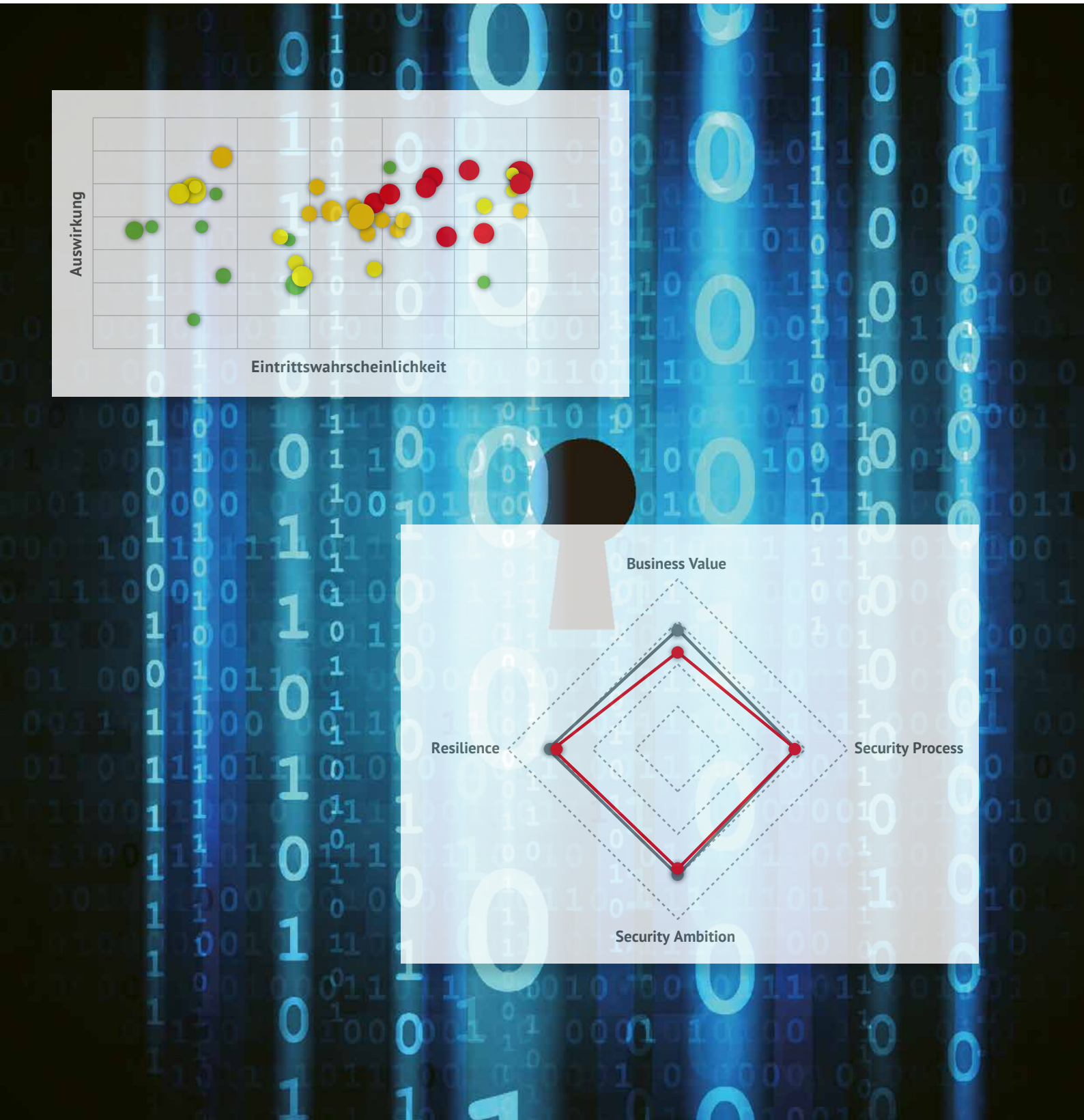
CYBER-RISIKEN ÖSTERREICH 2016

Cyber-Risikomatrix und Cyber-Security-Fitness-Index:
Bewertung der österreichischen Cyber-Risiko-Landschaft

KURATORIUM SICHERES ÖSTERREICH



Vorwort

»Der Cyber Raum und die Sicherheit der Menschen im Cyber Raum sind einer Vielzahl von Risiken und Bedrohungen ausgesetzt. (...) Moderne Cyber-Sicherheitspolitik ist ein Querschnittsthema, das in vielen Lebens- und Politikbereichen mitgedacht werden muss. Sie muss umfassend und integriert angelegt, aktiv gestaltet und solidarisch umgesetzt werden«
Österreichische Strategie für Cyber-Sicherheit, 2013, S. 6 f

Durch die rasch fortschreitende Digitalisierung aller Lebensbereiche wird die Sicherheit der digitalen Infrastrukturen und Dienstleistungen zu einem kritischen Thema. Um die Diskussion über sinnvolle und notwendige Maßnahmen zur Herstellung von *Cyber-Sicherheit* zielgerichtet gestalten zu können, ist das Wissen um die jeweils aktuellen Risiken und den Grad der Vorbereitung auf das Eintreten dieser Risiken essentiell.

Das Kuratorium Sicheres Österreich (KSÖ) führt deshalb seit 2011 in Partnerschaft mit dem Bundesministerium für Inneres (BMI) eine Cybersecurity Initiative durch, in deren Rahmen dieses Wissen aufgebaut und laufend aktualisiert wird. Die dabei 2011 erstellte Cyber-Risikomatrix war über Jahre hinweg maßgeblicher Anhaltspunkt zur Evaluierung der Cyber-Risikolandschaft Österreichs. Jedoch hat sich seit ihrer Erstellung 2011 die Bedrohungslage wesentlich verändert, wodurch eine Aktualisierung notwendig wurde.

Ergänzend zu dieser Risikomatrix dokumentiert der vom KSÖ im Jahr 2014 erstmals durchgeführte Cyber-Security-Fitness-Index Austria den Grad der Vorbereitungen von ausgewählten Unternehmen in Bezug auf ihre Maßnahmen im Bereich Cyber-Sicherheit. Mit seiner Aktualisierung im Jahr 2016 werden positive und negative Trends in diesem Bereich aufgezeigt.

Die Ergebnisse dieser beiden Arbeiten wurden in der Studie *Cyberbericht 2016* zusammengefasst.

Der Bericht stellt die Risiken, denen sich Österreich im Cyber-Bereich gegenüber sieht, und den Grad der Vorbereitung von Unternehmen auf diese Risiken in Relation zueinander und erlaubt damit eine detaillierte Analyse der aktuellen Lage. Er liefert dadurch einen wertvollen Beitrag zu der in der Österreichischen Sicherheitsstrategie (ÖSS) angesprochenen gesamtstaatlichen Risikobetrachtung indem er für den Cyber-Bereich einen Überblick schafft, auf Basis dessen zukünftige Strategien entwickelt werden können.

Dieser Folder soll Ihnen eine Übersicht über die Cybersecurity Risikomatrix 2016 und den Cyber-Security-Fitness-Index Austria 2016 geben und die wichtigsten Ergebnisse zusammenfassen. Für eine detaillierte Analyse steht Ihnen der *Cyberbericht 2016* auf unserer Website zu Verfügung (*www.kuratorium-sicheres-oesterreich.at*).

Wir machen mit diesen Ergebnissen einen weiteren wichtigen Schritt auf unserem Weg im Rahmen der Cybersecurity Initiative. Wie auch der Rechts- und Technologiedialog zum Cybersicherheitsgesetz, die Cybersecurity Planspiele und viele weitere unserer Projekte soll Ihnen dieser Bericht dabei helfen, die wichtigen und richtigen Maßnahmen zu treffen damit Österreich cybersicherer wird. Ich danke Ihnen für Ihr Interesse und Ihre Unterstützung.

Mag. Erwin Hameseder
Präsident Kuratorium Sicheres Österreich

Wir danken dem KSÖ Cybersecurity Forum für die Unterstützung.

Ergebnisse

Die Ergebnisse der **Cyber-Risikomatrix 2016** zeigen sieben besonders relevante Risiken auf:

Die wichtigsten Risiken der Cyber-Risikomatrix 2016

Abhängigkeit von ausländischen (Sicherheits-) Technologien

Cyberspionage

Fehlende Definition der Verantwortlichkeit bei Softwarefehlern

Kritische und weitreichende Schwachstellen in grundlegenden Technologien

Mangelndes Sicherheitsbewusstsein

Ungenügender Anreiz für Sicherheitsinvestitionen

Unsichere IoT Systeme

In der Spalte rechts sehen Sie die Veränderung im Vergleich zur Cybersecurity Risikomatrix 2011: *Das Plus* bezeichnet Risiken, die 2011 noch nicht in der Risikomatrix enthalten waren. *Die Pfeile* bezeichnen die Veränderung der Risikoeinschätzung bei Risiken, die bereits 2011 bewertet wurden.

Die Untersuchung der einzelnen Risiken und ihre Veränderung im Vergleich zur Cyber-Risikomatrix 2011 reflektieren zum Großteil die Makro-Trends im Cyber-Bereich: Cybercrime, Spionage, Terrorismus, staatliche Aktivitäten, zunehmende Vernetzung und steigende Komplexität wirken sich alle auf die Risikolage insofern aus, als dass die damit verbunden Risiken als hoch oder höher als 2011 einzustufen sind bzw. erstmalig erfasst wurden.

Die zusätzliche Bewertung der Preparedness ermöglichte die Einteilung in 4 Cluster und damit eine eindeutigere Aussage darüber, welchen Risiken bereits durch Maßnahmen begegnet wurde. Damit wurde allerdings auch die unmittelbare Vergleichbarkeit mit der Risikomatrix 2011 reduziert.

Der **Cyber-Security-Fitness-Index Austria 2016** stellt den österreichischen Unternehmen insgesamt ein gutes Zeugnis (Schulnote 2) aus. Dennoch zeigt er insbesondere im Vergleich zu 2014 auf, dass weiterhin in vielen Unternehmen Kennzahlensysteme fehlen um Managemententscheidungen unterstützen zu können. Auf Seite des Managements wird wiederum der Bedarf nach einer intensiveren Beschäftigung mit dem Risikomanagement und der Sicherheit eigener Softwareentwicklung aufgezeigt. Die derzeitigen Maßnahmen im Bereich Bewusstseins- und Weiterbildung sollten nach Aussage der Kennzahlen aufrechterhalten werden.

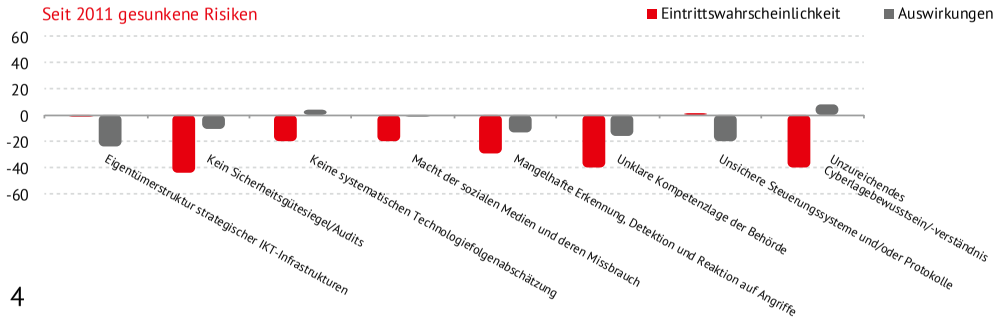
Der Vergleich mit 2014 zeigt damit aber auch, dass keine wesentlichen Verbesserungen eingetreten sind: die Ambitionen beschränken sich auf die Optimierung vorhandener Prozesse, ihre Resilienz stagniert und dynamische Innovation ist nicht absehbar. Dies steht im Widerspruch zu nachweislich getätigten Investitionen und deutet damit darauf hin, dass gleichzeitig mit den Investitionen die Bedrohungslage und damit das Aufgabenspektrum seit 2014 stark angestiegen sind.

Trotz der nur geringen Veränderung in den Kennzahlen lässt sich zeigen, dass die Ergebnisse in der Dimension *Resilience* besser sind als die der Dimension *Security Process*. Sollten die *Security Processes* aber in Zukunft nicht gestärkt werden, wird auch die *Resilience* weiter absinken. Die *Security Ambition* ist wiederum auf die Größenordnung der *Security Processes* abgesunken und deutet damit darauf hin, dass auch hier in Zukunft ohne entschlossene Gegenmaßnahmen keine Verbesserungen zu erwarten sind. Am deutlichsten wird aber das Fehlen von Kennzahlen zur Erfassung von Cyber-Sicherheit aufgezeigt. Dies äußert sich durch einen relativ geringen Wert für die Dimension *Business Value* und zeigt ein wesentliches Handlungsfeld für das Management auf.

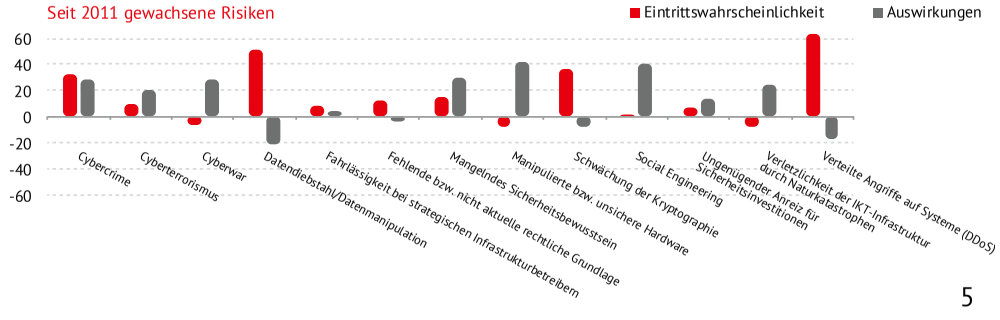
Cyber-Risikomatrix 2016

Cyber-Risikomatrix 2016

Seit 2011 gesunkene Risiken



Seit 2011 gewachsene Risiken



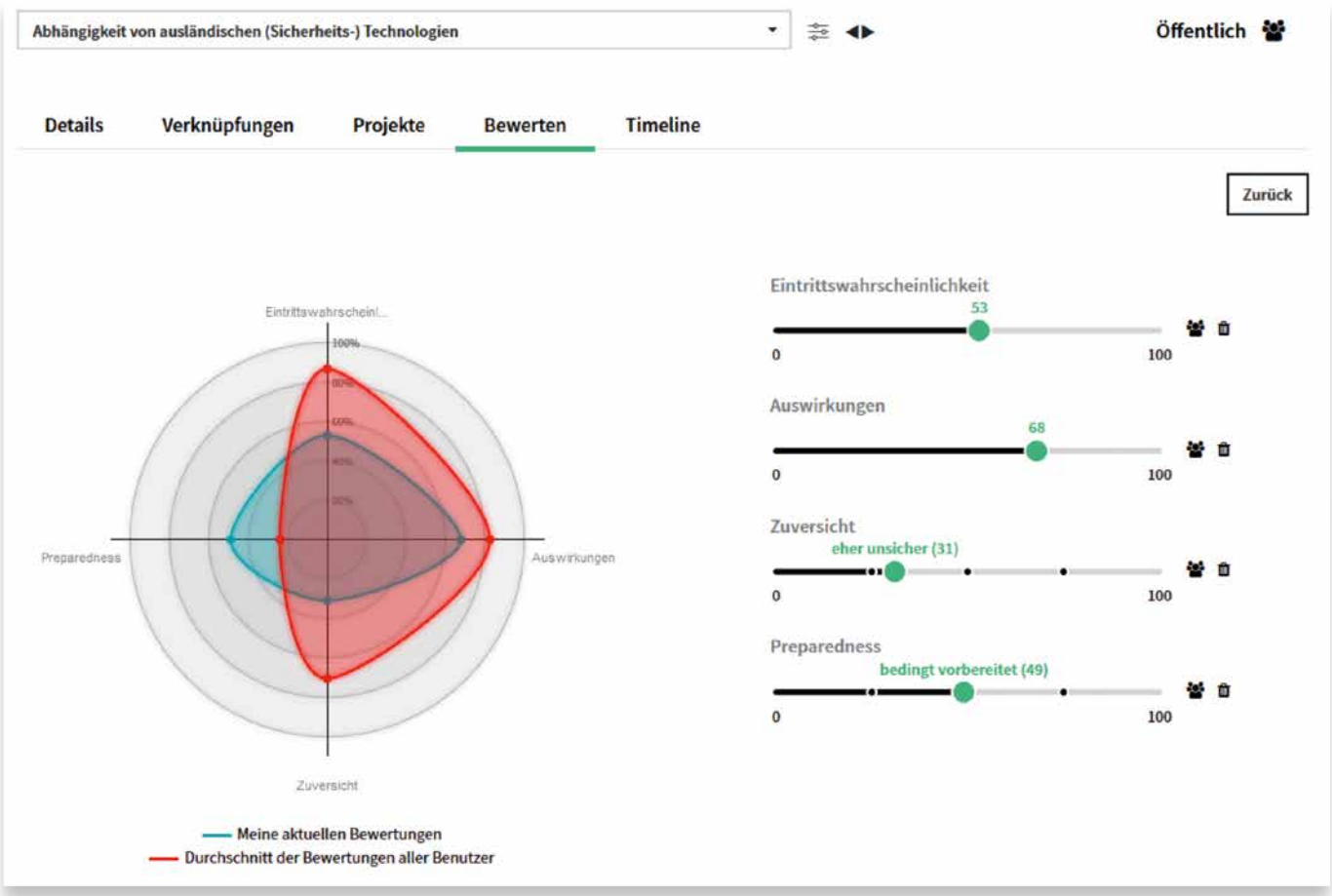
Cyber-Risikomatrix 2016

Die KSÖ Cyber-Risikomatrix 2016 ist eine gesamtstaatliche Sicht auf die Cyber-Risikolage aus Sicht von Experten unterschiedlicher Sektoren. Dazu wurden die Teilnehmer gebeten, die Cyber-Risiken für Österreich zu bewerten und die Antworten wurden zu einer Gesamtrisikolage aggregiert. Im Gegensatz zu einer klassischen Risikomatrix wurden zu jedem Risiko vier Dimensionen abgefragt:

- Die **Eintrittswahrscheinlichkeit** des jeweiligen Risikos
- Die **Auswirkungen** des jeweiligen Risikos
- Die **Preparedness**, also der Grad der Fähigkeit des Sektors, dem Risiko adäquat begegnen zu können
- Die **Zuversicht** des Teilnehmers, korrekte Aussage über das betreffende Risiko zu können.

Zur Ermittlung eines Expertenkonsenses und zur Erstellung der Risikomatrix wurde das Online-Tool *Foresight Cockpit* eingesetzt, das eine Befragung und Bewertung auf granularer Ebene ermöglichte.

Benutzeroberfläche Foresight Cockpit

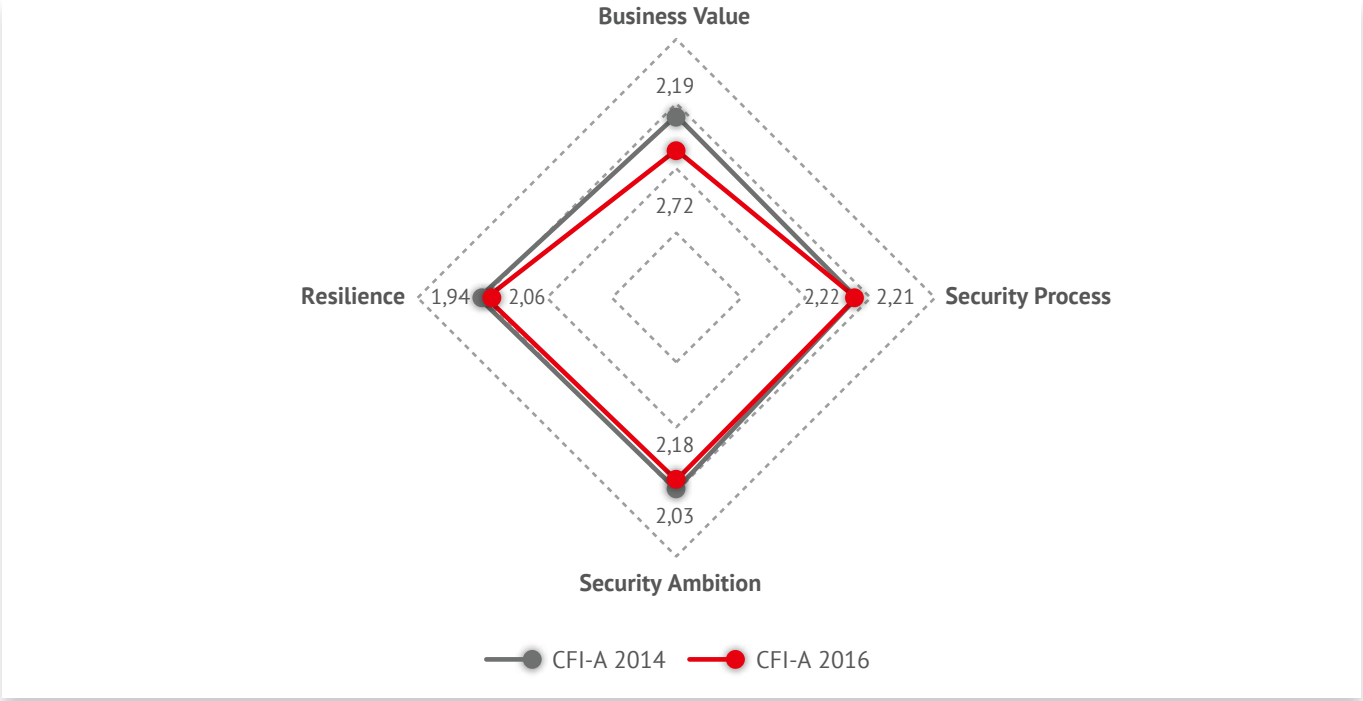


Die Eckdaten der Befragung:

- Ermittlung von 40 Risiken durch Expertenworkshops
- Online-Konsultationsverfahren mittels Foresight Cockpit:
  - Bewertung von vier Dimensionen auf einer Skala von 1-100 je Risiko durch Experten
  - Berechnung von Durchschnittswerten
  - Durch die Dimension Zuversicht konnten sehr starke Trendabweichungen erkannt und Risiken differenzierter bewertet werden
- Positionierung der Risiken in der Matrix aufgrund von Durchschnittswerten
- Kategorisierung der Risiken durch Expertenkonsens in vier Cluster:
  - Ermittlung der Risikozahl: Risikozahl = Auswirkungen x Eintrittswahrscheinlichkeit
  - Festlegung von Thresholds durch Expertenkonsens bei Risikozahl und Preparedness
  - Kombination der beiden Thresholds: endgültiger Cluster der Risiken richtet sich nach dem niedrigeren Threshold bei Risikozahl und Preparedness
  - Cluster I: sehr hohes Risiko (rot) – Cluster IV: geringes Risiko (grün)

Der Cyber-Security-Fitness-Index Austria baut auf einem Kennzahlensystem auf, mit dessen Hilfe die unternehmerische Cyber-Sicherheitsvorsorge in Österreich erfasst und bewertet werden kann. Ziel des Index ist es, eine rasche Beurteilung des Status und der Veränderungen der Cyber-Security-Anstrengungen von Organisationen zu ermöglichen und sowohl eine aggregierte Sicht als auch eine Detailanalyse zu erlauben.

Cyber-Security-Fitness-Index Austria 2016 im Vergleich zu 2012



Der Cyber-Security-Fitness-Index Austria basiert auf dem Ansatz der *Balanced Score Card* und weist vier Hauptdimensionen auf, die den sicherheitspolitischen Kontext der Studie berücksichtigen:

- Die Dimension **Business Value** erfasst den Mehrwert für die eigene Organisation, der der Cyber-Sicherheitsvorsorge beigemessen wird.
- Die Dimension **Security Process** beschreibt die Effizienz und Effektivität der relevanten Prozesse, die ein Unternehmen im Bereich der Cyber-Sicherheitsvorsorge bereits implementiert hat.
- Die Dimension **Security Ambition** umfasst alle strategischen und zukunftsgerichteten Bestrebungen, um das Niveau der Cyber-Sicherheitsvorsorge eines Unternehmens aufrechtzuerhalten bzw. zu erhöhen.
- Die Dimension **Resilience-Perspektive** beschreibt die Widerstandsfähigkeit eines Unternehmens im Hinblick auf die notwendige Verfügbarkeit der jeweiligen Servicelevel.

Die Eckdaten der Befragung:

- Ermittlung von 121 Indikatoren und 47 Begleitinformationspunkte durch Expertenbefragung
- Durchführung von persönlichen Interviews mit Experten aus 36 ausgewählten Unternehmen (vor allem Betreiber kritischer Infrastrukturen)
- Aggregation der 121 Indikatoren zu 22 Sub-Dimensionen
- Zusammenführung der 22 Sub-Dimensionen zu vier Haupt-Dimensionen

Durch die Aggregation der 121 Indikatoren zu 22 Sub-Dimensionen ist eine sehr detaillierte Auswertung der Lage der Unternehmen möglich. Den Unternehmen kann damit in sehr feingranularer Weise ein Vergleich zur gesamtstaatlichen Sicht und zu ihrer Positionierung im Vergleich zu anderen Unternehmen ihres Sektors gegeben werden. Die vier Haupt-Dimensionen sollen wiederum der strategischen Führungsebene als Werkzeug zur raschen Beurteilung von Trends dienen.

Vergleich der Cyber-Risikomatrix 2016 und des Cyber-Security-Fitness Index Austria 2016

Es existiert eine Korrelation zwischen den wichtigsten Risiken der Cyber-Risikomatrix 2016 und denjenigen Bereichen, in denen der Cyber-Security-Fitness Index Austria 2016 den größten Handlungsbedarf verortet. Wo es um die Cyber-Security-Fitness heimischer Unternehmen am schlechtesten bestellt ist, sind auch die Risiken am größten.

Korrelation aufgezeigter Problemfelder

Risiko in der Cyber-Risikomatrix	Schlechte Bewertungen beim Cyber-Security-Fitness-Index Austria
• Abhängigkeit von ausländischen (Sicherheits-) Technologien • Kritischen Schwachstellen in grundlegenden Technologien/Protokollen	• Sub-Dimension Sichere Softwareentwicklung
• Mangelhafte Erkennung, Detektion und Reaktion auf Angriffe	• Sub-Dimension Risikomanagement
• Industrie 4.0 • Unsichere IoT-Systeme	• Sub-Dimension Awareness, Training und Fortbildung
• Ungenügender Anreiz für Sicherheitsinvestitionen	• Dimension Business Value bzw. Sub-Dimension Metriken und Kennzahlen

Aufbauend auf diesen Ergebnissen lassen sich die folgenden Maßnahmenempfehlungen ableiten:

To Do's:

- Strategische Schwerpunkte an geänderte Risiken anpassen
- Die Österreichische Strategie für Cyber Sicherheit aktualisieren
- Den heimischen Cyber-Sicherheits-(Software)-Sektor durch die Implementierung eines Cyber-Sicherheitsclusters stärken
- Marktanreize im Cyber-Sicherheitssektor schaffen
- Fokussierung des Arbeitsmarktes auf Ausbildung von Cyber-Sicherheitsexperten
- Zur Lösung der Haftungsfrage bei Softwarefehlern in rechtswissenschaftliche Forschung investieren
- Die Geschwindigkeit regulatorischer Prozesse an die technischen Veränderungen anpassen
- Bereits vorhandene rechtliche Rahmenbedingungen effektiver durchsetzen
- Betriebswirtschaftliche Kennzahlen zur Steuerung von Cyber-Sicherheitsmaßnahmen entwickeln
- Fokus auf Risiko- und Business Continuity-Management, sichere Softwareentwicklung und Awareness legen
- Notfalltests öfter durchführen
- Eigene Softwareentwicklung vorantreiben

Impressum

Kuratorium Sicheres Österreich
Kärntner Ring 5-7
A-1010 Wien
Generalsekretär Dr. Alexander Janda
ZVR-Zahl: 444913001
https://kuratorium-sicheres-oesterreich.at/
office@kuratorium-sicheres-oesterreich.at