CENTRE FOR
CYBERSECURITY
BELGIUM

CyberGrundlagen

BASIC

Version: 01.03.2023

Centre for Cybersecurity Belgium
Unter der Autorität des Premierministers

Inhaltsübersicht

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.

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.

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.

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).

Referenzen

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Kritische Sicherheitskontrolle 12
IEC 62443-2-1:2010, Klausel 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.

Für die Sicherheitsstufe "Basis" werden keine Anforderungen festgelegt, aber es werden Leitlinien zur Erhöhung der Informationssicherheit bereitgestellt.

Leitfaden

Outsourcing von Systemen, Softwareplattformen und Anwendungen, die innerhalb der Organisation genutzt werden, wird in ID.AM-1 & ID.AM-2 behandelt.

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.

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

Die Richtlinien, Grundsätze und Verfahren 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 Cybersicherheitspolitik wird festgelegt und 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, die von 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.

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.

Die rechtlichen und regulatorischen Anforderungen an die Informations-/Cybersicherheit, einschließlich der Verpflichtungen zum Schutz der Privatsphäre, müssen verstanden und umgesetzt werden.

Leitfaden

Es gibt keine zusätzlichen Leitlinien.

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 berücksichtigen 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.

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 Auftrag, Funktionen, Image oder Reputation), für die Vermögenswerte der Organisation und für Einzelpersonen darstellt.

ID.RA-1: Die Schwachstellen der Anlagen sind 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.

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-5: Bedrohungen, Schwachstellen, Wahrscheinlichkeiten und Auswirkungen werden zur Bestimmung des Risikos 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.

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

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.
- Schlüsselmaßnahme -

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.

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.

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.

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).

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 der geringsten Rechte und der Aufgabentrennung verwaltet .

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

- Schlüsselmaßnahme -

Leitfaden

Dabei sollte Folgendes berücksichtigt 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).

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.

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.

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 Integrität des Netzes (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 jedem Ihrer Computer und in jedem Ihrer Netzwerke, auch wenn Sie einen Cloud-Service-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.

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

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 zu erfüllen.

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.

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

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 den Einsatz 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.

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.

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

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.

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 der gesamten Dauer des Umzugs, des Transfers 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.

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

Für die Sicherheitsstufe "Basis" werden keine Anforderungen festgelegt, aber es werden Leitlinien zur Erhöhung der Informationssicherheit bereitgestellt.

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

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-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 Sicherungen der Computerkonfiguration, Sicherungen 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).

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-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.

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

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.

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

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.

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-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 von Nachrichtenanhängen 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.

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

Die Aktivitätsprotokollierungsfunktion von Schutz-/Erkennungshardware oder -software (z. B. Firewalls, Antivirenprogramme) sind 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.

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

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.

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

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).

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 Erwägung 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.

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

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

RS.RP-1: 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 Beteiligten genau festlegen.

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-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

Es gibt keine zusätzlichen Leitlinien.

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

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.

Referenzen

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

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

RC.RP-1: Wiederherstellungsplan wird während oder nach einem Vorfall im Bereich der Cybersicherheit 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.

Dieser 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 gehört 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.

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

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.

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 Englisch verfasst sind. Diese Informationen über die Sicherheit von Netzen und Informationssystemen richten sich an IT-Dienste, die die englischen Begriffe der Computersprache verwenden. Eine Übersetzung dieser technischen Informationen ins Niederländische, Französische oder Deutsche kann jedoch bei der 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

Juristisches Depot

D/2023/14828/001