STORMSHIELD

EINHALTUNG DER CYBERSECURITY FÜR TRANSPORTUNTERNEHMEN

Im Transportsektor, wo die operative Systemverfügbarkeit unabdingbar ist, kann ein Cyberangriff Menschen und der Umwelt physischen Schaden zufügen. Risiken für Personen sind Unfälle, Entgleisungen, Kontrollverlust von Containerschiffen, die einen Unfall im Hafen haben, Feuer und Kohlenstoffmonooxidvergiftung in Tunnel aufgrund fehlender Ventilation usw. Umweltrisiken können Öllecks sein, die das Wasser verschmutzen und sich auf die Tierwelt auswirken.

> EUROPÄISCHE VERORDNUNGEN: MÜSSEN EINGEHALTEN WERDEN

> OPTIONALE COMPLIANCE

> LÄNDERSPEZIFISCHE VERORDNUNGEN

> STORMSHIELD HAT FÜR JEDES PROBLEM EINE LÖSUNG

> COMPLIANCE REICHT NICHT AUS

> EUROPÄISCHE VERORDNUNGEN: MÜSSEN EINGEHALTEN WERDEN

Unternehmen im Transportwesen müssen sich an die folgenden europäischen Verordnungen zur Cybersecurity halten:

Allgemeine Datenschutz-Grundverordnung (DSGVO)

Die DSGVO ist eine EU-Verordnung für die europaweite Harmonisierung von Datenschutzrichtlinien, den Schutz und die Stärkung der EU-Bürger und ihres Rechts auf Datenschutz und die neue Umgehensweise der Unternehmen mit Datenschutz. Das führt zu neuen Einschränkungen und Anforderungen für IT- und OT-Manager, CIO und CISO.

Ein wichtiger Bestandteil dieser Anforderungen nennt sich „standardmäßiger Datenschutz“. Das bedeutet, dass personenbezogenen Daten in Systemen und Diensten standardmäßig geschützt werden. Mit den Stormshield-Produkten verbessern Unternehmen die Cyber-Belastbarkeit ihrer Infrastruktur und können diese Anforderungen somit einhalten. Außerdem stellt Stormshield Data Security auch Möglichkeiten zur Datenverschlüsselung zur Verfügung, die laut der DSGVO als geeignete technische Maßnahme für die Beibehaltung des dem Risiko angepassten Sicherheitsgrads ist.

Richtlinie für Netzwerk- und Informationssicherheit (NIS)

Die NIS-Richtlinie ist die erste EU-weite Gesetzgebung zur Cybersecurity und soll das allgemeine Niveau der Cybersecurity in der EU fördern. Sie muss in der nationalen Gesetzgebung aller Mitgliedsstaaten umgesetzt werden. Unter der NIS muss jedes Land Betreiber wesentlicher Dienste (OES) in Branchen wie Energie, Transport, Wasser, Finanzen, Gesundheitswesen und digitale Infrastruktur benennen. Benannte Betreiber wesentlicher Dienste müssen dann die Richtlinie einhalten.

Mit den zertifizierten, vertrauenswürdigen Stormshield-Produkten können die Betreiber wesentlicher Dienste Sicherheitslösungen bereitstellen, die das Schutzniveau der wesentlichen Informationssysteme (EIS) verbessern. Stormshield Network Security kann zum Beispiel Netzwerkbereiche isolieren, sicheren Fernzugriff gewährleisten, Nutzer authentifizieren und Schwachstellen verwalten. Stormshield Endpoint Security (SES) gewährt in Zusammenarbeit mit einem Antivirenprogramm (wenn vorhanden) eingehenden Schutz des Arbeitsplatzes gegen ausgefeilte Bedrohungen. SES kann auch den Schutz von Legacy-Betriebssystemen verbessern, Vorfälle entdecken und verwalten und vor Bounce-Angriffen schützen.

> EUROPÄISCHE VERORDNUNGEN: MÜSSEN EINGEHALTEN WERDEN

Payment Card Industry Data Security Standard (PCI-DSS)

Der PCI-DSS ist ein Normenkatalog für Informationssicherheit für Unternehmen, die mit Markenkreditkarten von den großen Kreditkartenunternehmen arbeiten. Jeder Händler und jede Finanzinstitution oder andere Entität, die Daten von Karteninhabern speichert, verarbeitet oder übermittelt muss diese Standards einhalten. Dazu gehören auch die Bestimmungen für die Netzwerksicherheit, Datenverschlüsselung, Schwachstellenmanagement und gute Zugangskontrolle.

Mit den Stormshield-Produkten können Unternehmen die meisten wichtigen PCI-DSS-Anforderungen erfüllen. Stormshield Network Security (SNS) kann zum Beispiel Netzwerkbereiche isolieren, ausgehenden Verkehr verschlüsseln, Schwachstellen verwalten und Nutzer authentifizieren. Stormshield Data Security (SDS) verschlüsselt die Daten der Karteninhaber, um die Integrität und Vertraulichkeit der Daten zu gewährleisten. Stormshield Endpoint Security (SES) stärkt in Zusammenarbeit mit einem Antivirenprogramm den Schutz des Arbeitsplatzes gegen hochentwickelte Bedrohungen. SES kann auch den Schutz von Legacy-Betriebssystemen verbessern, Vorfälle entdecken und verwalten und vor Bounce-Angriffen schützen.

Richtlinie zur Wiederverwendung von Information des öffentlichen Sektors (PSI)

Die PSI-Richtlinie schafft einen gemeinsam Rechtsrahmen, der die EU-Mitgliedsstaaten dazu auffordert, so viele Informationen des öffentlichen Sektors wie möglich für die Wiederverwendung offenzulegen. Die PSI-Richtlinie betrifft alle Informationen, die die öffentlichen Organe erstellen, erfassen oder kaufen. Die PSI-Richtlinie und ihre Umsetzung in den nationalen Gesetzgebungen der Mitgliedsstaaten ist die Grundlage für die offene Datenpolitik der EU. Alle Unternehmen, die öffentliche Information verwalten oder Daten aus öffentlich finanzierten Forschungsprojekten generieren, müssen diese Daten in gewissem Umfang öffentlich machen.

Mithilfe der Stormshield-Produkte können Unternehmen die PSI-Richtlinie einfacher umsetzen. Vor allem Stormshield Network Security (SNS) ermöglicht die Mikro-Segmentierung des Netzwerks, sodass der Speicherbereich für öffentliche Daten isoliert werden kann. Mit seiner intuitiven Sicherheitspolitik erleichtert SNS die Identifikation von Netzwerkbereichen, den Zugriff per Nutzer und Gruppe und die zeitlichen Beschränkungen der Institutionen.

> EUROPÄISCHE VERORDNUNGEN: MÜSSEN EINGEHALTEN WERDEN

IEC 62443

Der Standard ISA-99/IEC 62443 wurde von der International Society of Automation ins Leben gerufen. Er ist der weltweite Standard für industrielle Kontrollsysteme (ICS) und behandelt die wachsende Anzahl an Cyberbedrohungen. Mithilfe dieses Standards können Unternehmen die digitale Sicherheit ihrer Prozesse und Kontrollsysteme, wie DCS, PLC, SCADA usw. verbessern. Der Standard wurde von der Serie ISO/IEC 27000 abgeleitet und an die industriellen Kontrollsysteme angepasst.

Die Verbesserung der Cybersecurity erfolgt in mehreren Schritten. Dazu gehören Governance, Sicherheit, Politik und Organisation. Die äußerst vertrauenswürdigen Lösungen von Stormshield, die über die Zertifizierung EU Restricted verfügen, können Unternehmen dabei helfen, sich selbst vor Cyberbedrohungen zu schützen.

Stormshield Network Security (SNS) kann beispielsweise Netzwerkbereiche isolieren, PLC-Befehle kontrollieren und Wartungszugang aus der Ferne sicherstellen. Außerdem gewährt Stormshield Endpoint Security (SES) in Zusammenarbeit mit einem Antivirenprogramm (wenn vorhanden) eingehenden Schutz des Arbeitsplatzes gegen ausgefeilte Bedrohungen. SES kann auch den Schutz von Legacy-Betriebssystemen verbessern, Vorfälle entdecken und verwalten und vor Bounce-Angriffen schützen.

Cybersecurity Act

Die europäische Verordnung Cybersecurity Act ist die Antwort auf die wachsende Bedrohung durch Cyberangriffe. Sie verstärkt die Befugnisse der Agentur der Europäischen Union für Cybersicherheit (ENISA) und schafft einen europäischen Rahmen für Cybersicherheitszertifizierung. Der europäische Rahmen für die Cybersicherheitszertifizierung zielt auf die Stärkung der Sicherheit der verbundenen Produkte, IoT-Geräte und der kritischen Infrastrukturen anhand von Zertifikaten ab. Eine Zertifizierung von Produkten, Prozessen und Diensten, die für alle EU-Mitgliedsstaaten gültig ist. Die 3 festgelegten Stufen („Niedrig“, „Mittel“, und „Hoch“) erlauben dem Nutzer, die Vertrauenswürdigkeitsstufe für Sicherheit zu bestimmen und werden sicherstellen, dass die Sicherheitselemente auf unabhängige Weise geprüft sein werden.

Die Produkte von Stormshield haben bereits die Stufe „Standardqualifikation“ erreicht, die von der französischen Agentur für Sicherheit der Informationssysteme (ANSSI) zuerkannt wird. Da die Stufe „Hoch“ des europäischen Rahmens der Stufe „Grundlegende Qualifikation“ der ANSSI – die niedriger ist als die Stufe „Standardqualifikation“ – ist, entsprechen die Stormshield Produkte bereits jetzt den Anfordergen der ENISA in Bezug auf Cybersicherheit.

Möchten Sie dieses Thema vertiefen? Los geht's!

> OPTIONALE COMPLIANCE

Transportunternehmen können ihr Cybersecurity-Level mit den folgenden Standards verbessern, wenngleich ihre Einhaltung derzeit gesetzlich nicht vorgeschrieben ist.

Allgemeine Kriterien / Evaluation Assurance Levels (EAL3+, EAL4+ usw.)

Die Allgemeinen Kriterien für die Bewertung der Sicherheit von Informationstechnologie sind ein internationaler Standard (ISO/IEC 15408) für die Zertifizierung der Computersicherheit. Sie gewährleisten, dass der Prozess der Spezifikation, Implementierung und Bewertung eines Computersicherheitsprodukts gründlich, standardmäßig und wiederholbar durchgeführt wurde und zwar auf einem Level, das der verwendeten Zielumgebung entspricht. Das EAL (EAL3+, EAL4+ usw.) dieses Standards gibt an, wie gründlich das Produkt (beispielsweise eine Firewall) getestet wurde. Diese Zertifizierung wird von ungefähr 30 Ländern in Europa, Nordamerika, Asien und dem Nahen Osten anerkannt.

Die Stormshield-Produkte verfügen nicht nur über die Zertifizierung der Allgemeinen Kriterien, sondern auch über den höheren Grad „Standard Qualification" der französischen Agentur für Cybersecurity (ANSSI). Damit dieser besonders vertrauenswürdige Status verliehen wird, müssen die Produkte:

- eine hochrangige Zertifizierung mit einem von der ANSSI festgelegten und bestätigten Sicherheitsziel erhalten,
- einer Zusatzanalyse der ANSSI sowie einem Audit des Quellcodes des Produkts standhalten.

Der Status „Standard Qualification" ist eine Voraussetzung für den Erhalt der Kennzeichnungen „NATO Restricted" oder „EU Restricted", die für den Umgang mit vertraulichen Informationen notwendig sind.

ISO/IEC 27000 Informationstechnologie – Sicherheitstechniken – Managementsysteme für Informationssicherheit

Die ISO/IEC 27000-Serie ist eine Familie von Informationssicherheitsstandards, die einen weltweit anerkannten Rahmen für Best Practices im Bereich Managementsysteme für Informationssicherheit schafft. Die Serie hat einen absichtlich breiten Geltungsbereich und kann von Unternehmen jeder Größe in allen Branchen genutzt werden.

Das Managementsystem für Informationssicherheit (ISMS) ist ein systematischer Ansatz für den Schutz vertraulicher Infrastruktur. Angesichts der Dynamik von Informationsrisiken und Informationssicherheit umfasst das ISMS-Konzept ständiges Feedback und Verbesserungen, damit man auf sich ändernde Bedrohungen, Schwachstellen oder Auswirkungen von Vorfällen reagieren kann.

Stormshield-Produkte werden zum Schutz vertraulicher Infrastruktur entworfen. Mit einem standardmäßigen Protokollformat können Unternehmen alle Informationen zentral zusammenfassen und so Tendenzen und potenzielle Sicherheitslücken identifizieren. Dank der äußerst intuitiven GUI können Nutzer ganz einfach Verbesserungen durchführen.

> LÄNDERSPEZIFISCHE VERORDNUNGEN

FRANKREICH

Gesetz zur Militärplanung (LPM)

Das Gesetz zur Militärplanung (LPM) legt die Grundzüge der französischen Verteidigungspolitik fest. Angesichts vermehrter Cyberangriffe durch Hacker, Terroristen oder auch Staaten stellt die Cyberresilienz der Informationssysteme von Betreibern von essenzieller Bedeutung (OIV) einen klar definierten Schwerpunkt des LPM dar. Sie ist somit ein Bestandteil der Cybersicherheit und nimmt eine Auflistung der OIV vor, die sich auf zwölf Branchen verteilen, darunter auch den Transportsektor.

Das Vertrauen in die Produkte von Stormshield, die allesamt ANSSI-zertifiziert sind, ermöglicht den OIV die Umsetzung von Sicherheitslösungen für ein höheres Schutzniveau die für kritische Informationssysteme bestimmt sind. Stormshield Network Security stellt beispielsweise die Segmentierung der Netzwerke, die Sicherung von Fernzugriffen, die Nutzerauthentifizierung und die Verwaltung von Schwachstellen sicher. Stormshield Endpoint Security (SES) wird dagegen als Ergänzung zu einem Antivirus-Programm eingesetzt und bietet einen umfassenden Schutz des Arbeitsplatzes vor komplexen Angriffen. SES kann ebenfalls die Sicherheit veralteter Betriebssysteme verbessern, Störungen erkennen und dementsprechend handeln sowie einen Schutz vor Bounce-Angriffen gewährleisten.

Leitfäden für bewährte Praktiken von der ANSSI

Die französische Agentur für Sicherheit der Informationssysteme (ANSSI) ist ein echtes Antriebsorgan in puncto Cybersicherheit in Frankreich und veröffentlicht regelmäßig Leitfäden für bewährte Praktiken. Hierbei handelt es sich nicht um Vorschriften im eigentlichen Sinne, sondern eher um Entscheidungshilfen bezüglich der Auswahl Ihrer Dienstleister und Ihrer Cyber-Sicherheitslösungen sowie deren Umsetzung. Eine bereichernde und spannende Lektüre – von der Verschlüsselung der Arbeitsplätze bis hin zu den Netzwerken.

> LÄNDERSPEZIFISCHE VERORDNUNGEN

DEUTSCHLAND

IT-Grundschutz

Der IT-Grundschutz ist ein Normenkatalog des Bundesamts für Sicherheit in der Informationstechnik (BSI), mit dem die Anforderungen für ein angemessenes Level an Daten- und Informationssicherheit erfüllt werden können. Das IT-Grundschutz-Kompendium wird jedes Jahr im Februar veröffentlicht und erklärt die Gefahren und Sicherheitsanforderungen im Bereich Informationssicherheit.

Standards des Bundesamts für Sicherheit in der Informationstechnik (BSI)

Die BSI-Standards sind eine grundlegende Komponente der IT-Grundschutz-Methodologie. Das sind die aktuellen BSI-Standards:

- 200-1 (Allgemeine Anforderungen für Managementsysteme für Informationssicherheit)
- 200-2 (Grundlage für die Entwicklung eines soliden Managementsystems für die Informationssicherheit)
- 200-3 (Alle risikobezogenen Schritte in der Umsetzung der Basis des IT-Grundschutzes)

IT-Sicherheitsgesetz und BSI-Gesetz

Gemäß dem IT-Sicherheitsgesetz müssen die Betreiber kritischer Anlagen/Infrastrukturen im Transportsektor ein Mindestlevel an IT-Sicherheit einhalten und dem BSI wesentliche IT-Störungen melden. Absatz 8a des BSI-Gesetzes wurde vom IT-Sicherheitsgesetz erlassen und beschreibt das Mindestlevel auf abstrakte Art und Weise. Die BSI-Kritisverordnung wurde 2016 verabschiedet. Hier ist festgeschrieben, welche kritischen Systeme von den Bestimmungen des IT-Sicherheitsgesetzes abgedeckt werden müssen. Diese Verordnung deckt auch den Transportsektor ab.

Mit den zertifizierten, vertrauenswürdigen Stormshield-Produkten können Sicherheitslösungen bereitgestellt werden, die das Schutzniveau der IT-Systeme verbessern. Stormshield Network Security kann zum Beispiel Netzwerkbereiche isolieren, sicheren Fernzugriff gewährleisten, Nutzer authentifizieren und Schwachstellen verwalten. Stormshield Endpoint Security (SES) gewährt in Zusammenarbeit mit einem Antivirenprogramm (wenn vorhanden) eingehenden Schutz des Arbeitsplatzes gegen ausgefeilte Bedrohungen. SES kann auch den Schutz von Legacy-Betriebssystemen verbessern, Vorfälle entdecken und verwalten und vor Bounce-Angriffen schützen. Stormshield Data Security beugt Datenlecks vor, indem es vertrauliche Informationen verschlüsselt.

> LÄNDERSPEZIFISCHE VERORDNUNGEN

ITALIEN

Gesetzesverordnung 18. Mai 2018, Nr. 65 (Implementierung der Richtlinie (EU) 2016/1148 - NIS)

Das Gesetz legt Sicherheitsmaßnahmen auf nationaler Ebene fest. Dazu gehört auch die Einrichtung eines CSIRT (auch bekannt als CIRT). Das sind die so genannten „kritische Marktteilnehmer“ und digitalen Dienstleiter für die Bereiche Maßnahmen bei Sicherheitsverletzungen, internationale Kooperation bei Sicherheitsthemen und die Verabschiedung einer nationalen Cybersecurity-Strategie.

Mit den zertifizierten, vertrauenswürdigen Stormshield-Produkten können die Betreiber wesentlicher Dienste Sicherheitslösungen bereitstellen, die das Schutzniveau der wesentlichen Informationssysteme (EIS) verbessern. Stormshield Network Security kann zum Beispiel Netzwerkbereiche isolieren, sicheren Fernzugriff gewährleisten, Nutzer authentifizieren und Schwachstellen verwalten. Stormshield Endpoint Security (SES) gewährt in Zusammenarbeit mit einem Antivirenprogramm (wenn vorhanden) eingehenden Schutz des Arbeitsplatzes gegen ausgefeilte Bedrohungen. SES kann auch den Schutz von Legacy-Betriebssystemen verbessern, Vorfälle entdecken und verwalten und vor Bounce-Angriffen schützen.

D.P.C.M. 17. Februar 2017 (Ausrichtung zur Nationalen Informationstechnologiesicherheit und Cybersecurity - Gentiloni-Verordnung)

Die Richtlinie schafft eine institutionelle Organisation, die sich um die nationale IT-Sicherheit und Cybersecurity kümmert, Pflichten und Aufgaben jeder Entität (CISR, CISR Tecnico, DIS-Rolle- und Richtlinien, Nucleo per la Sicurezza Cibernetica) festlegt. Die Richtlinie legt auch Maßnahmen für „kritische Marktteilnehmer“ und Kommunikationsanbieter fest.

D.P.C.M. 27. Januar 2014 (Nationale Rahmenstrategie für Cyberspace - QSN)

Die nationale Rahmenstrategie für Cyberspace verfolgt das Ziel, die Effizienz und Interoperabilität der Ressourcen für die gemeinsame Verteidigung sicherzustellen und die komplette Integration der Cyberdomäne in den Planungsprozess für die NATO-Verteidigung und in die militärische Lehre unterstützt und somit die Bereitstellung einer robusten Strategie gegen Cyberangriffe.

Stormshield Network Security hat die Zertifizierung EU Restricted erhalten. Als solche können diese Produkte in vertraulichen Umgebungen bereitgestellt werden, um eine sichere Übermittlung von vertraulichen Informationen zu gewährleisten. So kann die internationale Interoperabilität mit den EU-Institutionen aufrechterhalten werden.

> LÄNDERSPEZIFISCHE VERORDNUNGEN

SPANIEN

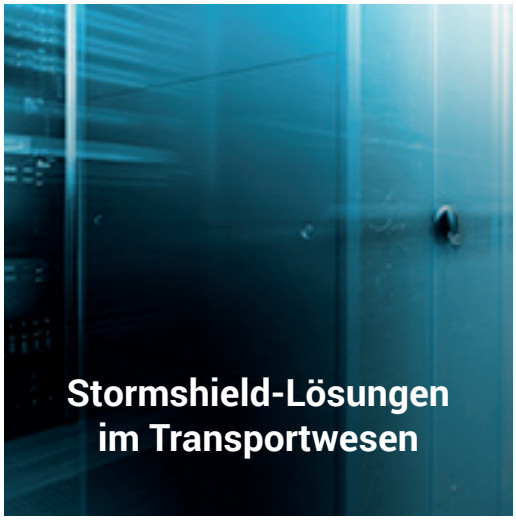
PIC-Gesetz (Schutz Öffentlicher Infrastrukturen - Ley PIC)

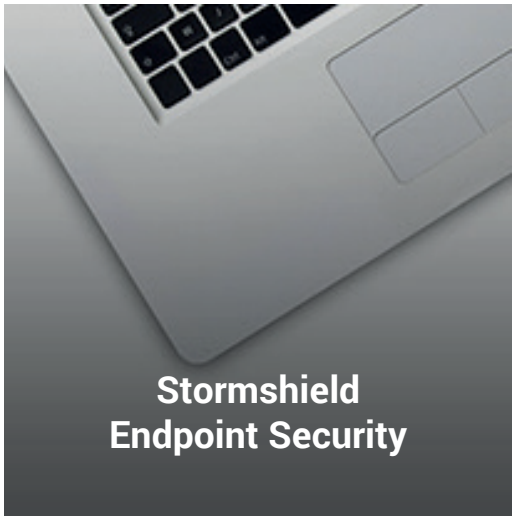
Das Gesetz zum Schutz Kritischer Infrastruktur (Ley PIC 8/2011) is wird durch das Königliche Dekret 704/2011 ergänzt. Die zwei Hauptziele dieses Standards sind: Katalogisierung der Infrastrukturen, die kritische Dienste für unsere Gesellschaft bereitstellen und Entwurf eines Plans mit effektiven Präventions- und Schutzmaßnahmen vor möglichen Bedrohungen für diese Infrastrukturen, sowohl in Bezug auf die physische Sicherheit, als auch in Bezug auf die Sicherheit der Informations- und Kommunikationstechnologien.

Mit den zertifizierten, vertrauenswürdigen Stormshield-Produkten können kritische Infrastrukturen Sicherheitslösungen bereitstellen, die das Schutzniveau der wesentlichen Dienste Informationssysteme verbessern. Stormshield Network Security kann zum Beispiel Netzwerkbereiche isolieren, sicheren Fernzugriff gewährleisten, Nutzer authentifizieren und Schwachstellen verwalten. Stormshield Endpoint Security (SES) gewährt in Zusammenarbeit mit einem Antivirenprogramm (wenn vorhanden) eingehenden Schutz des Arbeitsplatzes gegen ausgefeilte Bedrohungen. SES kann auch den Schutz von Legacy-Betriebssystemen verbessern, Vorfälle entdecken und verwalten und vor Bounce-Angriffen schützen.

> STORMSHIELD HAT FÜR JEDES PROBLEM EINE LÖSUNG.

Stormshield-Produkte und -Lösungen im Transportwesen





> COMPLIANCE REICHT NICHT AUS

Die Vielzahl an Verordnungen und Standards bereitet allen Unternehmen Kopfzerbrechen. Dieser Leitfaden schafft einen Überblick darüber, welche Verordnung für welchen Sektor relevant ist, aber Compliance reicht nicht aus. Es ist wichtig, sich vor Augen zu führen, dass jedes Unternehmen seine Risiken identifizieren und verwalten und so seine eigene Sicherheit garantieren muss.