IT-Sicherheit für Unternehmen

IHK-Positionspapier

Auf einen Blick

Die Bedrohung im Cyberraum ist laut Bundesamt für Sicherheit in der Informationstechnik (BSI) so hoch wie nie zuvor. Die IHK-Digitalisierungsumfrage[1] zeigt, dass jedes fünfte Unternehmen 2023 Opfer eines Angriffs wurde. Cyberattacken haben dabei meist entlang der Lieferkette Auswirkungen über das betroffene Unternehmen hinaus. In Unternehmen werden dadurch jährliche Schäden von über 178 Milliarden Euro verursacht.[2] Für die eigene IT-Sicherheit zu sorgen, liegt in der Verantwortung eines jeden Unternehmens. Trotzdem werden Schutzmaßnahmen in Unternehmen mangels Ressourcen und Knowhow nur schleppend ausgebaut.
Erfolgreiche Cyberabwehr ist ein elementarer Standortfaktor, der über Wohlstand und Sicherheit entscheidet. Dafür müssen sich Wirtschaft, Gesellschaft und Staat gemeinsam engagieren:

1. Unternehmen in IT-Sicherheitsmaßnahmen praxisnah unterstützen
- Gesetzliche Verpflichtungen angemessen und rechtssicher umsetzen
- Wirtschaft durch staatliche Einrichtungen zielgerichtet unterstützen
- Verlässliche Anbieter, Dienstleister und Produkte kennzeichnen

2. Ökosystem für innovative IT-Sicherheitsprodukte und -Services stärken
- Forschungstransfer verbessern
- Innovationspotenzial von Startups stärken
- Entwicklung von Schlüsseltechnologien zur IT-Sicherheit vorantreiben
- Faire Marktchancen für EU-Anbieter sicherstellen
- IT-Sicherheit in Open Source unterstützen

3. Gemeinsam IT-Sicherheitsbedrohungen entgegentreten
- Schlagkraft der Sicherheitsbehörden erhöhen
- Ethische Schwachstellenforschung legalisieren
- Mit IT-Sicherheitslücken verantwortungsbewusst umgehen
- Austausch aller Betroffenen fördern - Lagebild und Nutzen verbessern
- Schlüsselrollen bei Cyberangriffen besser einbinden

4. Kompetenzen für IT-Sicherheit auf allen Ebenen ausbauen
- IT-Sicherheits-Kompetenzen in allen Phasen umfassend stärken
- Neue Generation von IT-Sicherheitsfachkräften entwickeln

[1] IHK-Digitalisierungsumfrage 2023
[2] Bitkom-Studie „Wirtschaftsschutz 2024"

Die Position „IT-Sicherheit für Unternehmen" wurde von der IHK-Vollversammlung am 26.11.2024 mit 47 Zustimmungen, 2 Enthaltungen und 0 Gegenstimmen beschlossen.

IHK München und Oberbayern

Wirtschaft für Zukunft

IT-Sicherheit überfordert Unternehmen häufig

Unternehmen sind sich zwar der Gefahren von Cyberattacken bewusst, aber vor allem kleine und mittlere Betriebe setzen oftmals trotzdem nicht die erforderlichen Schutzmaßnahmen um. Sie sehen sich konfrontiert mit hoher Komplexität, fehlendem Knowhow und Ressourcen, unklaren Pflichten, einem vielfältigen IT-Markt und unübersichtlichen Unterstützungsangeboten.
Die Gesetzgebung auf Bundes- und EU-Ebene reagiert mit zusätzlicher Regulierung wie dem IT-Sicherheitsgesetz (ITSichG), NIS-2-Richtlinie (NIS2) und dem Cyber Resilience Act (CRA). Regulierung bedeutet immer auch zusätzliche Bürokratielasten für Unternehmen. Um mehr IT-Sicherheit zu erreichen, benötigen Unternehmen in erster Linie klare Rahmenbedingungen und zielgerichtete Unterstützung.

Unternehmen in IT-Sicherheitsmaßnahmen praxisnah unterstützen

Das Risiko eines Cyberschadens sowie mögliche Auswirkungen in Unternehmen muss auf ein akzeptables Niveau gesenkt werden. Hierfür braucht es unterstützende Maßnahmen zur Prävention und Vorbereitung gegen einen Cyberangriff. Im Falle eines Sicherheitsvorfalls sollte das Unternehmen damit in der Lage sein, zügig zu reagieren und den Schaden zu minimieren. Gesetzliche Regelungen sollen dabei stärken und nicht belasten. Maßnahmen hierfür sind:

- **Gesetzliche Verpflichtungen angemessen und rechtssicher umsetzen:**
  Gesetzliche Verpflichtungen für Unternehmen, sich um die eigene IT-Sicherheit zu kümmern, müssen bürokratiearm, praxisorientiert, klar verständlich, rechtssicher, angemessen und aufeinander abgestimmt sein. EU-Regelungen müssen einheitlich umgesetzt werden. Unklarheiten der Zuständigkeiten oder eine etwaige Doppelregulierung sind zu vermeiden. Sonst besteht die Gefahr, dass Unternehmen aus Deutschland oder der EU abwandern sowie der Startup-Standort Deutschland leidet. Dies gilt insbesondere für die europäische NIS-2-Richtlinie (Betroffenheit, Maßnahmen, Meldepflichten), die CER-Richtlinie (Critical Entities Resilience Richtlinie / KRITIS-Dachgesetz), DORA (Digital Operational Resilience Act), neue EU-Maschinenverordnung oder CRA. Um Aufwand zu reduzieren, müssen Standards und Zertifizierungen wie z. B. Tisax, ISO 27001 oder IT-Grundschutz bei der Umsetzung der verschiedenen gesetzlichen Anforderungen anrechenbar sein. Darüber hinaus soll verstärkt ein spürbarer gemeinschaftlicher Nutzen aus den Verpflichtungen entstehen, z. B. über die geplante Austauschplattform. Diese soll den Austausch von Erfahrungen und Warnungen untereinander einfach ermöglichen. Dabei sollten auch Behörden einheitlich bei Bund und Ländern die NIS2-Anforderungen erfüllen.

- **Wirtschaft durch staatliche Einrichtungen zielgerichtet unterstützen:**
  Unternehmen sind bei Präventionsmaßnahmen und im Falle eines Cyberangriffs oftmals überfordert. Impulse und Einstiegsinformationen zu IT-Sicherheit ebenso wie Ersthilfe im Notfall tragen zu einer höheren Sicherheit für den Wirtschaftsstandort bei. Es gibt bereits einige sehr hilfreiche Unterstützungsangebote durch die öffentliche Hand zur IT-Sicherheit in Unternehmen. Diese sind Unternehmen jedoch oftmals nicht bekannt und in den Zuständigkeiten stark segmentiert. Zu einer deutlich effektiveren Unterstützung können folgende Maßnahmen beitragen:

    - **Unabhängige, zentrale Lotsenstelle etablieren:** Staatliche Unterstützungsangebote auf Bundes- und Landesebene (z. B. BSI, ZAC) müssen sichtbarer und bekannter gemacht sowie die Zuständigkeiten besser vermittelt werden. Unternehmen benötigen bei Fragen zur Prävention ebenso wie bei einem Cybersicherheitsvorfall eine leicht auffindbare, bekannte Anlaufstelle, um einen schnellen Überblick über alle Unterstützungsangebote zu IT-Sicherheit zu erhalten. Für einen möglichst offenen und neutralen Zugang ist es erforderlich, diese Lotsen-Anlaufstelle für Unternehmen unabhängig von der Strafverfolgung zu etablieren. Beispiele dafür sind die Cyberwehr Baden-Württemberg, Cyberwehr Nordrhein-Westfalen oder die Cyberhotline Berlin.

    - **Zielgruppenspezifische Angebote ausbauen:** Informationen und Unterstützungs-Angebote für mehr IT-Sicherheit in Unternehmen und spezifischen Branchen müssen erweitert werden. Positive Beispiele hierfür sind die Unterstützungsangebote des Bayerischen Landesamt für Sicherheit in der Informationstechnik (LSI), die für einzelne Branchen wie Wasserkraftwerke oder Kliniken entwickelt werden. Kleine Unternehmen benötigen besondere Unterstützung. Zielführend wäre es, nach dem Vorbild des BSI-CyberRisikoChecks nach DinSpec 27076 gemeinsam mit IT-Sicherheitsunternehmen weitere Standards und Hilfen zur IT-Sicherheit zu entwickeln.

    - **Sensibilisierung in Unternehmen stärken:** Der dringend notwendige Knowhow-Aufbau in Unternehmen muss durch zielgerichtete Sensibilisierungs- und Selbsthilfe-Angebote unterstützt werden wie z. B. durch die Vermittlung technischer Standards, Angebote zu anerkannten Musterunterlagen (z. B. Checklisten, IT-Notfallpläne), Gütesiegel für Weiterbildungsangebote (z. B. DSiN-Digitalführerschein) oder durch Gamification-Ansätze.

    - **Informieren zu Schwachstellen:** Staatliche Stellen informieren zielgerichtet und schnell über gefährliche Schwachstellen und geben Hinweise auf Handlungsoptionen. Die bereits vorhandenen positiven Ansätze des BSI und die direkten Warnhinweise an einzelne besonders gefährdete Firmen durch Sicherheitsbehörden müssen ausgebaut werden.

- **Verlässliche Anbieter, Dienstleister und Produkte kennzeichnen:**
  Unternehmen stehen bei der Auswahl geeigneter IT-Anbieter und IT-Dienstleister vor einem heterogenen Markt. Sie suchen in der Auswahl IT-sicherer Produkte und Dienstleistungen zuverlässige Entscheidungshilfen. Anwender wünschen sich oft ein robustes „Basispaket", das als sicheres IT-System im geschäftlichen Alltag eingesetzt werden kann. Hierfür ist die stärkere Etablierung einer Kennzeichnung notwendig: Der Ansatz des BSI-Sicherheitskennzeichens sollte analog zur CE-Kennzeichnung weiterentwickelt werden. Das beinhaltet eine Selbsterklärung der Hersteller, die gesetzlichen IT-Sicherheitsanforderungen zu erfüllen, die Kennzeichnung der Produkte sowie mögliche Prüfmechanismen durch Behörden. Die Akzeptanz und Bekanntheit dieser Kennzeichnung müssen dabei deutlich gesteigert werden. Anbieter von IT-Sicherheits-Lösungen sollen leichter auffindbar sein. Erste Ansätze hierfür gibt es mit der APT-Liste des BSI und der DinSpec 27076. Zur Sicherstellung der Qualifizierung von IT-Sicherheitsdienstleistern sollen Möglichkeiten für einen Befähigungsnachweis oder Sachkundeprüfung ausgebaut werden.

Ökosystem für innovative IT-Sicherheitsprodukte und -Services stärken

Die Entwicklung digitaler Technologien – auch für Cyberattacken – schreitet rasant voran. Um nicht den internationalen Anschluss zu verlieren, sondern mit eigenen Mitteln für innovativen Cyberschutz und damit für eine gewisse digitale Souveränität zu sorgen, braucht es ein starkes, innovatives Ökosystem für IT-Sicherheit.
Maßnahmen hierfür sind:

- **Forschungstransfer verbessern:**
  Die fortschreitende technische Entwicklung schafft kontinuierlich neue Wertschöpfungsmöglichkeiten. Deutschland zählt weltweit zu den führenden Nationen in der IT-Sicherheitsforschung. Es mangelt jedoch oft an der Produktumsetzung sowie am Wissenstransfer zu kleinen und mittelständischen Unternehmen. Entscheidend ist, Forschungsergebnisse in marktfähige Produkte für die IT-Sicherheit umzusetzen - auch in Kooperation mit mittelständischen Unternehmen.
  Maßnahmen hierfür sollten verstärkte Vermittlung von Entrepreneurship-Knowhow in der Wissenschaft und mehr Kooperationen mit der Wirtschaft, vor allem kleinen und mittleren Unternehmen, sein.
  Die Forschungsförderung muss die Produktentwicklung mit in den Fokus nehmen, z. B. durch stärkere Einbindung von Unternehmen.

- **Innovationspotenzial von Startups stärken:**
  Compliance und Finanzierung sind für Startups wesentliche Herausforderungen:
  Die Finanzierungsmöglichkeiten für Startups müssen verbessert werden, z. B. durch großvolumige Venture-Capital Fonds oder eine attraktive steuerliche Behandlung von Investitionen in sie (z. B. für Mitarbeiter). Das gilt insbesondere beim Übergang aus der Frühphase (z. B. Ende Exist-Gründerstipendium) in die Unternehmensphase.
  Strenge und umfangreiche Complianceanforderungen führen dazu, den Standort Deutschland und EU für Startups unattraktiv zu machen: Daher müssen alle Regulierungen (z. B. AI Act, NIS2, CRA) so gestaltet sein, dass sie Startups genügend Spielraum für die Entwicklung lassen.
  Die öffentliche Hand sollte das Innovationspotenzial von Startups bei Vergabeverfahren besser nutzen können.

- **Entwicklung von Schlüsseltechnologien zur IT-Sicherheit vorantreiben:**
  Technologische Weiterentwicklungen wie z. B. KI befördern Cyberangriffe, ermöglichen aber auch bessere Abwehr. Hier dürfen wir nicht ins Hintertreffen geraten. Der Staat soll die Produktentwicklung von IT-Sicherheits-Schlüsseltechnologien (z. B. IoT, KI, Blockchain, Quantencomputing) durch stärkeres Engagement in Initiativen wie der Agentur für Sprunginnovationen unterstützen. Der Staat beauftragt die Entwicklung von innovativen Anwendungen und setzt neue Entwicklungen als Pilotnutzer selbst ein.

- **Faire Marktchancen für EU-Anbieter sicherstellen:**
  IKT-Hersteller werden durch Regulierung, z. B. durch den Cyber Resilience Act in der Produkthaftung, stärker in die Verantwortung genommen. Dies muss so erfolgen, dass EU-Anbieter keine Wettbewerbsnachteile gegenüber Nicht-EU-Anbietern haben.

- **IT-Sicherheit in Open Source unterstützen:**
  Open Source-Software bildet die Grundlage nahezu sämtlicher Softwareprogramme. Beispielsweise laufen über 60% aller Websites auf der Open Source WordPress. Manche sehr zentrale Bibliotheken werden allerdings nur von sehr kleinen Communities, manchmal nur von Einzelpersonen getragen. Mehrfach wurden weitreichende Schwachstellen (z. B. Log4j, Heartbleed, xz-lib) in zentralen Open Source-Bibliotheken entdeckt, die fast das gesamte Internet betrafen. Deshalb ist es nötig, die Open Source Community aktiv und verstärkt hinsichtlich IT-Sicherheit zu unterstützen, z. B. über Initiativen wie der „Sovereign Tech Fund" oder der „PrototypeFund", die Open-Source-Ökosysteme im öffentlichen Interesse unterstützen. Auch Projekte wie die „Codeanalyse von Open Source Software" (CAOS 3.0) des BSI zusammen mit Sicherheitsfirmen können Open Source sicherer machen.

Gemeinsam IT-Sicherheitsbedrohungen entgegentreten

Die IT-Sicherheit von Unternehmen, öffentlichen Einrichtungen und Privatpersonen wird von anderen Staaten und Kriminellen bedroht. In nationaler und internationaler Zusammenarbeit müssen staatliche und private Einrichtungen noch stärker kooperieren und gemeinsam daran arbeiten, diese Bedrohung zu minimieren.
Maßnahmen hierfür sind:

- **Schlagkraft der Sicherheitsbehörden erhöhen:**
  Unternehmen brauchen kompetente und handlungsfähige Ansprechpartner und Schutz vor Kriminellen. Zur Unterstützung von Unternehmen sowie der Abwehr und Aufklärung von Cyberkriminalität sollten die Sicherheitsbehörden technisch und personell ausreichend ausgestattet werden. Spezialeinheiten sollten über föderale Ebenen hinweg und behördenübergreifend zusammenarbeiten, z. B. mit der Bundeswehr, um wirkungsvoller und effizienter Cyberbedrohungen entgegentreten zu können. Massive Cyberangriffe erfordern klare Zuständigkeiten und schnelle Koordination zwischen Bund und Ländern.

- **Ethische Schwachstellenforschung legalisieren:**
  Nach §202 StGB (sog. „Hackerparagraph") laufen IT-Sicherheitsunternehmen und IT-Sicherheitsforscher Gefahr, bei der Meldung von Schwachstellen kriminalisiert zu werden. Die Folge ist, dass IT-Sicherheitsforscher ggf. Betroffene nicht auf Schwachstellen hinweisen. Daher muss das Identifizieren von Schwachstellen, welche in der Absicht, dies den Betroffenen zu melden und damit vor Gefahren zu bewahren, legalisiert werden. Nach dem Vorbild der Niederlande sollten durch einen festgelegten „Coordinated-Vulnerability-Disclosure (CVD)-Prozess" für Melder von Schwachstellen und Betroffene klare Schritte zur Zusammenarbeit an die Hand gegeben werden.

- **Mit IT-Sicherheitslücken verantwortungsbewusst umgehen:**
  Grundsätzlich müssen alle Anstrengungen unternommen werden, bekannt gewordene Schwachstellen möglichst schnell zu schließen. Nur in außergewöhnlichen Fällen nationaler Sicherheit dürfen Schwachstellen temporär geheim gehalten werden. Der CVD-Prozess dafür muss klar und verbindlich definiert sein.

- **Austausch aller Betroffenen fördern – Lagebild und Nutzen verbessern:**
  Ein umfassendes Lagebild der IT-Sicherheit ist ein wesentlicher Schlüssel für mehr Sicherheit für Staat, Wirtschaft und Gesellschaft. Auf dieser Basis können Gegenmaßnahmen schnell eingeleitet und das Sicherheitsniveau insgesamt erhöht werden. Hierzu müssen IT-Sicherheits-Informationen zwischen allen Akteuren ausgetauscht, die Qualität von Lageinformationen verbessert und neue Datenquellen erschlossen werden. Aktuell beruhen die Lageinformationen insbesondere aus verpflichtenden Meldungen zu IT-Sicherheitsvorfällen, Strafanzeigen sowie Regelungen der NIS2- und DSGVO-Umsetzung. Ergänzend könnten auch Daten von abgewehrten Angriffen einbezogen werden, um Angriffsmuster frühzeitig zu erkennen und entsprechende Gegenmaßnahmen zeitnah einleiten zu können. Dazu ist die Zusammenarbeit staatlicher Einrichtungen mit Unternehmen nötig, insbesondere solchen, die über ein entsprechendes Monitoring verfügen (z. B. eigene CERTs).
  Die geplante Austauschplattform im Zuge der NIS2-Umsetzung soll für alle Beteiligten eine niederschwellige und einfache Möglichkeit schaffen, erfolgreich abgewehrte Angriffe zu melden.

- **Schlüsselrollen bei Cyberangriffen besser einbinden:**
  Die legalen und handelsüblichen Services von IT-Dienstleistern wie z. B. Domain-Registrare, Hosting-Anbieter oder Content Delivery Networks werden von Cyberkriminellen missbraucht und ermöglichen erst Cyberangriffe. Sie nehmen damit eine Schlüsselrolle bei Cyberangriffen ein. Staatliche Stellen sollen stärker in den Austausch mit solchen Einrichtungen in Schlüsselrollen gehen und gemeinsam Wege zur effektiveren Eindämmung von Cyberangriffen finden. Unternehmen, die solche missbrauchbare Infrastruktur anbieten, müssen wissen, wer ihre Kunden sind („Know Your Customer") und schnell reagieren, wenn ein Missbrauch belegt ist. Gleiches gilt auch für Einrichtungen, die der Abwehr von Cyberangriffen dienen wie z. B. Betreiber von IP- oder Spam-Blacklist-Servern. Besonders kritisch ist die Rolle von Internetdomains, die bei Phishing-Mails eine wesentliche Rolle spielen. Zumindest für die im eigenen Gesetzgebungsbereich befindlichen Domains (z. B. „.de" oder „.bayern") sollten besondere Qualitätsmerkmale etabliert werden, z. B. eine zuverlässige Identifizierung bei der Beantragung einer Domain. Missbrauch wie z. B. Fakeshops unter de-Domains sollten schnell abgeschaltet werden können. Hierzu könnte eine Meldemöglichkeit analog zur TKG-Lösung für Telefon-Spam eingerichtet werden. Dazu müssen staatliche Einrichtungen kurzfristig auf die in diesem Gebiet operativ tätigen Unternehmen einwirken können.

Kompetenzen für IT-Sicherheit auf allen Ebenen ausbauen

In den Unternehmen fehlen oftmals IT-Sicherheitsexpertise ebenso wie digitale Anwendungs-Kompetenzen. Dabei sind gerade Mitarbeitende trotz technischer Sicherheit ein großes Risiko für die IT-Sicherheit. Ohne entsprechendes Knowhow im Unternehmen kann ein ausreichender Cyberschutz nicht sichergestellt werden. Ziel muss sein, dass in Unternehmen alle IT-Anwendenden über grundlegendes Wissen in IT-Sicherheit und KI verfügen und ausreichend IT-Sicherheitsfachkräfte für Entwicklung wie Einsatz im Unternehmen vorhanden sind. Maßnahmen hierfür sind:

- **IT-Sicherheits-Kompetenzen in allen Phasen umfassend stärken:**
  Digitale Fähigkeiten, insbesondere zur IT-Sicherheit und KI müssen frühzeitig und umfassend in Schulen, Ausbildung, Studium und in den Betrieben vermittelt werden.

- **Neue Generation von IT-Sicherheitsfachkräften entwickeln:**
  Das Angebot spezialisierter Bildungswege zu IT-Sicherheitsfachkräften muss ausgeweitet und attraktiv gestaltet werden.
  Der Staat soll zudem mehr hochqualifizierte IT-Sicherheitsfachkräfte ausbilden. Dabei sollte er – über eine angemessene Bezahlung hinaus - seine besondere Attraktivität als Arbeitgeber in der IT-Sicherheit stärker hervorheben: Arbeitserfahrungen bei BSI, Strafverfolgungsbehörden oder Militär zielen direkt auf die nationale Sicherheit und den Schutz der Gesellschaft und können besonders lehrreich sein. Von Mitarbeitenden mit solchen Erfahrungen können auch Unternehmen anschließend profitieren.

Ansprechpartner:in

Bernhard Kux	089 5116-1705	kux@muenchen.ihk.de
Franziska Neuberger	089 5116-1260	neuberger@muenchen.ihk.de
Armin Barbalata	089 5116-1379	barbalata@muenchen.ihk.de