notification

- Notifikationspflicht nach § 24 Abs 2a DSG 2000, wenn:
  - dem Unternehmen bekannt wird, dass personenbezogene Daten „systematisch und schwerwiegend“ unrechtmäßig verwendet wurden und
  - den Betroffenen Schaden droht
  - Ausnahme: Notifikation unverhältnismäßig zu drohendem Schaden
  - Notifikation in „geeigneter“ Form und „unverzüglich“
- Notifikationspflicht nach § 95a TKG 2003, wenn
  - DSB von jeder Verletzung der Sicherheit personenbez. Daten zu informieren
  - Betroffene, wenn anzunehmen ist, dass Privatsphäre beeinträchtigt
- Vertragliche Notifikationspflicht
  - wenn dem Vertragspartner Schaden droht
  - Unabhängig, ob „systematisch und schwerwiegend“
- Ausblick: Notifikationspflicht nach NIS-Richtlinie
  - gegenüber nationaler NIS-Behörde, wenn erhebliche Auswirkungen

Verlust der Patentfähigkeit von Erfindungen

- Erfindungen können nur dann als Patent angemeldet werden, wenn sie insb „neu“ iSd § 3 PatG sind.
  - Dh nicht zum Stand der Technik gehören, der aus allem besteht, was der Öffentlichkeit vor der Anmeldung zugänglich war.
  - Auch von Hacker/Konkurrent veröffentliche Informationen können Verlust der Neuheit bewirken.
  - Einzige mögliche Verteidigung des Anmelders: Beweis des Zusammenhangs zwischen Hacking & neuheitsschädlicher Veröffentlichung (§ 3 Abs 4 Z 1 PatG).

Schadenersatzpflicht gegenüber Kunden

- Weitgehende Haftungsausschlüsse in Verträgen üblich
- Allerdings: Übliche Geheimhaltungsklauseln sind Einfallstor für Haftung:
  - *Der Vertragspartner verpflichtet sich, vertrauliche Informationen nicht offenzulegen und die Offenlegung mit demselben Maß an Sorgfalt zu verhindern, wie für seine eigenen vertraulichen Informationen – ohne dabei ein angemessenes Maß an Sorgfalt zu unterschreiten.*
- Haftung für sämtliche Vermögensschäden des Vertragspartners einschließlich entgangener Gewinn, Reputationsschäden etc.

Wie können Risiken sinnvoll bewertet werden?

Herausforderungen der Risikobewertung

- Betriebswirtschaftliche & regulatorische Notwendigkeit
  - → Wie effektiv (risikomindernd) müssen „angemessene“ Sicherheitsmaßnahmen sein?
  - → Wieviel soll ein Unternehmen ausgeben, um das Risiko X zu mindern?
- Qualitative Risikobewertung
  - niedrig – mittel – hoch
- Quantitative Risikobewertung
  - X Euro
- Risiko ist Kombination von
  - Potentiellem Schaden
  - Eintrittswahrscheinlichkeit des Schadens

Qualitative Risikobewertung (1/3)

Sehr beliebt: Risiko-Matrizen

	Kleiner Schaden	Mittlerer Schaden	Hoher Schaden
Niedrige Wahrscheinlichkeit			
Mittlere Wahrscheinlichkeit			
Hohe Wahrschein-lichkeit			

Qualitative Risikobewertung (2/3)

Sehr beliebt: Risiko-Matrizen

	Kleiner Schaden	Mittlerer Schaden	Hoher Schaden
Niedrige Wahrscheinlichkeit	Niedrig	Niedrig	Mittel
Mittlere Wahrscheinlichkeit	Niedrig	Mittel	Hoch
Hohe Wahrschein-lichkeit	Mittel	Hoch	Hoch

Qualitative Risikobewertung (3/3)

- Probleme der qualitativen Risikobewertung
  - Überprüfbarkeit der Risikobewertung?
  - Objektivität der Aussage? Bedeutet „mittel“ für alle dasselbe?
  - Range-Compression

	Kl. Schaden (<100k)	100k < x < 1M	>1M
Niedrige Wahrscheinlichkeit (<15%)			X
15% < x < 50%			
>50%			

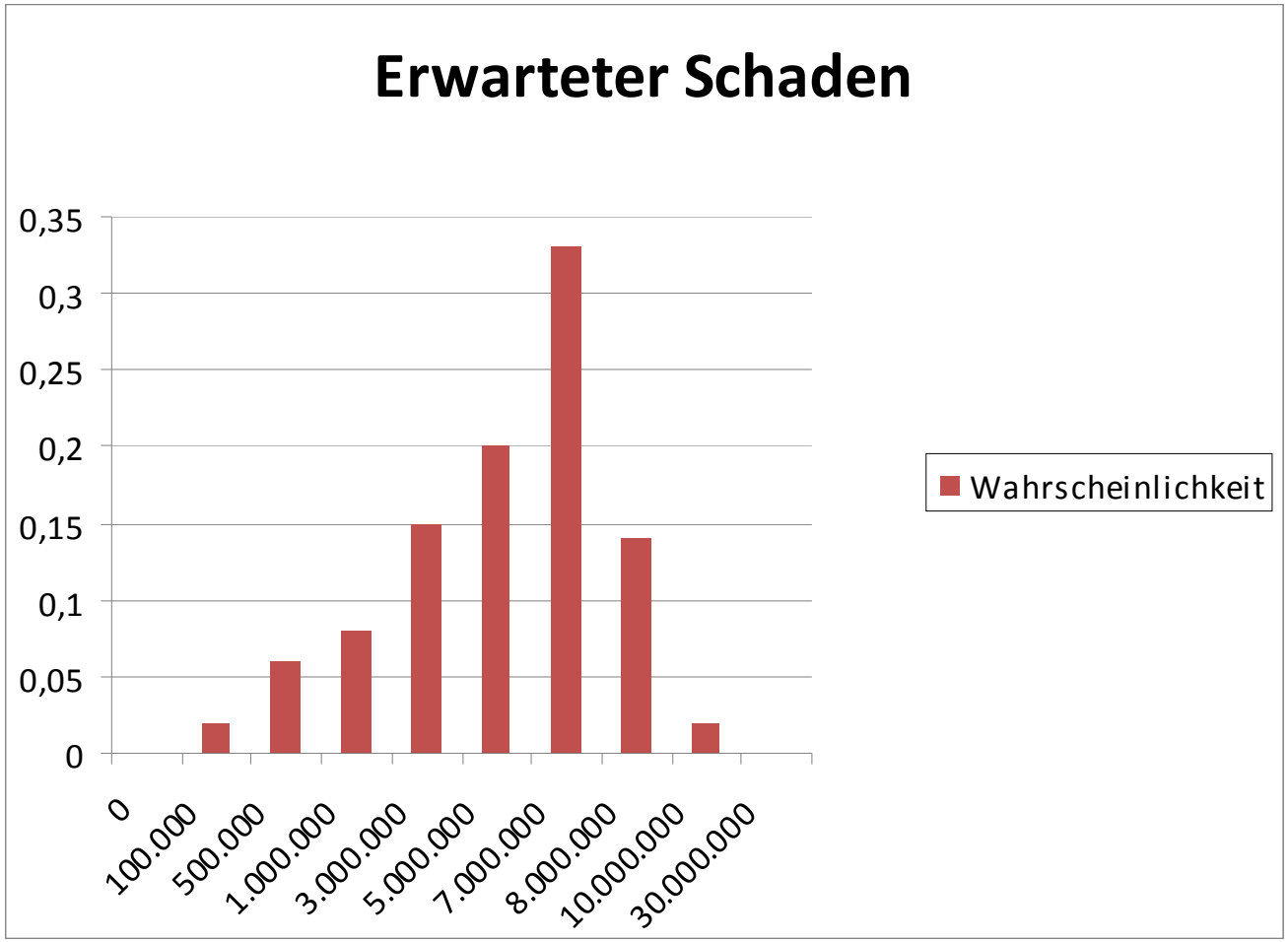
  - Risiko 1: Schaden v. € 100M, Wahrscheinlk. v. 1% → „mittel“ = 1M
  - Risiko 2: Schaden v. € 250M, Wahrscheinlk. v. 14% → „mittel“ = 35M

Quantitative Risikobewertung – Mathematische Ansätze

Risiko als Euro-Betrag: Annualized Loss Expectancy (ALE)

- ALE = Annualized Rate of Occurrence (ARO) * Single Loss Expectancy (SLE)
  - zB Risiko eines Festplattendefekts; zB: ARO = 0,1; SLE = € 100k
    → Wie viel für Backup pro Jahr ausgeben?
- Einwände gegen die Quantifizierung von ARO und SLE
  - Quantifizierung sei nicht möglich
    - Absolute Sicherheit ist nicht erforderlich!
  - Quantifizierung sei nicht ökonomisch oder setzt falsche Anreize
    - Unerwünschte Nebeneffekte großteils durch Messung der falschen Dinge
  - Quantifizierung sei nicht ethisch
    - Alle Ressourcen sind endlich; schlichte Notwendigkeit

Quantitative Risiko-bewertung – Modellierungsansätze (1/2)



Quantitative Risiko-bewertung – Modellierungsansätze (2/2)

Schaden	Wahrscheinlichkeit
0	0
100.000	2%
500.000	6%
1.000.000	8%
3.000.000	15%
5.000.000	20%
7.000.000	33%
8.000.000	14%
10.000.000	2%
30.000.000	0%

Möglichkeiten der Risiko-Behandlung

Grundsätzliche Möglichkeiten der Risikobehandlung

- Risiko-Vermeidung
  - Zero-Risk-Approach: Geschäftsprozess einstellen
- Risiko-Transfer
  - Übertragung des Risikos auf einen Dritten – Cybersecurity-Insurance
- Risiko-Minderung
  - Implementierung zusätzlicher Sicherheitsmaßnahmen & Zertifizierungen
- Risiko-Akzeptanz

Risiko-Transfer durch Cybersecurity-Insurance

- Marktentwicklungen
  - Kosten einer Sicherheitsverletzung können signifikant sein
    - Rechtliche Risiken
    - Wirtschaftliche Risiken (für die Geschäftsleitung haftbar sein kann)

    → Wachsende Anreize, Cybersecurity-Versicherungen abzuschließen
  - Versicherungsunternehmen bieten zunehmend Cybersecurity-Versicherungsprodukte an

Mögliche Bausteine für eine Cybersecurity-Versicherung

- Datenbeschädigung oder -verlust (Datenwiederherstellung, Forensik, Krisenkommunikation)
- Personal Data-Breach (Notifikationskosten, Verfahrenskosten, Verwaltungsstrafen, …)
- Haftung für Personal Data-Breach (Schadenersatzpflicht, Beratungs- und Vertretungskosten)
- Vertragshaftung (zB PCI-DSS oder Pönalen in Kundenverträgen)
- Sachschaden
- Betriebsunterbrechung (insb. entgangener Gewinn)
- Reputationsschaden
- Cyber-Epressung/Lösegeld

Tücken der Cybersecurity-Versicherung

- Gutes quantitatives Risk-Assessment als Vorbedingung
- Versicherungsschutz genau definieren
  - Schwachstellen in Standard-Software oft ausgenommen
    - „Class Breaks“ schwer versicherbar
    - Heartbleed, Shellshock, …
  - Outsourcing ausgenommen?
    - Daten auch versichert, wenn bei Dienstleister gespeichert?
  - Patentrecht ausgenommen?
    - Risiken insb. nach US-Recht schwer versicherbar

Rechtliche Bedeutung von Sicherheits-Zertifizierungen

- Minimierung des zivilrechtlichen Haftungsrisikos
  - OGH 20.08.1998, 10 Ob 212/98v: Ö-Normen bilden grds Haftungsmaßstab, da sie wiedergeben, was branchenüblich ist
  - Erleichterte Beweisführung, dass Sicherheitsverletzung nicht auf eigenes Verschulden zurückzuführen; z.B. § 33 Abs 3 DSG 2000
- Erleichterte Beweisführung, dass regulatorische Anforderungen erfüllt wurden
- Beurteilung, ob Dienstleister/Produkt die gesetzlichen Anforderungen erfüllt
  - Was sagt die Zertifizierung aus?

Notwendige Fragen zu jeder Zertifizierung

- Um welche Art der Zertifizierung handelt es sich?
  - Zertifizierung von Produkten, Prozessen oder Personen
- Wer führt die Prüfung & Zertifizierung durch?
  - Selbst-Zertifizierungen vs. Zertifizierungen durch Dritte
  - Unabhängigkeit des Dritten & negative Selektion
- Was wird zertifiziert?
  - Exakter Scope of Certification ist ausschlaggebend
- Wie wird zertifiziert?
- Wie lange ist eine Zertifizierung gültig?

Zertifizierung von Prozessen – ISO 27000

- Zertifizierung eines Information-Security-Management-Systems (ISMS) nach ISO 27001
  - ISMS ist
    - ein Management-System
    - allgemein
  - ISMS ist nicht
    - Regelung einzelner Sicherheitsmaßnahmen (keine Zertifizierung nach ISO 27002)
    - eine konkrete Handlungsanweisung
  - Welche Organisationseinheiten sind von der Zertifizierung umfasst?

Zertifizierungen von Produkten – Common Criteria (1/2)

- Grundlegende Herausforderungen
  - Komplexität moderner Produkte
  - Abhängigkeiten von anderen Produkten
  - Länge des Produktzyklus im Verhältnis zur Prüfungsdauer
- De-facto-Standard: Common Criteria (CC)
  - CC ist ein Prüf- und Zertifizierungs-Framework
  - CC selbst enthält keine Anforderungen an ein Produkt
  - Anwender: Spezifizieren ihre Sicherheitsanforderungen in einem Protection-Profile (PP)
  - Hersteller: Definiert ein Security-Target (ST) durch Verweis auf ein/mehrere PPs
  - Akkreditierte Prüfstelle (zB BSI): Prüft, ob Produkt dem ST entspricht
  - Prüftiefe: EAL1 bis EAL7

Zertifizierungen von Produkten – Common Criteria (2/2)

Wie sicher sind nach CC zertifizierte Produkte?

- Windows XP hatte zB eine EAL4+-Zertifizierung
- Hängt vom ST ab; im Fall von Windows:
  - „The TOE is applicable to networked or distributed environments only if the entire network operates under the same constraints and resides within a single management domain. There are no security requirements that address the need to trust external systems or the communications links to such systems.“

Baker & McKenzie denkt von Anfang an global. Seit der Gründung.
Internationalität liegt uns in den Genen.