STORMSHIELD

EINHALTUNG DER CYBERSECURITY FÜR VERTEIDIGUNGSUNTERNEHMEN

Die Informationssysteme von Militärorganisationen, Verteidigungsministerien und Streitkräften brauchen besonders leistungsstarken Schutz. In unserer Zeit spielt der Cyberkrieg eine Schlüsselrolle für die nationale Sicherheit und der beste Angriff ist eine unerschütterliche Verteidigung. Wenn so viel auf dem Spiel steht sind Sicherheit, Zuverlässigkeit und Verfügbarkeit von unschätzbarem Wert.

> 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

Verteidigungsorganisationen 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.

NATO Restricted

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

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

Cypersecurity 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

Verteidigungsunternehmen 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. Der Verteidigungssektor ist zu einem gewissen Grad von diesem Rechtsakt ausgenommen, vorausgesetzt, dass die personenbezogenen Daten zum Schutz der Bürger verwendet 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.

> 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 Verteidigungssektor.

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.

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.

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

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

Die Absätze 8a - 8d des BSIG sind äußerst relevant für die Sicherheit von für die Informationstechnologie kritischer Infrastruktur und die Betreiber digitaler Dienstleistungen.

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.

Bundesdatenschutzgesetz (BDSG)

Absatz 22 (2) BDSG behandelt spezifische Datenschutzanforderungen bei der Verarbeitung besonderer Kategorien personenbezogener Daten. § 64 (3) BDSG listet Zwecke auf, die mithilfe angemessener Maßnahmen Datenrisikobewertungen durchführen können.

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.

> 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 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.

> LÄNDERSPEZIFISCHE VERORDNUNGEN

ITALIEN

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.

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.

> LÄNDERSPEZIFISCHE VERORDNUNGEN

ITALIEN

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 Zertifizierungen „NATO Restricted“ und „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 NATO- und EU-Institutionen aufrechterhalten werden.

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 Unternehmen 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.

> 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.

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.

> LÄNDERSPEZIFISCHE VERORDNUNGEN

SPANIEN

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

Dieser Plan wird wie in allen anderen Regierungsorganisationen angewendet. Die Systeme, welche die klassifizierten Informationen verwalten, müssen sich zusätzlich an die Anforderungen der Produkte halten, die durch das Nationale Kryptologiezentrum (CCN) in Spanien qualifiziert wurden.

Mit den Stormshield-Produkten verbessern Unternehmen die Cyber-Belastbarkeit ihrer Infrastruktur und können sich somit an diesen Plan anpassen. 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 CCN mit „Productos Aprobados“ (zugelassene Produkte) qualifiziert ist. Sie entspricht daher der Anforderung eines qualifizierten Produkts. Stormshield Endpoint Security verbessert den Sicherheitsgrad traditioneller Antivirenprogramme zusätzlich, indem es auch komplexe Bedrohungen blockiert. Stormshield Data Security liefert Funktionen zur Datenverschlüsselung, die eine geeignete technische Maßnahme darstellen, um ein dem Risiko angepasstes Sicherheitsniveau zu gewährleisten.

> STORMSHIELD HAT FÜR JEDES PROBLEM EINE LÖSUNG.

Stormshield-Produkte und -Lösungen für Verteidigungsunternehmen

> 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.

Bildnachweis: ShutterStock©. aressy. com