European Union Agency
for Cybersecurity
Vasilissis Sofias Str 1
151 24 Maroussi | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

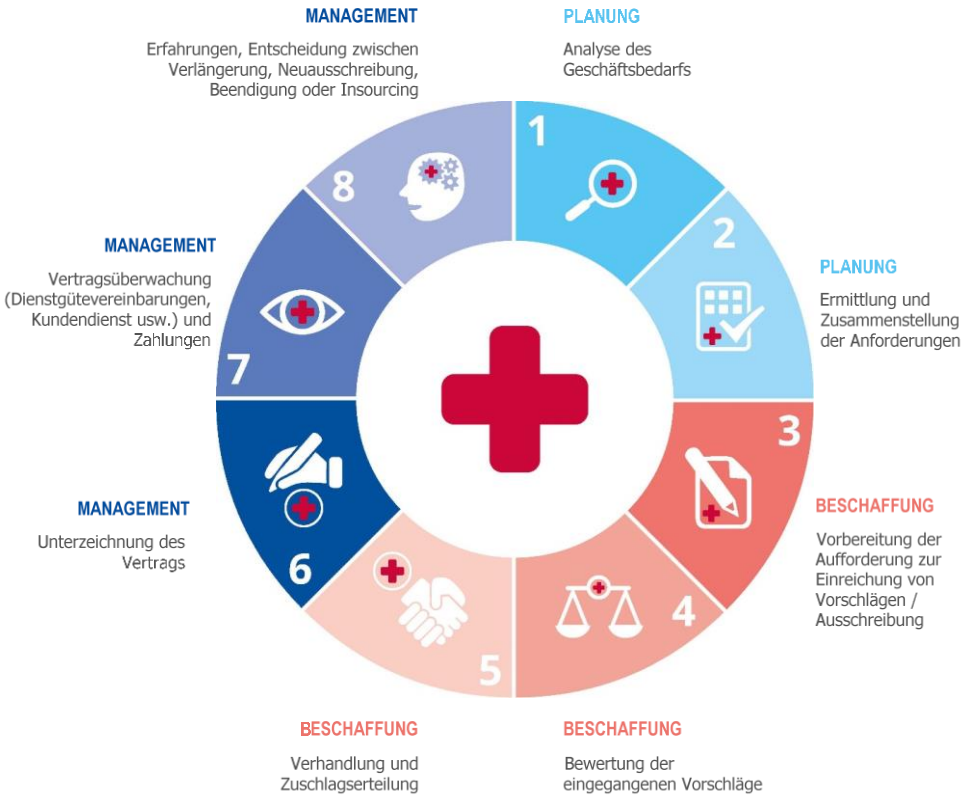
VERGABELEITLINIEN FÜR CYBERSICHERHEIT IN KRANKENHÄUSERN

Der Bericht ist als Leitfaden für Beschäftigte im Gesundheitswesen gedacht. Viele der hierin beschriebenen praktischen Maßnahmen und Empfehlungen sind auch für andere Organisationen der Gesundheitsversorgung nützlich, da die Vergabeverfahren sehr ähnlich sein können. Der Bericht kann Beschäftigten im Gesundheitswesen, die in technischer Funktion in Krankenhäusern tätig sind, Hilfestellung geben; folgende Positionen der Führungsebene kommen als Zielgruppe in Betracht: Leiter Informationstechnik (CIO), Gesamtverantwortliche für Informationssicherheit (CISO), Technikvorstände (CTO), IT-Teams und Vergabebeauftragte in Organisationen der Gesundheitsversorgung. In der vorliegenden Kurzfassung wurden die Hauptpunkte des Berichts zusammengestellt; nähere Einzelheiten sind der im Februar 2020 erschienenen Veröffentlichung der ENISA zu entnehmen: ENISA Good Practices for the Security of Healthcare Services.

VERGABEVERFAHREN

Da das Krankenhausökosystem aus mehreren IT-Komponenten besteht, sollte die Cybersicherheit bei allen diesen verschiedenen Komponenten gesondert untersucht werden. Cybersicherheit sollte auch in den verschiedenen Phasen des Vergabeverfahrens berücksichtigt werden. In diesem Abschnitt werden die üblichen Phasen des Vergabeverfahrens für die Beschaffung von Produkten und Dienstleistungen einschließlich medizinischer Geräte, Informationssysteme und Infrastrukturen vorgestellt.

Abbildung 1: Vergabeverfahrenszyklus für Krankenhäuser



- Planungsphase: Zunächst analysiert das Krankenhaus seinen Bedarf und stellt intern die Anforderungen verschiedener Abteilungen zusammen. Beispiel: Wenn ein neuer Cloud-Dienst beschafft werden soll, sollte der CTO den Bedarf ermitteln und sich darüber informieren, welchen Nutzen dieser Dienst bringen wird.

- Beschaffungsphase: Anschließend werden die Anforderungen in technische Spezifikationen übertragen, und in Zusammenarbeit mit der Vergabestelle wird das Beschaffungsverfahren eingeleitet (z. B. durch die Veröffentlichung einer Ausschreibung). Das Krankenhaus nimmt die entsprechenden Angebote entgegen; der Ausschuss (dem der CTO/CISO und/oder Mitglieder des IT-Teams angehören) bewertet die Angebote und wählt die am besten geeigneten Produkte aus. Anschließend finden die Verhandlungen mit dem Auftragnehmer statt, und der Auftrag wird erteilt.

- Managementphase: Schließlich wird der Vertrag (Management und Überwachung) an den Auftraggeber innerhalb des Krankenhauses übermittelt. Der Beauftragte ist für den Abschluss der Ausschreibung und die Entgegennahme von Rückmeldungen von Nutzern zur tatsächlichen Leistung der Ausrüstung/des Systems/der Dienstleistung zuständig.

BESCHAFFUNGSOBJEKTE IN KRANKENHÄUSERN

Tabelle 1: Beschaffungsobjekte (Anlagentaxonomie)

Beschaffungsobjekt	Beschreibung
Klinische Informationssysteme	Einschließlich der Beschaffung jeglicher Art von Software für den Bereich der medizinischen Versorgung
Medizinische Geräte	Sämtliche für Behandlung, Kontrolle oder Diagnose von Krankheiten bestimmte Geräte
Netzwerkausrüstung	Netzwerkkabel (Koaxialkabel, optische Kabel), Gateways, Router, Schalter, Firewalls, VPN, IPS, IDS usw.
Fernbehandlungssysteme	Anlagen oder Geräte für die Betreuung außerhalb des Krankenhauses, insbesondere für die so genannten „krankenhausbasierten häuslichen Pflegeleistungen“
Mobile Endgeräte	Sämtliche Software, die Gesundheitsbetreuung bietet oder Gesundheitsdaten erfasst und nicht direkt mit dem Krankenhausnetzwerk verbunden ist, wie z. B. Telemedizin-Apps
Identifizierungssysteme	Systeme für die eindeutige Erkennung von Patienten oder medizinischem Personal (biometrische Scanner, Kartenlesegeräte usw.) und die Sicherstellung der Identifizierung und/oder Berechtigungserteilung für den Zugang zu IT-Systemen
Gebäudemanagementsysteme	Alle Arten von Gebäuden, in denen medizinische Anlagen untergebracht werden können
Industrielle Steuerungssysteme	Systeme für die Steuerung aller physischen Aspekte der Zentralen z. B. Systeme für die Stromversorgung, Türverriegelung, Videoüberwachung
Fachliche Dienstleistungen	Alle Arten von ausgelagerten oder nicht ausgelagerten Dienstleistungen, die von Fachleuten oder Unternehmen erbracht werden: medizinische Dienstleistungen, Beförderung, Buchhaltung, Technik, IT, Recht, Wartung/Instandhaltung, Reinigung, Verpflegung usw.
Cloud-Dienste	Alle Arten von Kommunikations- und Informationssystemen oder sonstigen Informationssystemen, die nicht im Krankenhausgebäude oder in einem Rechenzentrum untergebracht sind, das von der IT-Abteilung der Krankenhauszentrale vollständig kontrolliert wird

GEFÄHRDUNGSTAXONOMIE

Verschiedene Beschaffungsobjekte sind mit unterschiedlichen Risiken für die IKT-Umgebung eines Krankenhauses verbunden. Prüfen Sie zusammen mit Ihrer Abteilung für IT-Sicherheit und IT-Risiken anhand dieser Gefährdungstaxonomie, welche Gefährdungen für Ihre Organisation die größte Bedeutung haben. Diese Prüfung sollte unabhängig vom Beschaffungspotenzial Bestandteil der IT-Aufgaben im Krankenhaus sein.

Tabelle 2: Gefährdungsarten (Gefährdungstaxonomie)

Gefährdung	Beispiele
Naturereignisse	Feuer, Hochwasser oder Erdbeben
Versagen der Lieferkette	Versagen des Cloud-Diensteanbieters, Versagen des Netzwerkanbieters, Ausfall der Stromversorgung, Versagen des Herstellers medizinischer Geräte / Nichthaftung
Menschliches Versagen	Fehler in der Konfiguration des Krankenhaussystems, Fehlen von Audit-Logs, Kontrolle des Zugangs durch Unbefugte / Fehlen von Verfahren, Nichteinhaltung der Vorschriften (BYOD), Versagen des medizinischen Personals / der Patienten
Böswilliges Handeln	Malware (Virus, Ransomware, BYOD), Hijacking (Cryptojacking, Medjacking), Social Engineering (Phishing, Ködern (Baiting), Geräteklonen), Diebstahl (Daten, Gerät), Manipulation medizinischer Geräte, Skimming, Denial of Service, webbasierte Angriffe, Angriffe über Webanwendungen, Insiderbedrohung, physische Manipulation / Beschädigung, Identitätsdiebstahl, Cyberspionage, mechanische Störung von Komponenten
Systemversagen	Softwareversagen, veraltete Firmware, Geräteversagen, Versagen von Netzwerkkomponenten, unzureichende Wartung / Instandhaltung

BEWÄHRTE VERFAHRENSWEISEN FÜR CYBERSICHERHEIT IM BESCHAFFUNGSWESEN

Die folgende Liste bewährter Verfahrensweisen (Good Practices, GP) ist keineswegs erschöpfend, bietet jedoch dem IT-Beauftragten im Gesundheitswesen, der für die Beschaffung von Ausrüstung in einem Krankenhaus zuständig ist, eine solide Orientierungshilfe. In diese Zusammenstellung bewährter Verfahrensweisen sind alle Anregungen eingeflossen, die die befragten Fachkräfte im Gesundheitswesen vorgebracht haben. Die Liste kann den Prioritäten der jeweiligen Organisation entsprechend angepasst werden.

GP 1. Einbeziehung der IT-Abteilung in die verschiedenen Phasen des Vergabeverfahrens, um die Berücksichtigung von Fachwissen in Fragen der Cybersicherheit sicherzustellen

Phasen des Vergabeverfahrens: Alle

Zugehörige Beschaffungsobjekte: Alle

Zugehörige Gefährdungen: Alle

GP 2. Einrichtung eines Verfahrens für die Ermittlung von Schwachstellen und für den Umgang mit Schwachstellen, um sicherzustellen, dass Schwachstellen vor der Beschaffung neuer Produkte oder Dienstleistungen berücksichtigt werden und dass Schwachstellen bei vorhandenen Produkten/Dienstleistungen während ihres gesamten Lebenszyklus überwacht werden

Phasen des Vergabeverfahrens: Alle

Zugehörige Beschaffungsobjekte: Klinische Informationssysteme, medizinische Geräte, Netzwerkausrüstung, Fernbehandlungssystem, mobile Endgeräte, Identifizierungssysteme, industrielle Steuerungssysteme, Cloud-Dienste

Zugehörige Gefährdungen: Alle

GP 3. Erarbeitung einer Strategie für die Aktualisierung von Hard- und Software, um sicherzustellen, dass bei Ihrem Betriebssystem und Ihrer Software die neuesten Patches installiert sind und dass die Antivirus-Software aktualisiert wird

Phasen des Vergabeverfahrens:: Alle

Zugehörige Beschaffungsobjekte:: Medizinische Geräte, klinische Informationssysteme, Netzwerkausrüstung, Fernbehandlungssystem, mobile Endgeräte, Identifizierungssysteme, industrielle Steuerungssysteme, Cloud-Dienste

Zugehörige Gefährdungen:: Böswilliges Handeln, Versagen der Lieferkette, Systemversagen

GP 4. Verstärkung der Sicherheitskontrollen für die drahtlose Kommunikation, um sicherzustellen, dass der Zugang zu den WiFi-Netzen des Krankenhauses begrenzt ist und streng kontrolliert wird

Phasen des Vergabeverfahrens:: Alle

Zugehörige Beschaffungsobjekte:: Medizinische Geräte, Remote-Client-Geräte, Identifizierungssysteme, Cloud-Dienste

Zugehörige Gefährdungen:: Böswilliges Handeln, menschliches Versagen

GP 5. Einführung von Teststrategien, um sicherzustellen, dass neu erworbene oder neu konfigurierte Produkte einem Penetrationstest unterzogen werden und dass Abhilfemaßnahmen in Einklang mit den Betriebsparametern der tatsächlichen Umgebung stehen

Phasen des Vergabeverfahrens:: Alle

Zugehörige Beschaffungsobjekte:: Klinische Informationssysteme, medizinische Geräte, Netzwerkausrüstung, Fernbehandlungssystem, mobile Endgeräte, Identifizierungssysteme, Gebäudeverwaltungssystem, industrielle Steuerungssysteme, Cloud-Dienste

Zugehörige Gefährdungen:: Böswilliges Handeln, Systemversagen, menschliches Versagen

GP 6. Einführung von Betriebskontinuitätsplänen, um sicherzustellen, dass das Versagen eines Systems nicht zur Unterbrechung der Kerndienste des Krankenhauses führt und dass die Aufgabe des Lieferanten klar abgegrenzt ist

Phasen des Vergabeverfahrens:: Alle

Zugehörige Beschaffungsobjekte:: Medizinische Geräte, klinische Informationssysteme, Netzwerkausrüstung, Fernbehandlungssystem, mobile Endgeräte, Identifizierungssysteme, industrielle Steuerungssysteme, Cloud-Dienste

Zugehörige Gefährdungen:: Böswilliges Handeln, Versagen der Lieferkette, Systemversagen

GP 7. Berücksichtigung von Fragen der Interoperabilität, um sicherzustellen, dass es keine Sicherheitslücken im Zusammenwirken mit den bereits vorhandenen Komponenten (bestehende IT-Ausrüstung) gibt

Phasen des Vergabeverfahrens: Alle

Zugehörige Beschaffungsobjekte:: Klinische Informationssysteme, medizinische Geräte, Fernbehandlungssystem, mobile Endgeräte, Identifizierungssysteme, industrielle Steuerungssysteme, Cloud-Dienste

Zugehörige Gefährdungen:: Systemversagen, menschliches Versagen, böswilliges Handeln

GP 8. Ermöglichung der Erprobung aller Komponenten, um zu gewährleisten, dass die Komponenten die ihnen zugesagte Leistung auch liefern: Überprüfung der Benutzerfreundlichkeit, Kontrolle der Richtigkeit der Ergebnisse im Betrieb und Kontrolle von Sicherheitsschwachstellen (unzureichende Passwortregeln, SQL-Einschleusung)

Phasen des Vergabeverfahrens:: Alle

Zugehörige Beschaffungsobjekte:: Klinische Informationssysteme, medizinische Geräte, Remote-Client-Geräte, Identifizierungssysteme, Cloud-Dienste, industrielle Steuerungssysteme, Fernbehandlungssystem, Gebäudeverwaltungssystem, mobile Endgeräte

Zugehörige Gefährdungen:: Böswilliges Handeln, menschliches Versagen, Systemversagen, Versagen der Lieferkette

GP 9. Einrichtung der Möglichkeit der Prüfung und der Protokollierung, um Angreifer zurückzuverfolgen und um festzustellen, wie viele Daten im Zuge einer Systemgefährdung verloren gegangen sind bzw. gestohlen wurden

Phasen des Vergabeverfahrens:: Alle

Zugehörige Beschaffungsobjekte:: Medizinische Geräte, Fernbehandlungssystem, mobile Endgeräte, Identifizierungssysteme, industrielle Steuerungssysteme

Zugehörige Gefährdungen:: Böswilliges Handeln, Versagen der Lieferkette, Systemversagen

GP 10. Verschlüsselung sensibler personenbezogener Daten während der Speicherung und der Übertragung durch die Festlegung einer Strategie für Systeme, Dienstleistungen oder Geräte für die Verarbeitung bestimmter Kategorien personenbezogener Daten nach Maßgabe von Artikel 9 DSGVO

Phasen des Vergabeverfahrens:: Alle

Zugehörige Beschaffungsobjekte:: Medizinische Geräte, klinische Informationssysteme, Netzwerkausrüstung, Fernbehandlungssystem, mobile Endgeräte, Identifizierungssysteme, industrielle Steuerungssysteme, Cloud-Dienste

Zugehörige Gefährdungen:: Böswilliges Handeln, Versagen der Lieferkette, Systemversagen

GP 11. Durchführung einer Risikobewertung im Rahmen des Vergabeverfahrens

Phasen des Vergabeverfahrens:: Planung

Zugehörige Beschaffungsobjekte:: Alle

Zugehörige Gefährdungen:: Alle

GP 12. Planung der Netzwerk-, Hardware- und Lizenzanforderungen im Voraus, um festzustellen, ob vor der Installation zusätzliche Aktualisierungen und/oder Käufe zur Anpassung an das neue System erforderlich sind

Phasen des Vergabeverfahrens:: Planung

Zugehörige Beschaffungsobjekte:: Klinische Informationssysteme, Netzwerkausrüstung, Identifizierungssysteme, industrielle Steuerungssysteme

Zugehörige Gefährdungen:: Versagen der Lieferkette, Systemversagen, Naturereignisse, menschliches Versagen

GP 13. Ermittlung der Gefährdungen im Zusammenhang mit der Beschaffung von Produkten oder Dienstleistungen und Gewährleistung, dass Gefährdungen während des gesamten Beschaffungszyklus kontinuierlich ermittelt werden

Phasen des Vergabeverfahrens:: Planung, Management

Zugehörige Beschaffungsobjekte:: Alle

Zugehörige Gefährdungen:: Alle

GP 14. Isolierung Ihres Netzwerks, um sicherzustellen, dass der Verkehr im Netzwerk isoliert und/oder gefiltert werden kann, um den Zugang zu Netzwerkbereichen zu begrenzen und/oder zu verhindern

Phasen des Vergabeverfahrens:: Planung, Beschaffung

Zugehörige Beschaffungsobjekte: Medizinische Geräte, klinische Informationssysteme, Netzwerkausrüstung, Fernbehandlungssystem, mobile Endgeräte, Identifizierungssysteme, industrielle Steuerungssysteme, Cloud-Dienste

Zugehörige Gefährdungen:: Böswilliges Handeln, Versagen der Lieferkette, Systemversagen

GP 15. Festlegung der Netzwerkanforderungen, um Interoperabilität sicherzustellen und um Lücken nach der Erstellung der Netzwerk- und Komponententopologie vorzubeugen

Phasen des Vergabeverfahrens:: Planung

Zugehörige Beschaffungsobjekte:: Klinische Informationssysteme, Netzwerkausrüstung, Identifizierungssysteme, industrielle Steuerungssysteme, Cloud-Dienste, Fernbehandlungssysteme, mobile Endgeräte

Zugehörige Gefährdungen:: Versagen der Lieferkette, Systemversagen, Naturereignisse

GP 16. Festlegung der sicherheitsbezogenen Grundanforderungen und Übertragung dieser Anforderungen in Zulassungskriterien für die Auswahl von Lieferanten

Phasen des Vergabeverfahrens:: Planung, Beschaffung

Zugehörige Beschaffungsobjekte:: Medizinische Geräte, klinische Informationssysteme, Netzwerkausrüstung, Fernbehandlungssystem, mobile Endgeräte, Identifizierungssysteme, industrielle Steuerungssysteme, Cloud-Dienste

Zugehörige Gefährdungen:: Böswilliges Handeln, Versagen der Lieferkette, Systemversagen

GP 17. Erstellung einer speziellen Aufforderung zur Einreichung von Vorschlägen für die Beschaffung von Cloud-Diensten unter Berücksichtigung der gesetzlichen und politischen Anforderungen

Phasen des Vergabeverfahrens:: Planung, Beschaffung

Zugehörige Beschaffungsobjekte:: Cloud-Dienste

Zugehörige Gefährdungen:: Böswilliges Handeln, Versagen der Lieferkette

GP 18. Festlegung einer Rangfolge für die Beschaffung von Vermögenswerten, die nach Cybersicherheitsregelungen/-standards zertifiziert sind

Phasen des Vergabeverfahrens:: Beschaffung

Zugehörige Beschaffungsobjekte:: Medizinische Geräte, klinische Informationssysteme, Netzwerkausrüstung, Fernbehandlungssystem, mobile Endgeräte, Identifizierungssysteme, industrielle Steuerungssysteme, Cloud-Dienste

Zugehörige Gefährdungen:: Böswilliges Handeln, Versagen der Lieferkette, Systemversagen

GP 19. Durchführung von Datenschutz-Folgenabschätzungen bei der Planung der Beschaffung eines neuen Systems oder einer neuen Dienstleistung

Phasen des Vergabeverfahrens:: Beschaffung

Zugehörige Beschaffungsobjekte:: Klinische Informationssysteme, medizinische Geräte, Netzwerkausrüstung, Fernbehandlungssystem, mobile Endgeräte, Identifizierungssysteme, fachliche Dienstleistungen, Cloud-Dienste

Zugehörige Gefährdungen:: Böswilliges Handeln, menschliches Versagen

GP 20. Einrichtung von Gateways, die die ständige Verbindung vorhandener Systeme/Maschinen sicherstellen, sowie von Kontrollen an den Nahtstellen dieser Systeme/Maschinen für den Fall von Problemen innerhalb dieser Gruppen

Phasen des Vergabeverfahrens:: Beschaffung, Management

Zugehörige Beschaffungsobjekte:: Medizinische Geräte, Fernbehandlungssystem, mobile Endgeräte, Identifizierungssysteme, industrielle Steuerungssysteme

Zugehörige Gefährdungen:: Böswilliges Handeln, Versagen der Lieferkette, Systemversagen

GP 21. Cybersicherheitsschulungen zu den Sicherheitsverfahren der Organisation, um die entsprechende Einweisung von internen Mitarbeitern oder externen Auftragnehmern/Beratern, die in den Räumlichkeiten der Organisation tätig sind, sicherzustellen

Phasen des Vergabeverfahrens:: Beschaffung, Management

Zugehörige Beschaffungsobjekte:: Alle

Zugehörige Gefährdungen:: Böswilliges Handeln, menschliches Versagen

GP 22. Erarbeitung von Reaktionsplänen bei Störfällen für die neu erworbenen Produkte oder Systeme

Phasen des Vergabeverfahrens:: Beschaffung, Management

Zugehörige Beschaffungsobjekte:: Medizinische Geräte, klinische Informationssysteme, Netzwerkausrüstung, Fernbehandlungssystem, mobile Endgeräte, Identifizierungssysteme, industrielle Steuerungssysteme, Cloud-Dienste

Zugehörige Gefährdungen:: Böswilliges Handeln, Versagen der Lieferkette, Systemversagen

GP 23. Einbindung des Verkäufers/Herstellers in das Störfallmanagement und Vorgabe klarer Bedingungen in der Aufforderung zur Einreichung von Vorschlägen

Phasen des Vergabeverfahrens:: Beschaffung, Management

Zugehörige Beschaffungsobjekte:: Medizinische Geräte, klinische Informationssysteme, Netzwerkausrüstung, Fernbehandlungssystem, mobile Endgeräte, Identifizierungssysteme, industrielle Steuerungssysteme, Cloud-Dienste

Zugehörige Gefährdungen:: Böswilliges Handeln, Versagen der Lieferkette, Systemversagen

GP 24. Festlegung eines Zeitplans für Wartungs-/Instandhaltungsarbeiten und Überwachung dieser Arbeiten für sämtliche Ausrüstung, um ein angemessenes Funktionsniveau sicherzustellen und über etwaige Aktualisierungen/Patches usw. zu entscheiden

Phasen des Vergabeverfahrens:: Beschaffung, Management

Zugehörige Beschaffungsobjekte:: Klinische Informationssysteme, Netzwerkausrüstung, medizinische Geräte, Gebäudeverwaltungssysteme, Fernbehandlungssystem, mobile Endgeräte, Identifizierungssysteme, industrielle Steuerungssysteme, Cloud-Dienste

Zugehörige Gefährdungen:: Menschliches Versagen, Systemversagen, Naturereignisse

GP 25. Der Fernzugriff sollte auf ein Mindestmaß zurückgeführt werden und geregelt sein, so dass die externe Kommunikation mit dem Lieferanten nur auf das zu kontrollierende Gerät beschränkt sein sollte.

Phasen des Vergabeverfahrens:: Beschaffung, Management

Zugehörige Beschaffungsobjekte:: Medizinische Geräte, klinische Informationssysteme, Netzwerkausrüstung, Fernbehandlungssystem, mobile Endgeräte, Identifizierungssysteme, industrielle Steuerungssysteme, Cloud-Dienste

Zugehörige Gefährdungen:: Böswilliges Handeln, Versagen der Lieferkette, Systemversagen, menschliches Versagen

GP 26. Anforderung von Patches für alle Komponenten und Aufnahme der Informationen in die Aufforderung zur Einreichung von Vorschlägen

Phasen des Vergabeverfahrens:: Beschaffung, Management

Zugehörige Beschaffungsobjekte:: Medizinische Geräte, klinische Informationssysteme, Netzwerkausrüstung, Fernbehandlungssystem, mobile Endgeräte, Identifizierungssysteme, industrielle Steuerungssysteme, Cloud-Dienste

Zugehörige Gefährdungen:: Böswilliges Handeln, Versagen der Lieferkette, Systemversagen

GP 27. Sensibilisierung der Mitarbeiter für Cybersicherheit, um sicherzustellen, dass sich die Mitarbeiter der Risiken bewusst sind, die mit neu erworbenen Produkten oder Dienstleistungen verbunden sind

Phasen des Vergabeverfahrens:: Steuerung

Zugehörige Beschaffungsobjekte:: Alle

Zugehörige Gefährdungen:: Alle

GP 28. Durchführung von Bestandsanlagen- und Konfigurationsmanagement, um sicherzustellen, dass die Bestandsanlagen bei Hinzufügung einer Komponente zur IKT-Umgebung oder bei Entfernung einer Komponente aus dieser Umgebung entsprechend aktualisiert werden und dass grundlegende Sicherheitskonfigurationen für IKT-Komponenten vorhanden sind und angemessen gemanagt werden

Phasen des Vergabeverfahrens:: Steuerung

Zugehörige Beschaffungsobjekte:: Klinische Informationssysteme, medizinische Geräte, Netzwerkausrüstung, Fernbehandlungssystem, mobile Endgeräte, Identifizierungssysteme

Zugehörige Gefährdungen:: Böswilliges Handeln, menschliches Versagen, Systemversagen

GP 29. Festlegung der speziellen Zugangskontrollmechanismen für medizinische Geräte, die auch physisch geschützt und nur bestimmten Mitarbeitern zugänglich sein sollten

Phasen des Vergabeverfahrens:: Steuerung

Zugehörige Beschaffungsobjekte:: Medizinische Geräte, Gebäudeverwaltungssystem, Identifizierungssysteme

Zugehörige Gefährdungen:: Böswilliges Handeln, menschliches Versagen

GP 30. Festlegung des Zeitplans für Penetrationstests, die häufig oder nach einer Veränderung der Architektur/des Systems durchgeführt werden sollten, und Aufnahme der Bedingungen in die Aufforderung zur Einreichung von Vorschlägen

Phasen des Vergabeverfahrens:: Beschaffung, Management

Zugehörige Beschaffungsobjekte:: Medizinische Geräte, klinische Informationssysteme, Netzwerkausrüstung, Fernbehandlungssystem, mobile Endgeräte, Identifizierungssysteme, industrielle Steuerungssysteme, Cloud-Dienste

Zugehörige Gefährdungen:: Böswilliges Handeln, Versagen der Lieferkette, Systemversagen