KURATORIUM SICHERES ÖSTERREICH

Cyber Security Fitness Index Austria

Führungsinstrument zur Bewertung der unternehmerischen Sicherheitsvorsorge im Cyberspace

Eine Gemeinschaftsstudie von

REPUCO Unternehmensberatung GmbH
Borchert Consulting & Research AG
SBA Research GmbH
Institut für Produktionsmanagement, WU Wien
Institute for Information Management and Control, WU Wien

Wien, Januar 2015

1 Zusammenfassung

Zielsetzung

- Der Cyber Security Fitness Index Austria (CFI-A) entwickelt ein Kennzahlensystem, um die unternehmerische Cybersicherheitsvorsorge österreichischer Betreiber der kritischen Infrastruktur zu bewerten. Die daraus gewonnenen Erkenntnisse vermitteln wichtige Anhaltspunkte für die Weiterentwicklung des regulativen Rahmens, den die staatlichen Behörden definieren. Wird der CFI-A kontinuierlich genutzt, ist es auch möglich, die Wirksamkeit dieses regulativen Rahmens im Sinne der von den Unternehmen tatsächlich ergriffenen Maßnahmen zur Sicherheitsvorsorge im Cyberspace zu überprüfen.

Anforderungen an den CFI-A

- Der CFI-A schließt eine methodische Lücke, die sich aus der Tatsache ergibt, dass bislang allgemein akzeptierte, einfache, pragmatische und plausible Modelle fehlen, um den Reifegrad der Cybersicherheitsvorsorge in Unternehmen zu messen. Der CFI-A erfasst führungsrelevante Informationen, damit Unternehmen fundierte Entscheidungen zur Cybersicherheitsvorsorge treffen können.
- Zu diesem Zweck muss der CFI-A (1) für alle Betreiber der kritischen Infrastrukturen gleichermaßen anwendbar sein. Er muss (2) in geeigneter Weise das Cybersicherheitsniveau in allen relevanten Perspektiven abbilden und es gleichzeitig erlauben, (3) in aussagekräftiger Form zwischen den maßgeblichen Teildimensionen der Cybersicherheitsvorsorge zu differenzieren. Jede Teildimension soll (4) durch Indikatoren dargestellt werden, die mit Hilfe einheitlicher Messverfahren und unter Anwendung einheitlicher Skalen hinreichend beschrieben werden. Auf dieser Grundlage sollen (5) alle Teilbereiche anhand definierter Kriterien aggregierbar sein, um Aussagen auf der Ebene eines Gesamtindex und verschiedener Teilindices zu ermöglichen.

Dimensionen des CFI-A

- Der CFI-A basiert auf dem Ansatz der Balanced Scorecard (BSC). Hierbei handelt es sich um ein anerkanntes und weit verbreitetes Managementinstrument zur Messung, Dokumentation und Steuerung einer Organisation anhand eines Kennzahlensystems.
- Der CFI-A ist ein mehrdimensionales und kennzahlenbasiertes Führungsinstrument, das auf vier Dimensionen basiert:
  - Die Business Value-Dimension erfasst den der Cybersicherheitsvorsorge beigemessen Wert.

  - Die Dimension Security Process beschreibt die Effizienz und Effektivität der relevanten Prozesse, die ein Unternehmen im Bereich der Cybersicherheitsvorsorge etabliert hat.
  - Die Security Ambition umfasst alle strategischen und zukunftsgerichteten Bestrebungen, um das Niveau der Cybersicherheitsvorsorge eines Unternehmens aufrecht zu erhalten bzw. zu erhöhen.
  - Die Resilience-Perspektive beschreibt die Widerstandsfähigkeit eines Unternehmens im Hinblick auf die notwendige Verfügbarkeit der jeweiligen Servicelevel.
- Der CFI-A wurde in einem mehrstufigen Verfahren entwickelt und verdichtet. Er besteht insgesamt aus knapp 100 Indikatoren, die für die Indexbildung herangezogen werden. Der Fragebogen, der für die persönlichen Interviews mit 30 Experten aus verschiedenen kritischen Infrastruktursektoren genutzt wurde, enthält zudem auch deskriptive Begleitfragen in offener und teilstrukturierter Form.

Ergebnisse

- Die Anwendung des CFI-A macht deutlich, dass die unternehmerische Cybersicherheitsvorsorge in den untersuchten kritischen Infrastruktursektoren generell einen hohen Reifegrad erreicht hat.
- Insgesamt liegen die aggregierten Einzelwerte[1] sehr nahe beieinander. Trotzdem ist eine vorsichtige Trendaussage dahingehend möglich, dass großer Handlungsbedarf im Bereich des Business Value besteht, der mit einem Wert von 2.19 auf Rang 3 der vier bewerteten Teildimensionen liegt. Diese Erkenntnis ist von zentraler Bedeutung, macht sie doch deutlich, dass die Unternehmen erst ansatzweise über die Führungsinformationen für Cybersicherheit verfügen, die sie für wirklich sinnvolle Entscheidungen benötigen.
- Zudem gibt es ein gewisses Spannungsfeld zwischen den Werten für die Dimensionen Resilience (1.94) und Security Process (2.21), deren Ursachen allerdings schwierig zu erklären sind. Wenn die Resilience das – zeitlich versetzte – Ergebnis der Bemühungen beschreibt, auf die der Security Process ausgerichtet ist, dann deutet der schlechtere Wert für die Prozessdimension darauf hin, dass sich die Resilience künftig verschlechtern könnte.
- Die Restulate machen auch deutlich, dass es keinen Infrastruktursektor gibt, der in allen vier Dimensionen als Leitsektor mit dem besten Wert abschneidet.
  Der IKT-Sektor kommt diesem Idealtyp jedoch mit dem Spitzenwert in drei Sektoren sehr nahe.[2] Lediglich beim Business Value schliesst die Finanzwirtschaft 0.03 Indexpunkte besser ab als die IKT-Branche. Die Energie- und Finanzwirtschaft lösen sich mit Ausnahmen des Business Value und der Resilience in beiden anderen Dimensionen auf den Plätzen 2 und 3 ab. Auf den Plätzen 4 und 5 folgen in der Regel der Transport- und der Gesundheitssektor in abwechselnder Reihenfolge.

[1] Alle Variablen, die in den Index einfließen wurden über eine einheitliche fünfstufige Likert-Skala gemessen, die das österreichische Schulnoten implementiert und somit intervallskalierte Antworten zwischen 1 (sehr gut) und 5 (nicht genügend) erlaubte. Die Schulnotenskala ermöglicht ein einfaches und einheitliches Verständnis der Skala unter allen Teilnehmer/innen.“ (S. 25)

[2] Die Ergebnisse für die Kategorie „Andere“ werden bei dieser Betrachtung ausgeklammert.

- Handlungsbedarf[3] besteht insbesondere bei
  - prozess- und organisationsübergreifenden Vernetzungsapspekten wie der Durchführung von Business Impact-Analysen sowie der Ermittlung der Abhängigkeiten zwischen kritischen Prozessen bzw. Servies;
  - der Vermittlung der Inhalte der unternehmerischen Cybersicherheitsvorsorge vor allem gegenüber Vertragspartnern und dem Senior Management;
  - dem regelmässigen Test von Notfallplänen in Übungen sowie
  - der Entwicklung geeigneter Führungskenngrössen, die qualifizierte Aussagen über den Nutzen und die Kosten der Maßnahmen im Bereich der Cybersicherheitsvorsorge erlauben.
- In Ergänzung der persönlichen Interviews zum CFI-A wurde im Rahmen des Studienprojekts auch der Fragebogen für einen KMU Cyber Security Monitor erarbeitet. Damit befragte das IFES – Institute für empirische Sozialforschung zwischen dem 26. November und 18. Dezember 2014 auf Basis telefonischer Interviews insgesamt 478 Mittelständler zu Fragen der IT-Nutzung, der Cybergefährdung und der Cybersicherheitsvorsorge in ganz Österreich. Aus den Ergebnissen:
  - SPAM und Schadsoftware sind die beiden Risikokategorien, von denen KMU im Alltag am häufigsten betrofen sind. Datenmanipulation und Datendiebstahl sind nach den Antworten von geringerer Bedeutung. Das ist vorsichtig zu interpretieren, denn oftmals ist den Angegriffenen gar nicht bewusst, dass sie Opfer entsprechender Taten waren, so dass Manipulation und Diebstahl nicht oder nur mit erheblicher zeitlicher Verzögerung erkannt werden.
  - Die Cybersicherheitsmaßnahmen sind klassich auf Virenschutz, Spamfilter und Firewall ausgerichtet. Maßnahmen wie die Netzwerküberwachung und das Netzwerkmonitoring werden dagegen erst vereinzelt umgesetzt.
  - Im Mittel stehen den Unternehmen gut 15 % des IT-Budgets für die Cybersicherheit zur Verfügung. Dieser Anteil hat sich im vergangenen Jahr bei 65 % der Befragten nicht verändert, und 64 % gehen davon aus, dass sich dieser Anteil auch im kommenden Jahr nicht verändern wird.
  - 40 % der Befragten unterhalten ihre IT-Systeme selbst. 34 % greifen auf externe Unterstützung zurück. Interessant ist, dass der Rückgriff auf Outsourcinglösungen mit der Grösse der Unternehmen deutlich abnimmt.
  - Wenn sich Mittelständler zu Fragen der Cybersicherheit informieren, nutzen 40 % das Internet als Informationsquelle, 36 % greifen auf die Unterstützung professioneller IT-Dienstleister zurück. Die Informationsangebot der Verbände werden kaum genutzt

[3] Handlungsbedarf wurde definiert als Fragestellung, die von mindestens fünf Befragten entweder mit der Note 4 oder der Note 5 bewertet wurde.

Empfehlungen

- Die Studie und die Anwendung des CFI-A im Rahmen von 30 persönlichen Interviews bestätigen die Validität des gewählten Ansatzes, um den Index zu entwickeln. Dieser ist damit als grundlegendes Führungsinstrument für die unternehmerische Sicherheitsvorsorge im Cyberspace zu verstehen.
- Für die Zukunft wird angeregt:
  - Die Datengrundlage des CFI-A durch zusätzliche Befragungen auszubauen und zu verstetigen; gleichzeitig sollte der CFI-A in ausgewählten methodischen Aspekten weiterentwickelt werden.
  - Gemeinsam mit ausgewählten Unternehmen sollte das Kuratorium Sicheres Österreich (KSÖ) Vorschläge zu spezifischen Kennzahlen für den Bereich der Cybersicherheit erarbeiten. Zudem sollten das Bundeskanzleramt und das KSÖ gemeinsam Impulse setzen, um Analyseinstrumente zur Bewertung unternehmensübergreifender Abhängigkeiten (z.B. Business Impact-Analysen) weiterzuentwickeln.
  - Noch fehlt ein Verständnis dafür, welches die genauen Konsequenzen sind, die sich aus dem Industrie 4.0-Paradigma für die Infrastrukturbetreiber und für die staatlichen Sicherheitsbehörden ergeben. Der Rechts-Technologie-Dialog, den das KSÖ 2015 führen wird, sollte genutzt werden, um diesen Aspekt vertiefend zu diskutieren. Die gewonnenen Erkenntnisse sollten in die Arbeit des geplanten Cybersicherheitsgesetz einfließen. Zudem wird angeregt, den Informationsaustausch zu diesem Aspekt auch im DACH-Kontext zu führen.
  - Maßnahmen zur Stärkung der Awareness im Rahmen der Cybersicherheitsvorsorge sind gezielt auf ihre Wirksamkeit zu überprüfen. Bundeskanzleramt, Bundesministerium für Inneres, die WKO, das KSÖ und relevante Verbände sollten hierzu eine Studie in Auftrag geben.
  - Die gesamtstaatliche Steuerungsgruppe zur Cybersicherheit sollte in Zusammenarbeit mit der Wirtschaft erörtern, welche Anreize erforderlich sind, um Notfallkonzepte im Rahmen unternehmerischer bzw. staatlicher Vorsorgeübungen regelmäßiger zu validieren.