STORMSHIELD

EINHALTUNG DER CYBERSECURITY FÜR UNTERNEHMEN IM GESUNDHEITSWESEN

Im Gesundheitswesen, wo die Dienstverfügbarkeit von großer Bedeutung ist, kann es bei einem Cyberangriff tatsächlich um Leben und Tod gehen. Außerdem sind Gesundheitsdienstleister gesetzlich dazu verpflichtet, Patientendaten zu schützen. Das trifft auch in der heutigen Zeit zu, in der Gesundheitssysteme immer häufiger mobile Daten nutzen, die nicht unbefugt eingesehen werden dürfen.

> 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 Gesundheitswesen 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 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 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.

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

Unternehmen im Gesundheitswesen 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.

Liste der Empfehlungen der ENISA

Die Europäische Agentur für Netz- und Informationssicherheit veröffentlichte eine Liste mit Empfehlungen zur Cybersicherheit im Rahmen von öffentlichen Aufträgen in Krankenhäusern, sowohl für Dienstleistungen und Produkte als auch für Infrastrukturen. Dieses Dokument ist für die IT-Verantwortlichen in den Gesundheitseinrichtungen bestimmt.

Die Produkte von Stormshield sind auf höchster europäischer Ebene zertifiziert und qualifiziert, was für Vertrauen und Robustheit bürgt. Sie ermöglichen es den Betreibern kritischer Dienste (OSE), Sicherheitslösungen zu implementieren, die das Schutzniveau der wesentlichen Informationssysteme (SIE) verbessern. Stormshield Network Security stellt beispielsweise die Segmentierung der Netzwerke, die Sicherung von Fernzugriffen, die Nutzerauthentifizierung und die Verwaltung von Schwachstellen sicher. Mit der Implementierung einer auf höchster europäischer Ebene zertifizierten und qualifizierten Lösung erhalten Sie ein Produkt, dessen Robustheit während des Zertifizierungsprozesses bestätigt wurde.

Möchten Sie dieses Thema vertiefen? Los geht's!

> OPTIONALE COMPLIANCE

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

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

Gesetz über das öffentliche Gesundheitswesen - Artikel für Hoster von Gesundheitsdaten

Der Artikel L1111-8 des französischen Gesetzes über das öffentliche Gesundheitswesen legt die Voraussetzungen für das Hosting von personenbezogenen Gesundheitsdaten fest. Der Hoster und sein Archivierungsdienst müssen demnach eine effiziente Sicherung der ihnen anvertrauten Gesundheitsdaten vornehmen.

Die Lösungen von Stormshield begleiten Sie dank einer breit gefächerten Palette an Funktionen bei der Erfüllung der Qualitätsanforderungen Ihrer Einrichtung. Das Angebot umfasst die Sicherung Ihrer Daten mit garantierter Compliance – selbst für die Speicherung vertraulicher Daten in der Cloud. Die Lösung Stormshield Data Security kann ganz unabhängig vom Standort verwendet werden.

Interministerielle Weisung Nr. 901/SGDSN

Die interministerielle Weisung Nr. 901 zum Schutz sensibler Informationssysteme gilt insbesondere für öffentliche oder private Einrichtungen, die an die Verordnung zum Schutz des wissenschaftlichen und technischen Potenzials der Nation (PPST) gebunden sind und sensible Informationssysteme nutzen. Die über diese sensiblen Informationssysteme verarbeiteten Daten – wie zum Beispiel Patente, die in einem begrenzten Zugangsbereich registriert werden müssen – müssen ebenfalls mit dem Vermerk „Beschränkte Verbreitung“ gekennzeichnet werden.

Zur Verhinderung der Kompromittierung sensibler Daten und zum Schutz des Images der Einheit ermöglicht die Lösung Stormshield Data Security eine End-to-End-Datenverschlüsselung. Eine verschlüsselte, nach EAL3+ zertifizierte Implementierung, die von ANSSI und NATO zugelassen ist, eignet sich für den Schutz von Daten mit dem Prädikat „Beschränkte Verbreitung“.

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.

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)

IT-Sicherheitsgesetz und BSI-Gesetz

Gemäß dem IT-Sicherheitsgesetz müssen Gesundheitsbetreiber 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. Zusätzlich dazu wurde 2016 die BSI-Kritisverordnung verabschiedet. Hier ist festgeschrieben, welche kritischen Systeme von den Bestimmungen des IT-Sicherheitsgesetzes abgedeckt werden müssen. Diese Verordnung deckt auch das Gesundheitswesen 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.

Bundesdatenschutzgesetz (BDSG)

Bei der Verarbeitung von Gesundheitsdaten 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 Gesundheitsdaten 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.

> LÄNDERSPEZIFISCHE VERORDNUNGEN

DEUTSCHLAND

E-Health-Gesetz und das 5. Sozialgesetzbuch

Das E-Health-Gesetz betrifft die elektronische Kommunikation und Anwendung im Gesundheitswesen. Es enthält einen konkreten Fahrplan für die Einrichtung einer sicheren Telematikinfrastruktur und die Einführung von Medizinanwendungen. Das E-Health-Gesetz ist ein Änderungsgesetz, das das 5. Sozialgesetzbuch ändert.

Mit den Stormshield-Produkten verbessern Unternehmen die Cyber-Belastbarkeit ihrer Infrastruktur und können diese Richtlinie 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. Stormshield Data Security hilft Ihnen letztendlich auch bei der Einhaltung der Datenschutzanforderungen.

> 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. 178 aus 2015 (E-Health-Dossier - Fascicolo Sanitario Elettronico - FSE)

Das E-Health-Dossier ist eine Aufzeichnung von Gesundheits- und sozio-sanitären Informationen zu klinischen Ereignissen von Patienten, deren Hauptziel in der Vereinfachung der Patientenunterstützung und der Verstärkung von Synergien im Bereich Gesundheitsversorgung und Unterstützung liegt. Die Einhaltung des Gesetzes (auch was die Sicherheit angeht) orientiert sich an der DSGVO und der Garante Provision (FSE).

Mit den Stormshield-Produkten verbessern Unternehmen im Gesundheitswesen 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

SPANIEN

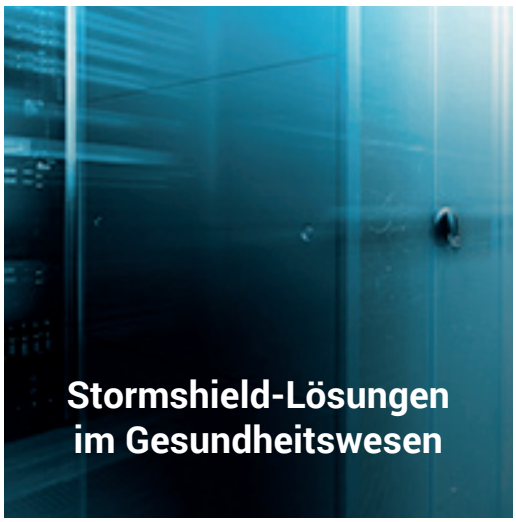
Nationaler Sicherheitsplan, Königliches Dekret 3/2010, vom 8. Januar

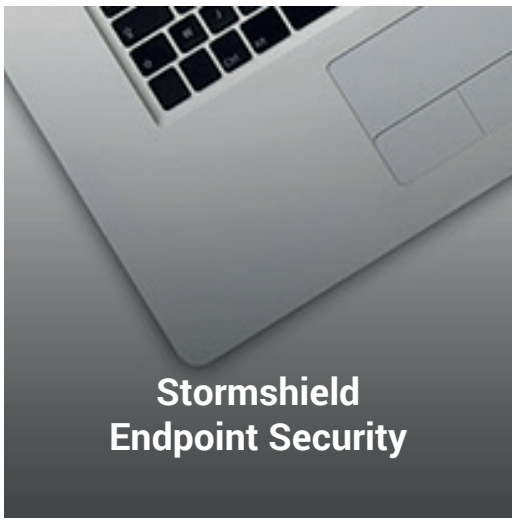
Wenn ein Krankenhaus als öffentlich-rechtliche Anstalt (in Verbindung mit oder abhängig von der staatlichen Verwaltung, autonomen Gemeinschaften oder lokalen Anstalten) eingestuft wird, gilt der folgenden Plan für die Tätigkeiten, die nicht unter Privatrecht ausgeführt werden.

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.

> STORMSHIELD HAT FÜR JEDES PROBLEM EINE LÖSUNG.

Stormshield-Produkte und -Lösungen im Gesundheitswesen





> 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