MEDIENINFORMATION

Bonn, 24. Juni 2020

Erster Bericht des Weisenrats für Cyber-Sicherheit veröffentlicht

- Konkrete Empfehlungen an Politik und Wirtschaft für mehr Sicherheit bei der Digitalen Transformation
- Erstellt von sechs unabhängigen Professorinnen und Professoren / führenden Experten im Bereich der Cyber-Sicherheit
- Beitrag zur Immunisierung der Gesellschaft gegen Cyber-Attacken

---

Der Weisenrat für Cyber-Sicherheit hat heute seinen ersten Bericht zu drängenden Fragen der digitalen Sicherheit veröffentlicht und diesen der Bundesregierung vorgelegt.
Das Cyber Security Cluster Bonn e.V. hat den unabhängigen Weisenrat für Cyber-Sicherheit 2019 ins Leben gerufen. Er besteht aus sechs renommierten Professorinnen und Professoren aus den wichtigsten Exzellenz-Clustern in Deutschland (siehe Anlage 1).

Mit der Veröffentlichung des ersten Berichts dieses Weisenrats für Cyber-Sicherheit sind acht Handlungsempfehlungen verbunden, die als Entscheidungshilfe für die Gestaltung der politischen und gesetzlichen Rahmenbedingungen verstanden werden sollen.

“Mit dem Bericht des Weisenrats für Cyber-Sicherheit wollen wir als Cluster unseren Beitrag zur Immunisierung der Gesellschaft gegen Cyber-Attacken leisten“, so Dirk Backofen, Vorstandsvorsitzender des Cyber Security Clusters Bonn e.V.

Ähnlich wie der Bericht der “Wirtschaftsweisen“, also der Bericht des Sachverständigenrats zur Begutachtung der gesamtwirtschaftlichen Entwicklung, wird

das Cyber Security Cluster Bonn e.V. künftig jährlich einen Bericht des Weisenrats für Cyber-Sicherheit vorlegen und Politik und Wirtschaft so mit aktuellen Impulsen zum Ausbau des Standort Deutschlands im Bereich Cyber-Sicherheit versorgen.

Handlungs-Empfehlungen des Weisenrats für Cyber-Sicherheit

Acht konkrete Empfehlungen sollen helfen, den Grundstein für ein Cyber-resilientes Deutschland zu legen:

- Technologie muss sich dem Menschen anpassen, um ihn zu entlasten und zu schützen
- Hersteller müssen sich zu regelmäßigen Schwachstellentests und Sicherheitsupdates verpflichten
- Digitale Prozesse und Infrastrukturen müssen angriffsresilienter werden
- Technologische Souveränität muss erhöht und bewahrt werden
- Digitale Infrastrukturen in smarten Städten müssen jederzeit, verfügbar, verständlich und beherrschbar bleiben
- KI-Systeme müssen transparent und zertifizierbar sein
- Langlebige Produkte müssen kryptoagil gestaltet werden
- Der Schutz der Demokratie muss online verstärkt werden

“Wir müssen heute in den Cyber-Sicherheits-Architekturen die Voraussetzungen für ein ständiges Dazulernen der Systeme schaffen. Wir empfehlen für IT-Lösungen, die eine lange Lebenszeit haben können, dass verwendete Krypto-Algorithmen ausgetauscht oder vorhandene Hardwarekomponenten neu programmiert werden können. Nur so können wir agil auf neue technische Herausforderungen reagieren und die Voraussetzungen für eine resiliente Cyber-Sicherheit schaffen“, so Frau Prof. Dr. Claudia Eckert, Leiterin des Fraunhofer AISEC-Instituts München und Leiterin des Lehrstuhls für Sicherheit in der Informationstechnik an der TU München.

“Starke Passwörter, die über einen langen Zeitraum nicht gewechselt werden müssen, sind schwachen Passwörtern mit einem häufigen Passwortwechsel

vorzuziehen. Um sich pro Dienst unterschiedliche Passwörter merken zu können, ist es empfehlenswert, sichere Passwortmanager zu nutzen. Zwei-Faktor-Authentisierung ist ebenfalls empfehlenswert, insbesondere bei wichtigen Applikationen, wobei bei allen Ansätzen immer auch auf die Einfachheit der Nutzung geachtet werden muss!“, das fordert Prof. Dr. Matthew Smith, Professor für Usable Security and Privacy an der Universität Bonn und Leiter der Abteilung „Usable Security and Privacy“ am Fraunhofer FKIE.

“Politik und Wirtschaft müssen die Rahmenbedingungen schaffen, um die technologische Souveränität im Cyber-Raum gestalten zu können. Wir müssen das ‘IT-Security made in Germany‘ zu einem anerkannten Qualitätssiegel machen“, sagt Prof. Dr. Norbert Pohlmann, Informatikprofessor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT.

Bericht des Weisenrats für Cyber-Sicherheit ist ein neuer Meilenstein für das Cyber Security Cluster Bonn e.V.

Mit der Veröffentlichung des ersten Berichtes des Weisenrats für Cyber-Sicherheit setzt das Cluster seine gesetzte Programmatik wie geplant in die Tat um. “Ich freue mich, dass alle Mitglieder und Partner im Cyber Security Cluster Bonn e.V. durch ihre engagierte Zusammenarbeit so starke und wichtige Impulse für die digitale Souveränität unserer Gesellschaft erarbeitet haben. Besonders freut es mich, dass mit dieser Initiative auch die verstärkte Zusammenarbeit mit den anderen Cyber Security Clustern in Deutschland gelungen ist“, sagt Ashok Sridharan, Oberbürgermeister der Stadt Bonn.

Warum brauchen wir einen Weisenrat für Cyber-Sicherheit ?

Sicherheit, Vertrauen, Verlässlichkeit und digitale Souveränität sind die Voraussetzungen für eine positive Gestaltung der Digitalisierung in unserer Demokratie. Nur über eine etablierte und gelebte Cyber-Sicherheit in allen Bereichen der Gesellschaft schaffen wir Vertrauen und Akzeptanz für digitale Lösungen.

Unternehmen und Politik stehen dabei vor großen Herausforderungen. Zwei Ansätze können hier aus Sicht des Cyber Security Clusters Bonn unterstützen: Zum einen praxisorientierte Programme, die das Know-How zum Thema Cyber-Sicherheit zu den Entscheidern in Unternehmen und Politik bringen. Zum anderen aber auch unabhängige Empfehlungen der Wissenschaft, auf die die deutsche Politik und Wirtschaft zurückgreifen können. Genau dieser Ansatz wird mit dem Weisenrat für Cyber-Sicherheit in die Tat umgesetzt.

Der Bericht des Weisenrats für Cyber-Sicherheit ist ab sofort frei zugänglich auf der Webseite des Cyber Security Cluster Bonn e.V. verfügbar.

Über das Cluster:
Das Cyber Security Cluster Bonn e.V. vereint mit mehr als 100 Mitgliedern und Partnern alle Security-relevanten Einrichtungen aus Wissenschaft, Wirtschaft und dem öffentlichen Sektor am Standort Bonn. So sind zum Beispiel das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Kommando Cyber- und Informationsraum der Bundeswehr, die Universität Bonn, die Hochschule Bonn-Rhein-Sieg, das Fraunhofer FKIE, die IHK Bonn/ Rhein-Sieg, die Bundesstadt Bonn, das Polizeipräsidium Bonn, die Telekom Security und viele mittelständische Firmen wie z.B. Bechtle und die CONET Solutions GmbH Teil des Clusters. Ziel der Initiative ist es, den Transfer von Cyber-Security-Wissen in die Wirtschaft, Politik und Gesellschaft zu unterstützen und so einen Beitrag zur Immunisierung der Gesellschaft gegen Cyber-Attacken zu leisten.

Pressekontakt

Cyber Security Cluster Bonn e.V.

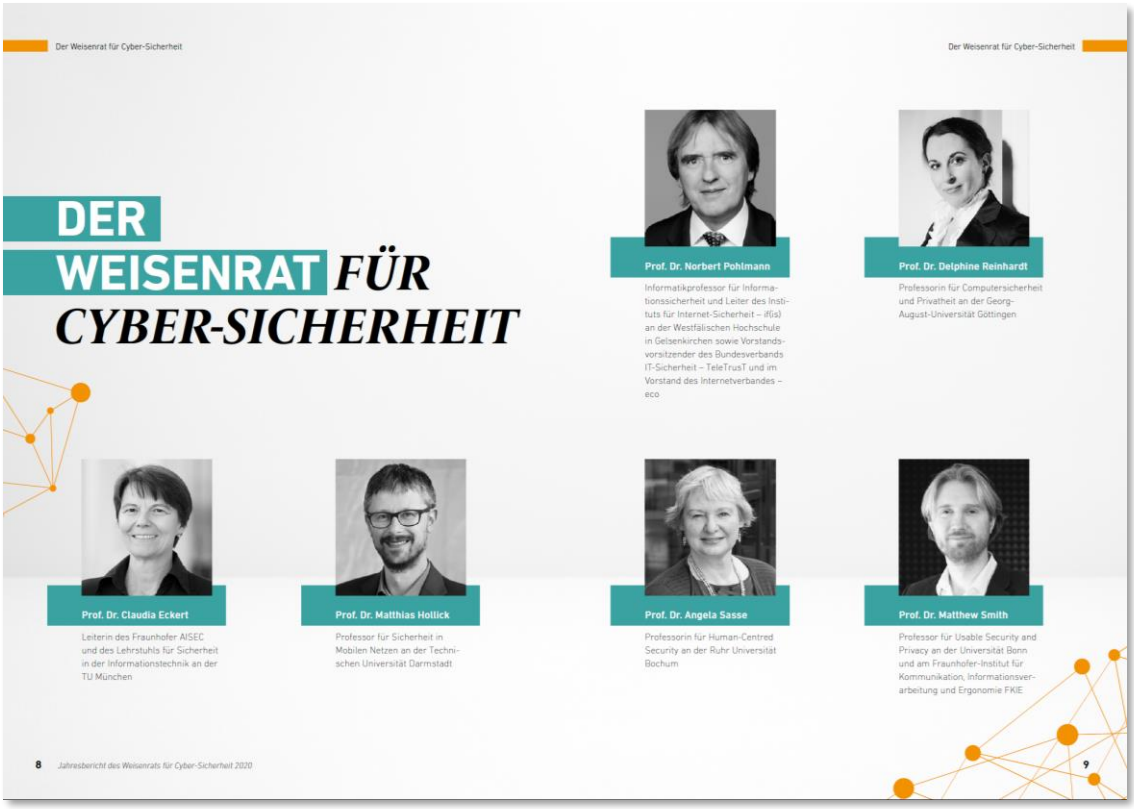
Cluster Management
Christian Schmickler

Tel.: +49 151-43862131
E-mail: : cschmickler@cyber-security-cluster.eu

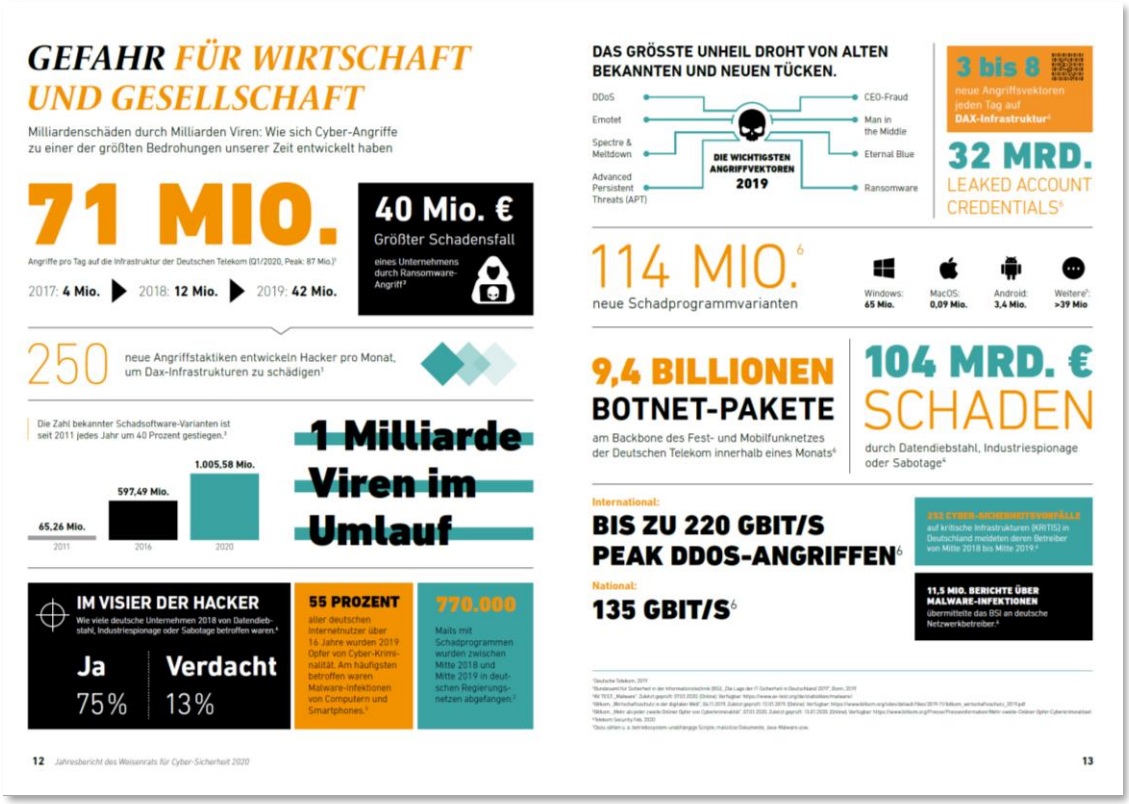
Weitere Informationen für Medienvertreter:

www.cyber-security-cluster.eu

Anlage 1: Weisenrat für Cyber-Sicherheit



Anlage 2: Bedrohungslage in Deutschland



Anlage 3: Empfehlungen des Weisenrats für Cyber-Sicherheit