

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-Attacks
-

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-Attacks 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

DER WEISENRAT FÜR CYBER-SICHERHEIT

Prof. Dr. Norbert Pohlmann
 Informatikprofessor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – ifiss an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrust und im Vorstand des Internetverbandes – eco

Prof. Dr. Delphine Reinhardt
 Professorin für Computersicherheit und Privatheit an der Georg-August-Universität Göttingen

Prof. Dr. Claudia Eckert
 Leiterin des Fraunhofer AISEC und des Lehrstuhls für Sicherheit in der Informationstechnik an der TU München

Prof. Dr. Matthias Hollick
 Professor für Sicherheit in Mobilien Netzen an der Technischen Universität Darmstadt

Prof. Dr. Angela Sasse
 Professorin für Human-Centred Security an der Ruhr Universität Bochum

Prof. Dr. Matthew Smith
 Professor für Usable Security and Privacy an der Universität Bonn und am Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE

8 Jahresbericht des Weisenrats für Cyber-Sicherheit 2020 9

Anlage 2: Bedrohungslage in Deutschland

GEFAHR FÜR WIRTSCHAFT UND GESELLSCHAFT

Milliardenschäden durch Milliarden Viren: Wie sich Cyber-Angriffe zu einer der größten Bedrohungen unserer Zeit entwickelt haben

71 MIO.

Angriffe pro Tag auf die Infrastruktur der Deutschen Telekom (Q1/2020, Peak: 87 Mio.)
 2017: 4 Mio. ▶ 2018: 12 Mio. ▶ 2019: 42 Mio.

40 Mio. €

Größter Schadensfall eines Unternehmens durch Ransomware-Angriff¹

250

neue Angriffstaktiken entwickeln Hacker pro Monat, um Dax-Infrastrukturen zu schädigen²

1 Milliarde Viren im Umlauf

Die Zahl bekannter Schadenssoftware-Varianten ist seit 2011 jedes Jahr um 40 Prozent gestiegen³

135 GBIT/S⁶

National: Peak DDOS-ANGRIFFEN⁶

104 MRD. € SCHADEN

durch Datendiebstahl, Industriespionage oder Sabotage⁴

9,4 BILLIARDEN BOTNET-PAKETE

am Backbone des Fest- und Mobilfunknetzes der Deutschen Telekom innerhalb eines Monats⁵

3 bis 8 neue Angriffsvektoren jeden Tag auf DAX-Infrastruktur⁷

114 MIO.⁶

neue Schadprogrammvarianten

32 MRD. LEAKED ACCOUNT CREDENTIALS⁸

BIS ZU 220 GBIT/S PEAK DDOS-ANGRIFFEN⁶

International:

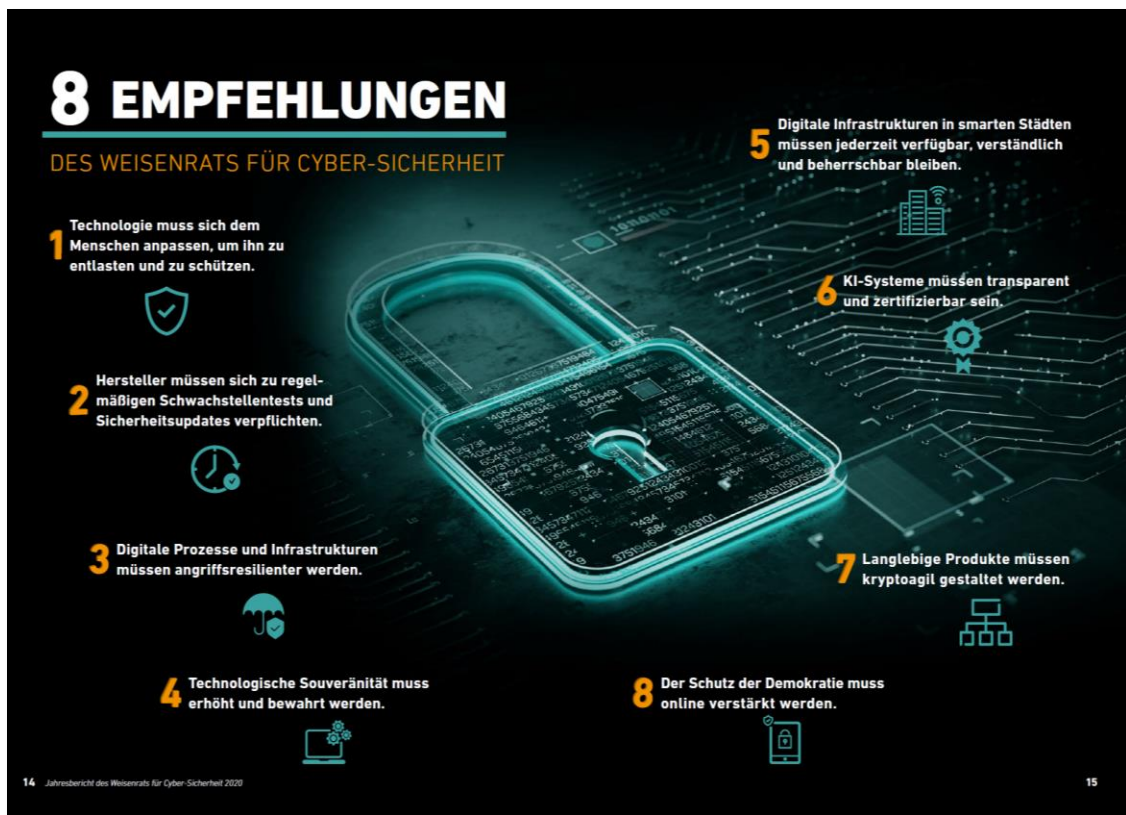
11,5 MIO. BERICHTE ÜBER MALWARE-INFESTIONEN

übermittelte das BSI an deutsche Netzwerkbetreiber⁹

¹Quelle: Telekom, 2019
²Wissenschaftlicher Dienst der Informationsdienste (WDI), Die Lage der IT-Sicherheit in Deutschland 2017, Bonn, 2019
³WDI, Cyberwar: Gefahr gegen IT-Infrastruktur, Berlin, 2018
⁴WDI, Cyberwar: Gefahr gegen IT-Infrastruktur, Berlin, 2018
⁵WDI, Cyberwar: Gefahr gegen IT-Infrastruktur, Berlin, 2018
⁶WDI, Cyberwar: Gefahr gegen IT-Infrastruktur, Berlin, 2018
⁷WDI, Cyberwar: Gefahr gegen IT-Infrastruktur, Berlin, 2018
⁸WDI, Cyberwar: Gefahr gegen IT-Infrastruktur, Berlin, 2018
⁹WDI, Cyberwar: Gefahr gegen IT-Infrastruktur, Berlin, 2018









12 Jahresbericht des Weisenrats für Cyber-Sicherheit 2020 13

Anlage 3: Empfehlungen des Weisenrats für Cyber-Sicherheit



8 EMPFEHLUNGEN

DES WEISERATS FÜR CYBER-SICHERHEIT

- 1** Technologie muss sich dem Menschen anpassen, um ihn zu entlasten und zu schützen.

- 2** Hersteller müssen sich zu regelmäßigen Schwachstellentests und Sicherheitsupdates verpflichten.

- 3** Digitale Prozesse und Infrastrukturen müssen angriffsresilienter werden.

- 4** Technologische Souveränität muss erhöht und bewahrt werden.

- 5** Digitale Infrastrukturen in smarten Städten müssen jederzeit verfügbar, verständlich und beherrschbar bleiben.

- 6** KI-Systeme müssen transparent und zertifizierbar sein.

- 7** Langlebige Produkte müssen kryptoagil gestaltet werden.

- 8** Der Schutz der Demokratie muss online verstärkt werden.


14 Jahresbericht des Weisenrats für Cyber-Sicherheit 2020 15