Bundesverband

White Paper

Handlungsfelder Cybersicherheit

Stand: 20. September 2017

Die Ausgangslage

Die deutsche Wirtschaft befindet sich mitten im Prozess der digitalen Transformation. Für den deutschen Mittelstand stellt dies teilweise eine enorme Herausforderung dar. Die Bedrohungslage hat sich trotz großer Anstrengungen seitens der Wirtschaft, der Wissenschaft und des Staates verschärft. Abwehrmaßnahmen und die Sicherheitsinformationstechnologie haben nicht Schritt gehalten mit Cyberangriffen.

Für Kriminelle wie für fremde Nachrichtendienste sind Cyberangriffe über das Internet hochattraktiv**,** da eine Vielzahl von Schwachstellen in Softwareprodukten permanent neue Ansatzpunkte für die Entwicklung von Schadprogrammen liefern.

Cybersicherheit ist ein entscheidender Erfolgsfaktor, da nur ein notwendiges Maß an Sicherheit für Anwender und Kunden Vertrauen in Digitalisierung schafft.

Daher hat sich auch das Rollenverständnis von Staat und Wirtschaft gewandelt und es ist erforderlich, dass der Staat angesichts der Bedeutung von Cybersicherheit stärkere Verantwortung in der Abwehr übernimmt, und dass gleichzeitig die Fähigkeiten der Anwender zur Selbstverteidigung durch Hilfe durch Selbsthilfe verbessert werden.

Die Handlungsfelder im Überblick

Handlungsfelder für den Staat

- Meldepflicht für kritische Schwachstellen in Software und Verpflichtung für Software-Updates sowie Haftung bei Nicht-Behebung
- Höhere staatliche Anforderungen und weitere Verpflichtungen
- Setzen klarer Leitplanken zur staatlichen Nutzung von Schwachstellen
- Stärkung internationaler politischer Zusammenarbeit zur Bekämpfung der Cyberkriminalität
- Transparenz zu Kompetenzen und Ansprechpartnern / Bessere Koordination
- Forschungsgelder wirksamer einsetzen

Handlungsfelder für die Wirtschaft

- Einführung von Grundsätzen und Standards für sichere IT-Systeme, die als Leitfaden für KMU dienen können
- Klare Trennung von Cyber Security Governance und IT-Sicherheits-Umsetzungsverantwortlichkeit
- Investitionen in die digitale Souveränität von Nationen

Gemeinsame Handlungsfelder für Staat und Wirtschaft

- Mehr Informationen teilen
- Kritische Infrastrukturen schützen
- Engere Verzahnung der Initiative Wirtschaftsschutz mit der Allianz für Cybersicherheit
- Bekanntheit der Initiativen zur Cybersicherheit erhöhen
- Gemeinsamer Radar und gemeinsame Abwehr
- Internationale Standards und Gütesiegel fördern

ASW Bundesverband | Allianz für Sicherheit in der Wirtschaft e.V.
Neue Schönhauser Straße 20 | 10178 Berlin
Telefon +49 (0)30 246 371 75 | Telefax +49 (0)30 200 77 056
info@asw-bundesverband.de | www.asw-bundesverband.de

Handlungsfelder für den Staat

Meldepflicht für kritische Schwachstellen in Software und Verpflichtung für Software-Updates sowie Haftung bei Nicht-Behebung

- Derzeit gibt es keine Haftung für fehlerhafte Software. Es sollte jedoch ein Haftungsanspruch entstehen, wenn bekannte Schwachstellen und Fehler nicht behoben werden. Wenn eine Behörde oder ein Unternehmen eine Schwachstelle erkennt, über die man in ein IT-System einbrechen könnte, sollte dies meldepflichtig sein. Aus unserer Sicht bietet sich das BSI als Meldestelle an.
- In der kommenden Legislaturperiode sollte eine Novelle des Produkthaftungsrechts erfolgen, durch die Soft- und Hardwarehersteller gesetzlich verpflichtet werden, für sicherheitskritische Schwachstellen tatsächlich auch zeitnah Sicherheits-Updates bereitzustellen und bei Unterlassung in Haftung genommen werden können.
- Ebenso müssen Hersteller verpflichtet werden, Transparenz über den jeweiligen Lebenszyklus von Software basierten Produkten zu schaffen. Produkte, deren bekannte Schwachstellen nicht vom Hersteller bereinigt wurden, müssen kenntlich gemacht werden. Ebenso sind Verfahren zu definieren, wie mit Software, die ihren End-of-Life Zeitpunkt erreicht hat, umzugehen ist. Veraltete Software, die nicht mehr unterstützt wird, bietet eine große Angriffsfläche.
- Die Haftung könnte nach folgendem Leitgedanken geregelt werden: Hersteller und Betreiber haften für unterlassene Software Updates, Verbraucher haften für nicht eingespielte Patches, Restrisiken werden über Risikogemeinschaften in Cyberversicherungen abgedeckt.

Höhere staatliche Anforderungen und weitere Verpflichtungen

- Aufgrund des volkswirtschaftlichen Schadens von geschätzten 50 Milliarden Euro pro Jahr bedarf es weiterer gesetzlicher Verpflichtungen, die über den KRITIS Sektor hinausgehen. Neben den im IT-Sicherheitsgesetz definierten Sektoren muss der Schutzbedarf in Breite und Tiefe ausgedehnt werden.
- Das Thema IT-Sicherheit hat eine überragende Bedeutung für die Volkswirtschaft und der alleinige Fokus auf die kritischen Infrastrukturen, wie es das IT-Sicherheitsgesetz vorsieht, reicht nicht mehr aus. Die bestehende Interpretation zu Existenz und Betrieb eines Risikomanagementsystems im KonTraG ist hier noch zu unkonkret, um diese Anforderungen angemessen zu erfüllen.
- Darüber hinaus muss der zunehmenden Fremdgefährdung entgegengewirkt werden (z. B. durch Botnet-Attacken mittels ungeschützter Computersysteme). Mit der wachsenden Vernetzung von Geräten im Internet der Dinge verschwimmen die Grenzen klassischer IT-Umgebungen. Es müssen Regeln entwickelt werden, die für hohe Standards bei IT-Sicherheit sorgen und die gesamte digitale Wertschöpfungskette zur Einhaltung dieser Standards verpflichtet. Dazu gehört auch, dass Hard- und Softwarehersteller Sicherheit für den gesamten Produktlebenszyklus vorwegdenken („Security by Design“) und ein entsprechend hohes Schutzniveau dauerhaft garantieren müssen.

Setzen klarer Leitplanken zur staatlichen Nutzung von Schwachstellen

- Der Aufbau der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) als zentraler technischer Unterstützer der Polizei und Nachrichtendienste wird grundsätzlich begrüßt. Generell sollte gelten, dass staatliche Stellen entsprechend angewiesen werden, bekanntgewordene Sicherheitslücken unverzüglich zu melden. Wir haben Verständnis für das Bedürfnis zur Nutzung von Schwachstellen, um Terrorismus und Kriminalität effektiv bekämpfen zu können. Daher muss dies in begrenztem

Umfang – unter Anwendung von klaren Regeln und Transparenz – ermöglicht werden. Beispielhaft könnten für die Nutzung von Lücken eine zeitliche Begrenzung oder Schwellwerte bezüglich der Anzahl bzw. der Kritikalität der betroffenen Systeme festgelegt werden.

Stärkung internationaler politischer Zusammenarbeit zur Bekämpfung der Cyberkriminalität

- Im Rahmen der Cyberaußenpolitik muss sich die Bundesregierung dafür einsetzen, dass jeder Staat seine Bemühungen zur Erhöhung der Cybersicherheit intensiviert und kritische IT-Infrastrukturen besser gegen Attacken geschützt werden sowie intensiv gegen Cyberkriminalität vorgegangen wird. Mittelfristiges Ziel muss die Verabschiedung eines verbindlichen Abkommens für verantwortliches Handeln im Cyberraum sein. Darüber hinaus bedarf es eines intensiveren Ressourcen- und Kapazitätsaufbaus im Verantwortungsbereich der Staaten, um Cyberkriminalität wirksam zu bekämpfen. Hier muss auf internationaler Ebene, über die Multi-Stakeholder-Ansätze hinaus, noch intensiver zusammengearbeitet werden.

Transparenz zu Kompetenzen und Ansprechpartnern / Bessere Koordination

- Einzelnen Unternehmen bleibt oft unklar, welche Sicherheitsbehörde mit welchen Kompetenzen ausgestattet ist, und wie die Aufgaben zwischen Bundes- und Landesämtern abgegrenzt sind. Exemplarisch hierfür sind die Doppelmeldungen an BSI und Bundesnetzagentur zu nennen, die in den verteilten Zuständigkeiten vom BMWi und BMI liegen. Da alle Behörden mit engen Ressourcen arbeiten müssen, ist eine effiziente Organisation umso wichtiger.
- Im konkreten Angriffsfall wird es gerade für KMU zunehmend von Bedeutung sein, dass auch die örtliche Polizeibehörde im Sinne eines Ersthelfers in die Lage versetzt wird, die richtigen Stellen in eine Strafverfolgung einzubeziehen. Ebenso wichtig wie eine Verstärkung der Ressourcen für die Polizeiarbeit ist die Transparenz über die Verantwortungsstrukturen bei der Bekämpfung von Cyberkriminalität.
- Notwendig ist nicht nur eine bessere Koordinierung, sondern auch eine stärkere gemeinsame Cyberabwehr der Sicherheitsbehörden im konkreten Angriffsfall auf europäischer Ebene. Schließlich treffen Cyberangriffe meist IT-Systeme in mehreren Staaten.

Forschungsgelder wirksamer machen

- Die Forschungsförderung im Bereich der Cyberabwehr führte bisher nicht zu konkreten Produktentwicklungen, die eine entsprechende Marktverbreitung in Deutschland erreichen konnten. Hier könnte sich Deutschland an Israel orientieren, wo die staatliche Förderung von Start-ups zentraler Bestandteil des Regierungsprogramms ist.
- Das BMI könnte sich hier an den Aktivitäten des BMVg zur zivilen Sicherheitsforschung orientieren.
- Positiv und weiter ausbaufähig sind die Entwicklungen der Cybersicherheitshubs in Berlin, München, Bonn und Darmstadt.

ASW Bundesverband | Allianz für Sicherheit in der Wirtschaft e.V.
Neue Schönhauser Straße 20 | 10178 Berlin
Telefon +49 (0)30 246 371 75 | Telefax +49 (0)30 200 77 056
info@asw-bundesverband.de | www.asw-bundesverband.de

Handlungsfelder für die Wirtschaft

Einführung von Grundsätzen und Standards für sichere IT-Systeme, die als Leitfaden für KMU dienen können.

Auch wenn die Sicht auf das Gesamtsystem bei der IT-Sicherheit für den Anwender Vorrang hat, bieten die folgenden Grundsätze eine Möglichkeit, IT-Systeme sicherer zu machen:

1. Sicherheit in die Designphase einbeziehen: Sicherheit sollte integraler Bestandteil jedes IT-Produktes sein.
2. Durchführung regelmäßiger Sicherheits-Updates und aktives Schwachstellenmanagement: Auch wenn die Sicherheit in der Designphase enthalten ist, können Schwachstellen in Produkten nach ihrer Bereitstellung entdeckt werden. Diese Fehler können durch Patching, Sicherheitsupdates und Strategien für die Anfälligkeitsverwaltung gemildert werden.
3. Bewährte Sicherheitspraktiken weiterentwickeln: Viele getestete Praktiken, die in der traditionellen IT- und Netzwerksicherheit verwendet werden, können als Ausgangspunkt für die IT-Sicherheit genutzt werden. Diese Ansätze können dazu beitragen, Schwachstellen oder Unregelmäßigkeiten zu erkennen, auf mögliche Zwischenfälle zu reagieren und um bei Schäden oder Störungen schnell wieder in den Betrieb zu kommen.
4. Priorisierung von Sicherheitsmaßnahmen nach potenziellen Auswirkungen: Risikomodelle unterscheiden sich in IT-Ökosystemen erheblich, ebenso die Konsequenzen von Sicherheitsvorfällen. Die Fokussierung auf die potenziellen Konsequenzen von Störungen, Verletzungen oder bösartigen Aktivitäten ist entscheidend für die Bestimmung, wo besondere Sicherheitsmaßnahmen aufgesetzt werden sollten.
5. Transparenz über IT fördern: Entwickler und Hersteller müssen ihre Supply Chain möglichst gut kennen – konkret, ob Schwachstellen bei Software- und Hardwarekomponenten von Anbietern außerhalb ihrer Organisation bestehen. Erhöhte Sensibilisierung kann ferner dazu beitragen, dass Hersteller und industrielle Anwender identifizieren, wo und wie man Sicherheitsmaßnahmen anwendet oder Redundanzen aufbaut.
6. Bewusste Netzanbindung: IT-Anwender, vor allem im industriellen Kontext, sollten bewusst darüber nachdenken, ob bei der Verwendung eines IT-Geräts und den damit verbundenen Risiken eine kontinuierliche Konnektivität erforderlich ist, bzw. in welcher Form eigene Kommunikations- und IT-Infrastrukturen aufzubauen sind. IT- und Kommunikationssystemen sind dabei ganzheitlich zu betrachten.

Klare Trennung von Cyber Security Governance und IT-Sicherheits-Umsetzungsverantwortlichkeit

- Es bedarf einer klaren Trennung und eines Vieraugenprinzips zwischen den strategischen, risikobasierten Vorgaben zur Cybersicherheit und der operativen Umsetzung. Darüber hinaus ermöglicht eine funktionale Trennung des IT-Sicherheitsbeauftragten weg vom CIO mehr Transparenz.
- Eine Zusammenführung der IT-Sicherheit mit der Konzernsicherheit könnte eine 360°-Betrachtung von Sicherheitsrisiken ermöglichen.

Investitionen in die digitale Souveränität von Nationen

- Mit der zunehmenden Digitalisierung unserer Gesellschaft und Wirtschaft gewinnt die digitale Souveränität von Nationen an Relevanz. Diese Souveränität ermöglicht es uns, eigene Produkte zu entwickeln und eigenständig Entscheidungen bezüglich der Einführung von Produkten vom globalen Markt zu treffen.
- Um dies zu ermöglichen ist es notwendig, dass Konzerne in die Forschung und Entwicklung von Cybersicherheitslösungen in Deutschland investieren. In diesem Prozess könnte das BSI als Gutachter auftreten, und Startups bekämen Vorteile bei nationalen Ausschreibungen.
- Für international agierende DAX-Unternehmen ist es wichtig, auch international zu investieren. Eine stärkere Finanzierung in Deutschland würde jedoch einen Markt für innovative Cybersicherheitslösungen schaffen. Die Förderung von Venture Capital Fonds, die mit privaten Finanzmitteln ausgestattet sind und zusätzlich von einer Unterstützung durch Wissenschaft und Staat profitieren, ist hier ein Lösungsansatz.

ASW Bundesverband | Allianz für Sicherheit in der Wirtschaft e.V.
Neue Schönhauser Straße 20 | 10178 Berlin
Telefon +49 (0)30 246 371 75 | Telefax +49 (0)30 200 77 056
info@asw-bundesverband.de | www.asw-bundesverband.de

Gemeinsame Handlungsfelder für Staat und Wirtschaft

Mehr Informationen teilen

- Der öffentliche Sektor und die private Wirtschaft sollten mehr Informationen über Cyberbedrohungen, Verwundbarkeit und Konsequenzen teilen. Durch zentral deutlich leichter zur Verfügung stehende Expertise kann nicht nur die Geschwindigkeit, sondern auch die Qualität einer angemessenen Reaktion erhöht werden. Dazu gehört auch, Ängste abzulegen und zuzugeben, dass man angegriffen wurde.

Kritische Infrastrukturen schützen

- Mit dem IT-Sicherheitsgesetz und der Implementierung der Anforderungen aus der NIS-Richtlinie wurde ein erster Rahmen zur Festlegung von Sicherheitsstandards im Bereich der kritischen Infrastrukturen geschaffen. Im Zuge der fortschreitenden Digitalisierung unserer Gesellschaft und Wirtschaft reicht dieser Rahmen nicht aus und ist entsprechend zu erweitern.
- Perspektivisch müssen alle Wertschöpfungspartner entlang der Cybersicherheitswertschöpfungskette entsprechend ihrer Verantwortung für die Gewährleistung von IT-Sicherheit verpflichtet werden – dies betrifft im besonderen Maße Hard- und Softwarehersteller.
- Durch erweiterte Befugnisse für Internet Service Provider (ISP) können Angriffe auch in der Infrastruktur besser bekämpft werden. Insbesondere in Bezug auf DDoS Angriffe können separate Service Anbieter ein überlagertes, sichereres Netzwerk erzeugen. Security sollte damit im ISP-Bereich als Standard gelten und nicht als optionaler Zusatzservice.

Engere Verzahnung der Initiative Wirtschaftsschutz mit der Allianz für Cybersicherheit

- Wir sehen eine Konvergenz von realen und Cyberangriffen. Die Angriffe gehen vielfach von ungestörten Rückzugsräumen aus dem Ausland aus – häufig auch mit einem korrespondierenden Innentäter innerhalb des Unternehmens. Reine IT-Sicherheit reicht daher nicht aus.
- Ein wichtiger Schritt wäre die Angleichung der Anmeldeprozeduren der beiden Initiativen für deren Informationsportale.

Bekanntheit der Initiativen zur Cybersicherheit erhöhen

- Der Allianz für Cybersicherheit, der Initiative IT-Sicherheit in der Wirtschaft und insbesondere der Initiative Wirtschaftsschutz fehlen es an Bekanntheit und Reichweite. Gerade bei KMU muss die Wahrnehmung weiter gestärkt werden. Eine bundesweite Awareness Kampagne könnte hier die nötige Aufmerksamkeit erzielen.

Gemeinsamer Radar und gemeinsame Abwehr

- Die Computer Emergency Response Teams (CERT) sind ein entscheidendes Element zur konkreten Gefahrenabwehr. Das BSI hat hier schon erfolgreich den CERT Verbund aufgebaut. Weitere CERTs müssen in der Wirtschaft noch zusätzlich eingerichtet werden, insbesondere bei KMU. Bei diesen sind mangelnde Ressourcen jedoch oftmals ein Hinderungsgrund. Eine mögliche Lösung wäre, dass lizensierte IT-Dienstleister diese Aufgaben übernehmen. Erfolgreiche Public-Private-Partnership-Modelle aus anderen Ländern könnten entsprechend adaptiert werden. Beispielhaft sei hier auf das südkoreanische Modell verwiesen, bei dem eine Kooperation im Bereich Incident Response zwischen staatli-

chen Ressourcen und professionellen CERTs aus der Wirtschaft erfolgt. Zur Erstellung des notwendigen Vertrauens wäre eine Akkreditierungs- und Zertifizierungslösung durch den Staat (siehe z.B. Finnland) ein denkbarer Ansatz.

- Es sollte daher über ein Rahmenwerk zur Ergänzung bzw. Erweiterung der mobilen Eingreiftruppen durch Public-Private-Partnerships nachgedacht werden. Dazu gehört dann auch die Einbindung der Wirtschaft in das Nationale Cyber-Abwehrzentrum und ein Konzept zur gemeinsamen Incident Response von Staat und Wirtschaft. Als weiteres Beispiel kann die US National Cyber-Forensics & Training Alliance genannt werden, wo staatliche und privatwirtschaftliche Akteure gemeinsam an der Aufklärung von Cyberattacken und an der Analyse von Tatwerkzeugen arbeiten.
- Bei der Aufklärung von Cyberangriffen sind die Parameter „Information“ und „Zeit“ kritische Faktoren: Um die Effizienz des Cyberrisikomanagements in den Wirtschaftssektoren zu verbessern, ist ein über den nationalen Fokus hinausgehend global-interoperables Lagebild anzustreben. Ein solches „Informationsaustauschkonzept“ kann und sollte unter der Federführung von beispielsweise der OECD und mit einem klaren Wirtschaftsfokus aufgebaut werden.

Internationale Standards und Gütesiegel

- Regierungsstellen, Sicherheitsbehörden und Wirtschaft müssen mit internationalen Partnern kooperieren, um die Entwicklung internationaler Standards zu unterstützen und sicherzustellen. Auch wenn global eine Standardisierung schwer umsetzbar scheint, sind freiwillige nationale Möglichkeiten analog zum „Blauen Umweltengel“ überprüfenswert.
- Der ASW Bundesverband begrüßt das Vorhaben der Bundesregierung (Federführung BMI, unter der Beteiligung von BMWi und BMJV), im Pilotprojekt IT-Sicherheitskennzeichnung von Routern an der Einführung eines Gütesiegels für IT-Sicherheit zu arbeiten.
- Der Verband sieht aber auch die Notwendigkeit, dass auf EU-Ebene Rahmenbedingungen für verbindliche IT-Sicherheitseigenschaften von internetfähigen Produkten geschaffen werden. Die EU Kommission plant Cyber- und Datensicherheitsmaßnahmen, um mit der europäischen Industrie bessere Lösungen zur Abwehr von Cybergefahren zu entwickeln. Ziel ist ein einheitlicher europäischer Markt für Cybersicherheit. Aus dem EU-Haushalt soll dies mit 450 Millionen Euro gefördert werden. Auch hier sind Investitionen der Wirtschaft notwendig. Deshalb soll es im Fall eines Cyberangriffs künftig einen Notfall-Fonds geben, der betroffenen EU-Staaten unbürokratisch hilft.

ASW Bundesverband | Allianz für Sicherheit in der Wirtschaft e.V.
Neue Schönhauser Straße 20 | 10178 Berlin
Telefon +49 (0)30 246 371 75 | Telefax +49 (0)30 200 77 056
info@asw-bundesverband.de | www.asw-bundesverband.de