CENTRE FOR
CYBERSECURITY
BELGIUM

CyberGrundlagen

ESSENTIAL

Version: 01.03.2023

Centre for Cybersecurity Belgium
Unter der Autorität des Premierministers

Inhaltsübersicht

EINLEITUNG 7
IDENTIFIZIEREN (IDENTIFY)
ID.AM-1: PHYSISCHE GERÄTE UND SYSTEME, DIE INNERHALB DER ORGANISATION VERWENDET WERDEN, SIND INVENTARISIERT. 9
ID.AM-2: DIE IN DER ORGANISATION VERWENDETEN SOFTWARE-PLATTFORMEN UND ANWENDUNGEN SIND INVENTARISIERT. 10
ID.AM-3: ORGANISATORISCHE KOMMUNIKATIONS- UND DATENFLÜSSE SIND ABGEBILDET 11
ID.AM-4: EXTERNE INFORMATIONSSYSTEME WERDEN KATALOGISIERT. 12
ID.AM-5: RESSOURCEN WERDEN AUF DER GRUNDLAGE IHRER KLASSIFIZIERUNG, IHRER KRITIKALITÄT UND IHRES GESCHÄFTSWERTS NACH PRIORITÄTEN GEORDNET 13
ID.AM-6: ROLLEN, VERANTWORTLICHKEITEN UND BEFUGNISSE IM BEREICH DER CYBERSICHERHEIT FÜR DIE GESAMTE BELEGSCHAFT UND DRITTE (Z.B. LIEFERANTEN, KUNDEN, PARTNER) SIND FESTGELEGT. 14
ID.BE-1: DIE ROLLE DER ORGANISATION IN DER LIEFERKETTE IST IDENTIFIZIERT UND KOMMUNIZIERT. 15
ID.BE-2: DIE STELLUNG DER ORGANISATION IN DER KRITISCHEN INFRASTRUKTUR UND IHREM WIRTSCHAFTSZWEIG IST IDENTIFIZIERT UND KOMMUNIZIERT. 15
ID.BE-3: PRIORITÄTEN FÜR DEN AUFTRAG, DIE ZIELE UND DIE AKTIVITÄTEN DER ORGANISATION SIND FESTGELEGT UND WERDEN KOMMUNIZIERT. 16
ID.BE-4: ABHÄNGIGKEITEN UND KRITISCHE FUNKTIONEN FÜR DIE ERBRINGUNG VON KRITISCHEN DIENSTEN SIND FESTGELEGT. 16
ID.BE-5: ANFORDERUNGEN AN DIE WIDERSTANDSFÄHIGKEIT ZUR UNTERSTÜTZUNG DER ERBRINGUNG KRITISCHER DIENSTE SIND FÜR ALLE BETRIEBSZUSTÄNDE FESTGELEGT (Z.B. UNTER DRUCK/ANGRIFF, WÄHREND DER WIEDERHERSTELLUNG, IM NORMALBETRIEB). 17
ID.GV-1: ORGANISATORISCHE CYBERSICHERHEITSRICHTLINIEN SIND FESTGELEGT UND WERDEN KOMMUNIZIERT. 18
ID.GV-3: RECHTLICHE UND REGULATORISCHE ANFORDERUNGEN AN DIE CYBERSICHERHEIT, EINSCHLIEßLICH DER VERPFLICHTUNGEN ZUM SCHUTZ DER PRIVATSPHÄRE UND DER BÜRGERLICHEN FREIHEITEN, WERDEN VERSTANDEN UND GEHANDHABT. 19
ID.GV-4: GOVERNANCE- UND RISIKOMANAGEMENTPROZESSE ADRESSIEREN CYBERSICHERHEITSRISIKEN. 19
ID.RA-1: SCHWACHSTELLEN VON VERMÖGENSWERTEN WERDEN IDENTIFIZIERT UND DOKUMENTIERT. 20
ID.RA-2: DIE INFORMATIONEN ÜBER CYBER-BEDROHUNGEN STAMMEN AUS FOREN UND QUELLEN FÜR DEN INFORMATIONSAUSTAUSCH. 21
ID.RA-5: BEDROHUNGEN, SCHWACHSTELLEN, WAHRSCHEINLICHKEITEN UND AUSWIRKUNGEN WERDEN ZUR RISIKOBESTIMMUNG VERWENDET 21
ID.RA-6: MAßNAHMEN GEGEN RISIKEN WERDEN ERMITTELT UND NACH PRIORITÄTEN GEORDNET 22
ID.RM-1: RISIKOMANAGEMENTPROZESSE SIND ETABLIERT, VERWALTET UND VON DEN ORGANISATORISCHEN STAKEHOLDERN AKZEPTIERT. 23
ID.RM-2: DIE RISIKOTOLERANZ DER ORGANISATION IST FESTGELEGT UND KLAR FORMULIERT. 23
ID.RM-3: DIE RISIKOTOLERANZ DER ORGANISATION WIRD DURCH IHRE ROLLE IN KRITISCHEN INFRASTRUKTUREN UND SEKTORSPEZIFISCHEN RISIKOANALYSEN BESTIMMT. 23
ID.SC-1: PROZESSE ZUM MANAGEMENT VON RISIKEN IN DER CYBER SUPPLY CHAIN SIND IDENTIFIZIERT, ETABLIERT, BEWERTET, VERWALTET UND VON ALLEN BETEILIGTEN IN DER ORGANISATION AKZEPTIERT. 24
ID.SC-2: LIEFERANTEN UND DRITTPARTEIEN VON INFORMATIONSSYSTEMEN, KOMPONENTEN UND DIENSTLEISTUNGEN WERDEN IDENTIFIZIERT, NACH PRIORITÄTEN GEORDNET UND MIT HILFE EINES PROZESSES ZUR RISIKOBEWERTUNG IN DER CYBER-LIEFERKETTE BEWERTET. 24
ID.SC-3: VERTRÄGE MIT LIEFERANTEN UND DRITTANBIETERN WERDEN GENUTZT, UM GEEIGNETE MAßNAHMEN UMZUSETZEN, DIE DIE ZIELE DES CYBERSICHERHEITSPROGRAMMS UND DES CYBER SUPPLY CHAIN RISK MANAGEMENT PLANS EINER ORGANISATION ERFÜLLEN. 26
ID.SC-4: LIEFERANTEN UND DRITTPARTNER WERDEN ROUTINEMÄßIG ANHAND VON AUDITS, TESTERGEBNISSEN ODER ANDEREN FORMEN DER BEWERTUNG BEURTEILT, UM ZU BESTÄTIGEN, DASS SIE IHREN VERTRAGLICHEN VERPFLICHTUNGEN NACHKOMMEN. 27
ID.SC-5: REAKTIONS- UND WIEDERHERSTELLUNGSPLANUNG UND -TESTS WERDEN MIT LIEFERANTEN UND DRITTANBIETERN DURCHGEFÜHRT. 27

SCHÜTZEN (PROTECT)

PR.AC-1: IDENTITÄTEN UND BERECHTIGUNGSNACHWEISE WERDEN FÜR AUTORISIERTE GERÄTE, BENUTZER UND PROZESSE AUSGESTELLT, VERWALTET, VERIFIZIERT, WIDERRUFEN UND GEPRÜFT. 28
PR.AC-2: DER PHYSISCHE ZUGANG ZU VERMÖGENSWERTEN WIRD VERWALTET UND GESCHÜTZT 29
PR.AC-3: DER FERNZUGRIFF WIRD VERWALTET. 30
PR.AC-4: ZUGRIFFSBERECHTIGUNGEN UND -AUTORISIERUNGEN WERDEN UNTER BERÜCKSICHTIGUNG DER GRUNDSÄTZE DES GERINGSTEN RECHTSANSPRUCHS UND DER AUFGABENTRENNUNG VERWALTET. 32
PR.AC-5: DIE NETZINTEGRITÄT (NETZTRENNUNG, NETZSEGMENTIERUNG ...) IST GESCHÜTZT. 34
PR.AC-6: IDENTITÄTEN WERDEN GEPRÜFT UND AN BERECHTIGUNGSNACHWEISE GEBUNDEN UND IN INTERAKTIONEN GELTEND GEMACHT. 36
PR.AC-7: IDENTITÄTEN WERDEN GEPRÜFT UND AN BERECHTIGUNGSNACHWEISE GEBUNDEN UND IN INTERAKTIONEN GELTEND GEMACHT. 36
PR.AT-1: ALLE NUTZER SIND INFORMIERT UND GESCHULT. 37
PR.AT-2: PRIVILEGIERTE BENUTZER VERSTEHEN IHRE ROLLEN UND VERANTWORTLICHKEITEN. 38
PR.AT-3: DRITTE STAKEHOLDER (Z.B. LIEFERANTEN, KUNDEN, PARTNER) VERSTEHEN IHRE ROLLEN UND VERANTWORTLICHKEITEN. 38
PR.AT-4: LEITENDE ANGESTELLTE VERSTEHEN IHRE AUFGABEN UND VERANTWORTLICHKEITEN. 39
PR.AT-5: DAS PERSONAL FÜR PHYSISCHE SICHERHEIT UND CYBERSICHERHEIT KENNT SEINE AUFGABEN UND VERANTWORTLICHKEITEN. 39
PR.DS-1: DATA-AT-REST IST GESCHÜTZT. 40
PR.DS-2: DATA-IN-TRANSIT IST GESCHÜTZT. 40
PR.DS-3: DIE VERMÖGENSWERTE WERDEN WÄHREND DES GESAMTEN UMZUGS, DER VERBRINGUNG UND DER VERÄUßERUNG FORMELL VERWALTET. 41
PR.DS-5: SCHUTZMAßNAHMEN GEGEN DATENLECKS SIND IMPLEMENTIERT 43
PR.DS-6: INTEGRITÄTSPRÜFUNGSMECHANISMEN WERDEN VERWENDET, UM DIE INTEGRITÄT VON SOFTWARE, FIRMWARE UND INFORMATIONEN ZU ÜBERPRÜFEN. 43
PR.DS-7: DIE ENTWICKLUNGS- UND TESTUMGEBUNG(EN) SIND VON DER PRODUKTIONSUMGEBUNG GETRENNT. 44
PR.DS-8: INTEGRITÄTSPRÜFUNGSMECHANISMEN WERDEN ZUR ÜBERPRÜFUNG DER HARDWARE-INTEGRITÄT VERWENDET. 44
PR.IP-1: ES WIRD EINE BASISKONFIGURATION VON INFORMATIONSTECHNISCHEN/INDUSTRIELLEN KONTROLLSYSTEMEN ERSTELLT UND GEPFLEGT, DIE SICHERHEITSGRUNDSÄTZE ENTHÄLT. 45
PR.IP-2: EIN SYSTEMENTWICKLUNGS-LEBENSZYKLUS ZUR VERWALTUNG VON SYSTEMEN WIRD EINGEFÜHRT 46
PR.IP-3: PROZESSE ZUR KONTROLLE VON KONFIGURATIONSÄNDERUNGEN SIND VORHANDEN 46
PR.IP-4: BACKUPS VON INFORMATIONEN WERDEN DURCHGEFÜHRT, GEPFLEGT UND GETESTET. 47
PR.IP-5: RICHTLINIEN UND VORSCHRIFTEN BEZÜGLICH DER PHYSISCHEN BETRIEBSUMGEBUNG FÜR DIE VERMÖGENSWERTE DER ORGANISATION WERDEN EINGEHALTEN. 48
PR.IP-6: DIE DATEN WERDEN GEMÄß DER RICHTLINIE VERNICHTET. 49
PR.IP-7: SCHUTZVERFAHREN WERDEN VERBESSERT. 49
PR.IP-8: DIE WIRKSAMKEIT VON SCHUTZTECHNOLOGIEN WIRD GEMEINSAM GENUTZT. 50
PR.IP-9: REAKTIONSPLÄNE (INCIDENT RESPONSE UND BUSINESS CONTINUITY) UND WIEDERHERSTELLUNGSPLÄNE (INCIDENT RECOVERY UND DISASTER RECOVERY) SIND VORHANDEN UND WERDEN VERWALTET. 51
PR.IP-11: DIE CYBERSICHERHEIT WIRD IN DIE PRAKTIKEN DES PERSONALWESENS EINBEZOGEN (DEPROVISIONIERUNG, PERSONALAUSWAHL...). 52
PR.IP-12: EIN PLAN FÜR DAS MANAGEMENT VON SCHWACHSTELLEN WIRD ENTWICKELT UND UMGESETZT. 52
PR.MA-1: WARTUNG UND REPARATUR VON ORGANISATIONSMITTELN WERDEN MIT GENEHMIGTEN UND KONTROLLIERTEN MAßNAHMEN DURCHGEFÜHRT UND PROTOKOLLIERT. 53
PR.MA-2: DIE FERNWARTUNG VON UNTERNEHMENSRESSOURCEN WIRD GENEHMIGT, PROTOKOLLIERT UND IN EINER WEISE DURCHGEFÜHRT, DIE UNBEFUGTEN ZUGRIFF VERHINDERT. 54
PR.PT-1: AUDIT-/PROTOKOLLAUFZEICHNUNGEN WERDEN IN ÜBEREINSTIMMUNG MIT DER RICHTLINIE FESTGELEGT, DOKUMENTIERT, UMGESETZT UND ÜBERPRÜFT. 56

PR.PT-2: WECHSELDATENTRÄGER SIND GESCHÜTZT UND IHRE NUTZUNG IST GEMÄß DER RICHTLINIE EINGESCHRÄNKT. 57
PR.PT-3: DAS PRINZIP DES GERINGSTEN FUNKTIONSUMFANGS WIRD BERÜCKSICHTIGT, INDEM DIE SYSTEME SO KONFIGURIERT WERDEN, DASS SIE NUR WESENTLICHE FUNKTIONEN BIETEN. 57
PR.PT-4: KOMMUNIKATIONS- UND KONTROLLNETZE SIND GESCHÜTZT. 58
ERKENNEN (DETECT)
DE.AE-1: EINE GRUNDLAGE FÜR DEN NETZBETRIEB UND DIE ERWARTETEN DATENSTRÖME FÜR NUTZER UND SYSTEME WIRD ERSTELLT UND VERWALTET. 59
DE.AE-2: ERKANNTE EREIGNISSE WERDEN ANALYSIERT, UM ANGRIFFSZIELE UND -METHODEN ZU VERSTEHEN. 59
DE.AE-3: EREIGNISDATEN WERDEN VON MEHREREN QUELLEN UND SENSOREN GESAMMELT UND KORRELIERT. 60
DE.AE-4: DIE AUSWIRKUNGEN VON EREIGNISSEN WERDEN ERMITTELT. 60
DE.AE-5: SCHWELLENWERTE FÜR STÖRFALLWARNUNGEN SIND FESTGELEGT. 61
DE.CM-1: DAS NETZWERK WIRD ÜBERWACHT, UM POTENZIELLE CYBERSICHERHEITS-EREIGNISSE ZU ERKENNEN. 62
DE.CM-2: DIE AKTIVITÄTEN DES PERSONALS WERDEN ÜBERWACHT, UM POTENZIELLE CYBERSICHERHEITSVORFÄLLE ZU ERKENNEN. 63
DE.CM-3: DIE AKTIVITÄTEN DES PERSONALS WERDEN ÜBERWACHT, UM POTENZIELLE CYBERSICHERHEITSVORFÄLLE ZU ERKENNEN. 63
DE.CM-4: BÖSARTIGER CODE WIRD ERKANNT. 64
DE.CM-5: UNERLAUBTER HANDY-CODE WIRD ERKANNT. 64
DE.CM-6: DIE AKTIVITÄTEN VON EXTERNEN DIENSTLEISTERN WERDEN ÜBERWACHT, UM POTENZIELLE CYBERSICHERHEITSREIGNISSE ZU ERKENNEN. 65
DE.CM-7: DIE ÜBERWACHUNG AUF UNBEFUGTES PERSONAL, VERBINDUNGEN, GERÄTE UND SOFTWARE WIRD DURCHGEFÜHRT. 65
DE.CM-8: SCHWACHSTELLEN-SCANS WERDEN DURCHGEFÜHRT. 66
DE.DP-2: DETEKTIONSTÄTIGKEITEN ERFÜLLEN ALLE GELTENDEN ANFORDERUNGEN. 67
DE.DP-3: ERKENNUNGSPROZESSE WERDEN GETESTET 67
DE.DP-4: INFORMATIONEN ZUR EREIGNISERKENNUNG WERDEN ÜBERMITTELT 67
DE.DP-5: DIE ERKENNUNGSVERFAHREN WERDEN KONTINUIERLICH VERBESSERT. 68
REAGIEREN (RESPOND)
RS.RP-1: DER REAKTIONSPLAN WIRD WÄHREND ODER NACH EINEM VORFALL AUSGEFÜHRT. 69
RS.CO-1: DAS PERSONAL KENNT SEINE ROLLE UND DIE REIHENFOLGE DER MAßNAHMEN, WENN EINE REAKTION ERFORDERLICH IST. 70
RS.CO-2: VORFÄLLE WERDEN GEMÄß DEN FESTGELEGTEN KRITERIEN GEMELDET. 70
RS.CO-3: DER INFORMATIONSAUSTAUSCH ERFOLGT IN ÜBEREINSTIMMUNG MIT DEN REAKTIONSPLÄNEN. 71
RS.CO-4: DIE KOORDINIERUNG MIT DEN BETEILIGTEN ERFOLGT IM EINKLANG MIT DEN REAKTIONSPLÄNEN. 71
RS.CO-5: ES FINDET EIN FREIWILLIGER INFORMATIONSAUSTAUSCH MIT EXTERNEN AKTEUREN STATT, UM EIN BREITERES BEWUSSTSEIN FÜR DIE LAGE IM BEREICH DER CYBERSICHERHEIT ZU SCHAFFEN. 72
RS.AN-1: MELDUNGEN VON DETEKTIONSSYSTEMEN WERDEN UNTERSUCHT. 73
RS.AN-2: DIE AUSWIRKUNGEN DES VORFALLS WERDEN VERSTANDEN. 73
RS.AN-3: FORENSISCHE UNTERSUCHUNGEN WERDEN DURCHGEFÜHRT. 74
RS.AN-4: ZWISCHENFÄLLE WERDEN IN ÜBEREINSTIMMUNG MIT DEN REAKTIONSPLÄNEN KATEGORISIERT. 74
RS.AN-5: ES SIND PROZESSE EINGERICHTET, UM SCHWACHSTELLEN ZU EMPFANGEN, ZU ANALYSIEREN UND DARAUF ZU REAGIEREN, DIE DER ORGANISATION AUS INTERNEN UND EXTERNEN QUELLEN (Z.B. INTERNE TESTS, SICHERHEITSBULLETINS ODER SICHERHEITSFORSCHER) BEKANNT WERDEN. 74
RS.MI-1: VORFÄLLE SIND EINGEDÄMMT. 76
RS.MI-2: ZWISCHENFÄLLE WERDEN ENTSCHÄRFT. 76
RS.MI-3: NEU ERKANNTE SCHWACHSTELLEN WERDEN ENTSCHÄRFT ODER ALS AKZEPTIERTE RISIKEN DOKUMENTIERT. 76
RS.IM-1: REAKTIONSPLÄNE BERÜCKSICHTIGEN DIE GEWONNENEN ERKENNTNISSE. 77
RS.IM-2: REAKTIONSPLÄNE BERÜCKSICHTIGEN DIE GEWONNENEN ERKENNTNISSE. 77

WIEDERHERSTELLEN (RECOVER)

RC.RP-1: DER WIEDERHERSTELLUNGSPLAN WIRD WÄHREND ODER NACH EINEM CYBERSICHERHEITSVORFALL AUSGEFÜHRT. ... 78
RC.IM-1: IN DEN WIEDERHERSTELLUNGSPLÄNEN WERDEN DIE GEWONNENEN ERKENNTNISSE BERÜCKSICHTIGT. ... 79
RC.IM-2: DIE WIEDERHERSTELLUNGSSTRATEGIEN WERDEN AKTUALISIERT. ... 79
RC.CO-1: DIE ÖFFENTLICHKEITSARBEIT WIRD GEREGELT. ... 80
RC.CO-2: DIE REPUTATION WIRD NACH EINEM VORFALL WIEDERHERGESTELLT. ... 80
RC.CO-3: DIE WIEDERHERSTELLUNGSMAßNAHMEN WERDEN DEN INTERNEN UND EXTERNEN INTERESSENVERTRETERN SOWIE DEN GESCHÄFTSFÜHRUNGS- UND MANAGEMENTTEAMS MITGETEILT. ... 81

ANHANG A: LISTE DER SCHLÜSSELMAßNAHMEN FÜR DAS SICHERHEITSNIVEAU "BASIS ... 82
ANHANG B: LISTE DER ZUSÄTZLICHEN SCHLÜSSELMAßNAHMEN FÜR DIE ZUVERLÄSSIGKEITSSTUFEN "WICHTIG" UND "WESENTLICH" ... 84
ANHANG C: LISTE DER ZUSÄTZLICHEN SCHLÜSSELMAßNAHMEN FÜR DIE ZUVERLÄSSIGKEITSSTUFEN "WESENTLICH ... 86

Einleitung

Der **CyberFundamentals Framework** ist eine Reihe konkreter Maßnahmen um:

- Daten zu schützen,
- das Risiko der häufigsten Cyberangriffe deutlich zu verringern,
- die Cyber-Resilienz einer Organisation zu erhöhen.

Die Anforderungen und Anleitungen werden durch die einschlägigen Erkenntnisse des NIST/CSF-Framework, der ISO 27001/ISO 27002, der IEC 62443 und der CIS Critical security Controls (ETSI TR 103 305-1) ergänzt.

Die Kodierung der Anforderungen entspricht den im NIST CSF Framework verwendeten Codes. Da nicht alle Anforderungen des NIST CSF anwendbar sind, können einige Codes, die im NIST CSF Framework vorhanden sind, fehlen.

Das Rahmenwerk und der verhältnismäßige Ansatz der Sicherheitsstufen wurden von Praktikern in der Praxis und unter Verwendung anonymisierter, realer Cyberangriffsinformationen validiert, die vom föderalen Cyber Emergency Response Team (CERT - der operative Dienst des Zentrums für Cybersicherheit Belgien) bereitgestellt wurden.

Der **CyberFundamentals Framework basiert auf** fünf Kernfunktionen: identifizieren, schützen, erkennen, reagieren und wiederherstellen. Diese Funktionen ermöglichen es, unabhängig von der Organisation und der Branche, die Kommunikation rund um die Cybersicherheit sowohl unter den technischen Fachleuten als dem restlichen Personal zu fördern, so dass cyberbezogene Risiken in die allgemeine Risikomanagementstrategie der Organisation einbezogen werden können.

- **Identifizieren Sie**
  Kennen Sie die wichtigsten Cyber-Bedrohungen für Ihre wertvollsten Güter. Im Grunde kann man nicht schützen, wovon man nicht weiß, dass es überhaupt existiert. Diese Funktion hilft dabei, ein organisatorisches Verständnis dafür zu entwickeln, wie Cybersicherheitsrisiken in Bezug auf Systeme, Menschen, Vermögenswerte, Daten und Fähigkeiten zu handhaben sind.
- **Schützen Sie**
  Die Schutzfunktion konzentriert sich auf die Entwicklung und Umsetzung von Schutzmaßnahmen, die zur Abschwächung oder Eindämmung eines Cyberrisikos erforderlich sind.
- **Erkennen Sie**
  Der Zweck der Detektierfunktion besteht darin, die rechtzeitige Erkennung von Cybersicherheitsvorfällen zu gewährleisten.
- **Antworten Sie**
  Bei der Funktion Reagieren handelt es sich um Kontrollen, die helfen auf Cybersicherheitsvorfälle zu reagieren. Die Funktion Reagieren unterstützt die Fähigkeit, die Auswirkungen eines potenziellen Cybersicherheitsvorfalls einzudämmen.

- **Wiederherstellen**
  Die Wiederherstellungsfunktion konzentriert sich auf die Schutzmaßnahmen, die zur Aufrechterhaltung der Widerstandsfähigkeit und zur Wiederherstellung von Diensten beitragen, die von einem Cybersicherheitsvorfall betroffen waren.

Um den Schweregrad der Bedrohungeiner Organisation gerecht zu werden, werden zusätzlich zur Ausgangsstufe ***Small*** drei weitere Sicherheitsstufen angeboten: ***Basic, Wichtig und Wesentlich***.

Die **Einstiegsstufe Small** ermöglicht es einer Organisation, eine erste Bewertung vorzunehmen. Sie ist für Mikro-Organisationen oder Organisationen mit begrenzten technischen Kenntnissen gedacht.

Die **Sicherheitsstufe Basic** enthält die Standard-Informationssicherheitsmaßnahmen für alle Unternehmen. Diese bieten einen effektiven Sicherheitswert mit Technologien und Prozessen, die im Allgemeinen bereits verfügbar sind. Wo es gerechtfertigt ist, werden die Maßnahmen angepasst und verfeinert.
Aufbauend auf der Sicherheitsstufe ***Basic*** können Sicherheitsmaßnahmen ergänzt wirden, um Organisationen vor erhöhten Cyberrisiken zu schützen und ein höheres Maß an Sicherheit zu erreichen.

Die **Sicherheitsstufe Wichtig** soll das Risiko gezielter Cyberangriffe durch Akteure mit einfachen Fähigkeiten und Ressourcen zusätzlich zu den bekannten Cybersicherheitsrisiken minimieren.

Die **Sicherheitsstufe Essential** geht noch einen Schritt weiter, um auch dem Risiko fortgeschrittener Cyberangriffe durch Akteure mit umfangreichen Fähigkeiten und Ressourcen zu begegnen.

Mehrere Kontrollen erfordern besondere Aufmerksamkeit; diese Maßnahmen sind als **- Schlüsselmaßnahme -** gekennzeichnet.

Das Rahmenwerk ist ein lebendiges Dokument und wird unter Berücksichtigung des Feedbacks der Interessengruppen, des sich entwickelnden Risikos spezifischer Cybersicherheitsbedrohungen, der Verfügbarkeit technischer Lösungen und fortschreitender Erkenntnisse ständig aktualisiert und verbessert.

Die Daten, Mitarbeiter, Geräte, Systeme und Einrichtungen, die es der Organisation ermöglichen, ihre Geschäftsziele zu erreichen, werden entsprechend ihrer relativen Bedeutung für die Unternehmensziele und die Risikostrategie der Organisation identifiziert und verwaltet.

ID.AM-1: Physische Geräte und Systeme, die innerhalb der Organisation verwendet werden, sind inventarisiert.

Ein Inventar von Vermögenswerten im Zusammenhang mit Informationen und Informationsverarbeitungseinrichtungen innerhalb der Organisation ist zu dokumentieren, zu überprüfen und bei Änderungen zu aktualisieren.

Leitfaden

- Zu diesem Bestand gehören stationäre und tragbare Computer, Tablets, Mobiltelefone, speicherprogrammierbare Steuerungen (SPS), Sensoren, Aktoren, Roboter, Werkzeugmaschinen, Firmware, Netzwerk-Switches, Router, Netzteile und andere vernetzte Komponenten oder Geräte.
- Dieses Inventar muss alle Anlagen umfassen, unabhängig davon, ob sie mit dem Netzwerk der Organisation verbunden sind oder nicht.
- Der Einsatz eines IT-Asset-Management-Tools kann in Betracht gezogen werden.

Das Inventar von Vermögenswerten im Zusammenhang mit Informationen und Informationsverarbeitungseinrichtungen muss Veränderungen im Kontext der Organisation widerspiegeln und alle Informationen enthalten, die für eine wirksame Rechenschaftspflicht erforderlich sind.

Leitfaden

- Zu den Bestandsspezifikationen gehören z. B. Hersteller, Gerätetyp, Modell, Seriennummer, Rechnernamen und Netzwerkadressen, physischer Standort...
- Rechenschaftspflicht bedeutet die Verpflichtung, sein Handeln zu erklären, zu rechtfertigen und die Verantwortung dafür zu übernehmen, und impliziert die Verantwortlichkeit für das Ergebnis einer Aufgabe oder eines Prozesses.
- Zu den Änderungen gehört auch die Stilllegung von Material.

Wird nicht zugelassene Hardware entdeckt, wird sie für eine mögliche Ausnahmebehandlung unter Quarantäne gestellt, entfernt oder ersetzt. Das Inventar wird entsprechend aktualisiert.

Leitfaden

- Jede nicht unterstützte Hardware ohne eine Ausnahmedokumentation wird als nicht autorisiert eingestuft.
- Nicht autorisierte Hardware kann bei der Inventarisierung, bei Supportanfragen durch den Benutzer oder auf andere Weise entdeckt werden.

Es sind Mechanismen zur Erkennung des Vorhandenseins nicht autorisierter Hardware- und Firmware-Komponenten innerhalb des Netzes der Organisation zu ermitteln.

Leitfaden

- Wo es sicher und machbar ist, sollten diese Mechanismen automatisiert werden.
- Es sollte ein Verfahren vorhanden sein, mit dem regelmäßig gegen nicht autorisierte Assets vorgegangen werden kann. Die Organisation kann das Asset aus dem Netzwerk entfernen, dem Asset den Fernzugriff auf das Netzwerk verweigern oder das Asset unter Quarantäne stellen.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 1
IEC 62443-2-1:2010, Abschnitt 4.2.3.4
IEC 62443-3-3:2013, SR 7.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.5, 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.9, 5.11, 7.9, 8.1

ID.AM-2: Die in der Organisation verwendeten Software-Plattformen und Anwendungen sind inventarisiert.

Ein Inventar, das wiedergibt, welche Softwareplattformen und -anwendungen in der Organisation verwendet werden, ist zu dokumentieren, zu überprüfen und bei Änderungen zu aktualisieren.

Leitfaden

- Dieses Inventar umfasst Softwareprogramme, Softwareplattformen und Datenbanken, auch wenn diese ausgelagert sind (SaaS).
- Outsourcings-Vereinbarungen sollten Teil der vertraglichen Vereinbarungen mit dem Anbieter sein.
- Die Informationen im Inventar sollten beispielsweise folgende Angaben enthalten: Name, Beschreibung, Version, Anzahl der Benutzer, verarbeitete Daten usw.
- Es ist zu unterscheiden zwischen nicht unterstützter Software und nicht autorisierter Software.
- Der Einsatz eines IT-Asset-Management-Tools könnte in Betracht gezogen werden.

Das Inventar der Software-Plattformen und -Anwendungen im Zusammenhang mit Informationen und Informationsverarbeitung muss Veränderungen im Kontext der Organisation widerspiegeln und alle für eine wirksame Rechenschaftspflicht erforderlichen Informationen enthalten.

Leitfaden

Das Inventar der Software-Plattformen und -Anwendungen sollte für jeden Eintrag den Titel, den Herausgeber, das Datum der Erstinstallation/Nutzung und den Geschäftszweck enthalten; gegebenenfalls sind auch der Uniform Resource Locator (URL), der/die App Store(s), die Version(en), der Bereitstellungsmechanismus und das Datum der Außerbetriebnahme anzugeben.

Die Personen, die für die Verwaltung von Softwareplattformen und -anwendungen innerhalb der Organisation verantwortlich und rechenschaftspflichtig sind, sind zu ermitteln.

Wird nicht zugelassene Software entdeckt, wird sie für eine mögliche Ausnahmebehandlung unter Quarantäne gestellt, entfernt oder ersetzt. Das Inventar wird entsprechend aktualisiert.

Leitfaden

- Jede nicht unterstützte Software ohne eine Ausnahmedokumentation wird als nicht autorisiert bezeichnet.
- Nicht autorisierte Software kann bei der Inventarisierung, bei Supportanfragen durch den Benutzer oder auf andere Weise entdeckt werden.

Es müssen Mechanismen zur Erkennung nicht autorisierter Software in der ICT/OT-Umgebung der Organisation identifiziert werden.

Leitfaden

- Wo es sicher und machbar ist, sollten diese Mechanismen automatisiert werden.
- Es sollte ein Verfahren geben, mit dem regelmäßig gegen nicht autorisierte Anlagen vorgegangen werden kann. Die Organisation kann die Anlage aus dem Netz entfernen, ihr den Fernzugriff auf das Netz verweigern oder die Anlage unter Quarantäne stellen.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 2
IEC 62443-2-1:2010, Abschnitt 4.2.3.4
IEC 62443-3-3:2013 SR 7.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.9

ID.AM-3: Organisatorische Kommunikations- und Datenflüsse sind abgebildet .

Die Informationen, die die Organisation speichert und verwendet, müssen identifiziert werden.

Leitfaden

- Beginnen Sie mit der Auflistung aller Arten von Informationen, die Ihr Unternehmen speichert oder verwendet. Definieren Sie den Begriff "Informationstyp" auf eine für Ihr Unternehmen sinnvolle Weise. Möglicherweise möchten Sie Ihre Mitarbeiter bitten, eine Liste aller Informationen zu erstellen, die sie im Rahmen ihrer regulären Tätigkeit verwenden. Listen Sie alles auf, was Ihnen einfällt. Hierfür müssen Sie nicht zu spezifisch sein. Sie können zum Beispiel Kundennamen und E-Mail-Adressen, Quittungen für Rohmaterial, Ihre Bankdaten oder andere geschützte Informationen auflisten.
- Erwägen Sie die Zuordnung dieser Informationen zu den zugehörigen Vermögenswerten, die in den Inventaren der physischen Geräte, Systeme, Softwareplattformen und Anwendungen, die innerhalb der Organisation verwendet werden, identifiziert wurden (siehe ID.AM-1 & ID.AM-2).

Alle Verbindungen innerhalb der IKT/OT-Umgebung der Organisation und zu anderen organisationsinternen Plattformen müssen abgebildet, dokumentiert, genehmigt und gegebenenfalls aktualisiert werden.

Leitfaden

- Zu den Verbindungsinformationen gehören z. B. die Merkmale der Schnittstelle, Datenmerkmale, Anschlüsse, Protokolle, Adressen, die Beschreibung der Daten, Sicherheitsanforderungen und die Art der Verbindung.
- Das Konfigurationsmanagement kann als unterstützende Maßnahme eingesetzt werden.
- Diese Dokumentation sollte nicht nur in dem Netz gespeichert werden, für das sie steht.
- Erwägen Sie eine Kopie dieser Dokumentation in einer sicheren Offline-Umgebung aufzubewahren (z. B. Offline-Festplatte, Papierausdruck, ...).

Die Informationsflüsse/Datenflüsse innerhalb der IKT/OT-Umgebung der Organisation sowie zu anderen organisationsinternen Systemen sind abzubilden, zu dokumentieren, zu autorisieren und bei Änderungen zu aktualisieren.

Leitfaden

- Wenn man die Informations-/Datenflüsse innerhalb eines Systems und zwischen Systemen kennt, kann man bestimmen, wohin Informationen gelangen können und wohin nicht.
- Bedenken Sie:
  - Durchsetzen von Kontrollen, die Verbindungen nur auf autorisierte Schnittstellen beschränken.
  - Verstärkung der Systemüberwachungsaktivitäten, wenn es Anzeichen für ein erhöhtes Risiko für die kritischen Abläufe und Vermögenswerte des Unternehmens gibt.
  - Schutz des Systems vor Informationsverlusten durch elektromagnetische Strahlung.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 12
IEC 62443-2-1:2010, Abschnitt 4.2.3.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.14

ID.AM-4: Externe Informationssysteme werden katalogisiert.

Die Organisation muss alle externen Dienste und die mit ihnen hergestellten Verbindungen abbilden, dokumentieren, genehmigen und bei Änderungen aktualisieren.

Leitfaden

- Outsourcing von Systemen, Softwareplattformen und Anwendungen, die innerhalb der Organisation genutzt werden, wird in ID.AM-1 & ID.AM-2 behandelt.
- Externe Informationssysteme sind Systeme oder Komponenten von Systemen, für die Organisationen in der Regel keine direkte Aufsicht und Befugnis über die Anwendung von Sicherheitsanforderungen und -kontrollen oder die Bestimmung der Wirksamkeit der für diese Systeme implementierten Kontrollen haben, d. h. Dienste, die in Cloud-, SaaS-, Hosting- oder anderen externen Umgebungen betrieben werden, API (Application Programming Interface)...
- Durch die Zuordnung externer Dienste und der zu ihnen hergestellten Verbindungen und deren vorherige Autorisierung wird die Verschwendung unnötiger Ressourcen bei der Untersuchung einer vermeintlich nicht authentifizierten Verbindung zu externen Systemen vermieden.

Der Informationsaustauschfluss zu/von externen Systemen muss abgebildet, dokumentiert, autorisiert und bei Änderungen aktualisiert werden.

Leitfaden

Erwägen Sie, von externen Dienstleistern zu verlangen, dass **sie** die für die Verbindungsdienste erforderlichen Funktionen, Ports, Protokolle und Dienste angeben und dokumentieren.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 12
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Anhang A (siehe ISO 27002**)**
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.12, 7.9

ID.AM-5: Ressourcen werden auf der Grundlage ihrer Klassifizierung, ihrer Kritikalität und ihres Geschäftswerts nach Prioritäten geordnet .

Die Ressourcen der Organisation (Hardware, Geräte, Daten, Zeit, Personal, Informationen und Software) müssen auf der Grundlage ihrer Klassifizierung, ihrer Kritikalität und ihres Geschäftswerts nach Prioritäten geordnet werden.

Leitfaden

- Bestimmen Sie die Ressourcen der Organisation (z. B. Hardware, Geräte, Daten, Zeit, Personal, Informationen und Software):
  - Was würde mit meinem Unternehmen passieren, wenn diese Ressourcen veröffentlicht würden, beschädigt würden, verloren gingen...?
  - Was würde mit meinem Unternehmen passieren, wenn die Integrität der Ressourcen nicht mehr gewährleistet ist?
  - Was würde mit meinem Unternehmen passieren, wenn ich/meine Kunden keinen Zugang zu diesen Ressourcen hätten? Ordnen Sie diese Ressourcen nach ihrer Klassifizierung, ihrer Kritikalität und ihrem Geschäftswert ein.
- Zu den Ressourcen sollten auch die Vermögenswerte des Unternehmens gehören.
- Erstellen Sie eine Klassifizierung für sensible Informationen, indem Sie zunächst Kategorien festlegen, z. B.
  - Öffentlich - frei zugänglich für alle, auch für Externe
  - Intern - nur für Mitglieder Ihrer Organisation zugänglich
  - Vertraulich - nur für diejenigen zugänglich, deren Aufgaben den Zugang erfordern.
- Teilen Sie diese Kategorien mit und geben Sie an, welche Arten von Daten in diese Kategorien fallen (Personaldaten, Finanzdaten, rechtliche Daten, persönliche Daten usw.).
- Erwägen Sie die Verwendung des Traffic Light Protocol (TLP).
- Die Datenklassifizierung sollte für die drei Aspekte gelten: C-I-A
- Erwägen Sie die Implementierung eines automatisierten Tools, z. B. eines Host-basierten Data Loss Prevention (DLP)-Tools, um alle sensiblen Daten zu identifizieren, die auf Unternehmensressourcen gespeichert, verarbeitet oder übertragen werden, einschließlich derjenigen, die sich vor Ort oder bei einem entfernten Dienstanbieter befinden.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 3
IEC 62443-2-1:2010, Klausel 4.2.3.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.12, 7.9

ID.AM-6: Rollen, Verantwortlichkeiten und Befugnisse im Bereich der Cybersicherheit für die gesamte Belegschaft und Dritte (z.B. Lieferanten, Kunden, Partner) sind festgelegt.

Die Rollen, Zuständigkeiten und Befugnisse im Bereich der Informations- und Cybersicherheit innerhalb der Organisation müssen dokumentiert, überprüft, autorisiert und aktualisiert und mit den organisationsinternen Rollen und externen Partnern abgeglichen werden.

Leitfaden

Dies sollte berücksichtigt werden:

- Beschreiben Sie die Rollen, Zuständigkeiten und Befugnisse im Bereich der Sicherheit: Wer in Ihrem Unternehmen sollte konsultiert, informiert und für alle oder einen Teil Ihrer Vermögenswerte verantwortlich gemacht werden?
- Bereitstellung von Sicherheitsrollen, Zuständigkeiten und Befugnissen für alle Schlüsselfunktionen im Bereich der Informations-/Cybersicherheit (rechtliche Aspekte, Aufdeckungstätigkeiten...).
- Aufnahme von Informations-/Cybersicherheitsrollen und -verantwortlichkeiten für Drittanbieter mit physischem oder logischem Zugang zur ICT/OT-Umgebung der Organisation.

Die Organisation muss einen Beauftragten für Informationssicherheit ernennen.

Leitfaden

Der Informationssicherheitsbeauftragte sollte für die Überwachung der Umsetzung der Informations-/Cybersicherheitsstrategie und der Schutzmaßnahmen der Organisation verantwortlich sein.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 17
IEC 62443-2-1:2010, Abschnitt 4.3.2.3.**3**
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 5.3, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.2, 5.4, 5.23, 5.24, 6.2, 6.5, 8.24

Der Auftrag, die Ziele, die Interessengruppen und die Aktivitäten der Organisation werden verstanden und nach Prioritäten geordnet; diese Informationen dienen als Grundlage für die Festlegung von Rollen, Zuständigkeiten und Entscheidungen im Bereich der Cybersicherheit.

ID.BE-1: Die Rolle der Organisation in der Lieferkette ist identifiziert und kommuniziert.

Die Rolle der Organisation in der Lieferkette muss identifiziert, dokumentiert und kommuniziert werden.

Leitfaden

- Die Organisation sollte in der Lage sein, klar zu erkennen, wer der Organisation vor- und nachgelagert ist und welche Lieferanten Dienstleistungen, Fähigkeiten, Produkte und Artikel für die Organisation bereitstellen.
- Die Organisation sollte ihren vor- und nachgelagerten Bereichen ihre Position mitteilen, damit klar ist, wo sie in Bezug auf die kritische Bedeutung für die Geschäftstätigkeit der Organisation stehen.

Die Organisation muss ihre IKT/OT-Umgebung vor Bedrohungen der Lieferkette schützen, indem sie Sicherheitsvorkehrungen als Teil einer dokumentierten umfassenden Sicherheitsstrategie anwendet.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.19, 5.20, 5.21, 5.22

ID.BE-2: Die Stellung der Organisation in der kritischen Infrastruktur und ihrem Wirtschaftszweig ist identifiziert und kommuniziert.

Die Stellung der Organisation in der kritischen Infrastruktur und in ihrem Wirtschaftszweig ist zu ermitteln und mitzuteilen.

Leitfaden

Die Organisation, die unter die NIS-Gesetzgebung fällt, ist dafür verantwortlich, die anderen Organisationen desselben Sektors zu kennen, um mit ihnen zusammenzuarbeiten, um die von der NIS für diesen speziellen Sektor festgelegten Ziele zu erreichen.

Referenzen

IEC 62443-2-1:2010, Klausel 4.2.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 4.1

ID.BE-3: Prioritäten für den Auftrag, die Ziele und die Aktivitäten der Organisation sind festgelegt und werden kommuniziert.

Es werden Prioritäten für die Geschäfte, Ziele und Aktivitäten der Organisation festgelegt und kommuniziert.

Leitfaden

- Der Auftrag, die Ziele und die Aktivitäten der Organisation sollten festgelegt und nach Prioritäten geordnet werden.
- Der Bedarf an Informationsschutz sollte ermittelt und die entsprechenden Prozesse gegebenenfalls überarbeitet werden, bis ein realisierbarer Satz erreicht ist.

Referenzen

IEC 62443-2-1:2010, Klausel 4.2.2, 4.2.3.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 5.1, 5.2, 6.1, 7.4, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.1

ID.BE-4: Abhängigkeiten und kritische Funktionen für die Erbringung von kritischen Diensten sind festgelegt.

Abhängigkeiten und missionskritische Funktionen für die Erbringung kritischer Dienste sind im Rahmen der Risikobewertung zu ermitteln, zu dokumentieren und nach ihrer Kritikalität zu ordnen.

Leitfaden

Zu den Abhängigkeiten und geschäftskritischen Funktionen sollten auch Unterstützungsdienste gehören.

Referenzen

IEC 62443-2-1:2010, Abschnitt 4.2.3.3
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.1, 8, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 7.11, 7.12, 8.6

ID.BE-5: Anforderungen an die Widerstandsfähigkeit zur Unterstützung der Erbringung kritischer Dienste sind für alle Betriebszustände festgelegt (z.B. unter Druck/Angriff, während der Wiederherstellung, im Normalbetrieb).

Um die Cyber-Resilienz zu unterstützen und die Bereitstellung kritischer Dienste zu sichern, werden die erforderlichen Anforderungen ermittelt, dokumentiert und ihre Umsetzung getestet und genehmigt.

Leitfaden

- Erwägen Sie die Implementierung von Ausfallsicherheitsmechanismen zur Unterstützung normaler und ungünstiger Betriebssituationen (z. B. Ausfallsicherheit, Lastausgleich, Hot Swap).
- Berücksichtigung von Aspekten des Business Continuity Management, z. B. in der Business Impact Analyse (BIA), dem Disaster Recovery Plan (DRP) und dem Business Continuity Plan (BCP).

Informationsverarbeitungs- und unterstützungseinrichtungen müssen Redundanz implementieren, um die von der Organisation und/oder den gesetzlichen Bestimmungen festgelegten Verfügbarkeitsanforderungen zu erfüllen.

Leitfaden

- Erwägen Sie die Bereitstellung einer angemessenen Daten- und Netzwerkredundanz (z. B. redundante Netzwerkgeräte, Server mit Lastausgleich, Raid-Arrays, Backup-Dienste, zwei getrennte Rechenzentren, ausfallsichere Netzwerkverbindungen, zwei Internetanbieter ...).
- Überlegen Sie, wie Sie kritische Geräte/Dienste vor Stromausfällen und anderen Ausfällen aufgrund von Unterbrechungen der Stromversorgung schützen können (z. B. USV und unterbrechungsfreie Stromversorgung, häufige Tests, Serviceverträge mit regelmäßiger Wartung, redundante Stromverkabelung, zwei verschiedene Stromanbieter usw.).

Es sind Ziele für die Wiederherstellungszeit und den Wiederherstellungspunkt für die Wiederherstellung wesentlicher IKT/OT-Systemprozesse zu definieren.

Leitfaden

- Ziehen Sie die Anwendung der 3-2-1-Backup-Regel in Betracht, um RPO und RTO zu verbessern (mindestens 3 Kopien Ihrer Daten, 2 davon an getrennten Orten und eine Kopie sollte an einem externen Ort gespeichert werden).
- Erwägen Sie die Implementierung von Mechanismen wie Hot Swap, Lastausgleich und Ausfallsicherheit, um die Ausfallsicherheit zu erhöhen.

Referenzen

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.29, 7.5, 8.14

Die Richtlinien, Verfahren und Prozesse zur Verwaltung und Überwachung der regulatorischen, rechtlichen, risikorelevanten, umweltbezogenen und betrieblichen Anforderungen der Organisation sind bekannt und bilden die Grundlage für das Management von Cybersicherheitsrisiken.

ID.GV-1: Organisatorische Cybersicherheitsrichtlinien sind festgelegt und werden kommuniziert.

Richtlinien und Verfahren für Informationssicherheit und Cybersicherheit werden erstellt, dokumentiert, überprüft, genehmigt und bei Änderungen aktualisiert.

Leitfaden

- Richtlinien und Verfahren dienen dazu, akzeptable Praktiken und Erwartungen für den Geschäftsbetrieb festzulegen, neue Mitarbeiter in den Erwartungen an die Informationssicherheit zu schulen und eine Untersuchung im Falle eines Vorfalls zu unterstützen. Diese Richtlinien und Verfahren sollten für die Mitarbeiter leicht zugänglich sein.
- Richtlinien und Verfahren für die Informations- und Cybersicherheit sollten klar beschreiben, welche Erwartungen Sie an den Schutz der Informationen und Systeme des Unternehmens haben. Zudem sollten diese die Erwartungen der Unternehmensleitung beschreiben, bezüglich der Ressourcen des Unternehmens, dievon allen Mitarbeitern genutzt und geschützt werden.
- Die Richtlinien und Verfahren sollten mindestens einmal jährlich sowie bei jeder Änderung in der Organisation oder der Technologie überprüft und aktualisiert werden. Bei jeder Änderung der Richtlinien sollten die Mitarbeiter auf die Änderungen aufmerksam gemacht werden.

Es wird eine organisationsweite Richtlinie für die Informations- und Cybersicherheit erstellt, dokumentiert, bei Änderungen aktualisiert, verbreitet und von der Geschäftsleitung genehmigt.

Leitfaden

Die Richtlinie sollte unter anderem Folgendes beinhalten:

- Die Identifizierung und Zuweisung von Rollen, Verantwortlichkeiten, Engagement des Managements, Koordination zwischen den Organisationseinheiten und Einhaltung der Vorschriften. Eine Anleitung zu Rollenprofilen zusammen mit ihren identifizierten Titeln, Missionen, Aufgaben, Fähigkeiten, Kenntnissen und Kompetenzen ist in den "European Cybersecurity Skills Framework Role Profiles" von ENISA verfügbar. (https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles)
- Ddie Koordinierung zwischen den Organisationseinheiten, die für die verschiedenen Sicherheitsaspekte zuständig sind (d.h. technische, physische, personelle, cyber-physische, informationelle, Zugangskontrolle, Medienschutz, Schwachstellenmanagement, Wartung, Überwachung)
- Die Abdeckung des gesamten Lebenszyklus der IKT/OT-Systeme.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 14
IEC 62443-2-1:2010, Abschnitt 4.3.2.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 4, 5, 7.5, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.1

ID.GV-3: Rechtliche und regulatorische Anforderungen an die Cybersicherheit, einschließlich der Verpflichtungen zum Schutz der Privatsphäre und der bürgerlichen Freiheiten, werden verstanden und gehandhabt.

Gesetzliche und behördliche Anforderungen an die Informations-/Cybersicherheit, einschließlich der Verpflichtung zum Schutz der Privatsphäre, müssen verstanden, umgesetzt und verwaltet werden.

Leitfaden

- Es sollten regelmäßige Überprüfungen stattfinden, um sicherzustellen, dass die rechtlichen und regulatorischen Anforderungen an die Informations-/Cybersicherheit, einschließlich der Verpflichtungen zum Schutz der Privatsphäre, kontinuierlich eingehalten werden.
- Diese Anforderung gilt auch für Auftragnehmer und Dienstleister.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 17
IEC 62443-2-1:2010, Abschnitt 4.4.3.7
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 4.1, 4.2, 7.4, 7.2, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.31, 5.32, 5.33, 5.34

ID.GV-4: Governance- und Risikomanagementprozesse adressieren Cybersicherheitsrisiken.

Als Teil des allgemeinen Risikomanagements des Unternehmens wird eine umfassende Strategie zur Bewältigung von Risiken im Bereich der Informations- und Cybersicherheit entwickelt und bei Änderungen aktualisiert.

Leitfaden

Diese Strategie sollte die Bestimmung und Zuweisung der erforderlichen Ressourcen zum Schutz der geschäftskritischen Vermögenswerte des Unternehmens beinhalten.

Die Risiken für die Informations- und Cybersicherheit werden dokumentiert, förmlich genehmigt und bei Änderungen aktualisiert.

Leitfaden

Erwägen Sie den Einsatz von Risikomanagement-Tools.

Referenzen

IEC 62443-2-1:2010, Klausel 4.2.3, 4.4.3.7
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 6

Die Organisation ist sich des Risikos bewusst, das die Cybersicherheit für den Betrieb der Organisation (einschließlich der Mission, der Funktionen, des Images oder des Rufs), für die Vermögenswerte der Organisation und für Einzelpersonen darstellt.

ID.RA-1: Schwachstellen von Vermögenswerten werden identifiziert und dokumentiert.

Die Bedrohungen und Schwachstellen sind zu ermitteln.

Leitfaden

- Eine Schwachstelle bezieht sich auf eine Schwachstelle in der Hardware, Software oder den Verfahren eines Unternehmens. Es handelt sich um eine Lücke, durch die ein bösartiger Akteur Zugang zu den Vermögenswerten der Organisation erlangen kann. Eine Schwachstelle bringt Bedrohungen für eine Organisation mit sich. Eine Bedrohung ist ein bösartiges oder negatives Ereignis, das eine Schwachstelle ausnutzt.
- Das Risiko ist das Potenzial für Verluste und Schäden, wenn die Bedrohung eintritt.

Es ist ein Verfahren einzurichten, mit dem die Schwachstellen der geschäftskritischen Systeme der Organisation kontinuierlich überwacht, ermittelt und dokumentiert werden.

Leitfaden

- Wo es sicher und machbar ist, sollte der Einsatz von Schwachstellen-Scans in Betracht gezogen werden
- Die Organisation sollte ein Testprogramm einführen und aufrechterhalten, das ihrer Größe, Komplexität und Reife angemessen ist.

Um sicherzustellen, dass der Betrieb der Organisation nicht durch den Testprozess beeinträchtigt wird, sind Leistungs-/Lasttests und Penetrationstests der Systeme der Organisation mit Sorgfalt durchzuführen.

Leitfaden

Erwägen Sie eine Validierung der Sicherheitsmaßnahmen nach jedem Penetrationstest.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 7
IEC 62443-2-1:2010, Klausel 4.2.3, 4.2.3.9, 4.2.3.12
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 6, 7, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.36, 8.8

ID.RA-2: Die Informationen über Cyber-Bedrohungen stammen aus Foren und Quellen für den Informationsaustausch.

Es wird ein Programm zur Sensibilisierung für Bedrohungen und Schwachstellen eingeführt, das einen organisationsübergreifenden Informationsaustausch ermöglicht.

Leitfaden

Ein Programm zur Sensibilisierung für Bedrohungen und Schwachstellen sollte einen ständigen Kontakt mit Sicherheitsgruppen und -verbänden beinhalten, um Sicherheitswarnungen und -hinweise zu erhalten. (Zu den Sicherheitsgruppen und -verbänden gehören z.B. spezielle Interessengruppen, Foren, Berufsverbände, Nachrichtengruppen und/oder Gruppen von Sicherheitsfachleuten in ähnlichen Organisationen) Dieser Kontakt kann den Austausch von Informationen über potentielle Schwachstellen und Zwischenfälle beinhalten. Dieser Informationsaustausch sollte sowohl den Austausch von nicht klassifizierten als auch von klassifizierten Informationen umfassen.

Es ist zu ermitteln, wo automatisierte Mechanismen eingesetzt werden können, um Informationen über Sicherheitswarnungen und -hinweise für die Beteiligten der Organisation verfügbar zu machen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 14
IEC 62443-2-1:2010, Klausel 4.2.3, 4.2.3.9, 4.2.3.12
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 4.2, 7.4, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.6

ID.RA-5: Bedrohungen, Schwachstellen, Wahrscheinlichkeiten und Auswirkungen werden zur Risikobestimmung verwendet

Die Organisation muss Risikobewertungen durchführen, bei denen das Risiko durch Bedrohungen, Schwachstellen und Auswirkungen auf Geschäftsprozesse und Vermögenswerte bestimmt wird.

Leitfaden

- Bedenken Sie, dass Bedrohungen Schwachstellen ausnutzen.
- Identifizieren Sie die Folgen, die ein Verlust der Vertraulichkeit, Integrität und Verfügbarkeit für die Vermögenswerte und die damit verbundenen Geschäftsprozesse haben kann.

Die Organisation muss Risikobewertungen durchführen und dokumentieren, bei denen das Risiko durch Bedrohungen, Schwachstellen, Auswirkungen auf Geschäftsprozesse und Vermögenswerte sowie die Wahrscheinlichkeit ihres Eintretens bestimmt wird.

Leitfaden

- Die Risikobewertung sollte Bedrohungen durch Insider und externe Parteien einschließen.
- Qualitative und/oder quantitative Risikoanalysemethoden
  (MAPGOOD, ISO27005, CIS RAM, ...) können zusammen mit Softwaretools verwendet werden.

Die Ergebnisse der Risikobewertung werden an die relevanten Interessengruppen weitergegeben.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 7, 10
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 5.1, 6.1, 7.4, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 8.8

ID.RA-6: Maßnahmen gegen Risiken werden ermittelt und nach Prioritäten geordnet.

Es ist eine umfassende Strategie zur Bewältigung der Risiken für die kritischen Systeme der Organisation zu entwickeln und umzusetzen, die auch die Ermittlung und Priorisierung von Risikomaßnahmen umfasst.

Leitfaden

- Management und Mitarbeiter sollten in die Informations- und Cybersicherheit einbezogen werden.
- Es sollte ermittelt werden, welches die wichtigsten Vermögenswerte sind und wie sie geschützt werden.
- Es sollte klar sein, welche Auswirkungen es haben wird, wenn diese Vermögenswerte gefährdet sind.
- Es sollte festgelegt werden, wie die Umsetzung angemessener Abhilfemaßnahmen organisiert werden soll.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 7, 10
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 5.1, 6.1.3, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 8.8

Die Prioritäten, Einschränkungen, Risikotoleranzen und Annahmen der Organisation werden festgelegt und zur Unterstützung von Entscheidungen über operationelle Risiken verwendet.

ID.RM-1: Risikomanagementprozesse sind etabliert, verwaltet und von den organisatorischen Stakeholdern akzeptiert.

Ein Cyber-Risikomanagementprozess, der die wichtigsten internen und externen Interessengruppen identifiziert und den Umgang mit risikobezogenen Fragen und Informationen erleichtert, muss erstellt, dokumentiert, überprüft, genehmigt und bei Änderungen aktualisiert werden.

Leitfaden

Zu den externen Stakeholdern gehören Kunden, Investoren und Aktionäre, Zulieferer, staatliche Stellen und die breitere Öffentlichkeit.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 7, **10**
IEC 62443-2-1:2010, Klausel 4.3.4.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 5.1, 5.2, 6.1.3, 8.3, 9.3

ID.RM-2: Die Risikotoleranz der Organisation ist festgelegt und klar formuliert.

Die Organisation muss ihre Risikobereitschaft eindeutig festlegen.

Leitfaden

Die Festlegung und Ausprägung der Risikotoleranz (Risikobereitschaft) sollte mit den Grundsätzen der Informations- und Cybersicherheit übereinstimmen, um den Nachweis der Kohärenz zwischen Grundsätzen, Risikotoleranz und Maßnahmen zu erleichtern.

Referenzen

IEC 62443-2-1:2010, Abschnitt 4.3.2.6.5
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 5.1, 5.2, 6.1.3, 7.4, 8.3, 9.3

ID.RM-3: Die Risikotoleranz der Organisation wird durch ihre Rolle in kritischen Infrastrukturen und sektorspezifischen Risikoanalysen bestimmt.

Die Rolle der Organisation im Bereich kritischer Infrastrukturen und ihres Sektors bestimmt die Risikobereitschaft der Organisation.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 5.1, 5.2, 6.1.3, 8.3, 9.3

Die Prioritäten, Einschränkungen, Risikotoleranzen und Annahmen der Organisation werden festgelegt und zur Unterstützung von Risikoentscheidungen im Zusammenhang mit dem Management von Lieferkettenrisiken verwendet. Die Organisation hat die Prozesse zur Identifizierung, Bewertung und Steuerung von Risiken in der Lieferkette eingeführt und umgesetzt.

ID.SC-1: Prozesse zum Management von Risiken in der Cyber Supply Chain sind identifiziert, etabliert, bewertet, verwaltet und von allen Beteiligten in der Organisation akzeptiert.

Die Organisation muss einen Prozess für das Cyber Supply Chain Risk Management dokumentieren, überprüfen, genehmigen, bei Änderungen aktualisieren und umsetzen, der die Identifizierung, Bewertung und Minderung der Risiken unterstützt, die mit der verteilten und vernetzten Natur der IKT/OT-Produkt- und Dienstleistungslieferketten verbunden sind.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

IEC 62443-2-1:2010, Abschnitt 4.3.4.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 5.1, 5.3, 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.19, 5.20, 5.21, 5.22

ID.SC-2: Lieferanten und Drittparteien von Informationssystemen, Komponenten und Dienstleistungen werden identifiziert, nach Prioritäten geordnet und mit Hilfe eines Prozesses zur Risikobewertung in der Cyber-Lieferkette bewertet.

Die Organisation muss mindestens einmal jährlich oder bei einer Änderung der kritischen Systeme, des betrieblichen Umfelds oder der Lieferkette der Organisation Risikobewertungen für die Cyber-Lieferkette durchführen; diese Bewertungen sind zu dokumentieren und die Ergebnisse sind an die relevanten Interessengruppen, einschließlich der für IKT/OT-Systeme Verantwortlichen, weiterzugeben.

Leitfaden

Bei dieser Bewertung sollten die potenziellen negativen Auswirkungen der Risiken, die mit der verteilten und vernetzten Natur der IKT/OT-Produkt- und Dienstleistungslieferketten verbunden sind, auf die Organisation ermittelt und priorisiert werden.

Eine dokumentierte Liste aller Lieferanten, Anbieter und Partner der Organisation, die in einen größeren Zwischenfall verwickelt sein könnten, ist zu erstellen, auf dem neuesten Stand zu halten und online und offline verfügbar zu machen.

Leitfaden

Diese Liste sollte die Kontaktdaten von Lieferanten, Anbietern und Partnern sowie die von ihnen erbrachten Dienstleistungen enthalten, damit sie im Falle eines Ausfalls oder einer Beeinträchtigung des Dienstes um Hilfe gebeten werden können.

Referenzen

IEC 62443-2-1:2010, Abschnitte 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 5.1, 5.3, 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.19, 5.20, 5.21, 5.22

ID.SC-3: Verträge mit Lieferanten und Drittanbietern werden genutzt, um geeignete Maßnahmen umzusetzen, die die Ziele des Cybersicherheitsprogramms und des Cyber Supply Chain Risk Management Plans einer Organisation erfüllen.

Auf der Grundlage der Ergebnisse der Risikobewertung für die Cyber-Lieferkette wird ein vertraglicher Rahmen für Lieferanten und externe Partner geschaffen, der die gemeinsame Nutzung sensibler Informationen und verteilter und miteinander verbundener IKT/OTProdukte und Dienste regelt.

Leitfaden

- Unternehmen, die nicht unter die NIS-Gesetzgebung fallen, sollten nur geschäftskritische Lieferanten und Drittpartner in Betracht ziehen.
- Denken Sie daran, dass die Anforderungen der Datenschutz-Grundverordnung erfüllt werden müssen, wenn Geschäftsinformationen personenbezogene Daten enthalten (gilt für alle Ebenen), d. h. Sicherheitsmaßnahmen müssen im vertraglichen Rahmen berücksichtigt werden.

Es werden vertragliche Anforderungen an die "Informationssicherheit und Cybersicherheit" für Lieferanten und Drittpartner eingeführt, um einen überprüfbaren Prozess zur Behebung von Mängeln zu gewährleisten und die Korrektur von Mängeln sicherzustellen, die bei der Prüfung und Bewertung der "Informationssicherheit und Cybersicherheit" festgestellt werden.
- Schlüsselmaßnahme -

Leitfaden

- Informationssysteme mit Software (oder Firmware), die von kürzlich bekannt gegebenen Softwarefehlern betroffen sind (und potenzielle Schwachstellen, die sich aus diesen Fehlern ergeben), sollten identifiziert werden.
- Neu veröffentlichte sicherheitsrelevante Patches, Service Packs und Hot Fixes sollten installiert werden, und diese Patches, Service Packs und Hot Fixes werden vor der Installation auf ihre Wirksamkeit und mögliche Nebenwirkungen auf die Informationssysteme des Unternehmens getestet. Schwachstellen, die bei Sicherheitsbewertungen, der kontinuierlichen Überwachung, der Reaktion auf Zwischenfälle oder der Fehlerbehandlung im Informationssystem entdeckt werden, werden ebenfalls zügig behoben. Die Behebung von Schwachstellen sollte als Notfalländerung in das Konfigurationsmanagement aufgenommen werden.

Die Organisation soll vertragliche Anforderungen festlegen, die es der Organisation erlauben, die von Zulieferern und Drittpartnern umgesetzten Programme für "Informationssicherheit und Cybersicherheit" zu überprüfen.
- Schlüsselmaßnahme -

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

IEC 62443-2-1:2010, Klausel 4.3.2.6.4, 4.3.2.6.7
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 6, 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.19, 5.20, 5.21, 5.22

ID.SC-4: Lieferanten und Drittpartner werden routinemäßig anhand von Audits, Testergebnissen oder anderen Formen der Bewertung beurteilt, um zu bestätigen, dass sie ihren vertraglichen Verpflichtungen nachkommen.

Die Organisation muss die Bewertung der Einhaltung der vertraglichen Verpflichtungen durch Lieferanten und Drittpartner durch routinemäßige Audits, Testergebnisse und andere Bewertungen überprüfen.

Leitfaden

Unternehmen, die nicht unter die NIS-Gesetzgebung fallen, könnten sich auf geschäftskritische Lieferanten und Drittpartner beschränken.

Die Organisation muss die Bewertung der Einhaltung der vertraglichen Verpflichtungen durch Lieferanten und Drittparteien überprüfen, indem sie routinemäßig unabhängige Audits, Testergebnisse und andere Bewertungen von Dritten überprüft.

Leitfaden

Die Tiefe der Überprüfung sollte von der Kritikalität der gelieferten Produkte und Dienstleistungen abhängen.

Referenzen

IEC 62443-2-1:2010, Abschnitt 4.3.2.6.7
IEC 62443-3-3:2013, SR 6.1
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 8.1, 9.2, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.22

ID.SC-5: Reaktions- und Wiederherstellungsplanung und -tests werden mit Lieferanten und Drittanbietern durchgeführt.

Die Organisation muss die wichtigsten Mitarbeiter von Zulieferern und Drittpartnern identifizieren und dokumentieren, um sie als Beteiligte in die Reaktions- und Wiederherstellungsplanung einzubeziehen.

Leitfaden

Unternehmen, die nicht unter die NIS-Gesetzgebung fallen, könnten sich auf geschäftskritische Lieferanten und Drittpartner beschränken.

Die Organisation muss die wichtigsten Mitarbeiter von Zulieferern und Drittpartnern identifizieren und dokumentieren, um sie als Beteiligte in die Tests und die Ausführung der Reaktions- und Wiederherstellungspläne einzubeziehen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 18
IEC 62443-2-1:2010, Klausel 4.3.2.5.7, 4.3.4.5.11
IEC 62443-3-3:2013, SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 6.1.3, 8.1, 8.3, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.29

Der Zugang zu physischen und logischen Vermögenswerten und zugehörigen Einrichtungen ist auf autorisierte Benutzer, Prozesse und Geräte beschränkt und wird in Übereinstimmung mit dem bewerteten Risiko eines unbefugten Zugangs zu autorisierten Aktivitäten und Transaktionen verwaltet.

PR.AC-1: Identitäten und Berechtigungsnachweise werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, widerrufen und geprüft.

Die Identitäten und Berechtigungsnachweise für autorisierte Geräte und Benutzer werden verwaltet.

- Schlüsselmaßnahmen -

Leitfaden

Die Identitäten und Berechtigungsnachweise für autorisierte Geräte und Benutzer können durch eine Passwortrichtlinie verwaltet werden. Eine Passwortrichtlinie ist eine Reihe von Regeln, die die IKT/OT-Sicherheit verbessern sollen, indem sie die Organisation dazu ermutigenum (nicht abschließende Liste und Maßnahmen, die je nach Bedarf zu berücksichtigen sind):

- alle Standardkennwörter zu ändern
- sicherstellen, dass niemand mit Administratorrechten für tägliche Aufgaben arbeitet.
- eine begrenzte und aktualisierte Liste der Systemadministratorkonten zu führen
- Passwortregeln durchzusetzen, z. B. müssen Passwörter länger sein als eine dem Stand der Technik entsprechende Anzahl von Zeichen mit einer Kombination von Zeichentypen und in regelmäßigen Abständen oder bei Verdacht auf Kompromittierung geändert werden.
- nur individuelle Konten zu verwenden und niemals Passwörter weiterzugeben.
- ungenutzte Konten sofort zu deaktivieren.
- Rechte und Privilegien von Benutzergruppen zu verwaltet.

Die Identitäten und Berechtigungsnachweise für autorisierte Geräte und Benutzer werden, soweit möglich, durch automatische Mechanismen verwaltet.

Leitfaden

- Automatisierte Mechanismen können dazu beitragen, die Verwaltung und Prüfung von Berechtigungsnachweisen für Informationssysteme zu unterstützen.
- - Erwägen Sie eine starke Benutzerauthentifizierung, d. h. eine Authentifizierung, die auf der Verwendung von mindestens zwei Authentifizierungsfaktoren aus verschiedenen Kategorien von entweder Wissen (etwas, das nur der Benutzer weiß), Besitz (etwas, das nur der Benutzer besitzt) oder Inhärenz (etwas, das der Benutzer ist) beruht, die insofern unabhängig sind, als die Verletzung eines dieser Faktoren die Zuverlässigkeit der anderen nicht beeinträchtigt, und die so konzipiert ist, dass die Vertraulichkeit der Authentifizierungsdaten geschützt wird.

Systemanmeldeinformationen müssen nach einer bestimmten Zeit der Inaktivität deaktiviert werden, es sei denn, dies würde den sicheren Betrieb von (kritischen) Prozessen gefährden.

Leitfaden

- Um den sicheren Betrieb zu gewährleisten, sollten für laufende Prozesse und Dienste Dienstkonten verwendet werden.
- Erwägen Sie die Anwendung eines formellen Zugangsverfahrens für externe Parteien.

Für Transaktionen innerhalb der kritischen Systeme der Organisation muss die Organisation Folgendes umsetzen:

- Multi-Faktor-Authentifizierung der Endnutzer (MFA oder "starke Authentifizierung").
- zertifikatsbasierte Authentifizierung für die Kommunikation von System zu System

Leitfaden

Erwägen Sie den Einsatz von SSO (Single Sign On) in Kombination mit MFA für die internen und externen kritischen Systeme der Organisation.

Die kritischen Systeme der Organisation müssen auf eine atypische Nutzung von Systemzugangsdaten überwacht werden. Berechtigungsnachweise, die ein erhebliches Risiko darstellen, sind zu deaktivieren.

Leitfaden

- Erwägen Sie, die Anzahl der fehlgeschlagenen Anmeldeversuche durch eine automatische Sperre zu begrenzen.
- Auf das gesperrte Konto kann nicht zugegriffen werden, bis es zurückgesetzt wurde oder die Dauer der Kontosperrung abgelaufen ist.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 1, 3, 4, 5, 12, 13
IEC 62443-2-1:2010, Klausel 4.3.3.5.1, 4.3.3.7.4
IEC 62443-3-3:2013, SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.16, 5.17, 5.18, 8.2, 8.5

PR.AC-2: Der physische Zugang zu Vermögenswerten wird verwaltet und geschützt .

Der physische Zugang zur Einrichtung, zu den Servern und zu den Netzkomponenten ist zu regeln.

Leitfaden

- Erwägen Sie eine strenge Verwaltung der Schlüssel für den Zugang zu den Räumlichkeiten und der Alarmcodes. Die folgenden Regeln sollten berücksichtigt werden:
  - Nehmen Sie immer die Schlüssel oder Ausweise eines Mitarbeiters zurück, wenn dieser das Unternehmen dauerhaft verlässt.
  - Ändern Sie häufig die Alarmcodes des Unternehmens.
  - Geben Sie niemals Schlüssel oder Alarmcodes an externe Dienstleister (Reinigungskräfte usw.) weiter, es sei denn, es ist möglich, diese Zugriffe zurückzuverfolgen und sie technisch auf bestimmte Zeitfenster zu beschränken.
- Ziehen Sie in Erwägung, interne Netzwerkzugänge nicht in öffentlichen Bereichen zugänglich zu machen. Diese öffentlichen Orte können Warteräume, Korridore... sein.

Der physische Zugang ist zu regeln, einschließlich Maßnahmen für den Zugang in Notsituationen.

Leitfaden

- Zu den physischen Zugangskontrollen gehören z. B. Listen autorisierter Personen, Identitätsnachweise, Begleitpersonal, Wachen, Zäune, Drehkreuze, Schlösser, Überwachung des Zugangs zur Einrichtung und Kameraüberwachung.
- Die folgenden Maßnahmen sollten in Betracht gezogen werden:
  - Einführung eines Ausweissystems und Schaffung verschiedener Sicherheitszonen.
  - Beschränken Sie den physischen Zugang zu Servern und Netzwerkkomponenten auf autorisiertes Personal.
  - Protokollierung aller Zugriffe auf Server und Netzwerkkomponenten.
- Es sollten Aufzeichnungen über den Zugang von Besuchern geführt, überprüft und bei Bedarf gehandelt werden.

Der physische Zugang zu kritischen Zonen ist zusätzlich zum physischen Zugang zur Einrichtung zu kontrollieren.

Leitfaden

z. B. Produktion, F&E, kritische Systemausrüstung des Unternehmens (Serverräume...)

Vermögenswerte, die sich auf kritische Zonen beziehen, müssen physisch geschützt werden.

Leitfaden

- Überlegen Sie, wie Sie Stromversorgungsgeräte, Stromkabel, Netzwerkkabel und Netzwerkzugangsschnittstellen vor versehentlicher Beschädigung, Unterbrechung und physischer Manipulation schützen können.
- Erwägen Sie die Implementierung redundanter und physisch getrennter Stromversorgungssysteme für kritische Betriebsabläufe.

Referenzen

IEC 62443-2-1:2010, Klausel 4.3.3.3.2, 4.3.3.3.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 7.1, 7.2, 7.3, 7.5, 7.6, 7.8, 7.9, 7.10, 7.12, 7.14, 8.1

PR.AC-3: Der Fernzugriff wird verwaltet.

Die drahtlosen Zugangspunkte der Organisation müssen gesichert sein.

Leitfaden

Beachten Sie bei der Verwendung von drahtlosen Netzwerken Folgendes:

- Ändern Sie das administrative Passwort bei der Installation eines drahtlosen Zugangspunkts.
- Stellen Sie den drahtlosen Zugangspunkt so ein, dass er seinen Service Set Identifier (SSID) nicht sendet.
- Stellen Sie Ihren Router so ein, dass er mindestens WiFi Protected Access (WPA-2 oder WPA-3, wenn möglich) mit dem Advanced Encryption Standard (AES) zur Verschlüsselung verwendet.
- Stellen Sie sicher, dass der drahtlose Internetzugang für Kunden von Ihrem Unternehmensnetz getrennt ist.
- Die Verbindung zu unbekannten oder ungesicherten/gastweisen drahtlosen Zugangspunkten sollte vermieden werden, und wenn dies unvermeidlich ist, sollte dies über ein verschlüsseltes virtuelles privates Netzwerk (VPN) erfolgen.
- Verwalten Sie alle Endgeräte (stationär und mobil) gemäß den Sicherheitsrichtlinien des Unternehmens.

Nutzungsbeschränkungen, Verbindungsanforderungen, Implementierungsrichtlinien und Berechtigungen für den Fernzugriff auf die kritische Systemumgebung der Organisation müssen ermittelt, dokumentiert und umgesetzt werden.

Leitfaden

Bedenken Sie Folgendes:

- Zu den Fernzugriffsmethoden gehören beispielsweise drahtlose Verbindungen, Breitbandverbindungen, Verbindungen über ein virtuelles privates Netzwerk (VPN), Verbindungen über mobile Geräte und die Kommunikation über externe Netzwerke.
- Die Anmeldedaten sollten mit den Richtlinien des Unternehmens zur Benutzerauthentifizierung übereinstimmen.
- Der Fernzugriff für Support-Aktivitäten oder die Wartung von Unternehmensressourcen sollte genehmigt und protokolliert werden und auf eine Weise erfolgen, die einen unbefugten Zugriff verhindert.
- Der Benutzer sollte durch eine optische Anzeige auf eine Fernverbindung zu seinem Gerät aufmerksam gemacht werden.

Der Fernzugriff auf die kritischen Systeme der Organisation ist zu überwachen, und es sind, soweit erforderlich, kryptographische Mechanismen einzusetzen.

Leitfaden

Dazu sollte gehören, dass nur die autorisierte Nutzung privilegierter Funktionen über den Fernzugriff erlaubt ist.

Der Fernzugriff auf die Netze der Organisation muss gesichert sein, unter anderem durch eine Multi-Faktor-Authentifizierung (MFA).

- Schlüsselmaßnahme -

Leitfaden

Erzwingen Sie MFA (z. B. 2FA) auf Systemen mit Internetzugang, wie E-Mail, Remote-Desktop und Virtual Private Network (VPNs).

Die Sicherheit von Verbindungen mit externen Systemen ist zu überprüfen und durch dokumentierte Vereinbarungen zu regeln.

Leitfaden

Der Zugang von vordefinierten IP-Adressen könnte in Betracht gezogen werden.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 5, 6, 13
IEC 62443-2-1:2010, Klausel 4.3.3.6.6, 4.3.3.7.4
IEC 62443-3-3:2013, SR 1.1, SR 1.13, SR 2.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.14, 6.7, 7.9, 8.1, 8.5, 8.20

PR.AC-4: Zugriffsberechtigungen und -autorisierungen werden unter Berücksichtigung der Grundsätze des geringsten Rechtsanspruchs und der Aufgabentrennung verwaltet.

Die Zugriffsberechtigungen für Benutzer auf die Systeme der Organisation müssen definiert und verwaltet werden.
- Schlüsselmaßnahme -

Leitfaden

Dabei sollte Folgendes beachtet werden:

- Erstellung und regelmäßige Überprüfung von Zugriffslisten für jedes System (Dateien, Server, Software, Datenbanken usw.), möglicherweise durch Analyse des Active Directory in Windows-basierten Systemen, mit dem Ziel, festzustellen, wer welche Art von Zugriff (privilegiert oder nicht) auf was benötigt, um seine Aufgaben im Unternehmen zu erfüllen.
- Richten Sie für jeden Benutzer (einschließlich aller Auftragnehmer, die Zugang benötigen) ein separates Konto ein und verlangen Sie, dass für jedes Konto sichere, eindeutige Kennwörter verwendet werden.
- Stellen Sie sicher, dass alle Mitarbeiter Computerkonten ohne administrative Berechtigungen verwenden, um typische Arbeitsfunktionen auszuführen. Dazu gehört auch die Trennung von persönlichen und administrativen Konten.
- Für Gastkonten sollten Sie die für Ihre geschäftlichen Anforderungen erforderlichen minimalen Berechtigungen (z. B. nur Internetzugang) verwenden.
- Die Verwaltung von Genehmigungen sollte in einem Verfahren dokumentiert und bei Bedarf aktualisiert werden.
- Verwenden Sie gegebenenfalls "Single Sign On" (SSO).

Soweit durchführbar, sind automatisierte Mechanismen zur Unterstützung der Verwaltung von Benutzerkonten auf den kritischen Systemen der Organisation zu implementieren, einschließlich der Deaktivierung, Überwachung, Berichterstattung und Löschung von Benutzerkonten.

Leitfaden

Ziehen Sie in Erwägung, jede Person, die Zugang zu den kritischen Systemen des Unternehmens hat, separat mit einem Benutzernamen zu identifizieren, um allgemeine und anonyme Konten und Zugriffe zu unterbinden.

Kontonutzungsbeschränkungen für bestimmte Zeiträume und Standorte sind in den Sicherheitszugangsrichtlinien der Organisation zu berücksichtigen und entsprechend anzuwenden.

Leitfaden

Spezifische Beschränkungen können z. B. die Beschränkung der Nutzung auf bestimmte Wochentage, Tageszeiten oder bestimmte Zeiträume sein.

Es ist festzulegen, wer Zugang zu den geschäftskritischen Informationen und Technologien der Organisation haben soll und wie der Zugang zu diesen Informationen und Technologien erfolgen kann.
- Schlüsselmaßnahme -

Leitfaden

Die Mittel, um Zugang zu erhalten, können sein: ein Schlüssel, ein Kennwort, ein Code oder eine administrative Berechtigung.

Der Zugang der Mitarbeiter zu Daten und Informationen ist auf die Systeme und spezifischen Informationen zu beschränken, die sie zur Erfüllung ihrer Aufgaben benötigen (Grundsatz des geringstmöglichen Privilegs).
- Schlüsselmaßnahme -

Leitfaden

- Das Prinzip der geringsten Rechte (Least Privilege) ist als Grundsatz zu verstehen, wonach eine Sicherheitsarchitektur so zu gestalten ist, dass jeder Mitarbeiter nur die Systemressourcen und -berechtigungen erhält, die er zur Ausübung seiner Funktion benötigt.
- Berücksichtigen Sie:
  - Kein Mitarbeiter darf Zugang zu allen Informationen des Unternehmens haben.
  - Begrenzung der Zahl der Internetzugänge und der Zusammenschaltungen mit Partnernetzen auf das notwendige Maß, um die Überwachung des Austauschs leichter zentralisieren und homogenisieren zu können.
  - Stellen Sie sicher, dass beim Ausscheiden eines Mitarbeiters aus dem Unternehmen der Zugang zu den Informationen oder Systemen des Unternehmens sofort gesperrt wird.

Bei der Verwaltung der Zugangsrechte muss eine Aufgabentrennung gewährleistet sein.

Leitfaden

Die Aufgabentrennung umfasst zum Beispiel:

- Aufteilung der operativen Funktionen und der Systemunterstützungsfunktionen auf verschiedene Rollen.
- Durchführung von Systemunterstützungsfunktionen mit verschiedenen Personen.
- - Lassen Sie nicht zu, dass eine einzelne Person eine (finanzielle oder andere) Transaktion sowohl initiiert als auch genehmigt kann. Sicherstellung, dass das Sicherheitspersonal, das die Zugangskontrollfunktionen verwaltet, nicht auch die Auditfunktionen verwaltet.

Niemand darf für die täglichen Aufgaben über Administratorrechte verfügen.
- Schlüsselmaßnahme -

Leitfaden

Bedenken Sie Folgendes:

- Trennen Sie Administratorkonten von Benutzerkonten.
- Berechtigen Sie keine Benutzerkonten zur Durchführung von Verwaltungsaufgaben.
- Erstellen Sie eindeutige lokale Administratorkennwörter und deaktivieren Sie ungenutzte Konten.
- Erwägen Sie, das Surfen im Internet von administrativen Konten aus zu verbieten.

Privilegierte Benutzer müssen verwaltet, überwacht und geprüft werden.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 3, 4, 6, 7, 12, 13, 16
IEC 62443-2-1:2010, Abschnitt 4.3.3.7.3
IEC 62443-3-3:2013, SR 2.1
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.3, 5.15, 8.2, 8.3, 8.4, 8.18

PR.AC-5: Die Netzintegrität (Netztrennung, Netzsegmentierung ...) ist geschützt.

In allen Netzen der Organisation sind Firewalls zu installieren und zu aktivieren.
- Schlüsselmaßnahme -

Leitfaden

Bedenken Sie Folgendes:

- Installieren und betreiben Sie eine Firewall zwischen Ihrem internen Netz und dem Internet. Dies kann eine Funktion eines (drahtlosen) Zugangspunkts/Routers sein, oder es kann eine Funktion eines Routers sein, der vom Internet Service Provider (ISP) bereitgestellt wird.
- Stellen Sie sicher, dass auf gekauften Firewall-Lösungen eine Antiviren-Software installiert ist und dass das Anmelde- und Administrationspasswort des Administrators bei der Installation und danach regelmäßig geändert wird.
- Installieren, verwenden und aktualisieren Sie eine Software-Firewall auf jedem Computersystem (einschließlich Smartphones und anderer vernetzter Geräte).
- Sorgen Sie für Firewalls auf allen Ihren Computern und Netzwerken, auch wenn Sie einen Cloud-Anbieter oder ein virtuelles privates Netzwerk (VPN) nutzen. Stellen Sie sicher, dass für Ihr Heimnetzwerk und Ihre Systeme Hardware- und Software-Firewalls installiert, betriebsbereit und regelmäßig aktualisiert sind.
- Erwägen Sie die Installation eines Intrusion Detection / Prevention Systems (IDPS). Diese Geräte analysieren den Netzwerkverkehr auf einer detaillierteren Ebene und können ein höheres Maß an Schutz bieten.

Gegebenenfalls ist die Netzintegrität der kritischen Systeme der Organisation durch Netzsegmentierung und -trennung zu schützen.
- Schlüsselmaßnahme -

Leitfaden

- Erwägen Sie die Einrichtung verschiedener Sicherheitszonen im Netz (z. B. grundlegende Netzsegmentierung durch VLANs oder andere Netzzugangskontrollmechanismen) und kontrollieren/überwachen Sie den Verkehr zwischen diesen Zonen.
- Wenn das Netz "flach" ist, kann die Kompromittierung einer wichtigen Netzkomponente zur Kompromittierung des gesamten Netzes führen.

Gegebenenfalls ist die Netzintegrität der kritischen Systeme der Organisation zu schützen durch
(1) identifizieren, dokumentieren und kontrollieren von Verbindungen zwischen Systemkomponenten.
(2) Begrenzung der externen Verbindungen zu den kritischen Systemen der Organisation.
- Schlüsselmaßnahme -

Leitfaden

Zu den Grenzschutzmechanismen gehören z. B. Router, Gateways, unidirektionale Gateways, Datendioden und Firewalls, die Systemkomponenten in logisch getrennte Netze oder Teilnetze aufteilen.

Die Organisation muss, soweit durchführbar, authentifizierte Proxy-Server für den definierten Kommunikationsverkehr zwischen den kritischen Systemen der Organisation und externen Netzen einsetzen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Die Organisation muss Verbindungen und Kommunikation an der Außengrenze und an wichtigen internen Grenzen innerhalb der kritischen Systeme der Organisation überwachen und kontrollieren, indem sie gegebenenfalls Grenzschutzvorrichtungen einsetzt.
- Schlüsselmaßnahme -

Leitfaden

Erwägen Sie die Umsetzung der folgenden Empfehlungen:

- Trennen Sie Ihr öffentliches WIFI-Netzwerk von Ihrem Unternehmensnetzwerk.
- Schützen Sie Ihr Unternehmens-WIFI mit modernster Verschlüsselung.
- Implementieren Sie eine Lösung für die Netzwerkzugangskontrolle (NAC).
- Verschlüsseln Sie Verbindungen zu Ihrem Unternehmensnetzwerk.
- Unterteilen Sie Ihr Netz nach Sicherheitsstufen und wenden Sie Firewall-Regeln an. Isolieren Sie Ihre Netzwerke für die Serververwaltung.
- VPN in öffentlichen Netzen erzwingen.
- Implementieren Sie eine geschlossene Richtlinie für Sicherheits-Gateways (Deny-All-Richtlinie: nur Verbindungen zulassen/öffnen, die ausdrücklich vorher autorisiert wurden).

Die Organisation muss sicherstellen, dass die kritischen Systeme der Organisation sicher ausfallen, wenn eine Grenzschutzeinrichtung ausfällt.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 3, 4, 7, 12, 16
IEC 62443-2-1:2010, Abschnitt 4.3.3.4
IEC 62443-3-3:2013, SR 3.1, SR 3.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.14, 8.20, 8.22, 8.26

PR.AC-6: Identitäten werden geprüft und an Berechtigungsnachweise gebunden und in Interaktionen geltend gemacht.

Die Organisation muss dokumentierte Verfahren zur Überprüfung der Identität von Personen einführen, bevor sie Berechtigungsnachweise ausstellt, die den Zugang zu den Systemen der Organisation ermöglichen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Die Organisation muss die Verwendung eindeutiger Berechtigungsnachweise sicherstellen, die an jeden verifizierten Benutzer, jedes Gerät und jeden Prozess gebunden sind, der mit den kritischen Systemen der Organisation interagiert; sie muss dafür sorgen, dass sie authentifiziert werden und dass die eindeutigen Kennungen bei der Durchführung von Systeminteraktionen erfasst werden.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 3, 4, 5, 6
IEC 62443-2-1:2010, Abschnitte 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4
IEC 62443-3-3:2013, SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.**1**
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7,5, 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.3, 5.15, 8.2, 8.3, 8.18

PR.AC-7: Identitäten werden geprüft und an Berechtigungsnachweise gebunden und in Interaktionen geltend gemacht.

Die Organisation führt eine dokumentierte Risikobewertung für die kritischen Systemtransaktionen der Organisation durch und authentifiziert Benutzer, Geräte und andere Vermögenswerte (z. B. Ein-Faktor-, Mehr-Faktor-Authentifizierung) entsprechend dem Risiko der Transaktion (z. B. Sicherheits- und Datenschutzrisiken des Einzelnen und andere organisatorische Risiken).
- Schlüsselmaßnahme -

Leitfaden

Für neue Systeme sollte ein Konzept der "Sicherheit durch Technik" in Betracht gezogen werden; für bestehende Systeme sollte eine separate Risikobewertung durchgeführt werden.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 3, 4, 5, 6, 9, 12, 13
IEC 62443-2-1:2010, Abschnitte 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9
IEC 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.**10**
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 6.1, 7.5, 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.16, 5.17, 5.34, 8.5

Das Personal und die Partner der Organisation werden für die Cybersicherheit sensibilisiert und darin geschult, ihre Aufgaben und Verantwortlichkeiten im Zusammenhang mit der Cybersicherheit im Einklang mit den entsprechenden Richtlinien, Verfahren und Vereinbarungen wahrzunehmen.

PR.AT-1: Alle Nutzer sind informiert und geschult.

Die Mitarbeiter sind entsprechend zu schulen.

Leitfaden

- Zu den Mitarbeitern gehören alle Nutzer und Manager von IKT/OT-Systemen, und sie sollten sofort bei ihrer Einstellung und danach regelmäßig über die Informationssicherheitsrichtlinien des Unternehmens geschult werden und darüber, was von ihnen erwartet wird, um die Geschäftsinformationen und die Technologie des Unternehmens zu schützen.
- Die Schulungen sollten ständig aktualisiert und durch Sensibilisierungskampagnen verstärkt werden.

Die Organisation muss das Erkennen und Melden von Insider-Bedrohungen in die Schulung des Sicherheitsbewusstseins einbeziehen.

Leitfaden

Berücksichtigen Sie das:

- Kommunizieren und diskutieren Sie regelmäßig, um sicherzustellen, dass sich jeder seiner Verantwortung bewusst ist.
- Entwickeln Sie ein Outreach-Programm, indem Sie in einem Dokument die Botschaften, die Sie Ihren Mitarbeitern vermitteln wollen (Themen, Zielgruppen, Ziele usw.), und Ihren Kommunikationsrhythmus in einem Kalender (wöchentlich, monatlich, einmalig usw.) zusammenfassen. Kommunizieren Sie kontinuierlich und auf eine ansprechende Art und Weise und beziehen Sie dabei das Management, die IT-Kollegen, den IKT-Dienstleister sowie die Personal- und Kommunikationsmanager ein.
- Behandelt werden Themen wie: Erkennung von Betrugsversuchen, Phishing, Umgang mit sensiblen Informationen, Zwischenfälle usw. Ziel ist es, dass alle Mitarbeiter wissen, wie sie Unternehmensdaten schützen können.
- Besprechen Sie mit Ihrer Geschäftsleitung, Ihren IKT-Kollegen oder Ihrem IKT-Dienstleister einige Übungsszenarien (z. B. was zu tun ist, wenn ein Virenalarm ausgelöst wird, wenn ein Sturm den Strom abstellt, wenn Daten blockiert werden, wenn ein Konto gehackt wird usw.).Legen Sie fest, welche Verhaltensweisen zu übernehmen sind, dokumentieren Sie diese und teilen Sie sie allen Ihren Mitarbeitern mit. Die zentrale Anlaufstelle für den Fall eines Vorfalls sollte allen bekannt sein.
- Organisieren Sie eine Simulation eines Szenarios, um Ihr Wissen zu testen. Erwägen Sie, die Übung beispielsweise mindestens einmal im Jahr durchzuführen.

Die Organisation muss eine Bewertungsmethode anwenden, um die Wirksamkeit der Sensibilisierungsschulungen zu messen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 14, 16
IEC 62443-2-1:2010, Abschnitt 4.3.2.4.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.2, 7.4, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 6.3, 8.7

PR.AT-2: Privilegierte Benutzer verstehen ihre Rollen und Verantwortlichkeiten.

Privilegierte Benutzer müssen qualifiziert sein, bevor sie Privilegien erhalten, und sie müssen nachweisen können, dass sie ihre Aufgaben, Verantwortlichkeiten und Befugnisse kennen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 4, 14, **16**
IEC 62443-2-1:2010, Klausel 4.3.2.4.2, 4.3.2.4.3
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 5.3, 7.2, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.2, 6.3

PR.AT-3: Dritte Stakeholder (z.B. Lieferanten, Kunden, Partner) verstehen ihre Rollen und Verantwortlichkeiten.

Die Organisation muss Sicherheitsanforderungen für geschäftskritische Drittanbieter und Benutzer festlegen und durchsetzen.

Leitfaden

Die Durchsetzung sollte beinhalten, dass die Nutzer von "Drittparteien" (z. B. Lieferanten, Kunden, Partner) nachweisen können, dass sie ihre Rolle und Verantwortung verstehen.

Drittanbieter sind verpflichtet, jeden Personalwechsel, jede Beendigung des Arbeitsverhältnisses oder jeden Wechsel von Mitarbeitern mit physischem oder logischem Zugang zu den Komponenten des geschäftskritischen Systems der Organisation zu melden.

Leitfaden

Zu den Drittanbietern gehören beispielsweise Dienstleister, Auftragnehmer und andere Organisationen, die Systementwicklung, technologische Dienstleistungen, ausgelagerte Anwendungen oder Netzwerk- und Sicherheitsmanagement anbieten.

Die Organisation muss geschäftskritische Dienstanbieter und Benutzer auf die Einhaltung der Sicherheitsvorschriften überwachen.

Leitfaden

Die Ergebnisse von Prüfungen durch Dritte können als Prüfungsnachweis verwendet werden.

Die Organisation muss geschäftskritische externe Dienstleister auf die Einhaltung der Sicherheitsvorschriften prüfen.

Leitfaden

Die Ergebnisse von Prüfungen durch Dritte können als Prüfungsnachweis verwendet werden.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 14
IEC 62443-2-1:2010, Klausel 4.3.2.4.2, 4.3.2.4.3
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 5.3, 8.1, 9.2, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.2, 5.4, 5.12, 6.3

PR.AT-4: Leitende Angestellte verstehen ihre Aufgaben und Verantwortlichkeiten.

Leitende Angestellte müssen nachweisen, dass sie ihre Aufgaben, Verantwortlichkeiten und Befugnisse kennen.

Leitfaden

Eine Anleitung zu Rollenprofilen mit den entsprechenden Titeln, Aufgaben, Fähigkeiten, Kenntnissen und Kompetenzen ist in den "European Cybersecurity Skills Framework Role Profiles" vonENISA zu finden.
(https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles)

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 14, 17
IEC 62443-2-1:2010, Abschnitt 4.3.2.4.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 4.1, 4.2, 5.3, 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.2, 5.4, 5.12, 6.3

PR.AT-5: Das Personal für physische Sicherheit und Cybersicherheit kennt seine Aufgaben und Verantwortlichkeiten.

Die Organisation muss sicherstellen, dass das Personal, das für den physischen Schutz und die Sicherheit der kritischen Systeme und Einrichtungen der Organisation verantwortlich ist, durch Schulungen qualifiziert wird, bevor ihnen Privilegien gewährt werden, und dass es ihre Verantwortung versteht.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 14
IEC 62443-2-1:2010, Klausel 4.3.2.4.2, 4.3.2.4.3
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 5.3, 7.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.2, 6.3

Informationen und Aufzeichnungen (Daten) werden im Einklang mit der Risikostrategie der Organisation verwaltet, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu schützen.

PR.DS-1: Data-at-rest ist geschützt.

Diese Kontrolle wird durch die anderen Bestandteile dieser Richtlinie abgedeckt; es werden keine zusätzlichen Anforderungen festgelegt.

Leitfaden

- Erwägen Sie die Verwendung von Verschlüsselungstechniken für die Datenspeicherung, die Datenübertragung oder den Datentransport (z. B. Laptop, USB).
- Erwägen Sie die Verschlüsselung von Endgeräten und Wechseldatenträgern mit sensiblen Daten (z. B. Festplatten, Laptops, mobile Geräte, USB-Speichergeräte, ...). Dies könnte z. B. mit Windows BitLocker®, VeraCrypt, Apple FileVault®, Linux® dm-crypt,... geschehen.
- Erwägen Sie die Verschlüsselung sensibler Daten, die in der Cloud gespeichert sind.

Diese Kontrolle wird durch die anderen Bestandteile dieser Richtlinie abgedeckt; es werden keine zusätzlichen Anforderungen festgelegt.

Leitfaden

Die folgenden Maßnahmen sollten in Betracht gezogen werden:

- Implementierung spezieller Schutzmaßnahmen zur Verhinderung des unbefugten Zugriffs, der Verfälschung oder Änderung von Systemdaten und Prüfungsaufzeichnungen (z. B. eingeschränkte Zugriffsrechte, tägliche Backups, Datenverschlüsselung, Firewall-Installation).
- Verschlüsseln Sie Festplatten, externe Medien, gespeicherte Dateien, Konfigurationsdateien und in der Cloud gespeicherte Daten.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 3
IEC 62443-3-3:2013, SR 3.4, SR 4.1
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 8.1, Anhang A (siehe ISO 27002**)**
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.10

PR.DS-2: Data-in-transit ist geschützt.

Da diese Kontrolle durch die anderen Bestandteile dieser Richtlinie abgedeckt wird,gibt es werden keine zusätzlichen Anforderungen. für das Sicherheitsniveau "Basic" Es werden spezifische Leitlinien zur Erhöhung der Informationssicherheit bereitgestellt.

Leitfaden

Wenn das Unternehmen häufig sensible Dokumente oder E-Mails versendet, empfiehlt es sich, diese Dokumente und/oder E-Mails mit geeigneten, unterstützten und zugelassenen Softwaretools zu verschlüsseln.

Die Organisation muss ihre kritischen Systeminformationen, die als kritisch eingestuft werden, während der Übertragung schützen.

Leitfaden

Wenn Sie sensible Dokumente oder E-Mails versenden, sollten Sie eine Verschlüsselung dieser Dokumente und/oder E-Mails in Betracht ziehen.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 3
IEC 62443-3-3:2013, SR 3.1, SR 3.8, SR 4.1, SR 4.**2**
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 8, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.10, 5.14, 8.20, 8.26

PR.DS-3: Die Vermögenswerte werden während des gesamten Umzugs, der Verbringung und der Veräußerung formell verwaltet.

Vermögenswerte und Medien sind sicher zu entsorgen.

Leitfaden

- Bei der Beseitigung von Sachanlagen wie Geschäftscomputern/Laptops, Servern, Festplatten und anderen Speichermedien (USB-Laufwerke, Papier...) ist sicherzustellen, dass alle sensiblen geschäftlichen oder personenbezogenen Daten sicher gelöscht (d. h. elektronisch "gewischt") werden, bevor sie entfernt und anschließend physisch vernichtet (oder wieder in Betrieb genommen) werden. Dies wird auch als "Bereinigung" bezeichnet und steht somit im Zusammenhang mit der Anforderung und Anleitung in PR.IP-6.
- Erwägen Sie die Installation einer Fernlöschanwendung auf Firmenlaptops, Tablets, Handys und anderen mobilen Geräten

Die Organisation muss die Rechenschaftspflicht für alle geschäftskritischen Güter während des gesamten Lebenszyklus des Systems durchsetzen, einschließlich Entfernung, Übertragung und Entsorgung.

Leitfaden

Die Rechenschaftspflicht sollte umfassen:

- Die Berechtigung für geschäftskritische Güter, die Einrichtung zu betreten und zu verlassen.
- Überwachung und Pflege der Dokumentation über die Bewegungen von geschäftskritischen Gütern.

Die Organisation muss sicherstellen, dass Entsorgungsmaßnahmen genehmigt, verfolgt, dokumentiert und überprüft werden.

Leitfaden

Zu den Entsorgungsmaßnahmen gehören Maßnahmen zur Mediensanierung (siehe PR.IP-6).

Die Organisation muss sicherstellen, dass die erforderlichen Maßnahmen für den Fall des Verlusts, des Missbrauchs, der Beschädigung oder des Diebstahls von Vermögenswerten getroffen werden.

Leitfaden

Dies kann durch Richtlinien, Prozesse und Verfahren (Berichterstattung), technische und organisatorische Mittel (Verschlüsselung, Zugriffskontrolle (AC), Mobile Device Management (MDM), Überwachung, sicheres Löschen, Awareness, unterzeichnete Benutzervereinbarung, Richtlinien und Handbücher, Backups, Aktualisierung des Inventars ...) geschehen.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 1
IEC 62443-2-1:2010, Klausel 4.3.3.3.9, 4.3.4.4.1
IEC 62443-3-3:2013, SR 4.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.5, 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.10, 7.10, 7.14

PR.DS-4: Angemessene Kapazitäten zur Gewährleistung der Verfügbarkeit werden aufrechterhalten.

Die Kapazitätsplanung soll angemessene Ressourcen für die Informationsverarbeitung, Vernetzung, Telekommunikation und Datenspeicherung der kritischen Systeme der Organisation sicherstellen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Die kritischen Systeme der Organisation sind gegen Denial-of-Service-Angriffe zu schützen oder zumindest die Auswirkungen solcher Angriffe zu begrenzen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Audit-Daten aus den kritischen Systemen der Organisation werden auf ein alternatives System übertragen.

Leitfaden

Seien Sie sich darüber im Klaren, dass die Protokolldienste zu einem Engpass werden und das ordnungsgemäße Funktionieren der Quellsysteme behindern können.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 1, 2
IEC 62443-2-1:2010, Klausel 4.3.3.3.9, 4.3.4.4.1
IEC 62443-3-3:2013, SR 4.2, SR 7.1, SR 7.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.1, 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 8.14, 8.32

PR.DS-5: Schutzmaßnahmen gegen Datenlecks sind implementiert .

Die Organisation muss geeignete Maßnahmen ergreifen, die zur Überwachung ihrer kritischen Systeme an den Außengrenzen und kritischen internen Punkten führen, wenn unbefugte Zugriffe und Aktivitäten, einschließlich Datenlecks, entdeckt werden.

Leitfaden

- Erwägen Sie die Einführung spezieller Schutzmaßnahmen (eingeschränkte Zugriffsrechte, tägliche Backups, Datenverschlüsselung, Installation von Firewalls usw.) für die sensibelsten Daten.
- Erwägen Sie eine häufige Prüfung der Konfiguration des zentralen Verzeichnisses (Active Directory in einer Windows-Umgebung), mit besonderem Augenmerk auf den Zugang zu den Daten von Schlüsselpersonen im Unternehmen.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 3
IEC 62443-3-3:2013 SR 5.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.3, 5.10, 5.13, 5.14, 5.15, 6.1, 6.2, 6.5, 6.6, 7.5, 7.6, 7.8, 8.2, 8.3, 8.4, 8.18, 8.20, 8.22, 8.24, 8.26

PR.DS-6: Integritätsprüfungsmechanismen werden verwendet, um die Integrität von Software, Firmware und Informationen zu überprüfen.

Die Organisation muss Software-, Firmware- und Informationsintegritätsprüfungen durchführen, um unbefugte Änderungen an ihren kritischen Systemkomponenten während der Lagerung, des Transports, der Inbetriebnahme und bei Bedarf zu erkennen.

Leitfaden

Modernste Integritätsprüfungsmechanismen (z. B. Paritätsprüfungen, zyklische Redundanzprüfungen, kryptografische Hashes) und entsprechende Tools können die Integrität von Informationssystemen und gehosteten Anwendungen automatisch überwachen.

Die Organisation muss, wo dies möglich ist, automatisierte Anwendungen einsetzen, um bei der Entdeckung von Unstimmigkeiten während der Integritätsprüfung eine Benachrichtigung zu übermitteln.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Die Organisation muss automatische Reaktionsmöglichkeiten mit vordefinierten Sicherheitsvorkehrungen einführen, wenn Integritätsverletzungen entdeckt werden.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 2, 7
IEC 62443-3-3:2013, SR 3.1, SR 3.3, SR 3.4, SR 3.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 8.7, 8.19, 8.26, 8.32

PR.DS-7: Die Entwicklungs- und Testumgebung(en) sind von der Produktionsumgebung getrennt.

Die Entwicklungs- und Testumgebung(en) müssen von der Produktionsumgebung isoliert sein.

Leitfaden

- Jede Änderung, die an der IKT/OT-Umgebung vorgenommen werden soll, sollte zunächst in einer anderen, von der Produktionsumgebung (Betriebsumgebung) getrennten Umgebung getestet werden, bevor diese Änderung tatsächlich umgesetzt wird. Auf diese Weise können die Auswirkungen dieser Änderungen analysiert und Anpassungen vorgenommen werden, ohne die betrieblichen Abläufe zu stören.
- Erwägen Sie das Hinzufügen und Testen von Cybersicherheitsfunktionen bereits während der Entwicklung (Grundsätze des sicheren Entwicklungslebenszyklus).

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 16,
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 8.31

PR.DS-8: Integritätsprüfungsmechanismen werden zur Überprüfung der Hardware-Integrität verwendet.

Die Organisation muss Hardware-Integritätsprüfungen durchführen, um unbefugte Eingriffe in die Hardware ihres kritischen Systems zu erkennen.

Leitfaden

Modernste Integritätsprüfungsmechanismen (z. B. Paritätsprüfungen, zyklische Redundanzprüfungen, kryptografische Hashes) und entsprechende Tools können die Integrität von Informationssystemen und gehosteten Anwendungen automatisch überwachen.

Die Organisation muss die Erkennung von unbefugten Eingriffen in die Hardware ihrer kritischen Systeme in die Fähigkeit der Organisation zur Reaktion auf Zwischenfälle einbeziehen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

IEC 62443-2-1:2010, Abschnitt 4.3.4.4.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 7.13

Sicherheitsrichtlinien (die den Zweck, den Umfang, die Rollen, die Zuständigkeiten, die Verpflichtung des Managements und die Koordinierung zwischen den Organisationseinheiten betreffen), Prozesse und Verfahren werden beibehalten und zur Verwaltung des Schutzes von Informationssystemen und Vermögenswerten eingesetzt.

PR.IP-1: Es wird eine Basiskonfiguration von informationstechnischen/industriellen Kontrollsystemen erstellt und gepflegt, die Sicherheitsgrundsätze enthält.

Die Organisation muss eine Basiskonfiguration für ihre geschäftskritischen Systeme entwickeln, dokumentieren und pflegen.
- Schlüsselmaßnahme -

Leitfaden

- Diese Kontrolle beinhaltet das Konzept der geringsten Funktionalität.
- Zu den Basiskonfigurationen gehören beispielsweise Informationen über die geschäftskritischen Systeme des Unternehmens, aktuelle Versionsnummern und Patch-Informationen zu Betriebssystemen und Anwendungen, Konfigurationseinstellungen/Parameter, Netzwerktopologie und die logische Anordnung dieser Komponenten innerhalb der Systemarchitektur.
- Die Netztopologie sollte die neuralgischen Punkte der IT/OT-Umgebung umfassen (externe Verbindungen, Server mit Daten und/oder sensiblen Funktionen, Sicherheit der DNS-Dienste usw.).

Die Organisation muss ihre geschäftskritischen Systeme so konfigurieren, dass nur wesentliche Funktionen zur Verfügung stehen. Daher ist die Basiskonfiguration zu überprüfen, und nicht benötigte Funktionen sind zu deaktivieren.

Leitfaden

- Die Konfiguration eines Systems, das nur die von der Organisation definierten, für den Einsatz wesentlichen Fähigkeiten bietet, wird als "Konzept der geringsten Funktionalität" bezeichnet.
- Zu den Fähigkeiten gehören Funktionen, Ports, Protokolle, Software und/oder Dienste.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 1, 7, 4, 12
IEC 62443-2-1:2010, Klausel 4.3.4.3.2, 4.3.4.3.3
IEC 62443-3-3:2013, SR 7.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 8.19, A.8.32

PR.IP-2: Ein Systementwicklungs-Lebenszyklus zur Verwaltung von Systemen wird eingeführt .

Der Lebenszyklus der System- und Anwendungsentwicklung muss Sicherheitsüberlegungen beinhalten.

Leitfaden

- Der Lebenszyklus der System- und Anwendungsentwicklung sollte den Beschaffungsprozess der geschäftskritischen Systeme der Organisation und ihrer Komponenten umfassen.
- Schulungen zur Sensibilisierung für Schwachstellen und zur Vorbeugung von Schwachstellen für (Webanwendungs-)Entwickler sowie fortgeschrittene Schulungen zur Sensibilisierung für Social Engineering für hochrangige Funktionen sollten in Betracht gezogen werden.
- Beim Hosten von Internetanwendungen sollte die Implementierung einer Web Application Firewall (WAF) in Betracht gezogen werden.

Der Entwicklungsprozess für kritische Systeme und Systemkomponenten muß den gesamten Entwurfszyklus abdecken und eine Beschreibung der funktionalen Eigenschaften der Sicherheitskontrollen sowie Informationen über den Entwurf und die Implementierung sicherheitsrelevanter Systemschnittstellen enthalten.

Leitfaden

Der Entwicklungszyklus umfasst:

- Alle Entwicklungsphasen: Spezifikation, Entwurf, Entwicklung, Implementierung.
- Konfigurationsmanagement für geplante und ungeplante Änderungen und Änderungskontrolle während der Entwicklung.
- Fehlersuche und -behebung.
- Sicherheitstests.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 16
IEC 62443-2-1:2010, Abschnitt 4.3.4.3.3
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.8, 8.25, 8.27

PR.IP-3: Prozesse zur Kontrolle von Konfigurationsänderungen sind vorhanden .

Änderungen müssen getestet und validiert werden, bevor sie in operative Systeme implementiert werden.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 4, 5, 12
IEC 62443-2-1:2010, Klausel 4.3.4.3.2, 4.3.4.3.3
IEC 62443-3-3:2013, SR 7.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.5, 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 8.19, 8.32

Bei geplanten Änderungen an den kritischen Systemen der Organisation ist vor der Implementierung in einer Betriebsumgebung eine Analyse der Sicherheitsauswirkungen in einer separaten Testumgebung durchzuführen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 4, 5, 12
IEC 62443-2-1:2010, Klausel 4.3.4.3.2, 4.3.4.3.3
IEC 62443-3-3:2013, SR 7.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.5, 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 8.19, 8.32

PR.IP-4: Backups von Informationen werden durchgeführt, gepflegt und getestet.

Backups der geschäftskritischen Daten der Organisation müssen auf einem anderen System als dem Gerät, auf dem sich die Originaldaten befinden, durchgeführt und gespeichert werden.
- Schlüsselmaßnahme -

Leitfaden

- Zu den geschäftskritischen Systemdaten eines Unternehmens gehören z. B. Software, Konfigurationen und Einstellungen, Dokumentation, Systemkonfigurationsdaten einschließlich Backups der Computerkonfiguration, Backups der Anwendungskonfiguration usw.
- Ziehen Sie ein regelmäßiges Backup in Betracht und stellen Sie es regelmäßig offline.
- Die Ziele für die Wiederherstellungszeit und den Wiederherstellungspunkt sollten berücksichtigt werden.
- Ziehen Sie in Erwägung, die Datensicherung des Unternehmens nicht im selben Netzwerk zu speichern wie das System, auf dem sich die Originaldaten befinden, und eine Offline-Kopie bereitzustellen. Dies verhindert u. a. die Verschlüsselung von Dateien durch Hacker (Gefahr von Ransomware).

Die Zuverlässigkeit und Integrität der Backups ist regelmäßig zu überprüfen und zu testen.

Leitfaden

Dazu gehört auch die regelmäßige Überprüfung der Verfahren zur Wiederherstellung von Sicherungskopien.

Die Überprüfung der Sicherheitskopien ist mit den Funktionen in der Organisation zu koordinieren, die für die entsprechenden Pläne zuständig sind.

Leitfaden

- Zu diesen Plänen gehören beispielsweise Pläne für die Geschäftskontinuität, Pläne für die Wiederherstellung im Katastrophenfall, Pläne für die Kontinuität des Betriebs, Pläne für die Krisenkommunikation, Pläne für kritische Infrastrukturen und Pläne für die Reaktion auf Cyber-Vorfälle.
- Die Wiederherstellung von Sicherungsdaten während der Prüfung des Notfallplans sollte vorgesehen werden.

Es ist ein separater alternativer Speicherort für Systemsicherungen zu betreiben. Hierbei sind dieselben Sicherheitsvorkehrungen wie für den primären Speicherort zu treffen.

Leitfaden

Eine Offline-Sicherung Ihrer Daten wird idealerweise an einem von der ursprünglichen Datenquelle getrennten physischen Ort und, wenn möglich, an einem externen Standort gespeichert, um zusätzlichen Schutz und Sicherheit zu gewährleisten.

Das Backup kritischer Systeme ist von dem Backup kritischer Informationen zu trennen.

Leitfaden

Die Trennung des Backups kritischer Systeme von dem Backup kritischer Informationen sollte zu einer kürzeren Wiederherstellungszeit führen.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 11
IEC 62443-2-1:2010, Abschnitt 4.3.4.3.9
IEC 62443-3-3:2013, SR 7.3, SR 7.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.5, 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.29, 5.33, 8.13

PR.IP-5: Richtlinien und Vorschriften bezüglich der physischen Betriebsumgebung für die Vermögenswerte der Organisation werden eingehalten.

Die Organisation muss Richtlinien und Verfahren für Notfall- und Sicherheitssysteme, Brandschutzsysteme und Umweltkontrollen für ihre kritischen Systeme festlegen, umsetzen und durchsetzen.

Leitfaden

Die folgenden Maßnahmen sollten in Betracht gezogen werden:

- Sichern Sie unbeaufsichtigte Computergeräte mit Vorhängeschlössern oder einem Schließfach- und Schlüsselsystem.
- Bei den Brandbekämpfungsmechanismen sollte die kritische Systemumgebung der Organisation berücksichtigt werden (z. B. können Wassersprinkleranlagen in bestimmten Umgebungen gefährlich sein).

Die Organisation muss Feuermeldevorrichtungen einrichten, die sich im Falle eines Brandes automatisch aktivieren und das Schlüsselpersonal benachrichtigen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

IEC 62443-2-1:2010, Abschnitte 4.3.3.3.1, 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 4.1, 6.1, 7.1, 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 7.5, 7.8, 7.11, 7.12

PR.IP-6: Die Daten werden gemäß der Richtlinie vernichtet.

Die Organisation muss sicherstellen, dass die Daten ihrer kritischen Systeme gemäß den Richtlinien vernichtet werden.

Leitfaden

- Zu den Entsorgungsmaßnahmen gehören Maßnahmen zur Mediensanierung (siehe PR.DS-3)
- Es gibt zwei Haupttypen von Medien, die allgemein verwendet werden:
  - Hardcopy-Medien (physische Darstellungen von Informationen)
  - Elektronische oder Softcopy-Medien (die Bits und Bytes, die in Festplatten, Arbeitsspeichern (RAM), Festwertspeichern (ROM), Disketten, Speichergeräten, Telefonen, mobilen Computern, Netzwerkgeräten usw. enthalten sind)

Die Sanierungsverfahren sind zu dokumentieren und zu testen.

Leitfaden

- Zu den Sanierungsverfahren gehören Verfahren und Ausrüstung.
- Erwägen Sie die Anwendung nicht-destruktiver Desinfektionsverfahren für tragbare Speichermedien.
- Überlegen Sie, ob die Sanierungsmaßnahmen im Verhältnis zu den Vertraulichkeitsanforderungen stehen.

Referenzen

IEC 62443-2-1:2010, Abschnitt 4.3.4.4.4
IEC 62443-3-3:2013, SR 4.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.5, Klausel 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.10, 7.10, 7.14

PR.IP-7: Schutzverfahren werden verbessert.

Die Organisation muss Verbesserungen, die sich aus der Überwachung, den Messungen, den Bewertungen und den gewonnenen Erkenntnissen ergeben, in die Aktualisierung der Schutzverfahren einbeziehen (kontinuierliche Verbesserung).

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Die Organisation muss unabhängige Teams einsetzen, um den/die Schutzprozess/e zu bewerten.

Leitfaden

- Zu den unabhängigen Teams können interne oder externe unparteiische Mitarbeiter gehören.
- Unparteilichkeit bedeutet, dass die Bewerter frei von vermeintlichen oder tatsächlichen Interessenkonflikten in Bezug auf die Entwicklung, den Betrieb oder die Verwaltung des zu bewertenden kritischen Systems der Organisation oder auf die Bestimmung der Wirksamkeit der Sicherheitskontrollen sind.

Die Organisation muss sicherstellen, dass der Sicherheitsplan für ihre kritischen Systeme die Überprüfung, das Testen und die ständige Verbesserung der Sicherheitsschutzverfahren erleichtert.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

IEC 62443-2-1:2010, Klausel 4.4.3
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 9, 10.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.27

PR.IP-8: Die Wirksamkeit von Schutztechnologien wird gemeinsam genutzt.

Die Organisation muss zusammenarbeiten und Informationen über sicherheitsrelevante Vorfälle in ihrem kritischen System und Maßnahmen zur Schadensbegrenzung mit den benannten Partnern austauschen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Die Mitteilung über die Wirksamkeit der Schutztechnologien wird an die zuständigen Stellen weitergeleitet.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Die Organisation soll, soweit möglich, automatisierte Mechanismen zur Unterstützung der Informationszusammenarbeit einsetzen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.4, Anhang A (siehe ISO 27002**)**
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.27

PR.IP-9: Reaktionspläne (Incident Response und Business Continuity) und Wiederherstellungspläne (Incident Recovery und Disaster Recovery) sind vorhanden und werden verwaltet.

Pläne zur Reaktion auf Vorfälle (Incident Response und Business Continuity) und Wiederherstellungspläne (Incident Recovery und Disaster Recovery) sind zu erstellen, zu pflegen, zu genehmigen und zu testen, um die Wirksamkeit der Pläne und die Bereitschaft zur Ausführung der Pläne zu ermitteln.

Leitfaden

- Der Plan zur Reaktion auf einen Vorfall ist die Dokumentation einer Reihe vorher festgelegter Anweisungen oder Verfahren zur Erkennung, Reaktion und Begrenzung der Folgen eines bösartigen Cyberangriffs.
- Die Pläne sollten Wiederherstellungsziele, Wiederherstellungsprioritäten, Metriken, Kontingenzrollen, Personalzuweisungen und Kontaktinformationen enthalten.
- Die Aufrechterhaltung wesentlicher Funktionen trotz einer Systemunterbrechung und die eventuelle Wiederherstellung der Systeme der Organisation sollten behandelt werden.
- Überlegen Sie, welche Arten von Vorfällen, Ressourcen und Managementunterstützung erforderlich sind, um die Reaktions- und Notfallkapazitäten effektiv zu erhalten und auszubauen.

Die Organisation muss die Entwicklung und das Testen von Notfall- und Wiederherstellungsplänen mit den für die entsprechenden Pläne verantwortlichen Akteuren koordinieren.

Leitfaden

Zu den entsprechenden Plänen gehören beispielsweise Pläne zur Aufrechterhaltung des Geschäftsbetriebs, Pläne zur Wiederherstellung des Betriebs im Katastrophenfall, Pläne für die Krisenkommunikation, Pläne für kritische Infrastrukturen, Reaktionspläne für Cybervorfälle und Notfallpläne für die Bewohner.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 17
IEC 62443-2-1:2010, Klausel 4.3.2.5.7, 4.3.4.5.11
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 4.1, 4.2, 6, 8, 10.2, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.24, 5.29

PR.IP-11: Die Cybersicherheit wird in die Praktiken des Personalwesens einbezogen (Deprovisionierung, Personalauswahl...).

Das Personal, das Zugang zu den wichtigsten Informationen oder Technologien der Organisation hat, muss überprüft werden.

Leitfaden

- Der Zugang zu kritischen Informationen oder Technologien sollte bei der Einstellung, während des Beschäftigungsverhältnisses und bei der Kündigung berücksichtigt werden.
- Bei der Überprüfung des Hintergrunds sollten die geltenden Gesetze, Vorschriften und ethischen Grundsätze im Verhältnis zu den geschäftlichen Anforderungen, der Klassifizierung der Informationen, auf die zugegriffen werden soll, und den wahrgenommenen Risiken berücksichtigt werden.

Entwicklung und Aufrechterhaltung eines Prozesses für die Informationssicherheit der Humanressourcen/Cybersicherheit, der bei der Einstellung, während der Beschäftigung und bei der Beendigung des Beschäftigungsverhältnisses Anwendung findet.

Leitfaden

Der Prozess der Personalinformation/Cybersicherheit sollte unter anderem den Zugang zu kritischen Informationen oder Technologien, die Überprüfung des Hintergrunds, einen Verhaltenskodex, Rollen, Befugnisse und Verantwortlichkeitenbeinhalten.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 4, 6
IEC 62443-2-1:2010, Abschnitt 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 4.1, 4.2, 7.1, 7.3, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.4, 5.11, 6.1, 6.2, 6.3, 6.4, 6.5

PR.IP-12: Ein Plan für das Management von Schwachstellen wird entwickelt und umgesetzt.

Die Organisation muss ein dokumentiertes Verfahren einführen und aufrechterhalten, das eine kontinuierliche Überprüfung von Schwachstellen und Strategien zu deren Minderung ermöglicht.

Leitfaden

- Erwägen Sie eine Bestandsaufnahme der Quellen, die wahrscheinlich Schwachstellen in den identifizierten Komponenten melden und Updates verteilen (Websites der Softwarehersteller, CERT-Website, ENISA-Website).
- Die Organisation sollte herausfinden, wo die Schwachstellen ihrer kritischen Systeme für Angreifer offen liegen könnten.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 2, 4, 5, 16, 18
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 6, 8, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.36, 6.8, 8.8, 8.32

Die Wartung und Reparatur von Komponenten industrieller Kontroll- und Informationssysteme erfolgt in Übereinstimmung mit Richtlinien und Verfahren.

PR.MA-1: Wartung und Reparatur von Organisationsmitteln werden mit genehmigten und kontrollierten Maßnahmen durchgeführt und protokolliert.

Patches und Sicherheitsupdates für Betriebssysteme und kritische Systemkomponenten sind zu installieren.

- Schlüsselmaßnahme -

Leitfaden

Dabei sollte Folgendes berücksichtigt werden:

- Beschränken Sie sich darauf, nur die Anwendungen (Betriebssysteme, Firmware oder Plugins) zu installieren, die Sie für den Betrieb Ihres Unternehmens benötigen, und führen Sie regelmäßig Patches/Aktualisierungen durch.
- Sie sollten nur eine aktuelle und vom Hersteller unterstützte Version der Software installieren, die Sie verwenden möchten. Es kann sinnvoll sein, jeden Monat einen Tag festzulegen, an dem nach Patches gesucht wird.
- Es gibt Produkte, die Ihr System scannen und Sie benachrichtigen können, wenn es eine Aktualisierung für eine von Ihnen installierte Anwendung gibt. Wenn Sie eines dieser Produkte verwenden, stellen Sie sicher, dass es für jede von Ihnen verwendete Anwendung nach Updates sucht.
- Rechtzeitige Installation von Patches und Sicherheitsupdates.

Die Organisation muss vorbeugende Instandhaltung und Reparaturen an ihren kritischen Systemkomponenten gemäß genehmigter Verfahren und Werkzeuge planen, durchführen und dokumentieren.

Leitfaden

Dabei sollte Folgendes berücksichtigt werden:

- Rechtzeitige Durchführung von Sicherheitsaktualisierungen für die gesamte Software.
- Automatisieren Sie den Aktualisierungsprozess und überprüfen Sie seine Wirksamkeit.
- Einführung einer internen Patching-Kultur für Desktops, mobile Geräte, Server, Netzwerkkomponenten usw., um sicherzustellen, dass Aktualisierungen nachverfolgt werden.

Die Organisation muss die unbefugte Entfernung von Wartungsgeräten verhindern, die kritische Systeminformationen der Organisation enthalten.

- Schlüsselmaßnahme -

Leitfaden

Diese Anforderung bezieht sich hauptsächlich auf OT/ICS-Umgebungen.

Die Organisation muss die Genehmigungsanforderungen, die Kontrolle und die Überwachung von Wartungswerkzeugen für den Einsatz in ihren kritischen Systemen durchsetzen.

Leitfaden

Zu den Wartungswerkzeugen können Hardware-/Software-Diagnosetestgeräte, Hardware-/Software-Paketschnüffler und Laptops gehören.

Wartungswerkzeuge und tragbare Speichermedien sind zu überprüfen, wenn sie in die Einrichtung gebracht werden, und sind durch Anti-Malware-Lösungen zu schützen, so dass sie auf bösartigen Code gescannt werden, bevor sie auf den Systemen der Organisation verwendet werden.
- Schlüsselmaßnahme -

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Die Organisation muss die Sicherheitskontrollen nach der Wartung oder Reparatur von Hardware überprüfen und gegebenenfalls Maßnahmen ergreifen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Die Organisation muss die Sicherheitskontrollen nach der Wartung oder Reparatur/Patching von Hardware und Software überprüfen und gegebenenfalls Maßnahmen ergreifen.
- Schlüsselmaßnahme -

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

IEC 62443-2-1:2010, Abschnitt 4.3.3.3.7
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 4.2, 7.1, 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 7.2, 7.9, 7.10, 7.13

PR.MA-2: Die Fernwartung von Unternehmensressourcen wird genehmigt, protokolliert und in einer Weise durchgeführt, die unbefugten Zugriff verhindert.

Fernwartung darf nur nach vorheriger Genehmigung, Überwachung zur Vermeidung unbefugten Zugriffs und Genehmigung des Ergebnisses der Wartungstätigkeiten, wie in genehmigten Prozessen oder Verfahren beschrieben, erfolgen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Die Organisation muss verlangen, dass Diagnosedienste im Zusammenhang mit der Fernwartung von einem System aus durchgeführt werden, das eine vergleichbare Sicherheit bietet wie das kritische System der entsprechenden Organisation.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Die Organisation muss sicherstellen, dass starke Authentifikationen, Aufzeichnungen und Sitzungsbeendigung für die Fernwartung implementiert sind.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 4, 7
IEC 62443-2-1:2010, Abschnitte 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 4.2, 7.1, 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.19, 5.22, 7.13

Technische Sicherheitslösungen werden so verwaltet, dass die Sicherheit und Widerstandsfähigkeit von Systemen und Anlagen im Einklang mit den entsprechenden Richtlinien, Verfahren und Vereinbarungen gewährleistet ist.

PR.PT-1: Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit der Richtlinie festgelegt, dokumentiert, umgesetzt und überprüft.

Die Protokolle sind zu führen, zu dokumentieren und zu überprüfen.
- Schlüsselmaßnahme -

Leitfaden

- Stellen Sie sicher, dass die Aktivitätsprotokollierungsfunktion von Schutz-/Erkennungshardware oder -software (z. B. Firewalls, Virenschutz) aktiviert ist.
- Die Protokolle sollten gesichert und für einen bestimmten Zeitraum gespeichert werden.
- Die Protokolle sollten auf ungewöhnliche oder unerwünschte Trends überprüft werden, z. B. eine starke Nutzung von Social-Media-Websites oder eine ungewöhnliche Anzahl von Viren, die regelmäßig auf einem bestimmten Computer gefunden werden. Diese Trends können auf ein ernsteres Problem hinweisen oder signalisieren, dass in einem bestimmten Bereich stärkere Schutzmaßnahmen erforderlich sind.

Die Organisation muss sicherstellen, dass die Protokolle eine maßgebliche Zeitquelle oder einen Zeitstempel der internen Uhr enthalten, der mit einer maßgeblichen Zeitquelle verglichen und synchronisiert wird.

Leitfaden

Zu den maßgeblichen Zeitquellen gehören z. B. ein interner NTP-Server (Network Time Protocol), eine Funkuhr, eine Atomuhr oder eine GPS-Zeitquelle.

Die Organisation muss sicherstellen, dass Fehler in der Prüfungsverarbeitung in den Systemen der Organisation Warnungen erzeugen und definierte Reaktionen auslösen.

Leitfaden

Die Verwendung von System Logging Protocol (Syslog)-Servern kann in Betracht gezogen werden.

Die Organisation muss autorisierten Personen die Möglichkeit geben, die Prüfungsmöglichkeiten zu erweitern, wenn dies aufgrund von Ereignissen erforderlich ist.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 1, 3, 4, 8
IEC 62443-2-1:2010, Abschnitte 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.4
IEC 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 9.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 8.15, 8.17, 8.34

PR.PT-2: Wechseldatenträger sind geschützt und ihre Nutzung ist gemäß der Richtlinie eingeschränkt.

Die Nutzungsbeschränkung für tragbare Speichermedien ist durch eine geeignete dokumentierte Richtlinie und entsprechende Sicherheitsvorkehrungen zu gewährleisten.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Tragbare Speichermedien, die Systemdaten enthalten, müssen während des Transports und der Lagerung kontrolliert und geschützt werden.
- Schlüsselmaßnahme -

Leitfaden

Zum Schutz und zur Kontrolle sollte das Scannen aller tragbaren Speichergeräte auf bösartigen Code erfolgen, bevor sie auf den Systemen des Unternehmens eingesetzt werden.

Die Organisation sollte den Anschluss von Wechseldatenträgern technisch verbieten, sofern dies nicht unbedingt erforderlich ist; in anderen Fällen sollte die Ausführung von Autostarts von solchen Datenträgern deaktiviert werden.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 3, 10
IEC 62443-3-3:2013, SR 2.3
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.1, 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.10, 5.12, 5.13, 7.7, 7.10

PR.PT-3: Das Prinzip des geringsten Funktionsumfangs wird berücksichtigt, indem die Systeme so konfiguriert werden, dass sie nur wesentliche Funktionen bieten.

Die Organisation muss die geschäftskritischen Systeme so konfigurieren, dass sie nur wesentliche Funktionen bereitstellen.

Leitfaden

Erwägen Sie die Anwendung des Prinzips der geringsten Funktionalität auf Zugangssysteme und -mittel (siehe auch PR.AC-4).

Die Organisation muss bestimmte Funktionen, Ports, Protokolle und Dienste innerhalb ihrer kritischen Systeme, die sie für unnötig hält, deaktivieren.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Die Organisation muss technische Sicherheitsvorkehrungen treffen, um eine "Deny-All"-Richtlinie und eine "Permission-by-Exception"-Richtlinie durchzusetzen, die nur die Ausführung von autorisierten Softwareprogrammen erlaubt.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 3, 4, 7
IEC 62443-2-1:2010, Abschnitte 4.3.3.5, 4.3.3.6, 4.3.3.7
IEC 62443-3-3:2013, SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.1, 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.15

PR.PT-4: Kommunikations- und Kontrollnetze sind geschützt.

Web- und E-Mail-Filter sind zu installieren und zu verwenden.

Leitfaden

- E-Mail-Filter sollten bösartige E-Mails erkennen, und die Filterung sollte auf der Grundlage des Typs der Nachrichtenanhänge konfiguriert werden, so dass Dateien der angegebenen Typen automatisch verarbeitet (z. B. gelöscht) werden.
- Web-Filter sollten den Nutzer benachrichtigen, wenn eine Website möglicherweise Malware enthält, und den Zugriff auf diese Website möglicherweise verhindern.

Die Organisation muss den Informationsfluss/Datenfluss innerhalb ihrer kritischen Systeme und zwischen miteinander verbundenen Systemen kontrollieren.

Leitfaden

Bedenken Sie Folgendes:

- Der Informationsfluss kann z. B. durch die Kennzeichnung oder Einfärbung von physischen Anschlüssen unterstützt werden, um das manuelle Anschließen zu erleichtern.
- Durch die Überprüfung des Nachrichteninhalts können Richtlinien für den Informationsfluss durchgesetzt werden. So kann beispielsweise eine Nachricht, die einen Befehl an ein Stellglied enthält, nicht zwischen dem Kontrollnetz und einem anderen Netz ausgetauscht werden.
- Physikalische Adressen (z. B. eine serielle Schnittstelle) können implizit oder explizit mit Bezeichnungen oder Attributen (z. B. Hardware-E/A-Adresse) verbunden sein. Manuelle Methoden sind in der Regel statisch. Kennzeichnungs- oder Attributregelungsmechanismen können in Hardware, Firmware und Software implementiert werden, die den Gerätezugriff steuern oder haben, wie z. B. Gerätetreiber und Kommunikationscontroller.

Die Organisation muss die Schnittstelle für externe Kommunikationsdienste verwalten, indem sie eine Richtlinie für den Verkehrsfluss festlegt, die die Vertraulichkeit und Integrität der übermittelten Informationen schützt.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 4, 10, 12, 13
IEC 62443-3-3:2013, SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 4.1, 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.14, 8.20, 8.26

Anomale Aktivitäten werden aufgedeckt und die potenziellen Auswirkungen von Ereignissen werden verstanden.

DE.AE-1: Eine Grundlage für den Netzbetrieb und die erwarteten Datenströme für Nutzer und Systeme wird erstellt und verwaltet.

Die Organisation muss sicherstellen, dass eine Grundlage für den Netzbetrieb und den erwarteten Datenfluss für ihre kritischen Systeme entwickelt, dokumentiert und gepflegt wird, um Ereignisse zu verfolgen.
- Schlüsselmaßnahme -

Leitfaden

- Ziehen Sie in Erwägung, die lokale Protokollierung auf all Ihren Systemen und Netzwerkgeräten zu aktivieren und sie für einen bestimmten Zeitraum aufzubewahren, zum Beispiel bis zu 6 Monate.
- Vergewissern Sie sich, dass Ihre Protokolle genügend Informationen enthalten (Quelle, Datum, Benutzer, Zeitstempel usw.) und dass Sie genügend Speicherplatz für ihre Erstellung haben.
- Erwägen Sie die Zentralisierung Ihrer Protokolle.
- Erwägen Sie den Einsatz eines SIEM-Tools (Security Information and Event Management), das die Korrelation und Analyse Ihrer Daten erleichtert.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 1, 8, 13
IEC 62443-2-1:2010, Abschnitt 4.4.3.3
ISO/IEC 27001:2012, Klausel 8.1, 9.1, 10.2, Anhang A (siehe ISO 27002**)**
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.37, 8.20, 8.21, 8.32

DE.AE-2: Erkannte Ereignisse werden analysiert, um Angriffsziele und -methoden zu verstehen.

Die Organisation muss festgestellte Ereignisse überprüfen und analysieren, um Angriffsziele und -methoden zu verstehen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Die Organisation muss, soweit möglich, automatisierte Mechanismen zur Überprüfung und Analyse der festgestellten Ereignisse einsetzen.

Leitfaden

Überprüfen Sie Ihre Protokolle regelmäßig, um Anomalien oder abnormale Ereignisse zu erkennen.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 1, 8, 13, 15
IEC 62443-2-1:2010, Klausel 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8
IEC 62443-3-3:2013, SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 8.1, 9.1, 10.2, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.24, 5.25, 8.15

DE.AE-3: Ereignisdaten werden von mehreren Quellen und Sensoren gesammelt und korreliert.

Die Aktivitätsprotokollierungsfunktion von Schutz-/Erkennungshardware oder -software (z. B. Firewalls, Antivirenprogramme) ist zu aktivieren, zu sichern und zu überprüfen.
- Schlüsselmaßnahme -

Leitfaden

- Die Protokolle sollten gesichert und für einen bestimmten Zeitraum gespeichert werden.
- Die Protokolle sollten auf ungewöhnliche oder unerwünschte Trends überprüft werden, z. B. eine starke Nutzung von Social-Media-Websites oder eine ungewöhnliche Anzahl von Viren, die regelmäßig auf einem bestimmten Computer gefunden werden. Diese Trends können auf ein ernsteres Problem hinweisen oder signalisieren, dass in einem bestimmten Bereich stärkere Schutzmaßnahmen erforderlich sind.

Die Organisation muss sicherstellen, dass Ereignisdaten über ihre kritischen Systeme hinweg zusammengestellt und korreliert werden, wobei verschiedene Quellen wie Ereignisberichte, Audit-Überwachung, Netzwerküberwachung, Überwachung des physischen Zugangs und Benutzer-/Administratorberichte genutzt werden.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Die Organisation muss die Analyse von Ereignissen nach Möglichkeit mit der Analyse von Schwachstellen-Scans, Leistungsdaten, der Überwachung kritischer Systeme und der Überwachung von Einrichtungen kombinieren, um die Fähigkeit zur Erkennung unangemessener oder ungewöhnlicher Aktivitäten weiter zu verbessern.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 1, 3, 8, 10, 13, 15
IEC 62443-3-3:2013, SR 6.1
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 8.1, 9.1, 10.2, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.28, 8.15

DE.AE-4: Die Auswirkungen von Ereignissen werden ermittelt.

Negative Auswirkungen auf die Abläufe, Vermögenswerte und Personen der Organisation, die sich aus den festgestellten Ereignissen ergeben, werden ermittelt und mit den Ergebnissen der Risikobewertung in Beziehung gesetzt.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 8, 13
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 8.1, 9.1, 10.2, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.25

DE.AE-5: Schwellenwerte für Störfallwarnungen sind festgelegt.

Die Organisation muss automatisierte Mechanismen und systemgenerierte Warnmeldungen einführen, um die Erkennung von Ereignissen zu unterstützen und bei der Bestimmung von Schwellenwerten für Sicherheitswarnungen zu helfen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Die Organisation muss Schwellenwerte für Vorfallswarnungen festlegen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 8, 13
IEC 62443-2-1:2010, Abschnitt 4.2.3.10
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 8.1, 9.1, 10.2, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.25

Das Informationssystem und die Anlagen werden überwacht, um Cybersecurity-Ereignisse zu erkennen und die Wirksamkeit der Schutzmaßnahmen zu überprüfen.

DE.CM-1: Das Netzwerk wird überwacht, um potenzielle Cybersicherheits-Ereignisse zu erkennen.

Firewalls sind an den Netzgrenzen zu installieren und zu betreiben und mit einem Firewall-Schutz an den Endpunkten zu ergänzen.

Leitfaden

- Zu den Endgeräten gehören Desktops, Laptops, Server...
- Erwägen Sie bei der Installation und dem Betrieb von Firewalls die Einbeziehung von Smartphones und anderen vernetzten Geräten, sofern dies möglich ist.
- Erwägen Sie eine Begrenzung der Anzahl der Verbindungsgateways zum Internet.

Die Organisation muss die unbefugte Nutzung ihrer geschäftskritischen Systeme durch die Erkennung unbefugter lokaler Verbindungen, Netzwerkverbindungen und Fernverbindungen überwachen und identifizieren.

- Schlüsselmaßnahme -

Leitfaden

- Die Überwachung der Netzkommunikation sollte an der Außengrenze der geschäftskritischen Systeme des Unternehmens und an wichtigen internen Grenzen innerhalb der Systeme erfolgen.
- Beim Hosten von Internetanwendungen sollte die Implementierung einer Web Application Firewall (WAF) in Betracht gezogen werden.

Die Organisation muss eine laufende Überwachung des Sicherheitsstatus ihres Netzes durchführen, um definierte Informations-/Cybersicherheitsereignisse und Indikatoren für potenzielle Informations-/Cybersicherheitsereignisse zu erkennen.

Leitfaden

Die Überwachung des Sicherheitsstatus sollte Folgendes umfassen:

- Generierung von Systemwarnungen, wenn Anzeichen für eine Gefährdung oder potenzielle Gefährdung auftreten.
- Erkennung und Meldung atypischer Nutzung der kritischen Systeme des Unternehmens.
- Erstellung von Prüfprotokollen für bestimmte Informations-/Cybersicherheitsereignisse.
- Verstärkung der Systemüberwachungsaktivitäten bei Anzeichen für ein erhöhtes Risiko.
- Physische Umgebung, Personal und Dienstleistungsanbieter.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 1, 8, 10, 13
IEC 62443-2-1:2010, Abschnitt 4.3.3.3.8
IEC 62443-3-3:2013, SR 6.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.5, 8, 9.1, 9.2, 10, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.22, 8.15, 8.30

Die physische Umgebung der Einrichtung wird auf potenzielle Informations-/Cybersicherheitsereignisse überwacht.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

DE.CM-2: Die Aktivitäten des Personals werden überwacht, um potenzielle Cybersicherheitsvorfälle zu erkennen.

Der physische Zugang zu den kritischen Systemen und Geräten der Organisation muss zusätzlich zur Überwachung des physischen Zugangs zur Einrichtung durch physische Einbruchalarme, Überwachungsgeräte und unabhängige Überwachungsteams verstärkt werden.

Leitfaden

Es wird empfohlen, alle Besucher zu registrieren.

Referenzen

IEC 62443-2-1:2010, Abschnitt 4.3.3.3.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.5, 8, 9.1, 9.2, 10, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.22, 7.1, 7.2, 8.15, 8.30

DE.CM-3: Die Aktivitäten des Personals werden überwacht, um potenzielle Cybersicherheitsvorfälle zu erkennen.

Es werden Endpunkt- und Netzschutzinstrumente zur Überwachung des Verhaltens der Endnutzer auf gefährliche Aktivitäten eingesetzt.

Leitfaden

Erwägen Sie den Einsatz eines Intrusion Detection/Prevention Systems (IDS/IPS).

Endpunkt- und Netzwerkschutz-Tools, die das Verhalten der Endnutzer auf gefährliche Aktivitäten überwachen, müssen verwaltet werden.

Leitfaden

- Erwägen Sie den Einsatz einer zentralisierten Protokollplattform für die Konsolidierung und Auswertung von Protokolldateien.
- Erwägen Sie, die aufgrund verdächtiger Aktivitäten generierten Warnungen aktiv zu untersuchen und geeignete Maßnahmen zu ergreifen, um die Bedrohung zu beseitigen, z. B. durch den Einsatz eines Security Operations Center (SOC).

Einschränkungen bei der Nutzung und Installation von Software sind durchzusetzen.

Leitfaden

Es sollte nur zugelassene Software verwendet werden, und die Zugriffsrechte der Benutzer sollten auf die spezifischen Daten, Ressourcen und Anwendungen beschränkt werden, die für die Ausführung einer erforderlichen Aufgabe erforderlich sind (Prinzip der geringsten Rechte).

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 3, 8, 13, 15
IEC 62443-3-3:2013, SR 6.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.5, 8, 9.1, 9.2, 10, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 8.15

DE.CM-4: Bösartiger Code wird erkannt.

Antiviren-, Spyware- und andere Malware-Programme müssen installiert und aktualisiert werden.

- Schlüsselmaßnahme -

Leitfaden

- Malware umfasst Viren, Spyware und Ransomware und sollte durch die Installation, Verwendung und regelmäßige Aktualisierung von Anti-Viren- und Anti-Spyware-Software auf allen im Unternehmen verwendeten Geräten (einschließlich Computern, Smartphones, Tablets und Servern) bekämpft werden.
- Antiviren- und Anti-Spyware-Software sollte automatisch in "Echtzeit" oder zumindest täglich nach Aktualisierungen suchen und das System gegebenenfalls überprüfen.
- Es sollte in Betracht gezogen werden, dieselben Mechanismen zum Schutz vor bösartigem Code für Heimcomputer (z. B. Telearbeit) oder private Geräte, die für die berufliche Arbeit verwendet werden (BYOD), bereitzustellen.

Die Organisation muss ein System zur Erkennung von Fehlalarmen bei der Erkennung und Beseitigung von bösartigem Code einrichten.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 8, 10, 13
IEC 62443-2-1:2010, Abschnitt 4.3.4.3.8
IEC 62443-3-3:2013, SR 3.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.5, 8, 9.1, 9.2, 10, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 8.7

DE.CM-5: Unerlaubter Handy-Code wird erkannt.

Die Organisation muss akzeptablen und inakzeptablen mobilen Code und mobile Code-Technologien definieren und die Verwendung von mobilem Code innerhalb des Systems genehmigen, überwachen und kontrollieren.

Leitfaden

- Mobiler Code umfasst alle Programme, Anwendungen oder Inhalte, die über ein Netzwerk übertragen werden können (z. B. eingebettet in eine E-Mail, ein Dokument oder eine Website) und auf einem entfernten System ausgeführt werden. Zu den Technologien für mobilen Code gehören zum Beispiel Java-Applets, JavaScript, HTML5, WebGL und VBScript.
- Entscheidungen über die Verwendung von mobilem Code in Organisationssystemen sollten auf der Grundlage des Potenzials des Codes getroffen werden, bei böswilliger Verwendung Schäden an den Systemen zu verursachen. Für die Auswahl und Verwendung des installierten mobilen Codes sollten Nutzungsbeschränkungen und Implementierungsrichtlinien gelten.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 8, 10
IEC 62443-3-3:2013 SR 2.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.5, 8, 9.1, 9.2, 10, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 8.19

DE.CM-6: Die Aktivitäten von externen Dienstleistern werden überwacht, um potenzielle Cybersicherheitsereignisse zu erkennen.

Alle externen Verbindungen von Anbietern, die IT/OT-Anwendungen oder Infrastrukturen unterstützen, müssen gesichert und aktiv überwacht werden, um sicherzustellen, dass während der Verbindung nur zulässige Aktionen stattfinden.

Leitfaden

Diese Überwachung umfasst den Zugang von unbefugtem Personal, Verbindungen, Geräten und Software.

Die Einhaltung der Sicherheitsrichtlinien und -verfahren des Personals und der vertraglichen Sicherheitsanforderungen durch externe Dienstleister wird im Hinblick auf ihre Cybersicherheitsrisiken überwacht.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

IEC 62443-2-1:2010, Abschnitt 4.3.3.3.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.5, 8, 9.1, 9.2, 10, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.22, 8.15, 8.30

DE.CM-7: Die Überwachung auf unbefugtes Personal, Verbindungen, Geräte und Software wird durchgeführt.

Die geschäftskritischen Systeme der Organisation müssen auf unbefugten Zugang von Mitarbeitern, Verbindungen, Geräten, Zugangspunkten und Software überwacht werden.

Leitfaden

- Unbefugter Personenzugang schließt den Zugang durch externe Dienstleister ein.
- Unstimmigkeiten im Systembestand sollten in die Überwachung einbezogen werden.
- Nicht autorisierte Konfigurationsänderungen an kritischen Systemen des Unternehmens sollten in die Überwachung einbezogen werden.

Unerlaubte Konfigurationsänderungen an den Systemen der Organisation sind zu überwachen und mit geeigneten Abhilfemaßnahmen anzugehen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 1, 2, 8, 13, 15
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.1, 7.5, 8, 9.1, 9.2, 10, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.22, 8.15, 8.30

DE.CM-8: Schwachstellen-Scans werden durchgeführt.

Die Organisation muss ihre kritischen Systeme und gehosteten Anwendungen überwachen und auf Schwachstellen prüfen und dabei sicherstellen, dass die Systemfunktionen durch den Prüfprozess nicht beeinträchtigt werden.

Leitfaden

Erwägen Sie die Einführung eines Programms zum kontinuierlichen Scannen von Schwachstellen, einschließlich der Erstellung von Berichten und Plänen zur Schadensbegrenzung.

Der Prozess des Scannens von Sicherheitslücken umfasst die Analyse, die Behebung und den Informationsaustausch.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 8, 10
IEC 62443-2-1:2010, Klausel 4.2.3.1, 4.2.3.7
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 8, 9.1, 9.2, 10, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 8.8, 8.29

Die Erkennungsprozesse und -verfahren werden gepflegt und getestet, um sicherzustellen, dass anormale Ereignisse erkannt werden.

DE.DP-2: Detektionstätigkeiten erfüllen alle geltenden Anforderungen.

Die Organisation führt Detektionstätigkeiten in Übereinstimmung mit den geltenden Bundes- und Landesgesetzen, Branchenvorschriften und -normen, Richtlinien und anderen geltenden Anforderungen durch.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.3, 7.4, 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.34, 5.36, 8.8

DE.DP-3: Erkennungsprozesse werden getestet .

Die Organisation muss überprüfen, ob die Prozesse zur Erkennung von Ereignissen wie vorgesehen funktionieren.

Leitfaden

- Zur Validierung gehören auch Tests.
- Die Validierung sollte nachweisbar sein.

Referenzen

IEC 62443-2-1:2010, Abschnitt 4.4.3.2
IEC 62443-3-3:2013, SR 3.3
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.3, 7.4, 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 8.29

DE.DP-4: Informationen zur Ereigniserkennung werden übermittelt .

Die Organisation muss Informationen über die Erkennung von Ereignissen an vordefinierte Stellen weiterleiten.

Leitfaden

Zu den Ereigniserkennungsinformationen gehören beispielsweise Warnungen über atypische Kontonutzung, unbefugten Fernzugriff, drahtlose Konnektivität, Verbindung mit mobilen Geräten, geänderte Konfigurationseinstellungen, abweichendes Inventar von Systemkomponenten, Verwendung von Wartungswerkzeugen und nicht ortsgebundener Wartung, physischer Zugang, Temperatur und Luftfeuchtigkeit, Lieferung und Entfernung von Geräten, Kommunikation an den Grenzen des Informationssystems, Verwendung von mobilem Code, Verwendung von Voice over Internet Protocol (VoIP) und Aufdeckung von Malware.

Referenzen

IEC 62443-2-1:2010, Abschnitt 4.3.4.5.9
IEC 62443-3-3:2013, SR 6.1
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.3, 7.4, 8.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 6.8

DE.DP-5: Die Erkennungsverfahren werden kontinuierlich verbessert.

Verbesserungen, die sich aus der Überwachung, Messung, Bewertung, Erprobung, Überprüfung und den gewonnenen Erkenntnissen ergeben, werden in die Überarbeitung des Nachweisverfahrens einbezogen.

Leitfaden

- Dies führt zu einer kontinuierlichen Verbesserung der Erkennungsprozesse.
- Der Einsatz unabhängiger Teams zur Bewertung des Aufdeckungsverfahrens könnte in Betracht gezogen werden.

Die Organisation führt spezielle Bewertungen durch, darunter eine eingehende Überwachung, Schwachstellen-Scans, Tests auf böswillige Benutzer, Bewertung von Insider-Bedrohungen, Leistungs-/Lasttests sowie Verifizierungs- und Validierungstests für die kritischen Systeme der Organisation.

Leitfaden

Diese Tätigkeiten können ausgelagert werden, vorzugsweise an zugelassene Organisationen.

Referenzen

IEC 62443-2-1:2010, Abschnitt 4.4.3.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.3, 7.4, 8.1, 9, 10.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.27

Reaktionsprozesse und -verfahren werden ausgeführt und aufrechterhalten, um die Reaktion auf erkannte Cybersicherheitsvorfälle zu gewährleisten.

RS.RP-1: Der Reaktionsplan wird während oder nach einem Vorfall ausgeführt.

Während oder nach einem Informations-/Cybersicherheitsereignis in den kritischen Systemen der Organisation muss ein Verfahren zur Reaktion auf einen Vorfall, einschließlich Rollen, Verantwortlichkeiten und Befugnisse, durchgeführt werden.

Leitfaden

- Der Prozess der Reaktion auf einen Vorfall sollte eine Reihe von Anweisungen oder Verfahren zur Erkennung, Reaktion und Begrenzung der Folgen eines bösartigen Cyberangriffs umfassen.
- Die Rollen, Zuständigkeiten und Befugnisse im Notfallplan sollten die beteiligten Personen, die Kontaktinformationen, die verschiedenen Rollen und Zuständigkeiten sowie die Entscheidung über die Einleitung von Wiederherstellungsmaßnahmen und die Kontaktaufnahme mit den entsprechenden externen Akteuren genau beschreiben.
- Es sollte in Erwägung gezogen werden, die Ursachen für ein Informations-/Cybersicherheitsereignis zu ermitteln und eine Korrekturmaßnahme durchzuführen, damit sich das Ereignis nicht wiederholt oder an anderer Stelle auftritt (eine Infektion durch bösartigen Code auf einem Rechner hat sich nicht an anderer Stelle im Netz ausgebreitet). Die Wirksamkeit der ergriffenen Abhilfemaßnahmen sollte überprüft werden. Die Abhilfemaßnahmen sollten den Auswirkungen des aufgetretenen Informations-/Cybersicherheitsvorfalls angemessen sein.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 17
IEC 62443-2-1:2010, Abschnitt 4.3.4.5.1
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 8.1, 8.3, 10, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.26

Reaktionsmaßnahmen werden mit internen und externen Akteuren koordiniert (z. B. externe Unterstützung durch Strafverfolgungsbehörden).

RS.CO-1: Das Personal kennt seine Rolle und die Reihenfolge der Maßnahmen, wenn eine Reaktion erforderlich ist.

Die Organisation muss sicherstellen, dass das Personal seine Aufgaben, Ziele, Prioritäten bei der Wiederherstellung, die Reihenfolge der Aufgaben (Arbeitsabläufe) und die Zuständigkeiten bei der Reaktion auf ein Ereignis kennt.

Leitfaden

Ziehen Sie die Verwendung des CCB-Leitfadens für das Management von Zwischenfällen als Leitfaden für diese Übung in Betracht und ziehen Sie bei Bedarf externe Experten hinzu. Testen Sie Ihren Plan regelmäßig und passen Sie ihn nach jedem Vorfall an.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 17
IEC 62443-2-1:2010, Klausel 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 5, 7.3, 7.4, 8.1, 8.3, 10, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.2, 5.24, 6.3

RS.CO-2: Vorfälle werden gemäß den festgelegten Kriterien gemeldet.

Die Organisation muss eine Berichterstattung über Informations-/Cybersicherheitsvorfälle auf ihren kritischen Systemen innerhalb eines von der Organisation festgelegten Zeitrahmens an von der Organisation festgelegte Personen oder Rollen einführen.

Leitfaden

Alle Nutzer sollten eine zentrale Anlaufstelle haben, um Vorfälle zu melden, und dazu ermutigt werden, dies auch zu tun.

Die Ereignisse sind gemäß den festgelegten Kriterien zu melden.

Leitfaden

Die Kriterien für die Meldung sollten in den Reaktionsplan auf Vorfälle aufgenommen werden.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 17
IEC 62443-2-1:2010, Abschnitt 4.3.4.5.**5**
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 5, 7.3, 7.4, 8.1, 8.3, 10, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.5, 6.8

RS.CO-3: Der Informationsaustausch erfolgt in Übereinstimmung mit den Reaktionsplänen.

Informationen über Cybersicherheitsvorfälle sind den Mitarbeitern der Organisation in einem für sie verständlichen Format zu übermitteln und mit ihnen zu teilen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Die Organisation gibt Informationen über Cybersicherheitsvorfälle an die relevanten Beteiligten weiter, wie im Reaktionsplan vorgesehen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 17
IEC 62443-2-1:2010, Abschnitt 4.3.4.5.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.3, 7.4, 8.1, 8.3, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 6.8

RS.CO-4: Die Koordinierung mit den Beteiligten erfolgt im Einklang mit den Reaktionsplänen.

Die Organisation muss die Maßnahmen zur Reaktion auf Informations-/Cybersicherheitsvorfälle mit allen vordefinierten Beteiligten koordinieren.

Leitfaden

- Zu den Interessenvertretern für die Reaktion auf Vorfälle gehören beispielsweise die Eigentümer der Mission/des Geschäfts, die Eigentümer kritischer Systeme des Unternehmens, Integratoren, Lieferanten, Personalabteilungen, Büros für physische und personelle Sicherheit, Rechtsabteilungen, Betriebspersonal und Beschaffungsbüros.
- Die Koordinierung mit den Beteiligten erfolgt im Einklang mit den Reaktionsplänen für Zwischenfälle.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 17
IEC 62443-2-1:2010, Abschnitt 4.3.4.5.5
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.3, 7.4, 8.1, 8.3, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.6, 5.26

RS.CO-5: Es findet ein freiwilliger Informationsaustausch mit externen Akteuren statt, um ein breiteres Bewusstsein für die Lage im Bereich der Cybersicherheit zu schaffen.

Die Organisation gibt Informationen bzw. Informationen über Cybersicherheitsereignisse gegebenenfalls freiwillig an externe Interessengruppen, Sicherheitsgruppen der Branche usw. weiter, um ein breiteres Informations- bzw. Cybersecurity-Situationsbewusstsein zu erreichen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 17
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.3, 7.4, 8.1, 8.3, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.6

Die Analyse wird durchgeführt, um eine wirksame Reaktion zu gewährleisten und die Wiederherstellungsmaßnahmen zu unterstützen.

RS.AN-1: Meldungen von Detektionssystemen werden untersucht.

Die Organisation muss die von den Erkennungssystemen generierten Meldungen im Zusammenhang mit Informationen und Cybersicherheit untersuchen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Die Organisation muss automatisierte Mechanismen einführen, die bei der Untersuchung und Analyse von Meldungen im Zusammenhang mit Informationen und Cybersicherheit helfen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 17
IEC 62443-2-1:2010, Klausel 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8
IEC 62443-3-3:2013 SR 6.1
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 9.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.26, 8.15

RS.AN-2: Die Auswirkungen des Vorfalls werden verstanden.

Eine gründliche Untersuchung und eine Analyse der Ergebnisse bilden die Grundlage für das Verständnis der gesamten Auswirkungen eines Vorfalls im Bereich der Informations- und Cybersicherheit.

Leitfaden

- Bei der Ergebnisanalyse kann die Korrelation zwischen den Informationen über das festgestellte Ereignis und den Ergebnissen der Risikobewertungen ermittelt werden. Auf diese Weise erhält man einen Einblick in die Auswirkungen des Ereignisses auf das gesamte Unternehmen.
- Erwägen Sie, die Erkennung nicht autorisierter Änderungen an ihren kritischen Systemen in ihre Fähigkeiten zur Reaktion auf Zwischenfälle aufzunehmen.

Die Organisation muss automatische Mechanismen zur Unterstützung der Analyse der Auswirkungen von Vorfällen einführen.

Leitfaden

Die Umsetzung kann von einem Ticketingsystem bis hin zu einem Security Information and Event Management (SIEM) reichen.

Referenzen

IEC 62443-2-1:2010, Klausel 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 4.1, 4.2, 9.1, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.25, 5.27

RS.AN-3: Forensische Untersuchungen werden durchgeführt.

Die Organisation stellt auf Anfrage eine Prüfung, Analyse und Berichterstattung für nachträgliche Untersuchungen von Informations-/Cybersicherheitsvorfällen bereit.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Die Organisation führt eine forensische Analyse der gesammelten Informationen/Cybersicherheitsvorfalldurch, um die Ursache zu ermitteln.

Leitfaden

Erwägen Sie die Ermittlung der Grundursache eines Vorfalls. Verwenden Sie dazu gegebenenfalls eine forensische Analyse der gesammelten Informationen bzw. der Informationen über Cybersicherheitsereignisse.

Referenzen

IEC 62443-3-3:2013, SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 4.1, 4.2, 9, 10.2, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.28

RS.AN-4: Zwischenfälle werden in Übereinstimmung mit den Reaktionsplänen kategorisiert.

Informations-/Cybersicherheitsvorfälle werden nach dem Schweregrad und den Auswirkungen in Übereinstimmung mit den Bewertungskriterien des Reaktionsplans für Vorfälle eingestuft.

Leitfaden

- Es sollte in Betracht gezogen werden, die Ursachen eines Informations-/Cybersicherheitsvorfalls zu ermitteln und Abhilfemaßnahmen zu ergreifen, damit sich der Vorfall nicht wiederholt oder anderswo auftritt.
- Die Wirksamkeit der ergriffenen Abhilfemaßnahmen sollte überprüft werden.
- Die Abhilfemaßnahmen sollten den Auswirkungen des aufgetretenen Informations-/Cybersicherheitsvorfalls angemessen sein.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 17
IEC 62443-2-1:2010, Abschnitt 4.3.4.5.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 6, 8.3, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.25

RS.AN-5: Es sind Prozesse eingerichtet, um Schwachstellen zu empfangen, zu analysieren und darauf zu reagieren, die der Organisation aus internen und externen Quellen (z.B. interne Tests, Sicherheitsbulletins oder Sicherheitsforscher) bekannt werden.

Die Organisation muss Prozesse und Verfahren für das Schwachstellenmanagement einführen, die die Verarbeitung, Analyse und Behebung von Schwachstellen aus internen und externen Quellen umfassen.
- Schlüsselmaßnahme -

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Die Organisation muss automatisierte Mechanismen zur Verbreitung und Überwachung von Behebungsmaßnahmen für Schwachstelleninformationen einführen, die aus internen und externen Quellen und von wichtigen Interessengruppen stammen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 17
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 6, 7.5, 8.3, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 8.8

Organisatorische Reaktionsmaßnahmen werden durch die Einbeziehung von Erkenntnissen aus laufenden und früheren Aufdeckungs-/Reaktionsmaßnahmen verbessert

RS.MI-1: Vorfälle sind eingedämmt.

RS.MI-2: Zwischenfälle werden entschärft.

RS.MI-3: Neu erkannte Schwachstellen werden entschärft oder als akzeptierte Risiken dokumentiert.

Die Organisation muss eine Fähigkeit zur Behandlung von Informations-/Cybersicherheitsvorfällen in ihren geschäftskritischen Systemen einführen, die Vorbereitung, Erkennung und Analyse, Eindämmung, Beseitigung, Wiederherstellung und dokumentierte Risikoakzeptanz umfasst.

Leitfaden

Eine dokumentierte Risikoakzeptanz bezieht sich auf Risiken, die von der Organisation als nicht gefährlich für die geschäftskritischen Systeme der Organisation eingeschätzt werden und bei denen der Risikoeigner das Risiko formell akzeptiert (in Verbindung mit der Risikobereitschaft der Organisation).

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 17
IEC 62443-2-1:2010, Abschnitt 4.3.4.5.6
IEC 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 6, 7.5, 8.3, 10.2, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.26, 8.7, 8.8

Organisatorische Reaktionsmaßnahmen werden durch die Einbeziehung von Erkenntnissen aus laufenden und früheren Aufdeckungs-/Reaktionsmaßnahmen verbessert

RS.IM-1: Reaktionspläne berücksichtigen die gewonnenen Erkenntnisse.

Die Organisation führt nach einem Vorfall Bewertungen durch, um die aus der Reaktion auf einen Vorfall und der Wiederherstellung gezogenen Lehren zu analysieren und folglich die Prozesse/Verfahren/Technologien zu verbessern, um ihre Cyber-Resilienz zu erhöhen.

Leitfaden

Erwägen Sie, die Beteiligten nach jedem Vorfall zusammenzubringen und gemeinsam darüber nachzudenken, wie das Geschehene verbessert werden kann, wie es geschehen ist, wie man reagierte, wie es hätte besser laufen können, was getan werden sollte, um zu verhindern, dass es wieder geschieht usw.

Die aus der Behandlung von Zwischenfällen gewonnenen Erkenntnisse werden in aktualisierte oder neue Verfahren zur Behandlung von Zwischenfällen umgesetzt, die getestet, genehmigt und geschult werden müssen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische **Sicherheitskontrolle**
IEC 62443-2-1:2010, Klausel 4.3.4.5.10, 4.4.3.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 6.1, 8.3, 10, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.26, 5.27

RS.IM-2: Reaktionspläne berücksichtigen die gewonnenen Erkenntnisse.

Die Organisation muss die Reaktions- und Wiederherstellungspläne aktualisieren, um Änderungen in ihrem Umfeld zu berücksichtigen.

Leitfaden

Der Kontext der Organisation bezieht sich auf die Organisationsstruktur, ihre kritischen Systeme, Angriffsvektoren, neue Bedrohungen, verbesserte Technologien, das Betriebsumfeld, Probleme, die bei der Umsetzung/Ausführung/Prüfung des Plans aufgetreten sind, und gewonnene Erfahrungen.

Referenzen

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 6.1, 8.3, 10, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.27

Wiederherstellungsprozesse und -verfahren werden durchgeführt und aufrechterhalten, um die Wiederherstellung von Systemen oder Anlagen zu gewährleisten, die von Cybersicherheitsvorfällen betroffen sind.

RC.RP-1: Der Wiederherstellungsplan wird während oder nach einem Cybersicherheitsvorfall ausgeführt.

Es wird ein Wiederherstellungsprozess für Katastrophen und Informations-/Cybersicherheitsvorfälle entwickelt und gegebenenfalls durchgeführt.

Leitfaden

- Es sollte ein Verfahren entwickelt werden, das festlegt, welche Sofortmaßnahmen im Falle eines Brandes, eines medizinischen Notfalls, eines Einbruchs, einer Naturkatastrophe oder eines Vorfalls im Bereich der Informations- und Cybersicherheit zu ergreifen sind.
- Der Prozess sollte Folgendes berücksichtigen:
  - Rollen und Zuständigkeiten, einschließlich der Frage, wer die Entscheidung über die Einleitung von Wiederherstellungsverfahren trifft und wer der Kontakt zu den entsprechenden externen Beteiligten ist.
  - Was ist mit den Informationen und Informationssystemen des Unternehmens im Falle eines Vorfalls zu tun? Dazu gehören das Herunterfahren oder Sperren von Computern, die Verlagerung an einen Backup-Standort, die physische Entfernung wichtiger Dokumente usw.
  - Wen Sie im Falle eines Vorfalls anrufen müssen.

Die wesentlichen Funktionen und Dienste der Organisation müssen ohne oder mit nur geringem Verlust der Betriebskontinuität fortgesetzt werden, und die Kontinuität muss bis zur vollständigen Wiederherstellung des Systems aufrechterhalten werden.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 11
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 8, 10.2, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.26

Wiederherstellungsprozesse und -verfahren werden durchgeführt und aufrechterhalten, um die Wiederherstellung von Systemen oder Anlagen zu gewährleisten, die von Cybersicherheitsvorfällen betroffen sind.

RC.IM-1: In den Wiederherstellungsplänen werden die gewonnenen Erkenntnisse berücksichtigt.

Die Organisation muss die aus den Wiederherstellungsaktivitäten bei Zwischenfällen gewonnenen Erkenntnisse in aktualisierte oder neue Systemwiederherstellungsverfahren einfließen lassen und diese nach der Erprobung durch entsprechende Schulungen ergänzen.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

IEC 62443-2-1:2010, Abschnitt 4.4.3.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.5, 8, 10.2, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.27

RC.IM-2: Die Wiederherstellungsstrategien werden aktualisiert.

Diese Anforderung ist mit RS.IM-2 kombiniert.

Leitfaden

Keine zusätzlichen Hinweise zu diesem Thema.

Referenzen

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 7.5, 8, 10.2, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.6

Wiederherstellungsprozesse und -verfahren werden ausgeführt und aufrechterhalten, um die Wiederherstellung von Systemen oder Anlagen zu gewährleisten, die von Cybersicherheitsvorfällen betroffen sind.

RC.CO-1: Die Öffentlichkeitsarbeit wird geregelt.

Die Organisation soll die Verbreitung von Informationen zentralisieren und koordinieren und die Darstellung der Organisation in der Öffentlichkeit steuern.

Leitfaden

Zum Management der Öffentlichkeitsarbeit gehören beispielsweise die Verwaltung der Medienkontakte, die Koordinierung und Protokollierung aller Interviewanfragen, die Bearbeitung von Telefonanrufen und E-Mail-Anfragen, der Abgleich von Medienanfragen mit geeigneten und verfügbaren internen Experten, die zu einem Interview bereit sind, die Prüfung aller den Medien zur Verfügung gestellten Informationen und die Sicherstellung, dass die Mitarbeiter mit den Richtlinien für Öffentlichkeitsarbeit und Datenschutz vertraut sind.

Es wird ein Beauftragter für Öffentlichkeitsarbeit ernannt.

Leitfaden

Der Beauftragte für Öffentlichkeitsarbeit sollte die Möglichkeit, vordefinierte externe Kontakte nutzen (z. B. Presse, Regulierungsbehörden, Interessengruppen).

Referenzen

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 5, 7.4, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.6

RC.CO-2: Die Reputation wird nach einem Vorfall wiederhergestellt.

Die Organisation muss eine Krisenreaktionsstrategie umsetzen, um die Organisation vor den negativen Folgen einer Krise zu schützen und ihren Ruf wiederherzustellen.

Leitfaden

Zu den Krisenbewältigungsstrategien gehören beispielsweise Maßnahmen, die darauf gerichtet sind, die Zuschreibung der Krise zu gestalten, die Wahrnehmung der in der Krise befindlichen Organisation zu ändern und die durch die Krise verursachten negativen Auswirkungen zu verringern.

Referenzen

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 5, 7.4, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.6

RC.CO-3: Die Wiederherstellungsmaßnahmen werden den internen und externen Interessenvertretern sowie den Geschäftsführungs- und Managementteams mitgeteilt.

Die Organisation muss die Wiederherstellungsaktivitäten an vordefinierte Interessenvertreter, Führungskräfte und Management-Teams kommunizieren.

Leitfaden

Die Mitteilung der Wiederherstellungsmaßnahmen an alle relevanten Beteiligten gilt nur für Einrichtungen, die den NIS-Vorschriften unterliegen.

Referenzen

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), Klausel 5, 7.4, Anhang A (siehe ISO 27002)
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Kontrolle 5.6

Anhang A: Liste der Schlüsselmaßnahmen für das Sicherheitsniveau "Basis

SCHÜTZEN

PR.AC-1: Identitäten und Berechtigungsnachweise werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, widerrufen und geprüft.

(1) Die Identitäten und Berechtigungsnachweise für autorisierte Geräte und Benutzer werden verwaltet.

PR.AC-3: Der Fernzugriff wird verwaltet.

(2) Der Fernzugriff auf die Netzwerke der Organisation muss gesichert sein, unter anderem durch Multi-Faktor-Authentifizierung (MFA).

PR.AC-4: Zugriffsberechtigungen und -autorisierungen werden unter Berücksichtigung des Prinzips der geringsten Rechte und der Aufgabentrennung verwaltet.

(3) Die Zugriffsrechte der Benutzer auf die Systeme der Organisation müssen definiert und verwaltet werden.

(4) Es ist festzulegen, wer Zugang zu den geschäftskritischen Informationen und Technologien der Organisation haben sollte und wie dieser Zugang zu erhalten ist.

(5) Der Zugang der Mitarbeiter zu Daten und Informationen ist auf die Systeme und spezifischen Informationen zu beschränken, die sie für ihre Arbeit benötigen.

(6) Niemand darf über Administratorrechte für die täglichen Aufgaben verfügen.

PR.AC-5: Die Integrität des Netzes ist geschützt (z.B. Netztrennung, Netzsegmentierung).

(7) In allen Netzen der Organisation sind Firewalls zu installieren und zu aktivieren.

(8) Gegebenenfalls ist die Netzintegrität der kritischen Systeme der Organisation durch Netzsegmentierung und -trennung zu schützen.

PR.IP-4: Backups von Informationen werden durchgeführt, gepflegt und getestet.

(9) Backups der geschäftskritischen Daten der Organisation müssen auf einem anderen System als demjenigen, auf dem sich die Originaldaten befinden, durchgeführt und gespeichert werden.

PR.MA-1: Wartung und Reparatur von Organisationsmitteln werden mit zugelassenen und kontrollierten Werkzeugen durchgeführt und protokolliert.

(10) Patches und Sicherheitsupdates für Betriebssysteme und kritische Systemkomponenten sind zu installieren.

PR.PT-1: Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.

(11) Die Protokolle müssen geführt, dokumentiert und überprüft werden.

ENTDECKEN

DE.AE-3: Ereignisdaten werden von mehreren Quellen und Sensoren gesammelt und korreliert.

(12) Die Aktivitätsprotokollierungsfunktion von Schutz-/Erkennungshardware oder -software (z. B. Firewalls, Antivirenprogramme) ist zu aktivieren, zu sichern und zu überprüfen.

DE.CM-4: Bösartiger Code wird erkannt.

(13) Antiviren-, Spyware- und andere Malware-Programme müssen installiert und aktualisiert werden.

Anhang B: Liste der zusätzlichen Schlüsselmaßnahmen für die Zuverlässigkeitsstufen "Wichtig" und "Wesentlich"

Die nachstehende Liste **ergänzt** die Schlüsselmaßnahmen für die Zuverlässigkeitsstufe "Basis".

IDENTIFIZIEREN (IDENTIFY)

ID.AM-6: Rollen, Zuständigkeiten und Befugnisse im Bereich der Cybersicherheit für die gesamte Belegschaft und für Drittparteien sind festgelegt.

(1) Rollen, Zuständigkeiten und Befugnisse im Bereich der Informations- und Cybersicherheit innerhalb der Organisation sind zu dokumentieren, zu überprüfen, zu autorisieren und zu aktualisieren und mit organisationsinternen Rollen und externen Partnern abzugleichen.

SCHÜTZEN (PROTECT)

PR.AC-3: Der Fernzugriff wird verwaltet.

(2) Nutzungsbeschränkungen, Verbindungsanforderungen, Implementierungsrichtlinien und Berechtigungen für den Fernzugriff auf die kritische Systemumgebung der Organisation müssen ermittelt, dokumentiert und umgesetzt werden.

PR.AC-5: Die Integrität des Netzes ist geschützt (z.B. Netztrennung, Netzsegmentierung).

(3) Gegebenenfalls ist die Netzintegrität der kritischen Systeme der Organisation zu schützen, indem (1) Verbindungen zwischen Systemkomponenten identifiziert, dokumentiert und kontrolliert werden und (2) externe Verbindungen zu den kritischen Systemen der Organisation eingeschränkt werden.

(4) Die Organisation muss Verbindungen und Kommunikation an der Außengrenze und an wichtigen internen Grenzen innerhalb der kritischen Systeme der Organisation überwachen und kontrollieren, indem sie gegebenenfalls Grenzschutzvorrichtungen einsetzt.

PR.DS-5: Schutzmaßnahmen gegen Datenlecks sind implementiert.

(5) Die Organisation ergreift geeignete Maßnahmen, die zur Überwachung ihrer kritischen Systeme an den Außengrenzen und kritischen internen Punkten führen, wenn unbefugte Zugriffe und Aktivitäten, einschließlich Datenlecks, festgestellt werden.

PR.IP-1: Es wird eine Basiskonfiguration von informationstechnischen/industriellen Kontrollsystemen erstellt und gepflegt, die Sicherheitsgrundsätze berücksichtigt.

(6) Die Organisation muss eine Basiskonfiguration für ihre geschäftskritischen Systeme entwickeln, dokumentieren und pflegen.

ENTDECKEN (DETECT)

DE.CM-1: Das Netz wird überwacht, um potenzielle Cybersicherheitsvorfälle zu erkennen.

(7) Die Organisation muss die unbefugte Nutzung ihrer geschäftskritischen Systeme durch die Erkennung unbefugter lokaler Verbindungen, Netzwerkverbindungen und Fernverbindungen überwachen und identifizieren.

REAGIEREN (RESPOND)

RS.AN-5: Es werden Verfahren eingerichtet, um Schwachstellen, die der Organisation aus internen und externen Quellen gemeldet werden, zu empfangen, zu analysieren und auf sie zu reagieren.

(8) Die Organisation muss Prozesse und Verfahren für das Schwachstellenmanagement einführen, die die Bearbeitung, Analyse und Behebung von Schwachstellen aus internen und externen Quellen umfassen.

Anhang C: Liste der zusätzlichen Schlüsselmaßnahmen für die Zuverlässigkeitsstufen "Wesentlich

Die nachstehende Liste **ergänzt** die Schlüsselmaßnahmen für die Zuverlässigkeitsstufe "Basis" und “Wichtig”.

IDENTIFIZIEREN (IDENTIFY)

ID.SC-3:	Verträge mit Lieferanten und Drittanbietern werden genutzt, um geeignete Maßnahmen umzusetzen, die die **Ziele** des Cybersicherheitsprogramms und des Cyber Supply Chain Risk Management Plans einer Organisation erfüllen.

(1) Es werden vertragliche Anforderungen an die "Informationssicherheit und Cybersicherheit" für Lieferanten und Drittpartner eingeführt, um einen überprüfbaren Prozess zur Behebung von Mängeln zu gewährleisten und die Korrektur von Mängeln sicherzustellen, die bei der Prüfung und Bewertung der "Informationssicherheit und Cybersicherheit" festgestellt werden.

(2) Die Organisation soll vertragliche Anforderungen festlegen, die es der Organisation erlauben, die von Zulieferern und Drittpartnern umgesetzten Programme für "Informationssicherheit und Cybersicherheit" zu überprüfen.

SCHÜTZEN (PROTECT)

PR.AC-7:	Identitäten werden geprüft und an Berechtigungsnachweise gebunden und in Interaktionen geltend gemacht.

(3) Die Organisation führt eine dokumentierte Risikobewertung für die kritischen Systemtransaktionen der Organisation durch und authentifiziert Benutzer, Geräte und andere Vermögenswerte (z. B. Ein-Faktor-, Mehr-Faktor-Authentifizierung) entsprechend dem Risiko der Transaktion (z. B. Sicherheits- und Datenschutzrisiken des Einzelnen und andere organisatorische Risiken).

PR.MA-1:	Wartung und Reparatur von Organisationsmitteln werden mit genehmigten und kontrollierten Werkzeugen durchgeführt und protokolliert.

(4) Die Organisation muss die unbefugte Entfernung von Wartungsgeräten verhindern, die kritische Systeminformationen der Organisation enthalten.

(5) Wartungswerkzeuge und tragbare Speichermedien sind zu überprüfen, wenn sie in die Einrichtung gebracht werden, und sind durch Anti-Malware-Lösungen zu schützen, so dass sie auf bösartigen Code gescannt werden, bevor sie auf den Systemen der Organisation verwendet werden.

(6) Die Organisation muss die Sicherheitskontrollen nach der Wartung oder Reparatur/Patching von Hardware und Software überprüfen und gegebenenfalls Maßnahmen ergreifen.

PR.PT-2:	Wechseldatenträger sind geschützt und ihre Nutzung ist gemäß der Richtlinie eingeschränkt.

(7) Tragbare Speichermedien, die Systemdaten enthalten, müssen während des Transports und der Lagerung kontrolliert und geschützt werden.

ENTDECKEN (DETECT)

DE.AE-1: Eine Grundlage für den Netzbetrieb und die erwarteten Datenströme für Nutzer und Systeme wird erstellt und verwaltet.

(8) Die Organisation muss sicherstellen, dass eine Grundlage für den Netzbetrieb und den erwarteten Datenfluss für ihre kritischen Systeme entwickelt, dokumentiert und gepflegt wird, um Ereignisse zu verfolgen.

Haftungsausschluss

Dieses Dokument und seine Anhänge wurden vom Zentrum für Cybersicherheit Belgien (CCB) erstellt, einer föderalen Verwaltung, die durch den Königlichen Erlass vom 10. Oktober 2014 geschaffen wurde und dem Premierminister untersteht.

Dieses Dokument enthält technische Informationen, die hauptsächlich in deutscher Sprache verfasst sind. Diese Informationen in Bezug auf
Diese Informationen über die Sicherheit von Netzen und Informationssystemen richten sich an IT-Dienste, die die deutschen Begriffe der Computersprache verwenden. Eine Übersetzung dieser technischen Informationen ins Niederländische, Französische oder Englische kann jedoch bei dem CCB angefordert werden.
Die CCB übernimmt **keine Verantwortung für den Inhalt** dieses Dokuments.
Die bereitgestellten Informationen:

- sind ausschließlich allgemeiner Natur und zielen nicht darauf ab, alle besonderen Situationen zu berücksichtigen.
- sind nicht notwendigerweise in allen Punkten erschöpfend, präzise oder auf dem neuesten Stand.

Verantwortlicher Redakteur

Zentrum für Cybersicherheit Belgien
Herr De Bruycker, Generaldirektor
Rue de la Loi, 18
1000 Brüssel

Rechtliches Depot
D/2023/14828/001