Fotolia © jijomathai

IHK-POSITION

IT-Sicherheit
für Unternehmen

Grundlage der Digitalisierung

IHK München und Oberbayern

Wirtschaft für Zukunft

München, März 2019

IT-Sicherheit für Unternehmen

Die aktuelle Situation der IT-Sicherheit für Unternehmen
Unternehmen benötigen ein digitales Ökosystem, in dem sie sicher agieren können: Nur mit einer angemessenen Verfügbarkeit, Vertraulichkeit und Integrität von Soft- und Hardware können Unternehmen sichere digitale Prozesse gestalten und Wertschöpfungen realisieren.

Zwar investieren Unternehmen viel Geld in IT-Sicherheit: Jährlich wächst der Markt für IT-Sicherheitsangebote um ca. 9% und hat 2018 erstmals die 4 Milliarden-Grenze überschritten, wovon etwa die Hälfte Dienstleistungen sind.
Dem gegenüber stehen aber jährliche Schäden von mehr als 50 Milliarden Euro, die z. B. durch Diebstähle von Daten, Hardware, Social Engineering oder Sabotage zustande kommen. Unternehmen, die gezielt in IT-Sicherheit investieren wollen, treffen aber bei der Auswahl von Soft- und Hardware auf große Schwierigkeiten, die richtige Wahl zu treffen. Dies liegt unter Anderem an

- grundsätzlichen, historisch bedingten Sicherheitsmängeln (Technologien wie z. B. E-Mail wurden nicht für den sicheren Masseneinsatz konzipiert),
- der Innovationsgeschwindigkeit und Komplexität der IKT-Technologie,
- der mangelnden IT-Sicherheitskompetenz und Awareness auf Hersteller- wie Anwenderseite,
- fehlenden Experten für IT-Sicherheit
- der fehlenden Wertschöpfungsmöglichkeit von IT-Sicherheit.

Insgesamt stellt sich die aktuelle Lage wie folgt dar:

- Ein angemessenes Schutzniveau gegen limitierte Angreifer (z. B. Kleinkriminelle) ist einigermaßen erreichbar, wenn die IKT auf dem Stand der Technik richtig eingesetzt wird und die Mitarbeiter in die Absicherung kompetent eingebunden werden.
- Gegen Angreifer mit staatlichem Hintergrund oder aus der organisierten Kriminalität bietet die aktuelle IKT-Technologie nur wenig Schutz oder muss extrem aufwändig maßgeschneidert aufgebaut werden.

In dieser Situation hat der Gesetzgeber neue Vorschriften wie das IT-Sicherheitsgesetz und für personenbezogene Daten die Datenschutzgrundverordnung eingeführt und erwägt weitere Regulierungen. Zudem wird mittels Forschungsförderung und staatlichen Angeboten zur IT-Sicherheit an der Verbesserung gearbeitet.

So soll es sein:
Unternehmen treffen bei der Auswahl von IKT-Produkten auf sichere Soft- und Hardware, die sich über den gesamten Anwendungszeitraum sicher betreiben lässt. Damit dies möglich ist, müssen die Akteure auf diesem Spielfeld intensiv mitwirken:

- **Informationssicherheit in Unternehmen unterstützen:**
  Orientierung geben, Sensibilisieren, Kompetenz aufbauen, Fördern und hilfreiche Angebote auf- und ausbauen.
- **Angemessene Rahmenbedingungen schaffen:**
  Gesetze durchsetzen als Grundvoraussetzung, statt Meldepflichten auszubauen, den Nutzen freiwilliger Meldungen erhöhen
- **Sichere technische Grundlagen für IT-Sicherheit schaffen:**
  Basistechnologien entwickeln, Sicherheitslücken schließen, Standards setzen und verbessern.
- **Chancen für sichere Soft- und Hardware:**
  Mit freiwilligen Gütesiegeln bzw. verpflichtenden Zertifizierungen Transparenz schaffen. Kritische Soft- und Hardware mit Zertifikaten sicher und transparent machen.

Folgende Vorschläge helfen dabei:

A. Informationssicherheit in Unternehmen unterstützen

Die meisten Unternehmen sind sich der allgemeinen Gefahrenlage bewusst. Was dies allerdings konkret für das Unternehmen bedeutet und welche Handlungsoptionen und Pflichten bestehen, ist oft unklar. Unternehmen sehen sich hier oft in den Entscheidungen überfordert: Z. B. was kann ein Unternehmen selbst tun, um die Sicherheit von E-Mails und Netzwerken zu verbessern? Welche Produkte sind sicher? Wann und wofür benötige ich einen Dienstleister? Wie finde ich einen passenden Dienstleister oder geeignete Produkte?

Die Unternehmen treffen bei der Auswahl ihrer Informations- und Kommunikationstechnologie und der Dienstleister auf einen unübersichtlichen Markt: Die Entscheidung, welche IKT zum Einsatz kommt, wird im Spannungsfeld Kosten, Kompatibilität, Knowhow, Datenschutz und IT-Sicherheit getroffen. Zudem ist die Herausforderung IT-Sicherheit nicht nur technischer Art: Selbst mit technisch perfekter IT-Sicherheit sind die Mitarbeiter eine der größten Risikoquellen für Unternehmen, da sie in komplexen IT-Systemen Fehler machen - unabsichtlich oder mit voller Absicht.

Parallel dazu gibt es eine Vielzahl von Angeboten zur IT-Sicherheit, die auf EU-, Bundes- und Landesebene sowie im privaten Bereich Unterstützung anbieten. Für Unternehmen besteht hier oft die Frage, welches Angebot und welche Maßnahmen dem spezifischen Schutzbedarf am besten gerecht wird.

Um vor diesem Hintergrund IT-Sicherheit zu schaffen, benötigen Unternehmen
- Orientierung
- Sensibilisierung
- Kompetenz
- Förderung
- Hilfreiche Angebote zur Selbsthilfe
- Sichere Hard- und Softwareprodukte

1. **Orientierung: Für Unternehmen zentrale und neutrale Lotsen- und Ansprechpartner schaffen**
   Unternehmen benötigen für IT-Sicherheit sowohl im Normal- wie im Krisenfall erhebliche Unterstützung. Diese bekommen sie in der Regel durch eigenen Kompetenzaufbau und IT-Sicherheitsdienstleister. Staatlicherseits sind vielfältige Bundes- und Landeseinrichtungen aktiv, die z. B. vorwettbewerbliche Sensibilisierungsschulungen anbieten, stichprobenartig Kontrollen durchführen und im Krisenfall bei der Strafverfolgung aktiv werden.
   Unternehmen fällt es oftmals schwer, sich zu orientieren, eine erste Beratung und passende Dienstleister zu finden, sowie sich in der Vielfalt der staatlichen wie privaten Angebote auszukennen.
   Im Rahmen der Initiative „Online – aber sicher!“ der Bayerischen Staatsregierung sind Aktivitäten wie eine Erfahrungsaustausch- und Vernetzungsplattform „Security Operation Center“, eine kostenlose „IT-Hotline“ bei Sicherheitsvorfällen, eine „Cyberabwehr Bayern“ zum internen Behördenaustausch und ein verstärkter Beratungseinsatz des beim Verfassungsschutz liegenden „Cyber Allianz Zentrums“ geplant.
   ► **Vorschlag:**
   In der Reihe von unterschiedlichen Unterstützungsmöglichkeiten brauchen Unternehmen eine zentrale Lotsen- und Anlaufstelle, die die Angebote zur IT-Sicherheit zentral koordiniert und ein rundes Angebot für Unternehmen zusammengestellt. Hierfür könnte das Angebot des Landesamtes für Informationssicherheit (LSI) oder auch die neu verkündete Initiative „Online – aber sicher!“ ausgebaut werden. Als erste Anlaufstelle und neutraler Ansprechpartner für Unternehmen sollte diese Einheit in einer Klammerfunktion sowohl Angebote des Freistaats, des Bundes und der EU als auch hilfreiche privatwirtschaftliche Angebote einbeziehen, sodass in Präventions- wie auch im Krisenfall Unternehmen schnell einen Überblick über ihre Handlungsoptionen bekommen.
   Auf EU- und Bundesebene sollen die Angebote für Unternehmen zur IT-Sicherheit ebenfalls ausgebaut und mit den bayerischen Aktivitäten eng verzahnt werden.

2. **Sensibilisierung und Kompetenzaufbau in Unternehmen**
   Um sichere digitale Prozesse aufzubauen, müssen die Mitarbeiter im digitalen Wandel sicher handlungsfähig sein. Das umfasst die grundsätzliche Verankerung von IT-Sicherheit in der Unternehmensorganisation sowie den Aufbau von Digitalkompetenzen im Allgemeinen und IT-Sicherheit im Speziellen. Mitarbeiter müssen immer wieder für IT-Sicherheit sensibilisiert und geschult werden. Z. B. sollten Unternehmen unterstützt werden, damit sie in der Lage sind, Daten im Hinblick auf ihre Sensibilität zu bewerten und entsprechende Sicherheitsstrategien dazu zu entwickeln.
   ► **Vorschlag:**
   In gemeinsamer Anstrengung von Staat und Wirtschaft sollen Unternehmen immer wieder für das Thema IT-Sicherheit sensibilisiert werden. Initiativen wie die „Allianz für Cybersicherheit“ oder das Zentrum Digitalisierung.Bayern leisten hier gute Arbeit, die weiter ausgebaut werden sollte, um noch mehr Unternehmen gezielter zu erreichen.
   Positiv zu bewerten ist das verstärkte Engagement der „Cyber-Allianz-Zentrums“ bei der Initiative „Online – aber sicher!“ für die Beratung und Schulung von Unternehmen insbesondere zur Früherkennung von Gefährdungslagen. Ebenso die geplante Erfahrungsaustausch- und Vernetzungsplattform „Security Operation Center“,
   Diese Angebote müssen auf die Bedürfnisse kleiner und mittelständischer Unter-

nehmen zugeschnitten, diese umfassend erreichen sowie unmittelbaren und erkennbaren Nutzen in den Unternehmen stiften.
Um Knowhow zur IT-Sicherheit aufzubauen, sollen Schulcurricular und die Lehrer- und Berufschullehrerausbildung darauf explizit eingehen. Auch bei der universitären Ausbildung sollte IT-Sicherheit in Fächern mit IT-Bezug ein wesentlicher Bestandteil sein.

3. **Förderung von Unternehmen**
   Die staatliche finanzielle Unterstützung zur Verbesserung der IT-Sicherheit in kleineren Unternehmen durch Förderprogramme ist sinnvoll. Auf bayerischer Ebene fördert der Digtalbonus IT-Sicherheit im Rahmen der Digitalisierung und der Zertifizierung. Auf Bundesebene können Unternehmen über „go digital“ Förderung zur IT-Sicherheitsberatung erhalten.
   Für die Initiative „Online – aber sicher!“ wurden hinsichtlich Förderung von IT-Sicherheitsforschung „spezielle Förderprogramme zur verstärkten Entwicklung von IT-Sicherheitslösungen“ in „Kooperation mit wissenschaftlichen Einrichtungen“ angekündigt.
   ► Vorschlag:
   Die Förderung von IT-Sicherheit durch den Digitalbonus und go digital sollte auch in Zukunft fortgesetzt werden.
   Bei den Förderprogrammen für IT-Sicherheitsforschung ist darauf zu achten, dass diese für kleine und mittelständische Unternehmen einfach und schnell handhabbar sind.

4. **Hilfreiche Angebote zur Selbsthilfe auf- und ausbauen**
   Initiativen aus der Wirtschaft heraus geben Unternehmen bereits Unterstützung: Beispiele sind die „Cyberwehr“ (Pilotprojekt in Karlsruhe mit telefonischer Experten-Soforthile im Krisenfall), CERT@VDE (z. B. können dort IT-Sicherheitsvorfälle in der Automatisierungsindustrie gemeldet werden) und der eco - Verband der Internetwirtschaft e.V. mit dem Siwecos-Service zur Beobachtung der eigenen Website.
   Zudem bieten auch Behörden wie das Bayerische Landesamt für Datenschutzaufsicht Online-Angebote wie einen https-Check an und überprüfen Websites.
   ► Vorschlag:
   Initiativen mit hilfreichen IT-Sicherheits-Angeboten insbesondere für kleine und mittelständische Unternehmen sollten im Zusammenspiel von Wirtschaft und Behörden weiter ausgebaut und beworben werden, z.B. mit einem „CERT für alle Unternehmen“.

B. Angemessene Rahmenbedingungen schaffen

1. **Gesetze durchsetzen**
   In der Praxis haben Unternehmen, die Gesetze nicht beachten, leider gute Chancen, dadurch Wettbewerbsvorteile zu erzielen. So ist z. B. eine Rechtsdurchsetzung schwierig, wenn asiatische Händler über Onlineplattformen unsichere Produkte verkaufen, die hiesigen Produktsicherheitsstandards oder Zertifikatsnotwendigkeiten für IT-Sicherheit nicht entsprechen - zum Nachteil von EU-Herstellern, die sich solche Praktiken nicht erlauben können. Nur wenn Gesetze durchgesetzt werden, haben alle Unternehmen die gleichen Chancen.

► **Vorschlag:**
Jede bestehende und geplante Gesetzgebung zur IT-Sicherheit ist auf die praktische Durchsetzbarkeit zu überprüfen und ggf. abzuändern.
Regelverstöße sind konsequent zu ahnden. Andernfalls bedeuten verschärfte Gesetze Wettbewerbsnachteile für EU-Hersteller und Händler.
Zu prüfen ist, inwiefern die mit der EU-Kommission vereinbarte Selbstverpflichtung großer Onlinehandelsplattformen zum Entfernen für Leib und Leben gefährdender Produkte („Rapid Alert System“) auch für Produkte mit erheblichen IT-Sicherheitsrisiken sinnvoll ist.

Damit sichere Produkte wettbewerbsfähig sind, ist die Chancengleichheit aller Marktteilnehmer das Fundament.

2. **Statt Meldepflichten auszuweiten: Nutzen freiwilliger Meldungen erhöhen**
Im Krisenfall eines erfolgreichen Angriffes sind Unternehmen unter bestimmten Umständen verpflichtet (z. B. über die DSGVO oder das IT-Sicherheitsgesetz für Betreiber kritischer Infrastrukturen), den Vorfall zu melden. Dies soll zum Lagebild beitragen, mit dem Behörden die Situation einschätzen und Maßnahmen ergreifen können. Geplant ist, diese Meldepflichten auf weitere Unternehmensgruppen auszuweiten. Dadurch soll sich das Lagebild vervollständigen und Behörden besser agieren können.
Für Unternehmen bedeuten solche Meldungen Aufwand ohne eigenen Nutzen. Einher geht die Befürchtung, dass Meldungen öffentlich werden und sich dadurch der Schaden vergrößert. Daher erfolgen aktuell freiwillige Meldungen selten.
Unternehmen sehen sich kontinuierlich Cyberangriffen ausgesetzt. Beispielsweise werden Websites beständig angegriffen (Loginversuche, Portchecks, CMS-Versionscheck...). Viele dieser Angriffe werden entdeckt und abgewehrt (z. B. sperrt die Software einen Angreifer für eine bestimmte Zeit). Allerdings besteht eine hohe Dunkelziffer unentdeckter Angriffe. Erfolgreich abgewehrte Angriffe bleiben für die Allgemeinheit i.d.R. unsichtbar und liegen beim Websitebetreiber oder bei einem Dienstleister. Wenn dieser z.B. IP-Nummern identifiziert, die beständig Websites angreifen, werden diese Angriffe für diesen Dienstleister und seine Software gut abgewehrt. Über die Daten bei den Unternehmen (sei es in CERTs größerer Unternehmen bis zu Sicherheitssoftware in Netzwerken und Websites von Unternehmen) laufen bereits jetzt viele Informationen zu Cyberangriffen zusammen. Eine Weitergabe dieser gesammelten Informationen an die Allgemeinheit erfolgt jedoch i.d.R. nicht.
► **Vorschlag:**
Statt die Meldepflichten auszuweiten, sollte der Nutzen freiwilliger Meldungen für Unternehmen vergrößert werden.
Wie in anderen Bundesländern schon möglich, sollte es bayerischen Unternehmen erleichtert werden, offensichtlich illegale Praktiken zu melden oder online Strafanzeige zu stellen. In Bayern können aktuell online nur Betrugsdelikte im Zusammenhang von Online-Auktionen (sowie Fahrrad- und Kfz-Diebstähle) gemeldet werden, während in anderen Bundesländern Phishing-Mails online zur Anzeige gebracht oder Landeskriminalämtern Spammails zur Auswertung zugeschickt werden können.

Eine zentrale, vertrauenswürdige und neutrale Einheit soll Daten erfolgloser wie erfolgreicher Angriffe auf freiwilliger Basis entgegennehmen, hier kann ein Einsatzgebiet des geplanten bayerischen „Security Operation Center“ liegen bzw. bei Pendants auf Bundes- oder EU-Ebene. Daraus werden so viele hilfreiche Informa-

tionen zu Cyberangriffen wie möglich gesammelt, bewertet und schnell zurück zu den Unternehmen und Sicherheitseinrichtungen gespiegelt. Durch eine zügige Meldung der gesammelten Sicherheitsinformationen profitieren die Unternehmen und werden motiviert, weitere Daten zu Sicherheitsvorfällen zur Verfügung zu stellen.

C. Sichere technische Grundlagen für IT-Sicherheit schaffen

Aus Sicht der Anwender-Unternehmen sollte die Vertrauenswürdigkeit im Hinblick auf Daten- und Informationssicherheit ein Leitprinzip bei der Erstellung und dem Inverkehrbringen soft- und hardwarebasierter Produkte und Anwendungen sein.

1. **Basistechnologien innerhalb der EU entwickeln:**
   Fast alle relevanten Teile der in der EU eingesetzten Soft- und Hardwareprodukte stammen aus den USA und Asien. Dies reicht von der Chip-Produktion bis zu den Betriebssystemen und Anwendungen für PCs und mobile Endgeräte. Dies ist nicht nur hinsichtlich der wirtschaftlichen Wertschöpfung für die EU nachteilig sondern begründet auch diverse Sicherheitsrisiken.
   Darüber hinaus haben viele Konzepte der aktuell verbreiteten IKT-Technologie grundsätzliche Konstruktionsmängel: Der Grund ist, dass die Konzepte dahinter 40 und mehr Jahre alt sind und nicht für die heutige, extrem vernetzte Weltwirtschaft entwickelt wurden. Beispiele sind E-Mail (mehr als 90% Spam), DNS (fehlende Verschlüsselung), SSL-Verschlüsselung ("Heartbleed", Angriffe auf Zertifikatsaussteller), Prozessoren ("Spectre", "Meltdown") oder Mobilfunknetze ("SS7").
   Angesichts dieses unsicheren Fundaments der IKT sind grundsätzlich neue Produkte und Angebote gefordert. Allerdings gibt es für diese Angebote wahrscheinlich zunächst nur einen beschränkten Markt, da neue Technologieansätze mitunter Inkompatibilitäten beinhalten.
   ► Vorschlag:
   Es gilt, auf politischer Ebene das Bewusstsein für die Abhängigkeit von den großen außereuropäischen Hardware- und Digitalfirmen zu schaffen und eine Antwort auf Bundes- und EU-Ebene entwickeln. Hierzu könnte der gezielte Aufbau von Unternehmen als Gegenpol gehören.
   Die IHK für München und Oberbayern fordert dazu die Einrichtung einer nationalen Agentur für Sprunginnovationen (IHK Vollversammlung vom 18.07.2018): Für gänzlich neue Technologien z. B. in der IT-Sicherheit sollte der Staat konkrete, reale Ziele definieren und erster Pilot-Anwender der neuen Technologien sein.
   Positiv zu bewerten ist, dass im Koalitionsvertrag die „Förderung von Sprunginnovationen und des Wissenstransfers in die Wirtschaft“ vereinbart wurde und eine „Agentur für Disruptive Innovationen in der Cybersicherheit und Schlüsseltechnologien“ aufgebaut werden soll.

2. **Standards setzen und verbessern:**
   Die technischen Standards und deren Umsetzung für die Digitalisierung werden oft von den großen Internetkonzernen sowie internationalen Gremien gesetzt und weiter entwickelt. Das ist an sich, weil diese Unternehmen und Gremien dies mit hoher Kompetenz, Dynamik und Einsatz verfolgen. In dieses Engagement spielen allerdings eigene Geschäftsinteressen mit hinein. Hinzu kommt, dass rein technische Standards Blaupausen für Angreifer sind. Daher ist entscheidend, dass technische Standards zusammen mit sicheren Prozessen definiert werden.
   Ein Beispiel ist das Domainnamen-System: Unternehmen benötigen Internet-

Domains für E-Mails und Websites. Hinsichtlich IT-Sicherheit ist es für Unternehmen ein Problem, wenn z. B. Angreifer zur Unternehmensdomain leicht abgeänderte Domains bei E-Mails oder Websites verwenden oder mittels technischer Tricks ("Punycode-Domains") "simulieren". Während bei Domains wie .de und .bayern bereits relative gute Sicherheitsstandards vorhanden sind, ist das bei anderen Domains nicht so: Bei Phishingangriffen spielen Domainnamen eine wesentliche Rolle. Hier sollte wesentlich sorgsamer mit Domains umgegangen werden. Die Spielregeln für die Domainvergabe werden dabei von internationalen Gremien (insbes. ICANN) festgelegt.

► **Vorschlag:**

Die gemeinsamen Standardisierungsaktivitäten von Staat und Unternehmen für sichere IT-basierte Produkte und Prozesse sollten mit mehr Nachdruck verfolgt und Neutralität sichergestellt werden. Die Bundesregierung sollte deshalb ihr Engagement in globalen Standardisierungsgremien ausweiten. Dies könnte z. B. über eine stärkere finanzielle Entsendung von IT-Sicherheitsexperten in diese Gremien erfolgen.

Beispielsweise ist ein Fokus auf IT-Sicherheitsforschung vorstellbar, durch die weltweite Standards für die Sicherheitsprüfung von Hard- und Software gesetzt werden.

3. **Sicherheitslücken schließen:**

Schwachstellen in Prozessen, Soft- und Hardware können für legale wie illegale Szenarien ausgenutzt werden. Selbst wenn Hersteller für bekannte Schwachstellen schnell Updates zur Verfügung stellen, werden diese von Anwendern oft nur zögerlich eingespielt.

Zudem existiert ein Markt von noch nicht veröffentlichten Schwachstellen („Zero Day Exploits“), an dem fast ausschließlich Staaten teilnehmen: Diese Schwachstellen sollen z. B. Sicherheitsbehörden die Möglichkeit der gezielten Strafverfolgung geben. Allerdings können solche Schwachstellen in den Händen von Angreifern großen Schaden anrichten.

► **Vorschlag:**

Damit sichere Soft- und Hardware zur Verfügung steht, müssen bekannte Schwachstellen möglichst zeitnah geschlossen und Updates eingespielt werden (z. B. durch verstärkten Einsatz von automatischen Updates). Die im IT-Sicherheitsgesetz geforderte Pflicht, IT-Produkte auf dem Stand der Technik zu halten, muss besser durchgesetzt werden. Zudem muss verhindert werden, dass Schwachstellen missbraucht werden.

Staatlicherseits darf IT nicht absichtlich geschwächt werden: Es darf z. B. keine Vorschriften geben, die Hersteller von Soft- und Hardware verpflichten, Hintertüren in ihre Produkte einzubauen.

4. **Sichere Verschlüsselung für Unternehmen**

Eine besondere Rolle in der IT-Sicherheit spielen Verschlüsselungsverfahren, mit denen Unternehmen Daten sicher transportieren und aufbewahren können. Aktuell sind Verschlüsselungen in Unternehmen noch zu wenig verbreitet (z. B. kaum verschlüsselte E-Mails) oder technisch nicht ausreichend verbaut (z. B. https-Verschlüsselung von Websites). Zudem ist unklar, ob man sich auf Verschlüsselungsverfahren verlassen kann. Hinsichtlich zukünftiger Quantencomputer besteht die Gefahr, dass gängige Verschlüsselungsverfahren entwertet werden.

► **Vorschlag:**

Unternehmen müssen auf einfache und sicher anwendbare Verschlüsselungsverfahren zurückgreifen können.

Das Zusammenwirken von Staat und Wirtschaft sollten darauf abzielen, sichere Verschlüsselungstechnologie zu entwickeln und diese vielen Unternehmen praktikabel zugänglich zu machen (z. B. Überprüfung von Verschlüsselungstechnologien, Forschung zur Post-Quantum-Kryptographie).

D. Chancen für sichere Soft- und Hardware

Als Kunde geht man in der Regel davon aus, dass Produkte sicher sind. IT-Sicherheit wird noch nicht immer als ein signifikanter Wettbewerbsvorteil gesehen, für den mehr Geld ausgegeben wird.
Viele Produkte sind zunächst sicher. Nur: Mit der technischen Weiterentwicklung und im praktischen Einsatz läuft man Gefahr, dass die IT-Sicherheit verloren geht.
Ziel muss sein, IKT-Produkte in Unternehmen von der Inbetriebnahme bis zur Ausmusterung sicher betreiben zu können. Grundprinzipien dafür sind:

1. Sicherheit in der Produktentwicklung / "security by design" (z. B. Einbau von Technologie für sichere Funk-Autoschlüssel, Zwei-Faktor-Authentifizierung)
2. Verfügbarkeit von Sicherheits-Updates (z. B. für Smartphones)
3. Konfigurationssicherheit / "security by default" (z. B. Änderungspflicht der Standardpasswörter von Webcams und Routern)
4. Regelmäßige Prüfung und Evaluierung der IKT-Produkte

Verzichtet ein Hersteller auf diese Maßnahmen, spart er Kosten in Entwicklung, Herstellung und Betreuung. Mit dem damit erzielten Preisvorteil kann ein sorgsamer Hersteller nicht konkurrieren.
Daher müssen Investitionen in die IT-Sicherheit von Produkten unterstützt werden, so dass idealerweise ein Wettbewerbsvorteil entsteht.
Dies kann durch freiwillige Gütesiegel oder bei kritischen Produkten durch Zertifizierungen erfolgen:

1. **Gütesiegel: Transparenz schaffen für Kauf- und Einsatzentscheidungen**
   Wenn ein Unternehmen bei seiner Kauf- und Einsatzentscheidungen besonders sichere IKT-Produkte auswählen will, sind diese oftmals schwer zu identifizieren. Eine verständliche und transparente Darstellung wäre hier hilfreich, z. B. wenn der Hersteller über durchgeführte Sicherheitstests, die Update-Verfügbarkeit und Sicherheitsrisiken informiert. Zu begrüßen ist, dass der Cybersecurity-Act auf EU-Ebene diese Ziele verfolgt und der Koalitionsvertrag ein "Gütesiegel" vorschlägt: Zunächst werden Prüfschemata entwickelt, die auf freiwilliger Basis zu Gütesiegeln von vernetzten Produkten durch unabhängige Stellen führen sollen.
   ► Vorschlag:
   Eine neutrale Institution soll für IKT-Produkte Gütesiegel konzipieren und überwachen: Dies kann stufenweise erfolgen, wie z.B. ein Basis-Gütesiegel („S+“) für die Einhaltung grundlegender IT-Sicherheitsstandards bis zu umfangreicheren Gütesiegeln mit unabhängigen Tests („S+++“). Für kleinere Unternehmen muss es ebenfalls möglich sein, solche Gütesiegel mit vertretbarem Aufwand zu erhalten. Bei der Ausgestaltung der Prüfregeln und Gütesiegeln ist die Wirtschaft zu beteiligen. Dies erfolgt im Idealfall EU-weit, notfalls nur für Deutschland. Dabei kann z. B. auf die Erfahrungen der EU-weiten CE-Kennzeichnungspflicht für Sicherheits- und Gesundheitsanforderungen, auf die EU-Energielabel sowie die Initiative „IT-Security made in Germany“ zurückgegriffen werden.
   Wichtig ist hier, dass ein einziges zentrales und zuverlässiges Gütesiegel etabliert

wird.

Wenn öffentliche Vergaben oder Förderrahmenbedingungen einen Datenschutzbezug haben, muss durch die Datenschutzgrundverordnung IT-Sicherheit ein wichtiges Kriterium bei der Vergabe bzw. Fördergestaltung sein. Dies sollte ausgeweitet werden: Auch bei Vergaben und Förderrahmenbedingungen ohne Datenschutzbezug sollte IT-Sicherheit ein hoch priorisierter Aspekt sein.
Mittels einer Informationskampagne wird über die Möglichkeit der Gütesiegel bei Herstellern informiert. Anwendende Unternehmen werden über Gütesiegel-Produkte informiert.

2. **Zertifikate: Kritische Soft- und Hardware besonders sicher und transparent machen**
   Soft- und Hardware, bei denen IT-Sicherheitsprobleme außergewöhnlich große Schäden verursachen können, bedürfen der besonderen Begutachtung. Beispielsweise wenn sehr viele Unternehmen eine bestimmte Soft- und Hardware einsetzen, motiviert dies Angreifer besonders, da Schwächen in diesen IKT-Produkten (z. B. Internet of things Geräte oder Netzwerktechnik) besonders lohnenswert sind. Bei solchen Produkten reichen Mindeststandards nicht mehr aus, da Sicherheitsprobleme zu schwerwiegend sein können.
   ► Vorschlag:
   Es ist festzulegen, welche kritische bzw. weit verbreitete IKT-Technik (insbesondere im Internet vernetzte Produkte) über die Transparenz hinaus besonderen Verpflichtungen für Mindeststandards unterliegen muss. Z. B. müssen Sicherheitstests bestanden werden und in einem verbindlich festgelegten Zeitraum Updates bereitgestellt werden. Produkte dieser IKT-Technik, die diese Mindeststandards nicht erfüllen, müssen besonders beobachtet werden: Ggf. müssen Nachbesserung eingefordert bzw. Sicherheitshinweise ausgesprochen werden. Nötigenfalls sind Produkte vom Markt zu nehmen.
   Wie bei den Gütesiegeln soll mittels einer Informationskampagne über zertifizierte Produkte informiert werden.

3. **Produkthaftung:**
   Es besteht kein Bedarf an einer Änderung oder Verschärfung des Produkthaftungsgesetzes oder des Deliktrechts. Die bestehenden Regelungen sind flexibel genug möglichen Gefahren technischer Neuerung zu begegnen. Verschärfungen würden sich nachteilig auf die internationale Wettbewerbsfähigkeit auswirken und Unternehmern die Entwicklung und Etablierung innovativer Produkte erschweren.
   ► Vorschlag:
   Die einzelnen Begriffe aus dem Produkthaftungsgesetz (wie „Produkt“, „Hersteller“, „Fehler“) haben ihre Grundlage in der EU-Produkthaftungsrichtlinie. Die darin enthaltenen Begriffsdefinitionen sind an die digitalisierte Welt anzupassen. Dies kann durch neue Leitlinien für die zeitgemäße Anwendung der Produkthaftungsrichtlinie geschehen. Die EU-Kommission hat eine Anpassung der Leitlinien an die Digitalisierung bis Mitte 2019 angekündigt.

Dem Positionspapier liegt eine fundierte Recherche zugrunde. Unternehmen und Experten aus dem Bereich IT-Sicherheit wurden im Rahmen von Expertengesprächen und durch den Arbeitskreis Digitalisierung und IKT sowie IHK-Experten konsultiert. Ihre Erfahrungen und Perspektiven sind in das Papier eingeflossen.

Fachliche Ansprechpartner:
Armin Barbalata, Tel.: 089 5116 1379; armin.barbalata@muenchen.ihk.de
Franziska Neuberger, Tel.: 089 5116 1260; franziska.neuberger@muenchen.ihk.de
Bernhard Kux, Tel.: 089 5116 1705; bernhard.kux @muenchen.ihk.de