The Software Alliance

BSA

EU Cybersecurity Dashboard

Cybersicherheit in Europa - der Weg zu einem sicheren virtuellen Raum in Europa

galexia

CONTENTS

EXECUTIVE SUMMARY

Die moderne vernetzte Welt verspricht unermesslich viel. Technologien sind heute ein integraler Bestandteil in fast allen Bereichen der Weltwirtschaft: im Banken- und Finanzwesen, in der Kommunikationsbranche oder im Energiesektor. Doch die Vorteile, die uns diese Technologien bieten können, sind bedroht.

Immer mehr Angreifer verfügen über immer raffiniertere Methoden, um das Versprechen der technologisch vernetzten Welt auszuhöhlen. Sie nutzen die Schwachstellen aus, indem sie Daten stehlen, Systeme erheblich stören oder gar vernichten. Mit wachsenden technischen Vorteilen nehmen auch die Bedrohungen zu. Um diesen Gefahren entgegenzutreten und die Abwehrbereitschaft unserer Cybersysteme zu sichern, ist Flexibilität, aber auch Entwicklungsfähigkeit gefragt.

Regierungen schützen sich vor Cyberangriffen, verringern im Falle eines Angriffs den Schaden und wirken den neu entstehenden Bedrohungen entgegen, indem sie Richtlinien zur Cybersicherheit einführen und anwenden. Drei Elemente sollten sich in diesen Richtlinien widerspiegeln: die geeigneten rechtlichen und politischen Rahmenbedingungen, die Beiträge der Öffentlichkeit und eine Infrastruktur zur Umsetzung der Rahmenwerke.

Gesetze, Regelungen, Institutionen und eine geeignete Struktur zur einfacheren Zusammenarbeit mit allen relevanten Interessensvertretern gelten als wichtigste Grundlage zur Unterstützung der Länder. Aber auch nichtstaatliche Institutionen sollten ihre Systeme schützen und dadurch Cyberangriffe verhindern oder abfedern beziehungsweise entsprechend auf Attacken reagieren können.

Diese politischen und rechtlichen Rahmenbedingungen sowie die geeigneten Umsetzungsstrukturen müssen stabil und klar definiert, dabei aber auch flexibel sein. Die Rahmenwerke müssen die Gefahren berücksichtigen, mit denen Technologien behaftet sind, und an neue Bedrohungen angepasst werden können.

Mit dem vorliegenden Bericht BSA EU Cybersecurity Dashboard, dem ersten seiner Art, sollen Regierungsbeamte in allen EU-Mitgliedsstaaten die Möglichkeit erhalten, die Richtlinien des jeweiligen Landes anhand von bestimmten Kennzahlen zu bewerten und mit ihren Nachbarstaaten in Europa zu vergleichen.

Die wichtigsten Ergebnisse aus dem Bericht lassen sich wie folgt zusammenfassen:

- Die meisten EU-Mitgliedsstaaten sind sich darüber im Klaren, dass die Themen Cybersicherheit und Cyberresilienz und vor allem der Schutz der kritischen Infrastrukturen, eine wichtige nationale Priorität darstellt.
- Unter den Mitgliedsstaaten bestehen erhebliche Unterschiede bei den Cybersicherheitsrichtlinien, Rechtsrahmen und operativen Kapazitäten, die europaweit zu erheblichen Lücken in der Cybersicherheit führen.
- Obwohl die 27 EU-Mitgliedsstaaten operative Einheiten wie beispielsweise Computer Emergency Response Teams (CERTs) eingerichtet haben, sind deren Ziele und Erfahrungswerte sehr unterschiedlich.
- Deutliche Diskrepanzen bestehen zudem in der mangelnden systematischen Zusammenarbeit mit nichtstaatlichen Einrichtungen und öffentlich-privaten Partnerschaften: Lediglich in fünf EU-Mitgliedsstaaten findet sich eine etablierte Struktur für derartige Partnerschaften. Damit besteht noch viel Raum für eine effektive und freiwillige Zusammenarbeit zwischen staatlichen Stellen und dem Privatsektor, der über die meisten kommerziellen und kritischen Infrastrukturdienste in Europa verfügt und diese auch betreibt.

Neben diesem Bericht stehen die Untersuchungsergebnisse online detailliert unter www.bsa.org/EUcybersecurity zur Verfügung.

- Das Ziel, einen kohärenten Ansatz und gemeinsame Ausgangsniveaus bei der Cybersicherheit in der EU zu erreichen, erfordert erhebliche Anstrengungen. Die Richtlinie zur Netz- und Informationssicherheit (NIS) und deren Umsetzung bietet die Chance, dass sich die EU-Mitgliedsstaaten auf den Schutz der kritischsten Dienste und Ressourcen konzentrieren. Damit nimmt die NIS-Richtlinie eine Schlüsselrolle in dem Vorhaben ein, die Cybersicherheitslücke in Europa zu schließen.

Der diesjährige Bericht beleuchtet einige grundlegende Aufgaben sowie wichtige Möglichkeiten zur Verbesserung der Cybersicherheit in der EU. Könnten die EU-Mitgliedsstaaten ihren Cybersicherheitsansatz anpassen und ihre Kapazitäten auf ein vergleichbares und kohärentes Ausgangsniveau bringen, wäre ein großer Schritt zur Umsetzung eines echten digitalen Binnenmarktes in der EU getan.

Cybersicherheit und Cyberresilienz gelten häufig als finanziell nicht machbare Herausforderungen, obwohl es sich primär um eine Verwaltungsaufgabe handelt. Die wesentlichen Schritte zur Steigerung der Cybersicherheit und Cyberresilienz aller EU-Mitgliedsstaaten sind die Einführung der geeigneten Richtlinien, der rechtlichen und operativen Rahmenbedingungen, die Verbesserung der Zusammenarbeit mit unterschiedlichen Interessensvertretern sowie der effiziente Austausch von Cybersicherheitsinformationen und die Priorisierung des Schutzes der kritischen Infrastrukturen.

Neben diesem Bericht stehen die Untersuchungsergebnisse online detailliert unter www.bsa.org/EUcybersecurity zur Verfügung.

Im gleichen Maße, in dem sich der Bereich der Cybersicherheit permanent verändert, soll auch dieser Bericht ein lebendiges Dokument darstellen. Während die Regierungen der EU-Mitgliedsstaaten und die Entscheidungsträger ihre Rahmenbedingungen aktualisieren, um Lücken zu schließen, wird auch diese Website ständig aktualisiert, um die Fortschritte in den betreffenden Bereichen aufzuzeigen. Wir laden Sie dazu ein, die Ergebnisse zu sichten und die BSA | The Software Alliance zu kontaktieren, wenn Sie Informationen zu relevanten Änderungen haben.

METHODOLOGIE

Die Studie basiert auf 25 Kriterien in fünf Themenbereichen (siehe Resultate, Seiten 8 bis 9). Jedes Kriterium wird entweder mit "ja", "nein", "teilweise" oder "nicht zutreffend" beantwortet. Die vorliegende Studie enthält keine Gesamtbewertungen oder Auswertungen.

Die Analyse ergibt sich aus der Sekundärforschung über öffentlich zugängliche Informationen und umfasst keine direkt durchgeführten Interviews mit den nationalen Behörden. Soweit möglich, wurden Links auf Zusatzinformationen und Quellen angegeben. Diese sind auf unserer Homepage verfügbar.

Die Untersuchung wurde zum 1. Januar 2015 abgeschlossen. Allgemeine Informationen in diesem Bericht sind bis zu diesem Stichtag korrekt widergegeben.

Detaillierte Informationen über die angewandte Methode können Sie auf unserer Webseite www.bsa.org/EUcybersecurity einsehen.

BAUSTEINE FÜR EINEN SOLIDEN RECHTSRAHMEN FÜR CYBERSICHERHEIT

Solide Rechtsgrundlagen schaffen

Regierungen sollten umfassende rechtliche und politische Rahmenbedingungen auf der Grundlage einer soliden nationalen Cybersicherheitsstrategie schaffen und diese darüber hinaus permanent aktualisieren. Die Rahmenbedingungen sollten auf den nachstehenden Grundsätzen aufbauen.

- **Risikoabhängig und auf Prioritäten ausgerichtet:** Cyberbedrohungen treten in vielen unterschiedlichen Formen und Größen sowie Schweregraden auf. Die Definition von Prioritäten gründet auf einer objektiven Risikobewertung, wobei kritische Ressourcen beziehungsweise kritische Sektoren die höchste Priorität erhalten. Damit wird ein effektiver Ausgangspunkt geschaffen und sicherstellt, dass die Cybersicherheitsmaßnahmen auf die Bereiche fokussiert sind, in denen das Schadenspotenzial am höchsten ist.
- **Technologieneutral:** Ein technologisch neutraler Cybersicherheitsansatz ist von entscheidender Bedeutung. Damit wird gewährleistet, dass die sichersten und effektivsten am Markt verfügbaren Lösungen eingesetzt werden. Spezielle Anforderungen oder Richtlinien, die eine Verwendung einer bestimmten Technologie bedingen, untergraben hingegen die Sicherheit, indem sie neu entstehende Sicherheitsmaßnahmen und Best-Practice-Verfahren einschränken und dadurch Fehlerquellen entstehen können.
- **Praktikabel:** Eine Strategie ist nur dann wirksam, wenn sie für möglichst alle Ressourcen und von möglichst allen kritischen Akteuren befolgt wird. Eine unverhältnismäßige und belastende Überwachung der privaten Betreiber durch staatliche Stellen oder Beeinträchtigungen der operativen Verwaltung von Cybersicherheitsrisiken durch die Aufsichtsbehörden erweisen sich sehr häufig als kontraproduktiv. Sie entziehen effektiven und anpassungsfähigen Sicherheitsmechanismen lediglich Ressourcen, die für fragmentierte Verwaltungsvorschriften eingesetzt werden müssen.
- **Flexibel:** Die Bewältigung von Cyberrisiken sollte fachübergreifend erfolgen; einen One-Size-fits-all-Ansatz gibt es allerdings nicht. Jede Branche, jedes System und Unternehmen ist mit unterschiedlichen Herausforderungen konfrontiert. Daher ist Flexibilität gefragt, um den individuellen Anforderungen gerecht zu werden.
- **Datenschutz und Bürgerrechte respektieren:** Sicherheitsvorschriften sollten den Datenschutz und Bürgerrechte berücksichtigen. Dabei ist sicherzustellen, dass die Forderungen und Verpflichtungen in einem angemessenen Verhältnis zueinander stehen, nicht mehr als unbedingt notwendig in die Grundrechte eingreifen, rechtsstaatlichen Prinzipien unterliegen und unter angemessener gerichtlicher Aufsicht stehen. Diese wichtigen Aspekte sollten in jedes Rahmenwerk für Cybersicherheit integriert sein.

Operative Einheiten mit Verantwortung für die Sicherheit einrichten

Regierungen sollten operative Einheiten etablieren, um Cybersicherheitsvorfälle zu verhindern und die entsprechende Reaktion auf derartige Vorfälle zu gewährleisten. Eine Kernkomponente ist der Aufbau eines operativen Teams, das zuständig ist für die Computersicherheit, Notfälle und die Reaktion auf Vorfälle.

Vertrauen aufbauen und die Zusammenarbeit im Rahmen von Partnerschaften fördern

Kein einzelnes Land und keine einzelne Regierung sind in der Lage, die Cybersicherheitsrisiken isoliert zu bekämpfen. Die Zusammenarbeit mit nichtstaatlichen Stellen und internationalen Partnern und Verbündeten gilt daher als wesentliche Komponente für einen effektiven Cybersicherheitsansatz.

- **Partnerschaften mit dem Privatsektor:** Die meisten Infrastrukturen werden vom Privatsektor betrieben. Aus diesem Grund sind wirksame öffentlich-private Kooperationen von wesentlicher Bedeutung. Die Zusammenarbeit verbessert zudem die Wirksamkeit des Risikomanagements durch Optimierung des Austauschs von Informationen, Erfahrungen und Meinungen aus den verschiedensten Quellen. Besondere Anstrengungen sind erforderlich, um das Vertrauen zu fördern sowie rechtliche Hindernisse, die den Aufbau von Vertrauen behindern, aus dem Weg zu räumen.
- **Global anstatt isoliert:** Aufgrund der Tatsache, dass Bedrohungen global stattfinden, müssen wirksame Richtlinien und Strategien zur Cybersicherheit international ausgerichtet sein und auf dem gemeinsamen Engagement von Partnern und Verbündeten aufbauen. Zudem sollten internationale, freiwillige und marktgerechte Standards eingeführt werden, um den überregionalen und globalen Informationsaustausch und den Schutz der Informationen zu maximieren.

Aufklärungsmaßnahmen und Bewusstseinsbildung über Cybersicherheitsrisiken fördern

Menschen, Prozesse und Technologien sind für die Gewährleistung der Cybersicherheit gleichermaßen wichtig. Denn auch die beste Technologie wird wirkungslos, wenn sie nicht richtig angewendet wird. Eine gesteigerte Bewusstseinsbildung, Aufklärungsmaßnahmen und Schulungen über klar definierte Prioritäten der Cybersicherheit, Grundsätze, Richtlinien, Verfahren und Programme sind essentielle Komponenten jeder Cybersicherheitsstrategie.

WESENTLICHE UNTERSUCHUNGSERGEBNISSE

Die neuesten, gravierenden Vorfälle im Bereich der Cybersicherheit belegen erneut die entscheidende Bedeutung, die eine Stärkung der Cyberresilienz im Allgemeinen sowie der Schutz der kritischen Infrastruktur vor Cyberbedrohungen im speziellen, sowohl in Europa als auch weltweit hat. Um diese Ziele zu erreichen, sind öffentliche und private Akteure dazu aufgerufen, sich mit den Kapazitäten auszustatten, die zu einer effektiven Vermeidung, Verringerung und zur entsprechenden Reaktion auf Cyberangriffe und -vorfälle führen.

Mit zunehmendem Fokus auf die Verbesserung der Cyberresilienz in den EU-Mitgliedsstaaten und auf EU-Ebene soll mit dem vorliegenden Bericht BSA EU Cybersecurity Dashboard, dem ersten seiner Art, ein umfassender Überblick über den Stand der aktuellen Rahmenbedingungen und Ressourcen für Cybersicherheit gegeben werden.

Der Bericht untersucht die fünf nachstehenden Schlüsselbereiche zum Thema Cybersicherheit in den EU-Mitgliedstaaten:

- Rechtsgrundlagen für Cybersicherheit
- Operative Kapazitäten
- Öffentlich-private Partnerschaften
- Branchenspezifische Programme zur Cybersicherheit
- Aufklärungsmaßnahmen

RECHTSGRUNDLAGEN

Die Politik nimmt eine Schlüsselrolle ein, wenn es darum geht, sowohl öffentliche Einrichtungen als auch Privatunternehmen so auszurüsten, dass sie sich den Herausforderungen der Cybersicherheit in einer immer stärker vernetzten Welt stellen können. Erreicht werden kann dies nicht nur durch Etablierung von geeigneten rechtlichen und politischen Rahmenbedingungen, sondern auch durch Förderung der Sensibilität für das Thema Cybersicherheit und die Zusammenarbeit mit verschiedenen Interessensvertretern, die an der Umsetzung der Cyberresilienz beteiligt sind.

Nationale Cybersicherheitsstrategien sind eine wichtige Komponente und in vielerlei Hinsicht das Fundament für diese Rahmenbedingungen. Sie sind entscheidend für die Bewältigung von Cybergefahren auf nationaler Ebene und die Entwicklung von geeigneten Rechtsvorschriften zur Unterstützung der entsprechenden Aktivitäten. Eine starke Cybersicherheitsstrategie sollte wie ein "lebendiges Dokument" sein, das in Zusammenarbeit mit den wichtigsten öffentlichen und privaten Interessensvertreter entwickelt und umgesetzt wird. Dabei sollten klar definierte Grundsätze und Prioritäten enthalten sein, die gesellschaftliche Werte, Traditionen und Rechtsgrundsätze widerspiegeln.

In dieser Hinsicht besteht die Notwendigkeit für eine weitere Verbesserung innerhalb der EU. Denn lediglich 19 der 28 EU-Mitgliedsstaaten nutzen mehr oder weniger detaillierte und umfassende Cybersicherheitsstrategien und acht EU-Mitgliedsstaaten verfügen über keinerlei Regelwerk. Auch in den Ländern, in denen Cybersicherheitsstrategien zur Anwendung kommen, variiert deren Qualität; viele Strategien sind vage und abstrakt und klare Umsetzungspläne fehlen.

Zudem sind die meisten Dokumente über die Cybersicherheitsstrategien statisch, denn nur eine geringe Anzahl der EU-Mitgliedsstaaten hat ihre anfänglichen Strategien bereits überarbeitet und verbessert sowie Aktualisierungen herausgegeben. Darüber hinaus hat nur eine Minderheit der EU-Mitgliedsstaaten ihre Cybersicherheitsstrategie durch entsprechende rechtliche und politische Instrumente gestärkt, anhand deren die Sicherheit, Verpflichtungen zur Informationsklassifizierung und Anforderungen zum Schutz von kritischen Informationsinfrastrukturen geregelt werden.

Auch Regierungen sollten Bewertungen durchführen und klare Prioritäten für die kritischen Dienste und Infrastrukturen schaffen, die primär geschützt werden müssen. Nicht alle Ressourcen, Systeme, Netzwerke, Daten und Dienste sind gleichermaßen wichtig. Entsprechend ausschlaggebend ist es, dass Entscheider die

Thomas Boué, Director of Policy EMEA der BSA: Die Politik spielt eine Schlüsselrolle, wenn es darum geht, sowohl öffentliche Einrichtungen als auch Privatunternehmen so auszurüsten, dass sie sich den Herausforderungen der Cybersicherheit in einer immer stärker vernetzten Welt stellen können.

Infrastruktur des Landes auf der Grundlage objektiver Kriterien und der Kommentierung durch die Öffentlichkeit bewerten und die Infrastrukturen definieren, auf denen die kritischen Dienste und Funktionen betrieben werden, deren Gefährdung, Beschädigung oder Zerstörung durch einen Cybersicherheitsvorfall von nationaler Bedeutung sein könnte.

Die Ergebnisse dieser Studie belegen, dass mehr als die Hälfte der EU-Mitgliedsstaaten diesen Evaluierungsprozess noch nicht durchlaufen hat und auch keine Strategie oder Programm nutzt, um ihre wichtigsten Ressourcen zu schützen.

Sobald diese kritischen Infrastrukturen ermittelt sind, muss deren Cyberresilienz bewertet werden, um Schwachstellen und Lücken zu identifizieren und entsprechend darauf zu reagieren.

Best-Practice-Verfahren, die im Privatsektor entwickelt wurden, umfassen häufig systematische interne Prüfungen sowie Prüfungen durch Dritte, um die Cyberresilienz der kritischen Systeme zu testen. Diese Vorgehensweise ist für den öffentlichen Sektor gleichermaßen nützlich. Dennoch hat die Studie ergeben, dass die meisten EU-Mitgliedsstaaten und öffentlichen Verwaltungen keine Best-Practice-Verfahren anwenden.

Ferner ist es aufgrund der immer lauter werdenden Forderung nach einer Meldepflicht für Cyberattacken wichtig zu beachten, dass die meisten europäischen Länder derartige Programme nur zögerlich einführen und viele die **formelle oder informelle Zusammenarbeit mit dem Privatsektor bevorzugen. Viele Länder befürchten, dass eine Meldepflicht für Cyberattacken** weniger effektiv sein könnte als der Informationsaustausch auf der Grundlage von gegenseitigem Vertrauen und kontinuierlicher Zusammenarbeit.

Falls tatsächlich eine Meldepflicht eingeführt werden sollte, sind sich die meisten EU-Mitgliedsstaaten einig, dass nur Vorfälle mit erheblichen Auswirkungen oder einem ernsthaften Schadensrisiko unter die Verpflichtung fallen sollten.

Der Austausch von cybersicherheitsrelevanten Informationen ist zweifelsohne ein wichtiger Aspekt für ein wirksames Vorgehen beim Thema Cyberresilienz, da davon sowohl öffentliche als auch private Interessensvertreter profitieren. Der Grund liegt darin, dass das Kollektivbewusstsein gesteigert wird und dadurch alle Interessensvertreter ihre Sicherheitsrichtlinien an die Entwicklung der Bedrohungslandschaft anpassen können.

Der wirksame Informationsaustausch erfordert allerdings den Schutz der Informationen, und daher sind entsprechende Vorgaben für die Klassifizierung von Informationen entscheidend. Dies wird von fast allen EU-Mitgliedsstaaten anerkannt und die meisten nutzen bereits derartige Klassifizierungsvorgaben.

Zudem sollten die Regierungen den Informationsaustausch erleichtern, indem sie die Bildung von öffentlich-privaten Partnerschaften und die branchenspezifische Zusammenarbeit (siehe unten) unterstützen. Sie sollten die erforderlichen personellen und technischen Ressourcen bereitstellen, für operative Einheiten und den gesetzlichen Schutz vor Kartellansprüchen, unangemessenen Offenlegungsvorschriften oder Verpflichtungen sorgen. Zudem sollten alle anderen politischen und rechtlichen Hindernisse identifiziert werden, die einen Informationsaustausch behindern könnten und die entsprechende Reaktion darauf erfolgen.

OPERATIVE EINHEITEN

Um auf die kritischsten und wesentlichen Vorfälle optimal zu reagieren, sollte eine Vorgehensweise definiert werden. Dabei handelt es sich um Vorfälle, die die Vertraulichkeit, Integrität oder Verfügbarkeit von wichtigen Informationsnetzwerken und Informationssystemen des Landes bedrohen. Computer Emergency Response Teams (CERTs) und Computer Security Incident Response Teams (CSIRTs) spielen eine entscheidende Rolle bei der Verbesserung der Widerstandsfähigkeit gegen Cyberangriffe.

Diese Teams reagieren auf Vorfälle und bieten Opfern von Angriffen entsprechende Dienste; leiten Informationen über Schwachstellen und Bedrohungen an die wichtigen Interessensvertreter in der Regierung, dem Privatsektor und in einigen Fällen auch an die Öffentlichkeit weiter und zeigen Methoden auf, wie die Computer- und Netzwerksicherheit verbessert werden kann.

Thomas Boué, Director of Policy EMEA der BSA: Effektive Partnerschaften zwischen dem öffentlichen und privaten Sektor sind umso wichtiger, da viele kritische Infrastrukturen, auf die wir uns tagtäglich verlassen, von nichtstaatlichen Organisationen verwaltet und betrieben werden. Beispielsweise das Transport- und Gesundheitswesen oder der Banken- und Energiesektor.

Angesichts dieser wichtigen Funktion ist es als positiv zu werten, dass die meisten EU-Mitgliedsstaaten über operative CERTs verfügen. Lediglich Zypern und Irland stehen noch vor der Aufgabe, ihre CERTs voll funktionsfähig zu machen.

Darüber hinaus haben die meisten Länder auch zuständige nationale Behörden für die Netzwerk- und Informationssicherheit eingerichtet.

ÖFFENTLICH-PRIVATE PARTNERSCHAFTEN

Die Kultur der Cybersicherheit erfordert gemeinsame Anstrengungen und die Koordinierung aller Interessensvertreter auf nationaler Ebene. Effektive Partnerschaften zwischen dem öffentlichen und privaten Sektor sind umso wichtiger, da viele kritische Infrastrukturen von nichtstaatlichen Organisationen verwaltet und betrieben werden, auf die wir uns tagtäglich verlassen, wie beispielsweise das Transport- und Gesundheitswesen oder der Banken- und Energiesektor.

Obwohl die Bedeutung der Zusammenarbeit in Europa außer Frage steht, gibt es bei diesem Thema viele unterschiedliche nationale Ansätze und Fortschrittsgrade. Fünf Länder, Österreich, Deutschland, die Niederlande, Spanien und das Vereinigte Königreich, sind hier Vorreiter. Diese Länder etablierten bereits formelle öffentlich-private Partnerschaften für Cybersicherheit.

Andererseits sind in der Mehrheit der EU-Mitgliedsstaaten öffentlich-private Partnerschaften im Bereich der Cybersicherheit entweder überhaupt nicht vorhanden, nur sehr beschränkt existent oder befinden sich noch in einem sehr frühen Entwicklungsstadium.

BRANCHENSPEZIFISCHE CYBERSICHERHEITSPROGRAMME

Während bestimmte Elemente der Cybersicherheit für alle Branchen gelten und Empfehlungen von nationalen und internationalen Organisationen zur Verfügung stehen, besteht auch ein Bedarf nach Leitlinien, die auf die Geschäftsanforderungen von bestimmten Organisationen ausgerichtet sind oder Methoden bereitstellen, um Risiken oder spezifische Vorgänge aufzugreifen, die für bestimme Sektoren gelten.

Hinzu kommt, dass die praktischen Umsetzungswege in den EU-Mitgliedsstaaten noch verhältnismäßig begrenzt sind - obwohl das Interesse am Aufbau von branchenspezifischen Reaktionen zunimmt. Die Länder, die Vorreiter sind bei der Umsetzung von öffentlich-privaten Partnerschaften und häufig branchenspezifische Dialoge und den Informationsaustausch mit dem Privatsektor führen, sind auch in diesem Bereich tonangebend. Entsprechende Maßnahmen können dazu führen, die geeignetsten und wirksamsten Leitlinien für die einzelnen Sektoren zu bestimmen.

AUFKLÄRUNGSMASSNAHMEN

Der Cyberraum kann aber weder von einzelnen Unternehmen noch von mehreren Interessensvertretern alleine gesichert werden; vielmehr trägt jeder Verantwortung für die Cybersicherheit. Nicht nur Regierungen und Organisation jeder Größenordnung, sondern auch Verbraucher müssen Maßnahmen ergreifen, um die Sicherheit der eigenen Systeme zu erhöhen. Aufklärungsmaßnahmen und die Steigerung der Bewusstseinsbildung spielen zusätzlich eine wichtige Rolle.

Dafür erforderlich sind aufklärende und bewusstseinsbildende Kampagnen sowie die Entwicklung und generelle Durchführung von Schulungen über Cybersicherheit an Universitäten und im Rahmen von vorausgehenden Ausbildungen.

Die Europäische Union hat sich für die Aufklärung und Bewusstseinsbildung rund um das Thema Cybersicherheit ausgesprochen und wird ihrem Engagement gerecht. So findet beispielsweise jeden Oktober europaweit der European Cyber Security Month statt, an dem sich die meisten EU-Mitgliedsstaaten beteiligen.

Demgegenüber müssen einige Länder, darunter Griechenland, Malta, Portugal und Slowenien ihre nationalen Strategien in diesem Bereich noch grundsätzlich entwickeln.

STOLPERSTEINE AUF DEM WEG ZU EINER ECHTEN SICHERHEIT

In einigen Staaten nehmen Regierungen Cybersicherheitsaspekte als Rechtfertigung für verschiedene Richtlinien, die weit über das hinausgehen, was für Sicherheitsbelange nötig ist. Tatsächlich untergraben derartige Richtlinien häufiger die Cybersicherheit als sie diese verbessern. Zudem schaffen sie, ob beabsichtigt oder nicht, unfaire Marktzugangsbeschränkungen gegenüber Herstellern und Diensteanbietern weltweit.

Unnötige und unvernünftige Forderungen vermeiden

Eine angemessene Cybersicherheitspolitik ermöglicht Organisationen die Entwicklung und den Einsatz einer möglichst großen Auswahl an innovativen Cybersicherheitslösungen. Damit können Unternehmen auch genau die Sicherheitsmaßnahmen ergreifen, die zur Verringerung der für sie relevanten Risiken am wirksamsten sind.

Stattdessen stellen einige Regierungen verschiedenste Forderungen auf, anhand deren sie die Auswahl einschränken, Kosten steigern und die Möglichkeiten verringern, dass Firmen im eigenen Land die am besten geeigneten Cybersicherheitswerkzeuge nutzen. Dazu gehören unter anderem länderspezifische Zertifizierungsbedingungen, lokale Testanforderungen; Vorschriften über die heimische Herstellung; Anforderungen zur Offenlegung von sensiblen Daten wie Quellcodes und Verschlüsselungsschlüssel; sowie Beschränkungen hinsichtlich ausländischen Haltern von Rechten an geistigem Eigentum.

Manipulation von Standards vermeiden

Technologiestandards spielen eine wichtige Rolle bei der Umsetzung und Verbesserung der Cybersicherheit. Durch die Unterstützung von international anerkannten technischen Standards, die mit Beteiligung der Branche entwickelt und marktübergreifend akzeptiert werden, können Unternehmen schneller neue und sicherere Produkte entwickeln und vertreiben.

Trotzdem haben einige Regierungen landesspezifische Standards eingeführt und argumentieren, dass nationale Regelungen zu erhöhter Cybersicherheit führen. Das Gegenteil ist jedoch der Fall. Standards, die von Regierungen auferlegt werden, stärken nicht die Sicherheit, sondern lassen die Innovationskraft erstarren und zwingen Verbraucher und Unternehmen dazu, Produkte zu verwenden, die möglicherweise ihren Anforderungen nicht gerecht werden.

Regelungen zur Datenlokalisierung vermeiden

Aufgrund der Zunahme der globalen Cloud-Computing-Dienste nutzen Unternehmen weltweit unabhängig von ihrer Größe leistungsstarke Ressourcen, die früher großen Konzernen vorbehalten waren. Das Cloud-Modell basiert auf Netzwerken, die eine Speicherung und Verarbeitung von Daten an mehreren Orten und sogar in mehreren Ländern ermöglichen. Da Daten ungehindert zwischen mehreren Märkten bewegt werden, bieten Cloud-Anbieter zahlreiche Vorteile wie Zuverlässigkeit, Abwehrbereitschaft und 24 Stunden Service-Support.

Aufgrund der Fehlannahme, dass Daten an einem bestimmten Ort sicherer sind, erlassen einige Länder Regelungen, die den grenzüberschreitenden Datentransfer untersagen oder wesentlich erschweren. Richtlinien, die den freien Datenfluss unnötigerweise beschränken, untergraben die Vorteile von Cloud Computing, indem sie die Kosten steigern und den Zugang zu neuen Cloud-Diensten gefährden.

Einheimische Technologien nicht bevorzugen

Innovative Produkte und Dienste entstehen durch die globale Zusammenarbeit der Forschungs- und Designzentren in vielen unterschiedlichen Ländern. Länder sollten daher Anreize für die grenzüberschreitende Zusammenarbeit schaffen und so den freiwilligen Technologietransfer und die schnelle Entwicklung und Bereitstellung von verbesserten Produkten und Diensten erleichtern.

In einigen Ländern wird allerdings der entgegengesetzte Weg eingeschlagen. Dort geht man davon aus, dass man die "Champions" im eigenen Lande durch Abschottung der ausländischen Konkurrenz schützen kann, im Land eine eigene Technologiebranche aufbauen und die Cybersicherheit so erhöhen kann. Per Definition sind einheimische Technologien eine Untergruppe der globalen Innovationen. Die Abschottung vom internationalen Wettbewerb senkt die Cybersicherheit, da Firmen und Agenturen daran gehindert werden, weltweit erstklassige Produkte und Dienste zu nutzen. Zudem beraubt eine derartige Politik die Technologiefirmen im Land der wertvollen Möglichkeit zur Zusammenarbeit mit den weltweiten Marktführern, nimmt in Kauf, dass die eigenen Firmen international weniger wettbewerbsfähig sind und schadet damit der globalen Innovationskraft.

CYBERSECURITY MATURITY DASHBOARD DER EUROPÄISCHEN UNION (2015)

✔ Ja ✖ Nein ◑ Teilweise

#	QUESTION	Belgien	Bulgarien	Dänemark	Deutschland	Estland	Finnland	Frankreich	Griechenland	Irland
	RECHTSGRUNDLAGEN									
1.	Besteht eine nationale Cybersicherheitsstrategie?	✔	✖	✖	✔	✔	✔	✔	✖	✖
2.	In welchem Jahr wurde die nationale Cybersicherheitsstrategie eingeführt?	2012	–	–	2011	2014	2013	2011	–	–
3.	Wird eine Strategie oder ein Programm zum Schutz kritischer Infrastrukturen angewandt?	◑	◑	✖	✔	✔	✔	✖	✔	✖
4.	Gibt es Gesetze/Richtlinien, welche die Ausarbeitung eines schriftlichen Informationssicherheitsprogramms erforderlich machen?	✖	✖	◑	✖	✔	◑	✖	◑	✖
5.	Gibt es Gesetze/Richtlinien, die eine Bestandsaufnahme der "Systeme" und die Klassifizierung der Daten erforderlich machen?	✔	✔	✔	✔	✔	✔	✔	✔	✖
6.	Gibt es Gesetze/Richtlinien, die es erforderlich machen, dass Sicherheitsverfahren/Sicherheitsanforderungen entsprechenden Risikostufen zugeordnet werden?	✔	✔	✔	✔	✔	✔	✔	✖	✖
7.	Gibt es Gesetze/Richtlinien, die vorsehen, dass eine Überprüfung der Cybersicherheit (mindestens) einmal pro Jahr durchgeführt wird?	✖	✖	✖	Entwurf	✔	✔	✖	✖	✖
8.	Gibt es Gesetze/Richtlinien, die vorsehen, dass ein öffentlicher Bericht über die Kapazitäten der Regierung im Bereich Cybersicherheit erstellt wird?	✖	✖	✖	Entwurf	✔	✔	✖	✖	✖
9.	Gibt es Gesetze/Richtlinien, die vorsehen, dass jede Behörde einen Chief Information Officer (CIO) oder einen Chief Security Officer (CSO) beschäftigen muss?	✖	✖	✖	✖	✖	✖	✔	✖	✖
10.	Gibt es Gesetze/Richtlinien, die eine Meldepflicht im Falle von Cybersicherheitsvorfällen vorsehen?	◑	✖	✖	✔	✔	✖	✖	✖	✖
11.	Umfassen Gesetze/Richtlinien eine ausreichende Definition des Begriffs "Schutz kritischer Infrastrukturen"?	✔	✔	✔	✔	✔	✔	✖	✔	✖
12.	Basieren die Anforderungen für die Beschaffung von Cybersicherheitslösungen im öffentlichen und privaten Bereich auf internationalen Akkreditierungs- bzw. Zertifizierungsprogrammen, ohne zusätzliche lokale Anforderungen zu berücksichtigen?	◑	Nicht zutreffend	✔	✔	✔	✔	◑	✔	Nicht zutreffend
	OPERATIVE EINHEITEN									
1.	Wurde ein nationales Computer Emergency Response Team (CERT) oder ein Computer Security Incident Response Team (CSIRT) eingerichtet?	✔	✔	✔	✔	✔	✔	✔	✔	◑
2.	In welchem Jahr wurde das Computer Emergency Response Team (CERT) eingerichtet?	2008	2008	2009	2012	2008	2014	2008	2009	–
3.	Gibt es eine zuständige nationale Behörde für die Netzwerk- und Informationssicherheit (NIS)?	✔	✔	✔	✔	✔	✔	✔	✔	✖
4.	Wurde eine Plattform für Berichte über Vorfälle eingerichtet, auf der Daten über Cybersicherheitsvorfälle erfasst werden?	✔	✔	✔	✔	✔	✔	✔	✔	✖
5.	Werden nationale Cybersicherheitsübungen durchgeführt?	✔	✔	✔	✔	✔	✔	✔	✔	✔
6.	Ist eine nationale Vorfallmanagementstruktur vorhanden, um auf Cybersicherheitsvorfälle reagieren zu können?	✖	◑	◑	✖	◑	✖	✖	✖	✖
	ÖFFENTLICH-PRIVATE PARTNERSCHAFTEN									
1.	Besteht eine klar definierte öffentlich-private Partnerschaft im Bereich Cybersicherheit?	◑	◑	✖	✔	◑	◑	✖	✖	✖
2.	Ist die Branche organisiert (z.B. im Rahmen eines Cybersicherheitsrates, der mit Unternehmens- oder Branchenvertretern besetzt ist)?	✔	◑	✔	✔	◑	✔	✖	✖	✔
3.	Sind neue öffentlich-private Partnerschaften geplant oder werden bereits etabliert (wenn ja, in welchen Schwerpunktbereichen)?	–	✖	✖	✔	✖	✖	◑	✖	✖
	SEKTORSPEZIFISCHE CYBERSSICHERHEITSPROGRAMME									
1.	Gibt es gemeinsame öffentlich-private Branchen-Programme im Bereich Cybersicherheit?	✖	✖	✖	✖	✖	◑	✔	✖	✖
2.	Wurden branchenspezifische Sicherheitsprioritäten definiert?	✖	✖	✖	✖	✖	✖	✖	✖	✖
3.	Wurden branchenspezifische Bewertungen der Cybersicherheitsrisiken durchgeführt?	✖	✖	✖	✖	✖	✖	✖	✖	✖
	AUFKLÄRUNGSMASSNAHMEN									
1.	Ist eine Aufklärungsstrategie vorhanden, welche die Kenntnisse und das Bewusstsein über die Cybersicherheit der Öffentlichkeit und auch der jungen Nutzer verbessert?	◑	◑	✖	◑	✔	✔	✔	✖	◑

Italien	Kroatien	Lettland	Litauen	Luxemburg	Malta	Niederlande	Österreich	Polen	Portugal	Rumänien	Schweden	Slowakei	Slowenien	Spanien	Tschechische Republik	Ungarn	Vereinigtes Königreich	Zypern
✔	✖	✔	✔	✔	✖	✔	✔	✔	Entwurf	✔	✖	✔	✖	✔	✔	✔	✔	✔
2014	–	2014	2011	2013	–	2013	2013	2013	–	2013	–	2008	–	2013	2011	2013	2011	2013
✔	✖	✖	◑	✖	◑	✔	✔	✔	✖	✔	✔	✔	✔	✔	✔	◑	✔	✖
✖	✖	✖	✖	✖	◑	◑	✖	✖	✖	✖	✔	◑	✖	✖	✔	✔	◑	✖
✔	✔	✔	✔	◑	◑	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	◑
✔	✔	✔	✔	✖	✖	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✖
✖	✖	✔	◑	◑	◑	◑	✔	✖	◑	✖	✖	✖	◑	◑	◑	✖	✖	✖
✔	◑	✖	◑	✖	✖	✔	◑	✖	◑	✖	✖	◑	✖	✖	✔	✔	◑	✖
✖	✖	✔	✖	✖	✖	✖	✖	✖	✖	✖	✔	✖	✖	✖	✖	✖	✖	✖
✖	✖	✔	✔	✖	✔	✖	✖	✔	✖	◑	✖	✖	✔	✖	✔	✖	✖	✔
✔	✖	✔	✔	✔	✔	✔	✔	✔	✖	✔	✔	✔	✔	✔	✔	✔	✔	✖
✔	Nicht zutreffend	◑	◑	◑	Nicht zutreffend	✔	✔	◑	Nicht zutreffend	◑	✔	✖	Nicht zutreffend	✔	◑	✔	◑	Nicht zutreffend
✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✖
2014	2009	2006	2006	2011	2002	2012	2008	2008	2008	2011	2003	2009	2010	2008	2011	2013	2014	–
✔	✔	✔	✔	◑	✔	◑	◑	◑	✔	✔	✔	✔	✔	✔	✔	✔	✔	◑
✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✖
✔	◑	✔	◑	◑	◑	✔	✔	◑	◑	◑	✔	✔	◑	◑	◑	◑	✔	◑
✔	✖	✔	◑	◑	✖	✔	✔	✔	◑	◑	◑	✖	✖	✔	✔	✔	✔	✖
◑	◑	✖	✖	✖	◑	✔	✔	✖	◑	✖	◑	✖	✖	✔	✖	◑	✔	◑
◑	✖	✖	◑	✖	✖	✔	✔	◑	✖	◑	◑	◑	◑	✔	✖	◑	✔	✖
◑	✖	◑	◑	◑	✖	–	✔	✖	✖	✔	✖	✖	✖	–	◑	✖	–	✖
✖	◑	✖	✖	✖	✖	✔	✔	✖	✖	✖	✖	✖	✖	✔	✖	◑	✔	◑
✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	◑	✖	✖	◑	✖
✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✔	✖	✖	✖
✔	✖	✔	✔	✔	✖	✔	✔	✔	✖	✔	✖	✔	✖	✔	✔	✔	✔	✖

ENTWICKLUNG EINES GEEIGNTEN RAHMENWERKS FÜR DEN SINNVOLLEN INFORMATIONSAUSTAUSCH

Cybersicherheitsvorfälle und Verletzungen der Cybersicherheit können sich drastisch auf Regierungen, Privatunternehmen und Einzelpersonen auswirken. Gravierende Verletzungen der Cybersicherheit haben Regierungen weltweit dazu bewogen, die Vermeidung, Erkennung und Reaktion auf die Vorfälle zu diskutieren.

Der Austausch und die gemeinsame Nutzung der entsprechenden Informationen zum richtigen Zeitpunkt sowie koordinierte Anstrengungen der relevanten Interessensvertreter gelten als optimaler Weg, um Risiken zu verringern, zu entschärfen und auf Cybervorfälle zu reagieren.

Entsprechend lautet die zentrale Frage, wie man einen sinnvollen und effektiven Informationsaustausch zwischen den Beteiligten am besten herbeiführt. Einige Länder erwägen die Einführung von Meldepflichtsystemen. Diese Systeme allein reichen aber nicht aus, um das Problem des Kollektivbewusstseins und der Abwehrbereitschaft zu lösen. Hier hat sich der freiwillige Informationsaustausch auf Grundlage von Vertrauen als effizienteste und erfolgreichste Methode erwiesen.

Allerdings ist der sinnvolle Informationsaustausch kein einfaches Unterfangen und kann nur erreicht werden, wenn er auch gefördert wird. Grundlagen dafür sind:

- **Vertrauen schaffen:** Der Informationsaustauch und ein Vorfallmeldesystem erfordern Absicherungsmechanismen und Anreize, um wirksam zu funktionieren. Sie schaffen das Vertrauen, das für den Betrieb eines derartigen Systems erforderlich ist. Dazu zählt die Garantie, dass die Organisation sich mit dem Informationsaustausch keinen unangemessenen Forderungen aussetzt, öffentlichen Herabsetzungen, Rechtsstreitigkeiten oder Sanktionen.
- **Sicherung eines hohen Vertraulichkeitsgrads:** Angesichts der sensiblen Informationen über einen Vorfall oder eine Cyberbedrohung einer kritischen Infrastrukturen, welche ausgetauscht werden, ist zu gewährleisten, dass die Vertraulichkeit und Sicherheit der Kommunikation zwischen dem Betreiber der Infrastruktur und den Aufsichtsbehörden im Rahmen der erforderlichen Transparenz der Behörde berücksichtigt und aufrechterhalten wird.

  Dennoch kann die Information der Öffentlichkeit über einen Vorfall in einigen Fällen erforderlich sein. In diesen Fällen sollte darauf geachtet werden, dass ein intensiver Dialog zwischen den Organisationen, die Opfer eines Vorfalls geworden sind, und den Behörden stattfindet, bevor eine Offenlegung erfolgt, um die Angriffsfläche für die Attacke nicht zu vergrößern und damit die Auswirkungen des Vorfalls zu vervielfachen, Panik zu erzeugen oder eine öffentliche Demontage herbeizuführen.
- **Grundlage der Gegenseitigkeit sicherstellen:** Da der Privatsektor Eigentümer und Betreiber vieler kritischer Infrastrukturen in den EU-Mitgliedsstaaten ist, sollte der Informationsaustausch nicht als einseitige Bereitstellung der relevanten Daten durch die privaten an die öffentlichen Organisationen angesehen werden. Vielmehr sollte ein echter und gegenseitiger Informationsaustausch stattfinden, der von Vertrauen und gegenseitigem Nutzen geprägt ist.
- **Anforderungen klar und konsequent über länderspezifische Zuständigkeiten hinweg formulieren:** Da Meldepflichten umfangreiche Gebiete und Regionen umfassen, steigt die Wahrscheinlichkeit, dass sich die gesetzlichen Vorschriften widersprechen. Und da verschiedene Organisationen in mehreren Sektoren und unterschiedlichen Ländern und Regionen tätig sind, stellt die Frage, worüber, wann und an wen Meldungen zu erstatten sind, eine wichtige Herausforderung an die Compliance dar. Sollte daher ein Pflichtmeldesystem eingeführt werden, ist es zwingend erforderlich, ein größtmögliches Maß an Übereinstimmung zu erreichen, nicht nur bezüglich der verschiedenen Meldepflichten, sondern auch im Hinblick auf die verschiedenen nationalen und regionalen Anforderungen.

CYBERSICHERHEIT IN DER EUROPÄISCHEN UNION ÜBERSICHT ÜBER DIE EINZELNEN LÄNDER

Nachstehende Übersichten geben einen Überblick über die Cybersicherheit auf Grundlage der oben genannten Kriterien. Sie beschreiben die wichtigsten gesetzlichen und politischen Aspekte rund um die Cybersicherheit und die derzeit in den jeweiligen Ländern eingerichteten operativen Einheiten. Detailliertere Informationen über die in der Studie untersuchten Länder entnehmen Sie bitte den Übersichten über die einzelnen EU-Mitgliedsstaaten unter www.bsa.org/EUcybersecurity.

BELGIEN

Belgiens Cybersicherheitsstrategie wurde 2012 von der Regierung verabschiedet. Der Rechtsrahmen für Cybersicherheit in Belgien ist allerdings etwas unklar und die verfügbaren Informationen zur Umsetzung der Strategie nur begrenzt vorhanden.

Andererseits verfügt Belgien über das Computer Emergency Response Team CERT.be und eine gut ausgebaute Meldestruktur für Vorfälle im Bereich der Cybersicherheit. Zudem hat Belgien kürzlich die Eröffnung eines neuen Cybersicherheitszentrums bekanntgegeben. Das Land unterstützt aktiv öffentlich-private Partnerschaften im Rahmen von BeINIS, einer staatlichen Stelle, die intensive Verbindungen zu privaten und halbprivaten Organisationen unterhält.

BULGARIEN

Bulgarien verfügt lediglich über einen begrenzten Rechtsrahmen für Cybersicherheit und keinerlei Cybersicherheitsstrategie. Zudem fehlen formalisierte öffentlich-private Partnerschaften, obwohl zahlreiche Veranstaltungen und wissenschaftliche Diskussionen die Themen Cybersicherheit und den Schutz der kritischen Informationsinfrastruktur behandeln.

Das CERT Bulgarien ist die wichtigste Einrichtung für Cybersicherheit und Ausdruck der jüngsten Bemühungen der Regierung zur Stärkung der Cybersicherheit.

DÄNEMARK

In Dänemark wurde bislang keine nationale Cybersicherheitsstrategie beziehungsweise ein diesbezügliches Gesetz etabliert. Allerdings verabschiedete Dänemark kürzlich ein Gesetz, um ein Cybersicherheitszentrum einzurichten, das das aktuelle CERT der Regierung beaufsichtigen und anschließend ersetzen soll. Der Handlungsspielraum und die Befugnisse des neuen Zentrums müssen noch bestätigt werden. Der dänische Privatsektor hat durch den Rat für Digitale Sicherheit (Council for Digital Security) einen formellen Rahmen für eine Kooperation im Bereich der Cybersicherheit definiert.

DEUTSCHLAND

Deutschland verfügt über eine umfassende Cybersicherheitsstrategie, die 2011 eingeführt wurde und von einem starken Rechtsrahmen für Cybersicherheit ergänzt wird. Die Existenz des Bundesamts für Sicherheit in der Informationstechnik (BSI), die für die Computer- und Kommunikationssicherheit zuständige staatliche Einrichtung des Bundes, ist klarer Beleg dafür, dass man sich des Themas Cybersicherheit auf höchster Regierungsebene annimmt. Deutschland verfügt zudem über ein Netz aus CERTs. Dabei arbeitet CERT-BUND, das deutsche CERT, intensiv mit staatlichen und nichtstaatlichen CERTs zusammen.

Darüber hinaus verfügt Deutschland über starke öffentlich-private Partnerschaften. Dazu gehören die Allianz für Cybersicherheit und die öffentlich-private Kooperation UP KRITIS. Insgesamt sind Richtlinien und Rechtsrahmen auf Kooperationen ausgerichtet.

ESTLAND

Estland war 2008 eines der ersten Länder, die eine nationale Cybersicherheitsstrategie entwickelten und aktualisierte diese im Jahr 2014. Zudem verfügt Estland über ein breites Spektrum gesetzgeberischer Maßnahmen zum Thema Informationssicherheit und Cybersicherheit. Estland unterhält ferner ein bewährtes CERT, das CERT Estland, das der Behörde für Informationssysteme (Information System Authority) unterstellt ist. Darüber hinaus ist auch die Tatsache nennenswert, dass sich das Cyber Security Centre of Excellence der NATO in Estland befindet.

Obwohl in Estland keine formalisierten öffentlich-privaten Partnerschaften bestehen, arbeiten die öffentlichen Stellen intensiv mit den relevanten Organisationen des Privatsektors zusammen.

FINNLAND

Finnland veröffentlichte eine umfassende Cybersicherheitsstrategie, die ergänzt wird durch einen insgesamt starken Rechtsrahmen, der wichtige Cybersicherheitsthemen behandelt. Die für Cybersicherheit in Finnland zuständige nationale Behörde befindet sich aufgrund der Integration von zwei staatlichen CERTs und der Etablierung eines Cybersicherheitszentrums in einer Übergangsphase.

FRANKREICH

Frankreich ist stark fokussiert auf die Verteidigung und nationale Sicherheit und das Land verfügt seit 2011 über eine nationale Cybersicherheitsstrategie.
Die Nationale Behörde für die Sicherheit von Informationssystemen (ANSSI) ist fest etabliert und widmet sich der Informationssicherheit. Die Behörde ist integriert in das Computer Emergency Response Team CERT-FR.

Die Cybersicherheitsstrategie umfasst Empfehlungen für eine intensivere Kooperation mit dem Privatsektor. Diese Kooperationen sind allerdings noch nicht sehr weit fortgeschritten. ANSSI hat bereits branchenspezifische Sicherheitsmaßnahmen herausgegeben. Frankreich ist damit eines der wenigen Länder in der EU, die bei der Cybersicherheit derart zielgerichtet vorgehen.

GRIECHENLAND

Griechenland hat keine Cybersicherheitsstrategie und kein gesondertes Gesetz zur Cybersicherheit. Zudem sind der Rechtsrahmen und der institutionelle Rahmen zur Förderung der Cybersicherheit begrenzt. Das nationale Computer Emergency Response Team NCERT-GR beschränkt sich in seiner Tätigkeit auf staatliche Stellen und die Betreiber von kritischen Infrastrukturen.

Darüber hinaus bestehen in Griechenland keine wesentlichen öffentlich-privaten Partnerschaften. Die griechische Regierung verfolgt deren Etablierung beziehungsweise die intensive Zusammenarbeit mit dem Privatsektor nicht.

IRLAND

In Irland sind die rechtlichen und politischen Rahmenbedingungen im Bereich der Cybersicherheit sehr begrenzt. Derzeit wird in Irland eine Cybersicherheitsstrategie entwickelt, allerdings liegt kein klarer Zeitrahmen für die Verabschiedung oder Umsetzung vor. Irland gehört zu einem der wenigen Länder in der Europäischen Union, die kein funktionsfähiges CERT betreiben; allerdings ist Irland dabei, ein CERT einzurichten.

Obwohl keine formalisierten öffentlich-privaten Partnerschaften im Bereich der Cybersicherheit bestehen, sind irische Privatunternehmen wie beispielsweise Infosecurity Ireland in diesem Feld aktiv. Irland führte außerdem eine Reihe erfolgreicher Aufklärungskampagnen zur Cybersicherheit wie "Make IT Secure" durch. Teil dieser Kampagne war die Bereitstellung von entsprechenden Informationen online sowie eine Werbekampagne im TV.

ITALIEN

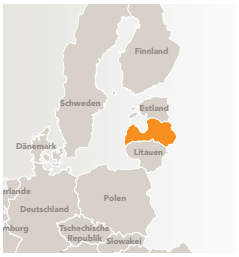
Italien aktualisierte 2007 seine Sicherheitsgesetze und führte 2013 und 2014 Cybersicherheitsprogramme ein. Damit wurde ein starker Rechtsrahmen zur Förderung der Cybersicherheit etabliert. Die italienische Cybersicherheitsstrategie fördert zudem öffentlich-private Partnerschaften; bislang bestehen allerdings noch keine formalisierten Kooperationen.

Das CERT-PA wurde 2014 eingerichtet und ist zuständig für Cybersicherheitswarnsysteme und die Koordinierung von Maßnahmen zur Reaktion auf Vorfälle bei staatlichen Stellen in Italien.

KROATIEN

Kroatien hat noch keine umfassende Cybersicherheitsstrategie beziehungsweise ein System aus öffentlich-privaten Partnerschaften eingeführt.

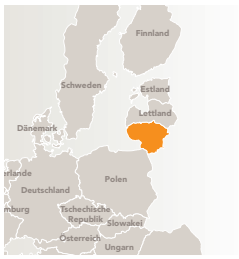
Das Land verfügt über zwei Computer Emergency Response Teams (CERTs). 2009 wurde das nationale CERT ins Leben gerufen, das verantwortlich zeichnet für die Koordinierung von Sicherheitsmaßnahmen und für Reaktionen auf Vorfälle, die bei allen Nutzern von kroatischen IP-Adressen oder der .hr-Domäne auftreten. Zudem ist das ZSIS CERT des Information Systems Security Bureau verantwortlich für die Cybersicherheit der staatlichen Stellen in Kroatien.



LETTLAND

Die 2014 veröffentlichte lettische Cybersicherheitsstrategie enthält eine Reihe von klar definierten Zielen mit konkreten Umsetzungsterminen. Lettland verfügt über einen starken Rechtsrahmen zur Förderung der Cybersicherheit. Eine wichtige Säule dieses Rechtsrahmens ist das Gesetz über Sicherheit in der Informationstechnologie, das 2010 verabschiedet wurde. Dieses Gesetz regelt die Aufgaben und Zuständigkeiten des nationalen Computer Emergency Response Teams CERT.LV.

Obwohl die Cybersicherheitsstrategie das Zustandekommen von formalisierten öffentlich-privaten Partnerschaften im Bereich der Cybersicherheit vorsieht, bestehen diese bisher noch nicht.



LITAUEN

Litauen veröffentlichte 2011 eine umfassende Cybersicherheitsstrategie, allerdings sind die Informationen über deren Umsetzung begrenzt. Das litauische Computer Emergency Response Team CERT-LT ist zuständig für alle Netzwerke in Litauen, nicht nur für die staatlichen Netzwerke. Das State Information Resources Management Council agiert als leistungsstarkes Politikgestaltungs- und Leitungsorgan.

Im Rahmen der Cybersicherheitsstrategie werden die Vorteile und die Notwendigkeit für öffentlich-private Partnerschaften herausgestellt; bislang bestehen aber noch keine formalisierten oder systematischen Kooperationen.

LUXEMBURG

In Luxemburg besteht eine relativ begrenzte, 2013 eingeführte Cybersicherheitsstrategie. Darin enthalten sind wesentliche Leitsätze, allerdings wenige Details über deren Umsetzung. Der Rechtsrahmen zur Förderung der Cybersicherheit bedarf noch einer Weiterentwicklung. Die Notwendigkeit zur Förderung von öffentlich-privaten Kooperationen wird als Grundsatz in der Cybersicherheitsstrategie erwähnt. Bislang sind aber keine formellen Kooperationen bekannt.

Luxemburg verfügt über zwei CERTs: CIRCL ist die Koordinierungsstelle, die sich mit Reaktionen auf Vorfälle befasst und zuständig ist für alle Organisationen in Luxemburg. Darüber hinaus ist GOVCERT.LU zuständig für Behörden. Die staatliche Informationssicherheitsbehörde CASES engagiert sich für die Durchführung von Aktivitäten zur Bewusstseinsbildung und Förderung von Best-Practice-Verfahren.

MALTA

Malta hat noch keinen umfassenden rechtlichen und politischen Rahmens zur Förderung der Cybersicherheit erarbeitet. Die Digital Malta Strategy und E-Government-Programme des Landes stellen allerdings die Entwicklung einer Cybersicherheitsstrategie in Aussicht.

The Malta Information Technology Agency (MITA) scheint im Bereich der Cybersicherheit aktiv zu sein. Das nationale CERT, CSIRT Malta, ist zuständig für die Koordinierung der Maßnahmen zur Reaktion auf Vorfälle und verantwortlich für Organisationen, die mit Maltas kritischer Infrastruktur betraut sind.

NIEDERLANDE

Die Niederlande verfügen über komplexe, ausgereifte rechtliche und politische Rahmenbedingungen für Cybersicherheit. Dazu gehört die 2013 eingeführte nationale Cybersicherheitsstrategie 2, die zweite Auflage der niederländischen Cybersicherheitsstrategie. Die Niederlande erneuern den Rechtsrahmen für Cybersicherheit alle zwei Jahre.

Darüber hinaus betreiben die Niederlande ein nationales Cybersicherheitszentrum, das die Aufgaben eines CERT übernimmt und sich auch als zentrale Anlaufstelle mit allen Verfahren und Praktiken im Zusammenhang mit der Cybersicherheit beschäftigt. Das Zentrum beteiligt sich auch aktiv an den Tätigkeiten der Information Sharing and Analysis Centres (ISACs) und ist für die Branchen zuständig, die mit kritischen Infrastrukturen beschäftigt sind.

ÖSTERREICH

Die österreichische Cybersicherheitsstrategie wurde 2013 eingeführt und ist Bestandteil einer umfassenden IKT-Sicherheitsinitiative der österreichischen Regierung, die im Rahmen der österreichischen IKT-Sicherheitsstrategie 2012 festgelegt wurde. Die Strategie umfasst ein umfangreiches Programm, das Cybersicherheitsziele in organisierte Aufgabengebiete verwandelt.

In Österreich wurde das Computer Emergency Response Team CERT.at eingerichtet, das über einen breiten und definierten Aktionsradius verfügt. Zudem bestehen einige öffentlich-private Partnerschaften im Bereich Cybersicherheit, beispielsweise das Zentrum für Sicherheitsinformationstechnologie Österreich (A-SIT) und das Kuratorium Sicheres Österreich.

Die Austrian Trust Circles bieten formelle Strukturen für den branchenspezifischen Informationsaustauch hinsichtlich kritischer Informationsinfrastrukturen in verschiedenen Branchen. Diese Plattformen sind mit der Entwicklung von branchenspezifischen Risikomanagementprogrammen beauftragt. Die Austrian Trust Circles sind eine Initiative der CERT.at und des österreichischen Bundeskanzleramts.

POLEN

Polen verfügt über eine umfassende Cybersicherheitsstrategie mit klaren Zielsetzungen. Die Strategie wurde 2013 eingeführt. Die meisten Vorschläge befinden sich daher noch in der Umsetzungsphase. Der Rechtsrahmen für Cybersicherheit ist noch nicht vollständig ausgebildet.

Polen betreibt mehrere CERTs, darunter CERT.GOV.PL, das zuständig ist für staatliche Stellen und kritische Infrastrukturen. Es agiert auch als Cybersicherheitsbehörde. CERT Polska ist ein akademisches CERT, das halboffiziell verantwortlich ist für das gesamte .pl-Netzwerk.

PORTUGAL

In Portugal bestehen bislang keine umfassenden rechtlichen und politischen Rahmenbedingungen für Cybersicherheit. Zudem wurde noch keine Cybersicherheitsstrategie erarbeitet. Formalisierte öffentlich-private Kooperationen sind nicht vorhanden.

Das Land betreibt allerdings das nationale CERT mit der Bezeichnung CERT-PT sowie ein nationales Cybersicherheitszentrum. Dieses Zentrum wurde von der nationalen Sicherheitsbehörde ins Leben gerufen und ist beauftragt, bei Cybersicherheitsvorfälle mit dem Privatsektor zusammenzuarbeiten.

RUMÄNIEN

Die 2013 in Rumänien eingeführte Cybersicherheitsstrategie ist relativ vage formuliert. Der Rechtsrahmen ist begrenzt, obwohl dem Parlament bereits Gesetzesvorlagen zur Annahme unterbreitet wurden. CERT-RO ist das nationale Computer Emergency Response Team und für alle Benutzer der rumänischen Netzwerke zuständig. Zudem wird im Rahmen der rumänischen Cybersicherheitsstrategie die Etablierung von zwei weiteren Cybersicherheitsbehörden angestrebt.

SCHWEDEN

In Schweden besteht noch keine nationale Cybersicherheitsstrategie. Allerdings wird derzeit eine Strategie entwickelt. Das Land hat bislang kein Gesetz speziell für den Bereich Cybersicherheit eingeführt.

Schweden hat jedoch mit CERT-SE ein funktionierendes CERT eingerichtet, in dessen Zuständigkeitsbereich alle schwedischen Netzwerke fallen. Desweiteren genießt Schweden aufgrund der Arbeit der schwedischen Zivilschutzorganisation (Civil Contingencies Agency, MSB) in punkto Cybersicherheit eine gute Reputation. Sie ist eine nationale Behörde und für Informationssicherheit zuständig. Die MSG ist die zentrale Informationssicherheitsbehörde in Schweden und in der Öffentlichkeit sehr präsent.

SLOWAKEI

Die Slowakei führte 2009 seine erste fünfjährige Cybersicherheitsstrategie ein. Details über die neue Strategie für 2014 bis 2020 sind nur begrenzt vorhanden. Die Slowakei verfügt über ein CERT, das sogenannte CSIRT.SK, das sich auf staatliche Stellen und Betreiber von kritischen Infrastrukturen konzentriert. Öffentlich-private Partnerschaften im Bereich der Cybersicherheit sind nicht vorhanden.

SLOWENIEN

Slowenien hat noch keinen umfassenden rechtlichen und politischen Rahmens zur Förderung der Cybersicherheit erarbeitet. Auch eine nationale Cybersicherheitsstrategie muss erst noch eingeführt werden. SI-CERT ist das nationale Computer Emergency Response Team in Slowenien. Das Team ist zuständig für alle slowenischen Netzwerke. Slowenien unterhält keine öffentlich-privaten Partnerschaften im Bereich der Cybersicherheit.

SPANIEN

Spanien führte seine nationale Cybersicherheitsstrategie 2013 ein. Dabei handelt es sich um eine umfassende Strategie mit festgesetzten Zielen und Vorgehensweisen. Die Strategie ist kompatibel mit dem nationalen Sicherheitsprogramm und den bestehenden Sicherheitsgesetzen; die Programme und Gesetze zur Cybersicherheit greifen ineinander.

Spanien verfügt über zwei CERTs, zum einen über das INTECO-CERT, zum anderen über das CCN-CERT sowie über das National Centre for Critical Infrastructure Protection (CNPIC). Das CNPIC ist offensichtlich die vorrangig zuständige Behörde für Informationssicherheit und Cybersicherheit. Die Aufgaben der CERTs sind hingegen auf den Umgang mit Vorfällen im Bereich der Cybersicherheit beschränkt. CNPIC ist für die Sicherstellung der Koordinierung sowie die Kooperation zwischen dem öffentlichen und privaten Sektor verantwortlich. Das Zentrum unterhält branchenübergreifende Arbeitsgruppen und entwickelt branchenspezifische Cybersicherheitsprogramme.

Zudem wird die Kooperation mit dem Privatsektor durch das National Advisory Council on Cybersecurity formalisiert. Die Mitglieder des 2009 gegründeten Gremiums sind Vertreter des Privatsektors. Obwohl der aktuelle Status etwas unklar ist, wurde das Gremium mit der politischen Beratungstätigkeit für die Regierung beauftragt. Zudem sind in Spanien privatwirtschaftliche Verbände aktiv. Dabei beschäftigen sich zwei wichtige Gremien mit allgemeinen IT-Themen und speziell mit Cybersicherheit und Informationssicherheit.

TSCHECHISCHE REPUBLIK

2011 wurde die Cybersicherheitsstrategie der Tschechischen Republik für die Jahre 2011 bis 2015 bekanntgegeben. Die Strategie umfasst allgemeine Grundsätze sowie klar definierte Ziele zur Wahrung der Cybersicherheit. Am 1. Januar 2015 wurde ein Gesetz zur Cybersicherheit in Kraft gesetzt. Das Gesetz enthält weitreichende Bestimmungen über die wesentlichen Punkte zum Thema Cybersicherheit und wird durch einige bedeutende Regelungen ergänzt.

Ferner hat die Tschechische Republik mit CSIRT.CZ ein CERT eingerichtet sowie speziell für Regierungsbehörden das CERT mit der Bezeichnung GOVCERT.CZ etabliert.

Ein nationales Cybersicherheitszentrum wurde am 1. Januar 2015 ins Leben gerufen, um öffentlich-private Partnerschaften zu fördern. Zudem führt die Tschechische Republik eine branchenbezogene Bewertung der Sicherheitsrisiken in Zusammenarbeit mit dem akademischen Bereich und dem Privatsektor durch. Das Projekt ist das erste, das sich dem Thema Cybersicherheit widmet.

UNGARN

In Ungarn wurde 2013 eine nationale Cybersicherheitsstrategie eingeführt. Die Strategie umfasst die wichtigsten Grundsätze der Cybersicherheit, einen Überblick über die aktuelle Cybersicherheitslage in Ungarn sowie die Ziele für Cybersicherheit in der Zukunft. Ungarn verfügt über einen begrenzten Rechtsrahmen für Cybersicherheit.

Verschiedene Behörden sind mit der Cybersicherheit betraut, so etwa die nationale Sicherheitsbehörde, die sich mit Informationssicherheit beschäftigt, oder das Cybersicherheitszentrum, das Bestandteil des ungarischen Nachrichtendienstes ist. Ungarn verfügt zudem über ein Computer Emergency Response Team. Die Zuständigkeit des CERT-Hungary beschränkt sich aber auf staatliche Stellen. Obwohl das nationale Cybersicherheitszentrum mit der Aufgabe der Zusammenarbeit mit dem Privatsektor betraut ist, bestehen keine formalisierten öffentlich-privaten Partnerschaften in Ungarn.

VEREINIGTES KÖNIGREICH

Im Vereinigten Königreich wurde eine umfassende Cybersicherheitsstrategie 2011 eingeführt. Ergänzt wird die Strategie von einem starken Rechtsrahmen für Cybersicherheit und zwei CERTs: Das CERT-UK unterstützt vor allem die Betreiber von kritischen Infrastrukturen; GovCertUK ist zuständig für staatliche Stellen. Weitere entsprechende Einrichtungen sind das National Security Council und das Office of Cyber Security and Information Assurance.

Das Vereinigte Königreich verfügt zudem über ein gut funktionierendes System aus öffentlich-privaten Partnerschaften, in dem sich der Privatsektor aktiv beteiligt. Der gemeinschaftliche Ansatz wird zudem intensiv durch die Cybersicherheitsstrategie des Landes unterstützt. So organisiert das Centre for the Protection of National Infrastructure (CPNI) beispielsweise den branchenspezifischen Informationsaustausch für 14 verschiedene Wirtschaftszweige.

ZYPERN

Zypern etablierte 2013 eine nationale Cybersicherheitsstrategie, die eine Verpflichtung zur Aktualisierung von wesentlichen Elementen des Rechtsrahmens für Cybersicherheit umfasst. Darüber hinaus arbeitet Zypern an der Etablierung eines nationalen CERTs, das 2015 seine Tätigkeit aufnehmen soll. Das Land verfolgt bei der Durchführung von Maßnahmen zur Cybersicherheit ein Interesse an branchenspezifischen Ansätzen mit potentiellem Fokus auf die Energie- und Finanzdienstleistungsbranche.

ÜBER BSA

BSA | The Software Alliance (www.bsa.org) ist die globale Stimme der Software-Industrie. In der BSA sind weltweit führende Unternehmen versammelt, die jährlich Milliardenbeträge in neue Softwarelösungen investieren, welche die Wirtschaft antreiben und das moderne Leben von heute prägen. Durch internationale Zusammenarbeit mit Regierungen, die Verfolgung von Urheberrechtsverletzung und breite Aufklärungsmaßnahmen arbeitet die BSA daran mit, den Horizont der digitalen Welt zu erweitern und das Vertrauen in neue Technologien zu stärken.

BSA-Website: EU: http://www.bsa.org/EU
International: http://www.bsa.org
Twitter: @BSANewsEU und @BSAnews

www.bsa.org

BSA Worldwide Headquarters

20 F Street, NW
Suite 800
Washington, DC 20001

T: +1.202.872.5500
F: +1.202.872.5501

BSA Asia-Pacific

300 Beach Road
#25-08 The Concourse
Singapur 199555

T: +65.6292.2072
F: +65.6292.6369

BSA Europe, Middle East & Africa

2 Queen Anne's Gate Buildings
Dartmouth Street
London, SW1H 9BP
Vereinigtes Königreich

T: +44.207.340.6080
F: +44.207.340.6090