



Bundeskriminalamt



## **Memorandum of Understanding**

**zwischen**

**dem Verband Deutscher Maschinen- und Anlagenbau (VDMA), Lyoner Str.  
18, 60528 Frankfurt**

**und**

**der Bundesrepublik Deutschland,  
vertreten durch das Bundesministerium des Innern, für Bau und Heimat,  
vertreten durch das Bundeskriminalamt, Thaerstr. 11, 65193 Wiesbaden**

### **1. Die Bedrohungslage durch Cybercrime**

Das Gefährdungspotenzial durch Cybercrime ist auf anhaltend hohem Niveau und steigt seit Jahren kontinuierlich. Das bei Cyberkriminellen etablierte Geschäftsmodell Cybercrime-as-a-Service führte zur Herausbildung einer globalen kriminellen Dienstleistungsindustrie im Internet, die immer neue Modi Operandi und teils maßgeschneiderte Malware hervorbringt. Cyberkriminelle sind flexibel, passen sich schnell an veränderte gesellschaftliche Situationen an und nutzen diese für ihre Zwecke aus. Die fortschreitende Digitalisierung und moderne Arbeitswelten bieten in diesem Zusammenhang zusätzliche Tatgelegenheiten für kriminelle Akteure.

Immer mehr steht dabei die Wirtschaft im Fokus der Cyberkriminellen. Neben breit gestreuten Angriffen sind zunehmend auch professionell vorbereitete und zielgerichtete Attacken auf Unternehmen ein gängiges Muster.

Hierbei sind insbesondere große Unternehmen aber auch immer wieder kleine und mittelständische Unternehmen Ziel von Cyberkriminellen. Bei Letzteren ist die Awareness und der Ressourceneinsatz gegen Cyberangriffe häufig niedriger als in Großunternehmen. Gerade für kleine und mittelständische Unternehmen kann der Ausfall der IT-Infrastruktur jedoch schnell existenzbedrohende Ausmaße annehmen.

Neben der Verschlüsselung von Systemen werden im Vorfeld regelmäßig massenhaft Daten durch die Täter exfiltriert und in einschlägigen Foren veröffentlicht oder Interessierten zum Kauf angeboten. Auch auf diese Weise droht der Abfluss von Know-how in unbekannte Richtung, mitunter auch an Wettbewerber. Die potenzielle Folge ist der Verlust von Expertise und damit einhergehend eine Schwächung der deutschen Wirtschaft gegenüber globaler Konkurrenz.

## **2. Der VDMA als Akteur im Kampf gegen Cybercrime**

Der Maschinen- und Anlagenbau steht für Digitalisierung und Innovation sowohl in Produkten als auch in Produktionsprozessen. Eine zunehmende Vernetzung von ebendiesen Produktionsprozessen führt aber auch zu größeren Angriffspotenzialen und damit zu einer höheren Wahrscheinlichkeit, Opfer eines Cyberangriffs zu werden. Hierunter fallen auch Supply-Chain-Angriffe, die zunächst nicht auf das Unternehmen selbst gerichtet sind, sondern auf dessen Zulieferer.

Der VDMA unterstützt seine Mitgliedsunternehmen beim Kampf gegen Cybercrime auf vielfältige Weise. Das VDMA Competence Center Industrial Security ist dabei der zentrale Ansprechpartner für Mitglieder, Forschung, Behörden und Politik.

Im VDMA-Netzwerk der über 3300 Mitgliedsunternehmen tauschen sich Fachexperten aus Produktion, Softwareentwicklung und IT-Sicherheit regelmäßig zu verschiedenen Themenfeldern der Cybersecurity aus. Im Zentrum steht dabei die Frage, wie man dem Komplex Cybersicherheit im eigenen Unternehmen begegnet, wo Risiken liegen und welche Abhilfemaßnahmen geeignet sind. Ziel ist, sich auf den „Cyber-Ernstfall“ angemessen vorzubereiten. Neben der Zusammenarbeit in diversen Arbeitskreisen wird auch die Zusammenarbeit mit Sicherheitsbehörden auf- und ausgebaut. Zudem bietet der VDMA direkte Unterstützungsangebote im Bereich Cyberversicherung (VDMA Cyber Police) sowie der Aus- und Fortbildung nach IEC 62443 an. In Europa setzt sich der VDMA für eine kohärente horizontale Cybersecurity-Regulierung ein und in internationalen Kooperationen, z.B. mit Japan, werden harmonisierte Standards zur Stärkung der Resilienz vernetzter Industrieanlagen vorangetrieben.

## **3. Das Bundeskriminalamt als Bestandteil der nationalen und internationalen Cyber-Sicherheitsarchitektur**

Das Bundeskriminalamt (BKA) ist wesentlicher Bestandteil der Cyber-Sicherheitsarchitektur in Deutschland und hierbei eng vernetzt mit weiteren Sicherheitsbehörden. Neben den klassischen Zentralstellenaufgaben gehören Auswertungen auf operativer und strategischer Ebene genauso wie Ermittlungen zu den Kernaufgaben des BKA im Phänomenbereich Cybercrime. Zur Erfüllung seines gesetzlichen Auftrages steht das Bundeskriminalamt hierbei in engem Austausch mit nationalen und internationalen Partnern sowohl aus dem behördlichen als auch privatwirtschaftlichen Umfeld.

Das BKA genießt aufgrund vielfältiger Ermittlungserfolge im Phänomenbereich Cybercrime nationales und internationales Renommee. Mit Blick auf diese Kompetenzen soll die Rolle des Bundeskriminalamtes als vertrauenswürdiger Partner für die deutsche Wirtschaft weiter gestärkt und über die Zusammenarbeit und den gegenseitigen Informationsaustausch hinaus, ein Mehrwert für die Bekämpfung der Cybercrime in Deutschland erreicht werden.

#### **4. Zielsetzung**

Der wirtschaftliche Erfolg deutscher Unternehmen ist Grundlage für Wohlstand und gesellschaftspolitische Stabilität.

Ein effektiver Schutz der Wirtschaft bedarf angesichts der geschilderten Bedrohungslage im Bereich der Cybercrime der engen Kooperation von Staat und Industrie im Hinblick auf Prävention im Vorfeld möglicher Cyberangriffe und Strafverfolgung nach Eintritt eines Schadensfalls. Vertrauen und gegenseitige Information sind hierbei Kern einer funktionierenden Zusammenarbeit. Das Bundeskriminalamt und der Verband Deutscher Maschinen- und Anlagenbau beabsichtigen daher, den gegenseitigen Erfahrungs- und Informationsaustausch auszubauen, mit dem Ziel, die Awareness für Cybercrime in den Unternehmen zu stärken und die Verfolgung von Cybertätern durch die deutschen Sicherheitsbehörden zu fördern.

Dieses Memorandum of Understanding unterstreicht den gegenseitigen Willen des VDMA und des Bundeskriminalamtes, sich im Rahmen der jeweiligen Möglichkeiten und Zuständigkeiten fachlich zu unterstützen.

#### **5. Vertrauensvolle Zusammenarbeit**

Die bisher schon vorhandenen Kontakte und Erfahrungen im VDMA bei der Sensibilisierung von Unternehmen des Maschinen- und Anlagenbaus für das Thema Cybercrime werden in Zusammenarbeit mit dem Bundeskriminalamt ausgebaut und verstetigt. Hierzu beabsichtigen VDMA und das Bundeskriminalamt, zielgruppengerechte Sensibilisierungs- und Informationsangebote für den Phänomenbereich Cybercrime zu entwickeln und durch gemeinsame Aktivitäten zu begleiten. Ferner sollen weitere konkrete Maßnahmen und Formate der Zusammenarbeit im regelmäßigen Austausch festgelegt und umgesetzt werden.

Die Unterzeichner sichern sich die Vertraulichkeit der erlangten Informationen zu; eine Weitergabe an Dritte erfolgt ausschließlich mit Zustimmung des Informationsgebers und betroffenen VDMA-Mitglieds. Der Austausch von Informationen erfolgt nach den geltenden Datenschutz- und Übermittlungsvorschriften. Gesetzliche Regelungen oder Weisungen durch das Bundesministerium des Innern, für Bau und Heimat als Dienst- und Fachaufsicht des Bundeskriminalamtes bleiben von diesem Memorandum of Understanding unberührt.

---

Martina Link, Bundeskriminalamt

---

Karl Haeusgen, VDMA

Berlin, den 26. Oktober 2021