STORMSHIELD

EINHALTUNG DER CYBERSECURITY FÜR ÖFFENTLICHE ORGANISATIONEN

Die allgemeine Öffentlichkeit besteht heute darauf, dass Regierungsinstitutionen Online-Informationen einfach, zuverlässig und zeitgerecht veröffentlichen. Allerdings sind öffentliche Behörden, dazu gehören Gemeinden, Behörden und Ministerien, häufig Opfer von Cyberangriffen. Öffentliche Organisationen stehen vor der Herausforderung, die Nutzererwartungen erfüllen zu müssen und gleichzeitig Servicekontinuität und sichere Informationssysteme sicherzustellen.

> 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

Öffentliche Organisationen 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.

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 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.

> EUROPÄISCHE VERORDNUNGEN: MÜSSEN EINGEHALTEN WERDEN

Richtlinie zur Wiederverwendung von Informationen 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.

EU Restricted

Die Geheimhaltungsstufe EU Restricted gilt für vertrauliche Informationen, deren unbefugte Offenlegung, Änderung oder Nichtverfügbarkeit sich auf die Interessen der EU oder eines oder mehrerer Mitgliedsstaaten nachteilig auswirken könnte. Für den Fall, dass Informationen, die als „EU Restricted“ eingestuft werden, außerhalb eines physisch eingeschränkten Sicherheitsbereich übermittelt werden, erfordert diese Geheimhaltungsstufe, dass die Informationen mithilfe zertifizierter Produkte verschlüsselt werden.

Stormshield Network Security und Stormshield Data Security haben die Zertifizierung EU Restricted erhalten. So können sie in vertraulichen Umgebungen zur Verschlüsselung von als „EU Restricted“ eingestuften Informationen und zur sicheren Übermittlung verwendet werden.

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

Öffentliche Organisationen 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

GROSSBRITANNIEN

Data Protection Act 2018

Der Data Protection Act ähnelt der DSGVO und gilt speziell für das Vereinigte Königreich. Es wird festgelegt, dass es für alle personenbezogenen Daten ein „angemessenes Schutzniveau“ gibt, das den Risiken einer Sicherheitsverletzung angepasst ist. Das umfasst ein Sicherheitsgrad zur Verhinderung von unbefugter oder rechtswidriger Verarbeitung, zufälligem Verlust, Zerstörung oder Beschädigung der Daten.

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.

> LÄNDERSPEZIFISCHE VERORDNUNGEN

FRANKREICH

Allgemeines Sicherheitshandbuch (RGS)

Das Allgemeine Sicherheitshandbuch (RGS) gilt für Informationssysteme, die von den Verwaltungsbehörden für die Beziehung mit den Nutzern eingesetzt werden. Sie sind verpflichtet, den elektronischen Austausch abzusichern. Dieses Handbuch bietet sowohl eine Methodik als auch Regeln und bewährte Praktiken für Verwaltungsstellen.

Datenschutz spielt hierbei eine grundlegende Rolle. Die Lösung Stormshield Data Security ermöglicht die Verschlüsselung von Daten und hält sich an die Qualifikationsanforderungen von Sicherheitsprodukten und Anbietern von Vertrauensdiensten. Die weiteren Produktreihen vom Stormshield ermöglichen den Verwaltungsstellen die Erfüllung dieser Anforderungen, wobei die Resilienz ihrer Infrastruktur gleichzeitig gesteigert wird.

Sicherheitsrichtlinie der für Informationssysteme des Staats (PSSIE)

Die PSSIE findet bei allen Informationssystemen von Regierungsbehörden (Ministerien, öffentliche Einrichtungen unter Aufsicht eines Ministeriums, dezentrale Dienststellen des Staates und unabhängige Verwaltungsbehörden) Anwendung. Sie legt Grundprinzipien fest wie die Wahl der vertrauenswürdigen Elemente zur Schaffung von Informationssystemen, die Sicherheits-Governance und die Sensibilisierung der Akteure. Unter diesen Prinzipien hebt das Rundschreiben die Notwendigkeit für die staatlichen Verwaltungsbehörden hervor, auf von der ANSSI qualifizierte Produkte und Dienste zurückzugreifen.

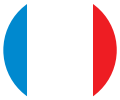
Stormshield schlägt eine Reihe von durch die ANSSI qualifizierte Produkte vor und erfüllt damit das Grundprinzip der PSSIE, vertrauenswürdige Produkte zu verwenden. Sie können daher in den Informationssystemen der staatlichen Verwaltungsbehörden installiert werden, um das Netz zu sichern, sensible Informationen zu schützen und den Schutz der Arbeitsplätze zu erhöhen.

Verordnung 2020-1407 vom 18. November 2020 zu den Aufgaben der regionalen Gesundheitsagenturen

Artikel 1 dieser Verordnung enthält die Pflicht zur Meldung von IT-Zwischenfällen an die zuständigen staatlichen Behörden und an die Nationale Agentur für öffentliche Gesundheit für alle Krankenhäuser und sanitären und medizinisch-sozialen Einrichtungen.approfondite.

Die Ereignisprotokolle, die die Stormshield-Lösungen für Sicherheitsereignisse enthalten, gehören zu den wesentlichen Informationen, die bei einem Zwischenfall den zuständigen Behörden gemeldet werden müssen. Die Weiterentwicklung der Lösung Stormshield Endpoint Security ist insbesondere eine Antwort auf diese Problematik, wenn es sich um einen ausgeklügelten Angriff handelt und wenn versucht wird, mit dem Angriff die Schutzmaßnahmen zu täuschen. Stormshield Endpoint Security Evolution blockiert proaktiv die raffiniertesten Angriffsarten und liefert darüber hinaus die Kontextualisierungs-Elemente, die für die gründliche Untersuchung von Sicherheitsvorkommnissen erforderlich sind.

> LÄNDERSPEZIFISCHE VERORDNUNGEN



FRANKREICH

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.

Mit dem Handbuch „Digitale Sicherheit für Gebietskörperschaften: Die wichtigsten Vorschriften“ erhalten Sie einen ergänzenden Leitfaden zu unserem eBook. Es handelt sich um ein synthetisches, praktisches und erschwingliches Dokument für Mandatsträger und Verwaltungsbeamte, die für die praktische Umsetzung und Einhaltung der Vorschriften verantwortlich sind.

> LÄNDERSPEZIFISCHE VERORDNUNGEN

DEUTSCHLAND

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)

Die BSI hat auf der Grundlage des BSI-Standards 200-2 „IT-Grundschutz-Methodik“ Mindestsicherheitsmaßnahmen festgelegt, die zum angemessenen Selbstschutz in Lokalverwaltungen implementiert werden müssen.

Gesetz zur Förderung der Elektronischen Verwaltung (EGovG)

Das EGov-Gesetz der Bundesregierung (und die der Länder) behandeln hauptsächlich administrative Tätigkeiten der Bundesbehörden. Fallen im Rahmen eines elektronisch durchgeführten Verwaltungsverfahrens Gebühren an, muss die Behörde laut Abschnitt 4 EgovG die Einzahlung dieser Gebühren oder die Begleichung dieser sonstigen Forderungen durch Teilnahme an mindestens einem im elektronischen Geschäftsverkehr üblichen und hinreichend sicheren Zahlungsverfahren ermöglichen.

Wenn eine Behörde ihre Akten elektronisch führt, gibt Absatz 6 EGovG an, dass sie durch geeignete technisch-organisatorische Maßnahmen nach dem Stand der Technik sicherstellen müssen, dass die Grundsätze ordnungsgemäßer Aktenführung eingehalten werden. Die Behörden des Bundes müssen durch geeignete technisch-organisatorische Maßnahmen nach dem Stand der Technik sicherstellen, dass die Grundsätze ordnungsgemäßer Aktenführung eingehalten werden.

> LÄNDERSPEZIFISCHE VERORDNUNGEN

DEUTSCHLAND

Bundesdatenschutzgesetz (BDSG)

Daten, die Informationen zu Rasse oder ethnischer Herkunft, politischen Meinungen, religiösen oder philosophischen Glaubenssätzen oder der Mitgliedschaft in Gewerkschaften geben sowie die Verarbeitung von genetischen Daten, biometrischen Daten für die unzweifelhafte Identifizierung einer natürlichen Person oder Daten über das Sexualleben oder die sexuelle Orientierung einer natürlichen Person fallen unter spezielle Kategorien von personenbezogenen Daten entsprechend Art. 9 DSGVO. Bei der Verarbeitung solcher Daten müssen spezifische und angemessene Maßnahmen eingeleitet werden, um das Interesse der Betroffenen in Einklang mit Absatz 22 (2) BDSG zu schützen. Dieser Absatz legt die technischen und organisatorischen Maßnahmen fest, die bei der Verarbeitung von Daten eingeleitet werden müssen.

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 eine geeignete technische Maßnahme für die Beibehaltung des dem Risiko angepassten Sicherheitsgrads ist.

Datenschutzgesetz der Bundesländer (beispielsweise Nordrheinwestfalen: DSG NRW)

Das DSG von NRW legt ergänzende Vorschriften für die Implementierung der Datenschutz-Grundverordnung (DSGVO) fest. So bestimmt Artikel 58 DSG NRW die Anforderungen für die Sicherheit der Datenverarbeitung, die dazu führen sollen, dass:

- die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden und
- die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

> LÄNDERSPEZIFISCHE VERORDNUNGEN

DEUTSCHLAND

De-Mail-Gesetz

Das De-Mail-Gesetz trat am 3. Mai 2011 in Deutschland in Kraft und wird von der Bundesverwaltung verwendet. Die Nachrichten werden ausschließlich über verschlüsselte Kanäle übermittelt und in verschlüsselter Form gespeichert. Gemäß Abschnitt 1(I) des De-Mail-Gesetzes sind De-Mail-Dienste Dienste auf einer elektronischen Kommunikationsplattform, die einen sicheren, vertraulichen und nachweisbaren Geschäftsverkehr für jedermann im Internet sicherstellen sollen.

Stormshield Data Security stellt einen End-to-End-E-Mail-Schutz zur Verfügung, damit diese Anforderungen für den sicheren E-Mail-Austausch erfüllt werden können. Diese Lösung bietet eine Reihe an Funktionalitäten, die den sicheren, vertraulichen und authentischen Austausch für jedermann im Internet garantieren.

eIDAS-Implementierungsgesetz und Vertrauensdienstegesetz (VDG)

Am 29.03.2017 verabschiedete die Bundesregierung das eIDAS-Implementierungsgesetz, das die eIDAS-Verordnung der EU ((EU) 910/2014) implementieren wird. Der eIDAS-Durchführungsrechtsakt verordnete das so genannte Vertrauensdienstegesetz (VDG). Der am besten bekanntestes Vertrauensdienst ist die „elektronische Signatur“. Artikel 13 VDG behandelt indirekt die IT-Sicherheit. Laut diesem Artikel hat der qualifizierte Vertrauensdiensteanbieter bestimmte Personen über die Maßnahmen zu unterrichten, die erforderlich sind, um zur Sicherheit der angebotenen qualifizierten Vertrauensdienste und deren zuverlässiger Nutzung beizutragen.

> LÄNDERSPEZIFISCHE VERORDNUNGEN

ITALIEN

Sicherheitsqualifikationen (DPCM (ital. Dekret) 22. Juli 2011)

Mit Sicherheitsqualifikationen (genannt AP und NOSI) können Organisationen einen Vertrag mit einer öffentlichen Verwaltung eingehen, um an Ausschreibungen für die Vergabe von Aufträgen teilzunehmen, die als „reserved" (vorbehalten) oder höher eingestuft werden. Dies gilt insbesondere für Ausschreibungen, die den Umgang mit Informationen einschließen, die als geheim/streng geheim/vertraulich/höchst vertraulich eingestuft werden. Solche Qualifikationen setzen voraus, dass die Organisationen spezifische Maßnahmen umsetzen. Dazu gehören logische, physische und technische Sicherheitsmaßnahmen.

Gesetz 124/2007 (Informationssystem für die Sicherheit der Italienischen Republik und neues Sicherheitsprotokoll) - geändert durch Gesetz 133/2012

Die italienische Abteilung für Sicherheitsinformationen (DIS), das italienische Amt für Informationen und äußere Sicherheit (AISE) und das italienische Amt für Informationen und innere Sicherheit (ASIS) können mit allen öffentlichen Verwaltungen und den Stellen kommunizieren, die durch eine Genehmigung, Konzession oder Konvention öffentliche Versorgungsdienstleistungen bereitstellen und ihnen eine Zusammenarbeit zur Erfüllung ihrer institutionellen Funktionen anbieten. Zu diesem Zweck können Sie mit den vorgenannten Stellen eine Vereinbarung abschließen (siehe Art.13 des Gesetzes für weitere Details).

D.P.C.M. 6. November 2015 (Protokoll für die elektronische Signatur für geheime/vertrauliche Dokumente)

Das Protokoll ist verbindlich für alle öffentlichen und privaten Vertreter, die die erforderlichen Sicherheitsqualifikationen für die Verwaltung vertraulicher Informationen besitzen. Das Protokoll legt außerdem fest, wie man digitale Signaturen erstellt, unterzeichnet und überprüft und wie vertrauliche elektronische Dokumente vorübergehend validiert werden können.

Richtlinie 1. August 2015 (Nationaler Rahmen für die Umsetzung von Cybersecurity)

Die Richtlinie setzt Ziele durch, die innerhalb des Nationalen Rahmens für Cybersecurity festgelegt sind und stärkt die Koordination zwischen den öffentlichen Behörden sowie Partnerschaften mit allen nicht öffentlichen Betreibern von IT- und Telematik-Infrastrukturen, die auf nationaler Ebene als kritisch angesehen werden. Die Richtlinie weist der Agentur für ein Digitales Italien (AgID) die Aufgabe zu, Verwaltungsstandards zu entwickeln.

> 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 ausgefeilten 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 und die 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 und somit die Bereitstellung einer robusten Strategie gegen Cyberangriffe zu unterstützen.

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

ITALIEN

Dreijahresplan 2019-2021 für die öffentlichen Verwaltungen von der AgID

Der Plan legt regulatorische Maßnahmen für öffentliche Verwaltungen fest. Dazu gehören Plattformimplementierung, ein Test für die nationale, automatische Übermittlung von qualifizierten IoC, nationale Richtlinien für öffentliche Verwaltungen zu Cybersecurity und die verpflichtende Umsetzung der AgID-Richtlinien über Sicherheitsmaßnahmen.

Mindestsicherheitsmaßnahmen der AgID (Implementierung der DPCM 1. August 2015)

Diese Richtlinie soll die AgID-Maßnahmen umsetzen, mit denen Bedrohungen für die Cybersecurity bekämpft und notwendige Sicherheitsmaßnahmen für den Verteidigungssektor technisch und organisatorisch bereitgestellt werden können.

Mit den Stormshield-Produkten verbessern öffentliche Organisationen die Cyber-Belastbarkeit ihrer Infrastruktur und können diese Anforderungen somit einhalten.
Unter diesen Anforderungen unterstützt der Stormshield Network Vulnerability Manager (Manager für die Netzwerksicherheit) auf Netzwerkebene die Produkte von Stormshield Network Security und hilft beim Schwachstellenmanagement.
Stormshield Endpoint Security verbessert den Sicherheitsgrad traditioneller Antivirenprogramme zusätzlich, indem es die hochentwickelte Bedrohungen blockiert.
Stormshield Data Security, das Produkt mit dem Zertifikat „EU Restricted“, hilft Ihnen bei der Einhaltung der Datenschutzanforderungen.

D.P.C.M. 3. Dezember 2013 (Technische Regeln für Speichersysteme)

Das DPCM legt einschlägige Anforderungen für Speichersysteme mit Blick auf elektronische Dokumente (einschließlich administrative Dokumente und verwandte Metadaten) und elektronische Dossiers sowie Regeln zur Sicherstellung von Integrität, Zuverlässigkeit und Verfügbarkeit solcher Dokumente und Anforderungen zu funktionellen Komponente der Verwaltung der Speichersysteme fest.

> LÄNDERSPEZIFISCHE VERORDNUNGEN

SPANIEN

Cybersecurity-Gesetzbuch

Dieses Gesetzbuch stellt Anwälten ein Tool zur Verfügung, in dem sie die aktualisierten Vorschriften finden, die einen direkten Einfluss auf die Cybersecurity haben, und erleichtert somit die notwendige Überprüfung und Analyse eines Themas, das für den ausreichenden Schutz von Unternehmen, Institutionen und Bürgern innerhalb eines sozialen und demokratischen Rechtsstaates unbedingt erforderlich ist.

Mit den Stormshield-Produkten verbessern Unternehmen die Cyber-Belastbarkeit ihrer Infrastruktur und können diese Anforderungen somit einhalten. Stormshield Network Security garantiert Randschutz mit UTM-Funktionen (Unified Threats Management). Stormshield Endpoint Security verbessert den Sicherheitsgrad traditioneller Antivirenprogramme zusätzlich, indem es die hochentwickelte Bedrohungen blockiert. Schließlich stellt Stormshield Data Security auch Möglichkeiten zur Datenverschlüsselung zur Verfügung, die eine geeignete technische Maßnahme für die Beibehaltung des dem Risiko angepassten Sicherheitsgrads ist.

Nationaler Sicherheitsplan, Königliches Dekret, 3/2010, vom 8. Januar

Dieser Plan ist allgemein anwendbar auf elektronische Seiten, elektronische Register und Informationssysteme, auf die Bürger elektronisch zugreifen können (zur Ausübung von Rechten, Pflichterfüllung, Einholung von Informationen und dem Stand des Verwaltungsverfahrens).

Die Stormshield Produkte unterstützen Organisationen, sich an diesen Plan anzupassen und die Cyber-Belastbarkeit ihrer Infrastruktur zu verbessern. Stormshield Network Security garantiert einen branchenführenden Schutz mit UTM-Funktionen (Unified Threats Management). Unsere SNS-Reihe ist übrigens die einzige europäische Produktlinie mit der Qualifikation „Productos Cualificados“ (qualifizierte Produkte) und die einzige Firewall-Reihe, die durch das Nationale Kryptologiezentrum in Spanien (CCN) mit „Productos Aprobados“ (zugelassene Produkte) qualifiziert ist. Stormshield Endpoint Security verbessert den Sicherheitsgrad traditioneller Antivirenprogramme zusätzlich, indem es auch komplexe Bedrohungen blockiert. Schließlich stellt Stormshield Data Security auch Möglichkeiten zur Datenverschlüsselung zur Verfügung, die eine geeignete technische Maßnahme für die Beibehaltung des dem Risiko angepassten Sicherheitsgrads ist.

> LÄNDERSPEZIFISCHE VERORDNUNGEN

SPANIEN

PIC-Gesetz (Schutz öffentlicher Infrastrukturen - Ley PIC)

Das Gesetz zum Schutz kritischer Infrastruktur (Ley PIC 8/2011) 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 öffentlichen Sektor

> 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.