DIHK-Positionspapier „Daten- und Informationssicherheit“

Daten- und Informationssicherheit

Nachhaltig Vertrauen schaffen

DIHK Deutscher Industrie- und Handelskammertag

#GemeinsamSicherHandeln


www.dihk.de

Inhaltsverzeichnis

Die Herausforderungen der Digitalisierung ---- 4

1. Mehr Sicherheit für angreifbare Produkte und Systeme ---- 6

2. Integration von Daten und Informationssicherheit in den Alltag von Geschäftsführung und Mitarbeitern ---- 10

3. Für eine bessere Reaktionsfähigkeit von Unternehmen und Staat im Schadensfall ---- 14

Impressum ---- 16

Die Herausforderungen der Digitalisierung

Je mehr ein Unternehmen digitalisiert ist, desto stärker hängt sein gesamter Fortbestand von funktionierenden Informations- und Kommunikationsinfrastrukturen sowie einer sicheren Datenverarbeitung und -speicherung ab.
Für Unternehmen ist die Sicherheit ihrer Daten und Informationen deshalb eine der größten Herausforderungen bei der Digitalisierung. Deren volkswirtschaftliche Potenziale werden nur dann umfassend erschlossen, wenn Daten und Informationen sicher übertragen und verarbeitet werden.

Unternehmen benötigen ein digitales Ökosystem, in dem sie sicher agieren können. Der Gesetzgeber hat dafür in der letzten Legislaturperiode Regelungen geschaffen, die erst nach und nach zur Umsetzung kommen. Im neuen Koalitionsvertrag sind bereits weitere Regelungen vorgesehen. Vor der Schaffung neuer gesetzlicher Vorgaben sollten die bisherigen Regelungen jedoch evaluiert werden. In jedem Fall gilt es, zusätzliche Belastungen der Wirtschaft dem erwarteten Sicherheitsgewinn gegenüberzustellen und die Maßnahmen in ein Gesamtkonzept einzubetten.

Ein vertrauensvolles Miteinander braucht eine schlüssige Gesamtstrategie

In fast allen Unternehmen wurden entsprechende Maßnahmen bereits ergriffen. Aber es bleibt noch viel zu tun, um das Sicherheitsniveau in der Wirtschaft insgesamt zu heben und die Unternehmen für künftige Herausforderungen zu wappnen. Der DIHK schlägt eine Gesamtstrategie vor, die Politik, Hersteller, IT-Sicherheitsanbieter und Anwender beteiligt und die Voraussetzungen für ein vertrauensvolles Miteinander innerhalb der Wirtschaft und zwischen Unternehmen und der öffentlichen Hand schafft.

Folgende Eckpunkte sollte eine Gesamtstrategie für mehr Daten- und Informationssicherheit in der deutschen Wirtschaft enthalten:

1. Mehr Sicherheit für angreifbare Produkte und Systeme: Die Vertrauenswürdigkeit im Hinblick auf Daten- und Informationssicherheit sollte elementarer Bestandteil soft- und hardwarebasierter Produkte und Anwendungen sein.

2. Integration von Daten und Informationssicherheit in den Alltag von Geschäftsführung und Mitarbeitern: Die Geschäftsführung jedes Unternehmens sollte Daten- und Informationssicherheit als Bestandteil einer guten Unternehmensführung betrachten. Der Bildungskanon sollte erweitert werden, damit Mitarbeiter über Kompetenzen für einen sicheren Umgang mit IT-Systemen verfügen.

3. Für eine bessere Reaktionsfähigkeit von Unternehmen und Staat im Schadensfall: Die Herausforderungen im Bereich Daten- und Informationssicherheit können nur dank einer vertrauensvollen Zusammenarbeit aller Beteiligten erfolgreich gemeistert werden. Erforderlich sind ein Kompetenzaufbau in den Sicherheitsbehörden und eine verbesserte Zusammenarbeit zwischen Sicherheitsbehörden und Wirtschaft.

1. Mehr Sicherheit für angreifbare Produkte und Systeme

Unternehmen bieten Produkte und Dienstleistungen an und nutzen Vorprodukte, die Software und Hardware enthalten. Hier sind zahllose IT-Anwendungen im Einsatz, und im sogenannten Internet der Dinge, in der Industrie 4.0 oder im Smart Home werden immer kleinere Geräte und Sensoren miteinander vernetzt. Durch diese zunehmende Vernetzung vergrößert sich die Angriffsfläche enorm. Die Vertrauenswürdigkeit im Hinblick auf Daten- und Informationssicherheit sollte ein Leitprinzip bei der Erstellung und dem Inverkehrbringen soft- und hardwarebasierter Produkte und Anwendungen sein.

Ganzheitlicher Ansatz für sichere Produkte

Im Koalitionsvertrag vom 7. Februar 2018 ist u. a. vorgesehen, das Entwicklungsprinzip „Security by Design" zu fördern, IT-Sicherheitsstandards für internetfähige Produkte zu entwickeln und deren Einhaltung mit einem „Gütesiegel" transparent zu gestalten. Hersteller und Anbieter müssen Sicherheitslücken bekannt machen und schnellstmöglich beheben. Darüber hinaus sollen klare Produkthaftungsregeln für die digitale Welt aufgestellt werden.

Für die genannten Maßnahmen sollte vorab ein Gesamtkonzept erarbeitet werden, das das Zusammenspiel freiwilliger und verpflichtender Vorhaben transparent macht. Der Gesetzgeber sollte den Prozess von der Standardisierung über die Einführung eines „Gütesiegels" bis hin zur Marktüberwachung von Anfang an zusammen denken und ausgestalten. Dabei sind grundsätzlich Lösungen für den europäischen Markt anzustreben.

Bei der Entwicklung von Produkten „Security by Design" umsetzen

Anbieter und Hersteller sollten Daten- und Informationssicherheit bereits bei der Planung von Produkten mitberücksichtigen, also von vornherein auf „Security by Design" achten. „Security by Design" sollte ein obligatorischer Bestandteil der Standardisierungsprozesse beispielsweise bei Werkzeugen, Produktions- oder Softwarekomponenten sein.

Zusätzlich zu einem sicheren Zustand bei der Auslieferung sollte über einen definierten Zeitraum eine sichere Nutzung durch Sicherheitsupdates gewährleistet werden. Der Hersteller ist in der Verantwortung, diese für einen angemessenen Zeitraum zur Verfügung zu stellen, dem Anwender obliegt es, diese einzuspielen.

IT-Sicherheitsstandardisierung mit mehr Nachdruck voranbringen

Die gemeinsamen Standardisierungsaktivitäten von Staat und Unternehmen für sichere IT-basierte Produkte sollten mit mehr Nachdruck verfolgt werden.

Die Förderung von Forschungsvorhaben sollte auch auf europäischer Ebene vorangetrieben und anwendungsorientiert ausgestaltet sein, so dass in diesem schnelllebigen Umfeld verwertbare Forschungsergebnisse erzielt und eine schnelle Diffusion in europäische und internationale Standardisierungsgremien gewährleistet werden.

Die Bundesregierung sollte darüber hinaus ihre aktive Präsenz in globalen Standardi-

sierungsgremien zur internationalen Durchsetzung von Sicherheitsanforderungen ausweiten. Dies könnte über eine stärkere finanzielle Unterstützung, etwa für die Entsendung von IT-Sicherheitsexperten aus Wirtschaft, Wissenschaft und Verwaltung in diese Gremien, erfolgen.

Mehr Transparenz über die Sicherheitseigenschaften von softwarebasierten Produkten

Eine spezielle IT-Sicherheitskennzeichnung kann zu mehr Transparenz über die Sicherheitseigenschaften und zu einer Sensibilisierung der Nutzer für sicherere IT-basierte Produkte beitragen. Ein IT-Sicherheitskennzeichen wird sich aber nur durchsetzen, wenn es europaweite Gültigkeit besitzt und sein Aussagewert allgemein verständlich ist. Das im Koalitionsvertrag angestrebte „Gütesiegel" könnte falsche Erwartungen bei den Nutzern wecken, indem es umfassende IT-Sicherheit suggeriert. Sinnvoller wäre deshalb eine IT-Sicherheitskennzeichnung mit verständlichen Informationen zu den IT-Sicherheitseigenschaften eines Produkts, z. B. dass das Produkt die entsprechenden Sicherheitsstandards erfüllt, und wie lange der Hersteller Sicherheitsupdates zur Verfügung stellt.

Bei der Einführung eines IT-Sicherheitskennzeichens sollte zudem darauf geachtet werden, dass die zusätzlichen Belastungen gerade für kleine und mittlere Unternehmen – insbesondere die Hürden für Hersteller – möglichst gering gehalten werden. Sinnvoll ist ein abgestuftes Vorgehen je nach erforderlichem Sicherheitsniveau der Produkte. Die Sicherheitsanforderungen der jeweiligen Produktklassen (z. B. Router, vernetzter Herd) und die erforderliche Prüftiefe durch die Marktaufsicht sollten verhältnismäßig sein und gemeinsam mit den betroffenen Unternehmen (vor allem kleinen und mittleren sowie Start-ups) erarbeitet werden. Die Erfüllung von Sicherheitsstandards können Hersteller als Selbstauskunft (ähnlich dem Prozess beim CE-Kennzeichen) erklären, eine stichprobenweise Marktüberwachung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist ausreichend. Produkte, die aufgrund ihrer Eigenschaften (z. B. mögliche Schadenshöhe, Preis, Lebensdauer) besondere Sicherheitsstandards erfüllen müssen, sollten vor ihrem Einsatz IT-sicherheitszertifiziert werden.

Keine neuen Produkthaftungsvorschriften für Software

Die Nutzer müssen sich darauf verlassen können, dass Sicherheitsstandards eingehalten werden. Bei Verstößen ist das bestehende Haftungsrecht weitestgehend auf IT-Produkte der Hersteller und der Inverkehrbringer anwendbar. Der Gesetzgeber sollte evaluieren, ob ggf. Nachjustierungen bei der Rechtssetzung bzw. der Rechtsdurchsetzung erforderlich sind und wie die Anwendbarkeit auch gegenüber Anbietern aus Drittstaaten außerhalb der Europäischen Union gewährleistet werden kann. Ein eigenes Produkthaftungsrecht für IT-Produkte ist aus heutiger Sicht nicht erforderlich.

Gesetzliche IT-Sicherheitsanforderungen mit Augenmaß weiterentwickeln

Mit dem IT-Sicherheitsgesetz von 2015 verpflichtet der Gesetzgeber die Betreiber besonders gefährdeter Infrastrukturen wie Energie, Wasser, Gesundheit oder Telekommunikation, ihre Netze besser vor Angriffen zu schützen. Neben der obligatorischen Meldung von IT-Sicherheitsvorfällen gelten branchenbezogene Mindeststandards für die IT-Sicherheit.

Für eine gemeinsame Gestaltung und Optimierung laufender Prozesse

In diesem Bereich ist das verabschiedete IT-Sicherheitsgesetz ein wichtiger Baustein in einer Gesamtarchitektur für mehr Sicherheit in Deutschland. Der Koalitionsvertrag sieht eine Ausweitung der gesetzlichen Verpflichtungen auf weitere Branchen vor. Hierfür muss zunächst für die jeweilige Branche die Verhältnismäßigkeit belegt werden, insbesondere mit Blick auf die Folgen für kleine und mittlere Unternehmen. In jedem Fall ist eine Kosten-Nutzen-Betrachtung unter Einbeziehung der betroffenen Unternehmen notwendig, bevor das Gesetz ausgeweitet wird.

IT-Sicherheitsinfrastrukturen einfach nutzbar machen und verbreiten

Um Daten vor unberechtigten Zugriffen Dritter zu schützen, sollten diese automatisch verschlüsselt sein und auch verschlüsselt übertragen werden. Eine weitere sinnvolle Maßnahme wäre die Ausweitung der Forschungsvorhaben zur einfachen Verschlüsselung sowie eine stärkere Förderung auf diesem Gebiet. Es gilt hier, benutzerfreundliche Lösungen zu entwickeln.

Mit dem Instrument des Elektronischen Siegels für juristische Personen eröffnet die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste („eIDAS-Verordnung) sinnvolle Einsatzszenarien für Transaktionen und die sichere Identifizierung von Unternehmen und Behörden. Das neue Instrument der Elektronischen Siegel bietet eigene Anwendungsmöglichkeiten für juristische Personen, die eine Willenserklärung damit digital einreichen können. Wenn eine Behörde oder eine Firma ein Dokument elektronisch siegelt, so ist sie als Absender des Dokuments dauerhaft erkennbar. Gleichzeitig ist das elektronische Dokument vor unbemerkten Veränderungen geschützt. Damit sich vertrauenswürdige Produkte und Dienstleistungen am Markt entwickeln können, sind alle Bundesressorts und die Länder gefordert, in den jeweiligen Fachgesetzen Einsatzmöglichkeiten zu eröffnen.

Daten- und Informationssicherheit als Entscheidungskriterium bei Investitionen der öffentlichen Hand etablieren

Die öffentliche Hand sollte bei IT-Beschaffungsvorhaben Investitionen in die IT-Sicherheit der Systeme von Beginn an obligatorisch einbeziehen. Der Mitteleinsatz sollte sich am Schutzbedarf und an der Risikoabschätzung orientieren.

2. Integration von Daten und Informationssicherheit in den Alltag von Geschäftsführung und Mitarbeitern

Die Entwicklung und Etablierung von sicheren Produkten, Lösungen und Dienstleistungen sowie sichere unternehmensinterne Prozesse bieten einen erheblichen Wettbewerbsvorteil und entscheiden mit über den künftigen Geschäftserfolg der Unternehmen. Die Geschäftsführung eines jeden Unternehmens ist deshalb gut beraten, Daten- und Informationssicherheit als strategisches Thema mitzudenken und als Bestandteil einer guten Unternehmensführung zu betrachten. Dazu zählen technische und organisatorische Maßnahmen sowie Investitionen in sichere Vorprodukte, Lösungen und Dienstleistungen. Bei Beschäftigten ist ein starkes Bewusstsein für den sicheren Umgang mit IT erforderlich.

Unterstützungsangebote für kleine und mittlere Unternehmen weiter fortführen und ausbauen

Der Gesetzgeber ist bereits tätig geworden, um den Herausforderungen der Digitalisierung zu begegnen. Die Europäische Datenschutzgrundverordnung und das IT-Sicherheitsgesetz fordern ein Basis-Sicherheitsniveau. Das IT-Sicherheitsgesetz betrifft Betreiber kritischer Infrastrukturen, die Datenschutzgundverordnung jedes Unternehmen. Eine angemessene Datensicherheit ist Teil der Sorgfaltspflicht eines ehrbaren Kaufmanns, sie muss in der Umsetzung bürokratiearm und praktikabel sein. Die Digitalisierung im Betrieb gelingt insbesondere dann, wenn das Thema IT-Sicherheit von vornherein mitgedacht und sukzessive umgesetzt wird.

Staat, Verbände, Kammern und andere Initiativen sensibilisieren und unterstützen Unternehmen und Startups, wie z. B. die Initiative „IT-Sicherheit in der Wirtschaft", die „Initiative Wirtschaftsschutz", „Deutschland sicher im Netz" und die „Allianz für Cybersicherheit". Die Industrie- und Handelskammern bringen sich selbst in die Debatte ein und unterstützen Unternehmen. Sie sind für diese vielfach erster Ansprechpartner in der Region. Die bestehenden Angebote der unterschiedlichen Akteure sollten weiter ausgebaut und noch besser aufeinander abgestimmt werden.

Transparenz, Evaluation und Erweiterung bestehender Angebote

Darüber hinaus bieten Bund und Länder auch finanzielle Unterstützung für neutrale Beratungsangebote, Weiterbildungen oder die Einführung sicherer technischer Lösungen in kleinen und mittleren Unternehmen. Dies ist ein sinnvoller Ansatz für den Einstieg in die konkrete Umsetzung, der systematisch weiter ausgebaut werden sollte. Finanzielle Unterstützungsangebote werden durch die Unternehmen allerdings zum Teil nicht genutzt, weil sie nicht bekannt sind. Diese Angebote sollten evaluiert, transparenter gemacht und unbürokratisch ausgestaltet sein. Für eine Breitenwirkung sollten die nötigen organisatorischen Strukturen in den Ländern aufgebaut werden.

Mitarbeiter befähigen

Eine digitalisierte Wirtschaft benötigt Mitarbeiter, die nicht nur über Fachwissen und Führungsqualitäten, sondern zunehmend auch über „Digitalkompetenzen" verfügen. Diese sind Voraussetzung dafür, dass das Thema IT-Sicherheit besser verstanden und eingeschätzt werden kann. Der Erwerb digitaler Kompetenzen sollte von der Schule über die duale Ausbildung, die Hochschule bis hin zur beruflichen Weiterbildung Bestandteil der Wissensvermittlung sein.

> Digitale Kompetenzen sind eine Schlüsselqualifikation mit Zukunft

Die IHKs tragen mit eigenen Weiterbildungen und der Vermittlung weiterer Angebote dazu bei. Sie überführen außerdem alle IHK-Ausbildungsberufe und die darauf aufbauenden Fortbildungsabschlüsse sukzessive in die digitale Welt. Die erforderlichen Kenntnisse dürfen aber nicht erst in der Ausbildung vermittelt werden. Vielmehr sollten die Inhalte bereits in der Schule auf dem Lehrplan stehen. Wesentlich stärker als bisher muss deshalb bereits in den Schulcurricula sowie in der Lehrer- und Berufsschullehreraus- und -fortbildung die Vermittlung einschlägiger Basiskompetenzen erfolgen. Die Kultusministerkonferenz sollte sich des Themas aktiver als bislang annehmen. Sie sollte außerdem dafür sorgen, dass das Thema IT-Sicherheit in den bestehenden Studiengängen im IT-Bereich eine stärkere Gewichtung erhält.

Voraussetzung für den Erwerb digitaler Kompetenzen ist auch eine angemessene technische Ausstattung der Schulen mit einem qualifizierten und sicheren IT-Support. Der Digitalpakt der Bundesregierung soll 5 Milliarden Euro für die IT-Ausstattung der Schulen bereitstellen. Dies wird voraussichtlich lediglich für die Anbindung der Schulen ans Glasfasernetz reichen, aber bei Weitem nicht für die technische Ausstattung und eine Sicherstellung des laufenden Betriebs in den Schulen und Berufsschulen. Hierfür sollten ausreichende Mittel zur Verfügung gestellt werden.


Jun
Jul
Sep
Oct
Nov
Dec

3. Für eine bessere Reaktionsfähigkeit von Unternehmen und Staat im Schadensfall

Die Herausforderungen bei der Daten- und Informationssicherheit lassen sich nur in vertrauensvoller Zusammenarbeit aller Beteiligten erfolgreich meistern. Vor allem kleine und mittlere Unternehmen kommunizieren derzeit noch zu wenig mit Sicherheitsbehörden und anderen Unternehmen. Gefragt ist deshalb ein effektiveres Zusammenspiel von Staat und Wirtschaft.

Kommunikationswege zwischen Staat und Wirtschaft verbessern

Nur ein gemeinsames, planvolles Handeln von Staat und Wirtschaft und eine gute Vernetzung können den Diebstahl von Wissen und Sabotage verhindern. Die „Allianz für Cybersicherheit", in der sich Wirtschaft, Wissenschaft, IHK-Organisation, Verbände und staatliche Stellen für mehr Daten- und Informationssicherheit vernetzen, ist insofern eine wichtige Initiative.

Gegenseitige Informationspflichten zu IT-Sicherheitsvorfällen und entsprechende Warnhinweise wurden mit dem IT-Sicherheitsgesetz für kritische Infrastrukturen bereits etabliert. Für mehr Akzeptanz auch freiwilliger, weitergehender Meldungen von Unternehmen an das BSI sollte den Unternehmen der Mehrwert dieses Ansatzes klarer vermittelt werden (z. B. Warnung anderer Unternehmen, Beitrag zum Lagebild für eine qualifizierte Bewertung der Sicherheitslage und Ableitung präventiver Maßnahmen).

Daten- und Informationssicherheit basiert auf Vertrauen – in die Technik, aber auch die Partner vor Ort. Unternehmen brauchen versierte Ansprechpartner in den Regionen, die es z. B. bei IHKs gibt, und kürzere Kommunikations- und Meldewege zu den Sicherheitsbehörden auf Landesebene, um im Schadensfall schneller zu reagieren.

Unterstützung durch Sicherheitsbehörden gewährleisten

Gegen gezielte Cyberangriffe durch enorm ressourcenstarke Organisationen (z. B. Staaten, organisierte Kriminalität) können sich Unternehmen allein kaum schützen. Hier sind mehr Unterstützung und eine engere Zusammenarbeit mit Sicherheitsbehörden und die Vernetzung mit anderen Unternehmen vonnöten.

Sinnvoll ist die Bündelung der technischen Expertise beim BSI, das sich als zentraler Kompetenzpartner für Bund, Länder, Kommunen und Unternehmen etabliert hat. Um den zunehmenden Anforderungen gerecht zu werden, sollte es angemessen ausgestattet sein. Auch die Sicherheitsbehörden der Länder brauchen mehr Kompetenzen für Analyse und Reaktion, hier besteht vielerorts Nachholbedarf.

Gleichzeitig ist eine effektivere Arbeitsteilung und Kooperation der Sicherheitsbehörden von Bund und Ländern notwendig.

Ständige Anpassung erforderlich

Angesichts rasanter technischer Entwicklungen und Veränderungen von Angriffsmustern sollte die Cybersicherheitsstrategie der Bundesregierung regelmäßig überprüft und alle 3 Jahre fortgeschrieben werden.

Inhaltlich verantwortlich:
Dr. Katrin Sobania

Gestaltung:
ideengut I Agentur für Kommunikation
Bild Seite 13: SFIO CRACHO/shutterstock

Stand:
August 2018

IHKs und DIHK engagieren sich

Industrie- und Handelskammern sind aktiv, um Unternehmen zu sensibilisieren, zu informieren und einen Erfahrungsaustausch zu ermöglichen. Sie führen zahlreiche Veranstaltungen durch, und in fast allen IHKs gibt es direkte Ansprechpartner für das Thema. Sprechen Sie uns an.

Gerade für Unternehmen, die über keine eigenen IT-Fachkräfte verfügen, ist es wichtig, auf vertrauenswürdige Dienstleister zuzugreifen. Für die Beurteilung der Vertrauenswürdigkeit von IT-Dienstleistern hat der DIHK Kriterien entwickelt. Diese könnten – statt rechtlicher Vorgaben für die verbindliche Einhaltung von IT-Sicherheitsstandards für IT-Dienstleistungen – als Basis für eine Steuerung durch das Einkaufsverhalten der Anwender dienen.

Die DIHK-Bildungs-GmbH hat ein modulares Qualifizierungsangebot für unterschiedliche Zielgruppen im Portfolio.

www.dihk.de/it-sicherheit

DIHK Deutscher Industrie- und Handelskammertag