cegid

IT-Sicherheitsplan

CEGID

22.03.2024

www.cegid.com

Über dieses Dokument

Der Zweck dieses Dokuments ist es, den IT-Sicherheitsplan von Cegid vorzustellen.

Vertraulichkeitsstufe	Öffentlich
Letzte Aktualisierung	22.03.2024

INHALTSVERZEICHNIS

1. ENTWICKLUNG DES DOKUMENTS

Die Daten in der folgenden Tabelle geben den Verlauf der Änderungen des Dokuments an:

Datum	Autor	Art der Änderung
03.11.2016	Cegid Sicherheitsteam	Ursprüngliche Version
02.02.2018	Cegid Sicherheitsteam	Durchsicht des Dokuments
30.07.2018	Cegid Sicherheitsteam	Durchsicht des Dokuments
23.05.2019	Cegid Sicherheitsteam	Durchsicht des Dokuments
07.10.2020	Cegid Sicherheitsteam	Durchsicht des Dokuments
08.08.2022	Cegid Sicherheitsteam	Zusammenführung der bestehenden IT-Sicherheitsplänen-von Cegid
03.04.2023	Cegid Sicherheitsteam	Überprüfung des Dokuments, Ergänzung der betreffenden Angebote und typografische Korrekturen
20.03.2024	Cegid Sicherheitsteam	Überarbeitung des Dokuments, Ergänzung der betreffenden Angebote und Zertifizierungen und typografische Korrekturen

2. EINFÜHRUNG

2.1. Zweck des Dokuments

Dieses Dokument ist der IT-Sicherheitsplan, der Kundenverträgen beigefügt werden kann. Es beschreibt die Verpflichtungen, die Cegid eingegangen ist, um die vertraglichen Anforderungen an die Sicherheit der Informationssysteme (IS) zu erfüllen, die auf Folgendes abzielen:

- Schutz der IT-Ressourcen, die für die Durchführung der Aktivitäten und die Bereitstellung der vertraglich vereinbarten Ergebnisse verwendet werden
- Den Kunden vor Schäden bewahren, die ihm aufgrund der Nichtverfügbarkeit dieser Ressourcen, einer Verletzung ihrer Integrität oder ihrer Vertraulichkeit entstehen könnten

In diesem IT-Sicherheitsplan sind die Sicherheitsbestimmungen aufgeführt, die sich auf die eingesetzten physischen, organisatorischen, verfahrenstechnischen und technischen Maßnahmen beziehen.

Die in diesem Dokument beschriebenen Maßnahmen können durch diejenigen ergänzt werden, die in der Broschüre mit den Allgemeinen Geschäftsbedingungen für das betreffende Cegid-Angebot beschrieben sind.

2.2. Anwendungsbereich

Dieses Dokument gilt für SaaS-Dienste, die von den Cegid Cloud Teams betrieben und bereitgestellt werden, sowie für die Aktivitäten dieser Teams.

2.3. Entwicklung des IT-Sicherheitsplans

Jede Weiterentwicklung des IT-Sicherheitsplans ist Bestandteil einer neuen Version dieses Dokuments. Änderungen werden in der Änderungstabelle am Anfang des Dokuments protokolliert.

Eine geringfügige Änderung[1] führt nicht zwangsläufig zu einer sofortigen neuen Version des IT-Sicherheitsplans. Diese Änderung wird in die nächste Version des Dokuments aufgenommen.

Jede Weiterentwicklung des IT-Sicherheitsplans ist zwingend Teil desselben und verpflichtet die Parteien gleichermaßen.

Bei einer Änderung des Dokuments gilt die auf der offiziellen Cegid-Website veröffentlichte Version als Referenz. Anhand der Version, die dem Kundenvertrag beigefügt ist, kann sichergestellt werden, dass keine Regression vorliegt.

[1] Änderung, die keine Auswirkungen auf die Sicherheitsanforderungen hat.

Der IT-Sicherheitsplan wird mindestens einmal pro Jahr überprüft. Eine solche Überarbeitung kann zur Herausgabe einer neuen Version dieses Dokuments führen.

2.4. Definitionen

Aktiva: Gesamtheit der Güter oder Dienstleistungen, die es ermöglichen, die Angebote von Cegid zur Verfügung zu stellen

ASVS: Application Security Verification Standard

BSIMM: Building Security In Maturity Model

CAB: Change Advisory Board

Kunde: Kunde einer durch dieses Dokument abgedeckten Lösung

CMP: Cloud Management Platform

DPO: Data Privacy Officer

EDM: Elektronisches Dokumentenmanagement

IPS: Intrusion Prevention System

ISMS: Informationssicherheits-Managementsysteme

Service-Handbuch: Dokument, in dem die besonderen Bedingungen beschrieben werden, die mit jedem SaaS-Angebot von Cegid verbunden sind

Cegid Cloud: Organisation innerhalb von Cegid, die für die Konzeption, den Betrieb und den technischen Support der SaaS-Plattform von Cegid zuständig ist (siehe Präsentation der Cegid Cloud).

ISO: International Standard Organization

OWASP: Open Web Application Security Project

PAM: Privileged Access Management

SRI: Sicherheitsrichtlinie für Informationssysteme

DSGVO: Datenschutz-Grundverordnung

CISO: Beauftragter für die Sicherheit von Informationssystemen

RPO: Recovery Point Objective oder Wiederherstellungspunkt der Daten

RTO: Recovery Time Objective oder Wiederherstellungsdauer des Dienstes

SAMM: Software Assurance Maturity Model

WSIS: Managementsystem für Informationssicherheit. Dieser Begriff bezeichnet eine Reihe von Richtlinien, die das Management der Informationssicherheit betreffen

VM: Virtual Machine

VPN: Virtuelles Privates Netzwerk

2.5. Referenzdokumente

AGB: Allgemeine Geschäftsbedingungen für die Nutzung der Services von Cegid. Sie sind verfügbar auf der Cegid Website unter https://www.cegid.de.

ISO 27001:2013: Anforderungsstandard für Informationssicherheits-Managementsysteme (ISMS)

ISO 27002:2013: Leitfaden für gute Praktiken im ISMS

ISO 27005:2018: Standard für das Risikomanagement in Bezug auf Informationssicherheit

Service-Handbücher: Dokumente, die die besonderen Bedingungen beschreiben, die mit jedem SaaS-Angebot von Cegid verbunden sind. Diese können unter https://www.cegid.de eingesehen werden.

3. ROLLEN UND VERANTWORTLICHKEITEN

Im Rahmen der Erbringung seiner Dienstleistungen stützt sich Cegid auf Infrastrukturen, die von seinen Partnern zur Verfügung gestellt werden. Für den Aufbau und die Instandhaltung dieser Infrastruktur sind diese Partner verantwortlich.

4. BESCHREIBUNG DER DIENSTE

Die von Cegid gelieferten anwendungsspezifischen Dienste und deren Beschreibung sind in den Servicehandbüchern enthalten.

5. GUTE PRAKTIKEN

Die Sicherheit von Cegid wird von einem zentralen Team gesteuert, das sich konzernweit an der ISO 27001 Norm orientiert. Cegid ist nach ISO 27001:2013[2] für die folgenden Bereiche zertifiziert:

- „Dienst, der das Hosting von Applikationen mit von Kunden bereitgestellten Daten in einer Cloud-Umgebung ermöglicht."
  Zertifikat Nr. IS 666376, ausgestellt von BSI
  Standorte in Frankreich: Lyon (69), Vénissieux (69), Boulogne Billancourt (92), Nantes (44)
  Cegid SaaS-Dienste von dieser Zertifizierung betroffen sind: Cegid Expert, Cegid Fiscalité (ehemals Cegid Fiscalité), Cegid HR Sprint, Cegid HR Ultimate, Cegid Loop, Cegid Optitaxes, Cegid Portail Etafi, Cegid PMI, Cegid Quadra (ehemals-Cegid Quadra Expert), Cegid Quadra Entreprise, Cegid Retail Y2, Cegid RHP, Cegid RHPi, Cegid Talentsoft, Cegid Tax Ultimate, Cegid XRP Flex, Cegid XRP Sprint

- „SaaS HR- und Lohnabrechnungsdienste, die in Form von verschiedenen Servicemodellen bereitgestellt werden, um die Personalverwaltung für Kunden in Spanien zu erleichtern"
  Zertifikat Nr. IS 589848, ausgestellt von BSI
  Standort in Spanien: Madrid
  Cegid SaaS-Dienste, die von dieser Zertifizierung betroffen sind: Cegid Peoplenet in Spanien

- „Dienst, der das Hosting von Applikationen für die Verwaltung und Entwicklung von Humanressourcen ermöglicht, die von Kunden bereitgestellte Daten enthalten, in einer Cloud-Umgebung"
  Zertifikat Nr. CA09/77186, ausgestellt von SGS
  Standort in Kanada: Montreal
  Standort in USA: New York
  Standort in Frankreich: Paris (75)
  SaaS-Dienste, die von dieser Zertifizierung betroffen sind: Cegid Talent

- „Proprietäres Informationssystem von Robotics für Wartung, Verwaltung, Software as a Service (SaaS) und Kundeneinrichtungen, die für die angemessene Bereitstellung von Zeit- und Anwesenheitsdiensten sowie Zugangskontrolle erforderlich sind"
  Zertifikat Nr. SI-0424/21, ausgestellt von LGAI Technological Center
  Standort in Spanien: Barcelona
  Von dieser Zertifizierung abgedeckte Dienste: Cegid VisualTime

- „Konzeption, Bereitstellung und laufende Unterstützung der Anwendung StorIQ"
  Zertifikat n°20/3244 ausgestellt von CfA
  Standort in Großbritannien: London
  Cegid SaaS Dienstleistungen, die von dieser Zertifizierung abgedeckt werden: Cegid Retail Store Excellence

[2] Die Arbeiten zur Umstellung auf ISO 27001:2022 sind in den verschiedenen oben genannten Bereichen im Gange.

- Informationssicherheits-Managementsystem, das SaaS (Software as a Service) für die Zeitwirtschaft mit der Lösung Cegid VisualTime unterstützt, gemäß der Anwendbarkeitserklärung mit der Version 2.1 und dem Datum 24/04/2023

  Zertifikat Nr. SI-0424/21 ausgestellt vom Technologischen Zentrum LGAI
  Standort Spanien: Barcelona
  Von dieser Zertifizierung abgedeckte Dienstleistungen: Cegid VisualTime

- Konzeption, Bereitstellung und laufende Unterstützung der StorIQ-Anwendung"
  Zertifikat n°20/3244 ausgestellt von CfA
  UK-Standort: London
  Cegid SaaS Dienstleistungen, die von dieser Zertifizierung abgedeckt werden: Cegid Einzelhandelsgeschäft Exzellenz

- ISAE 3402 Typ II Bericht über Cegid Tax Ultimate (nur Frankreich)

- SOC1 Typ II Bericht über Peoplenet Payroll (Argentinien und Mexiko)

- SOC2 Typ II Bericht über Peoplenet Payroll (Spanien, Portugal, Argentinien, Mexiko, Kolumbien und Chile)

- SOC 1 Typ I Bericht über Talentsoft Career

- ISAE 3402 Typ II Bericht über PeopleNet Frankreich

- Zertifizierung Kundensicherheitsprogramm (CSP) Swift für Cegid Treasury auf der Grundlage des CSCF

Die folgenden Cegid SaaS-Dienste werden von diesem Security Assurance Plan abgedeckt, obwohl sie nicht in den Geltungsbereich der vorherigen Zertifizierungen fallen: Cegid Assurex, Cegid Digitalrecruiters, Cegid ISIE, Cegid Orli, Cegid Peoplenet in Frankreich und Lateinamerika, Cegid Peoplenet Dedicated, Cegid Retail UR, Cegid XRP Ultimate, Cegid Treasury.

Wenn Sie Ihr Produkt in oben genannter Liste nicht finden können, zögern Sie nicht, unsere Vertriebsabteilung für weitere Informationen zu kontaktieren. Ziel ist es, Funktionen und Informationen vor Verlust, Diebstahl oder Manipulation zu schützen und Computersysteme vor Eindringlingen oder Katastrophen zu bewahren.

Die Einhaltung eines sicheren Softwareentwicklungs-Lebenszyklus gewährleistet ein hohes Maß an Sicherheit für die gehosteten Applikationen. Dieser Lebenszyklus basiert auf den Prinzipien der OWASP SAMM-, BSIMM- und OWASP ASVS-Richtlinien.

6. RISIKOVERWALTUNG

Der Risikobewertungsprozess umfasst die Identifizierung, Analyse und Management der Risiken, die mit dem Geschäftsmodell und den Nutzereinheiten verbunden sind.

Das Risikomanagement ist für Cegid ein wesentlicher Bestandteil der Geschäftstätigkeit. Die Geschäftsleitung hat in vier Bereichen eine Risikobewertung für Cegid Cloud festgelegt:

Risiken im Zusammenhang mit:

- Humanressourcen
- Strategische Risiken
- IT-Risiken
- Sonstige Risiken

Dieser Prozess ermöglicht es der Geschäftsleitung von Cegid relevante Risiken, die das Unternehmen betreffen können, zu verstehen und nachzuverfolgen sowie Maßnahmen zu deren Minderung zu ergreifen.

Darüber hinaus werden spezifische Risikoanalysen für die verschiedenen ISMS durchgeführt, die auf den Grundsätzen der ISO 27005 und international anerkannten Methoden (EBIOS 2010, EBIOS RM, MAGERIT, Octave usw.) basieren.

Die Risikoanalyse ist ein integraler Bestandteil der Informationssicherheit von Cegid. Diese wird kontinuierlich in den operativen Teams und den Sicherheitsteams durchgeführt.

7. RICHTLINIE ZUR INFORMATIONSSICHERHEIT

Die Aktivitäten von Cegid werden von Richtlinien zur Informationssicherheit begleitet. Diese Richtlinien wurden ab 2008 eingeführt und werden jedes Jahr überprüft. Sie basieren auf den Grundsätzen und guten Praktiken der Normen ISO 27001:2013 und ISO 27002:2013.

Diese Richtlinien zielen darauf ab, kritische Informationen von Cegid, seinen Kunden und Partnern zu schützen.

Die Richtlinien werden den betroffenen Personen mitgeteilt. Um die Sicherheit und Integrität seiner Plattformen bestmöglich zu wahren, gibt Cegid die Namen und Informationen über die implementierten Sicherheitselemente (Lieferanten, Herausgeber usw.) nicht bekannt.

8. ORGANISATION DER INFORMATIONSSICHERHEIT

8.1. Interne Organisation

8.1.1. Rollen und Verantwortlichkeiten

Die Verantwortlichkeiten für die IT-Sicherheit wurden festgelegt und zugewiesen.

Cegid ernennt für alle Aktivitäten einen CISO. Dem CISO untersteht ein engagiertes Team, das sich um die IT-Sicherheit kümmert.

Die an der Informationssicherheit beteiligten Akteure sind:

8.1.2. Trennung von Aufgaben und Verantwortungsbereich

Um das Risiko einer unbefugten oder unbeabsichtigten Änderung oder Verfälschung von Assets zu begrenzen, werden die Aufgaben und Verantwortungsbereiche der Teams getrennt.

Insbesondere sind alle Hosting-Aktivitäten für unsere Kunden sowohl organisatorisch als auch technisch von den übrigen Unternehmensumgebungen getrennt.

Darüber hinaus wird im Rahmen der Hosting-Aktivitäten für unsere Kunden ein Prinzip der Aufgabentrennung durch die Verwaltung von Rechten, die mit den geschäftlichen Anforderungen verbunden sind, umgesetzt.

Eine Matrixorganisation des Konzerns ermöglicht es, die Verantwortungsbereiche nach Geschäftsbereichen zu definieren, insbesondere diejenigen, die mit der Verantwortung für die Sicherheit der Kundendaten und der Vermögenswerte und Risiken verbunden sind, die die Bereitstellung von Cloud-Diensten ermöglichen.

8.1.3. Governance

Auf strategischer und operativer Ebene wurden Governance-Instanzen mit dedizierten Ausschüssen eingerichtet.

Diese Gremien treffen sich regelmäßig, um Themen zu verfolgen, die die Sicherheit der Informationssysteme betreffen. Die Protokolle werden im Dokumentenmanagementsystem gespeichert.

8.1.4. Beziehung zu Organisationen und Behörden

Cegid ist Mitglied von Berufsverbänden (CLUSIR (französischer Club für Netzwerk-Informationssicherheit), CLUSIF (französischer Club für Informationssicherheit), CESIN (französischer Club für Experten für digitale Informationssicherheit), Incibe (spanisches nationales Institut für Cybersicherheit), usw.), Club ISO27001. Cegid unterhält Beziehungen zu den Behörden (ANSSI (französische Agentur für die Sicherheit von Informationssystemen), CNIL (französische Datenschutzbehörde), CCN-CERT (spanisches nationales kryptologisches Zentrum - Computer Emergency Response Team), AEPD (spanische Datenschutzbehörde), CERT-MX (mexikanisches Computer Emergency Response Team), usw.), um die Entwicklungen im Bereich der Informationssicherheit zu verfolgen.

8.1.5. Überwachung und Sicherheit

Die technische und rechtliche Sicherheit wird überwacht und innerhalb der Cegid-Aktivitäten durchgeführt. Sie dient der Vermeidung von Risiken, die spezifisch mit den Aktivitäten von Cegid verbunden sind.

Cegid nutzt die CERT-Dienste von Unternehmen, die auf Sicherheitsüberwachung spezialisiert sind, um seine Suchkapazitäten zu erhöhen. Diese Methode der Mehrfachsuche ermöglicht es, die gefundenen Informationen zu überlagern und Ergebnisse zu erhalten, die im Kontext der Geschäftstätigkeit von Cegid angepasst und relevant sind.

9. SICHERHEIT IM ZUSAMMENHANG MIT HUMANRESSOURCEN

9.1. Rekrutierung

Die Überprüfung der Informationen von Bewerbern erfolgt in Übereinstimmung mit den Vorschriften, der Ethik, den Gesetzen und allen einschlägigen Gesetzen, die in der jeweiligen Gerichtsbarkeit gelten. Sie stehen in einem angemessenen Verhältnis zu den Anforderungen der Rolle , der Klassifizierung der zugänglichen Informationen und den identifizierten Risiken.

Es werden folgende Informationen der Bewerber überprüft:

- Überprüfung des Lebenslaufs des Bewerbers
- Überprüfung der Kompetenzen in Bezug auf die Stelle
- Kopien der im Lebenslauf angegebenen Abschlüsse, Ausbildungen und beruflichen Qualifikationen
- Unabhängige Identitätsprüfung, Reisepass oder Personalausweis
- Überprüfung der Gültigkeit der Arbeitserlaubnis und der Aufenthaltserlaubnis, wenn die Bewerberin/der Bewerber eine Zuwanderin/ein Zuwanderer ist

9.2. Verwaltung der Privatsphäre

Die folgenden Aspekte werden in den Verträgen, der Hausordnung und der IT-Charta abgedeckt:

- Respekt des geistigen Eigentums
- Einhaltung der Rechtsvorschriften zum Schutz personenbezogener Daten
- Schutz von Informationen, informationsbezogenen Vermögenswerten, Applikationen des Unternehmens und Kunden
- Schutz von Informationen, die von Partnern, anderen Organisationen oder Dritten stammen

In den folgenden Situationen können besondere Bestimmungen gelten:

- Auslösung eines formellen und allgemein bekannten Disziplinarverfahrens gegen Mitarbeitende, die gegen die Regeln der Informationssicherheit verstoßen haben. Dabei handelt es sich um ein abschreckendes Element, das die Mitarbeitenden davon abhält, gegen die Sicherheitsrichtlinien und -verfahren des Unternehmens sowie andere Sicherheitsregeln zu verstoßen
- Im Arbeitsvertrag festgelegte Verantwortlichkeiten, die für eine bestimmte Zeit nach Beendigung des Arbeitsvertrags weiter gelten

Alle Mitarbeitenden sind vertraglich zu Verschwiegenheit verpflichtet. Alle Informationen, die von den Kunden durch Dokumente oder Besprechungen zur Verfügung gestellt werden, sind von dieser Vertraulichkeitsverpflichtung betroffen.

9.3. Kompetenzverwaltung

9.3.1. Sicherheitsbewusstsein

Neue Mitarbeitende durchlaufen im Zuge des Onboardings einen Einführungskurs, der eine Sensibilisierung für Sicherheit und Datenschutz beinhaltet.

Ein Sensibilisierungsplan und spezielle Tools ermöglichen eine regelmäßige Überwachung sensibler Sicherheitsthemen (Phishing-Kampagne, Safe Desk usw.).

9.3.2. Kompetenz und Entwicklung

Um das Know-how zu erhalten, den Schulungsbedarf zu ermitteln und den Wissensaustausch zu ermöglichen, werden jedes Jahr Leistungs- und Zielvereinbarungsgespräche zwischen Cegid-Mitarbeitenden und Cegid-Führungskräften durchgeführt. Bei diesen Gesprächen werden Entwicklungspläne besprochen. Die Personalabteilung baut auf dieser Grundlage und zusammen mit der Unternehmensstrategie einen jährlichen Entwicklungsplan auf.

10. Asset Management

10.1. Inventar

Cegid führt Bestandsaufnahmen der wesentlichen und der unterstützenden Vermögenswerte durch. Diese werden in Risikoanalysen aufgelistet, sodass die damit verbundenen Risiken zentral erfasst werden können.

Wenn es technisch machbar und relevant ist, gleicht ein automatisierter Aktualisierungsprozess den Bestand und die im SaaS-Perimeter vorhandenen Assets ab.

10.2. Identifizierung von Assets

Die Identifizierung der Vermögenswerte, die bei der Bereitstellung der von Cegid erbrachten Dienstleistungen verwendet werden, basiert auf formalisierten Namenskonventionen. In den meisten Fällen, und wenn es relevant ist, ermöglichen diese Namenskonventionen keine direkte Verbindung zu den Kunden.

10.3. Dokumentenmanagement

Cegid hat Dokumentenmanagementsysteme eingerichtet, die die Prozesse und Verfahren berücksichtigen, die für den Betrieb der für die Kunden erbrachten Dienstleistungen erforderlich sind.

10.4. Verwaltung von Medien und Materialien, die sich auf Kundendaten auswirken

10.4.1. Speicherung

Wechselmedien mit Kundendaten werden an einem sicheren Ort aufbewahrt, wenn diese nicht in Gebrauch sind.

Nicht entfernbare Datenträger mit Kundendaten werden in Rechenzentren untergebracht.

10.4.2. Physische Übertragung

Für die physische Übertragung eines Mediums, das nicht-öffentliche Daten enthält, verwendet Cegid ausschließlich anerkannte und zuverlässige Transportunternehmen, die eine Nachverfolgung und einen Nachweis der Lieferung anbieten. Sollte Cegid Daten auf einem Medium zurückgeben, das auf Initiative eines Kunden übermittelt wurde, so werden diese Daten mit denselben Techniken und Mitteln übermittelt, die zum Zeitpunkt ihres Eingangs verwendet wurden.

10.4.3. Entsorgung

Die Entsorgung von Assets unterliegt einem besonderen Verfahren zur Entfernung vertraulicher Daten. Dieses Verfahren schreibt vor, dass Medien, die vertrauliche Daten beinhalten, sicher entfernt oder physisch zerstört werden müssen.

10.4.4. Wartung

Die Verantwortung für Hardwaregeräte, die Kundendaten enthalten, liegt bei den Infrastrukturanbietern von Cegid.

10.5. Verwaltung der Hardware von Cegid Mitarbeitern

10.5.1. Wartung der Ausrüstung

Cegid-Mitarbeiterarbeitsplätze werden durch die IT-Abteilung von Cegid bereitgestellt. Die Hardware-Wartung dieser Maschinen wird durch die IT-Abteilung von Cegid und ihren Lieferanten durchgeführt. Es wird ein Inventar über die Zuordnung dieser Posten geführt und die Mitarbeitenden werden für ihre physische Sicherheit verantwortlich gemacht.

10.5.2. Entsorgung

Die Speichermedien, die sich in den ausrangierten Geräten befinden, werden gemäß den geltenden Verfahren auf sichere Weise zerstört (Software zur Datenlöschung, Löschen der Verschlüsselungsschlüssel der Festplatten usw.).

10.5.3. Verwaltung von Wechselmedien

Für die Mitarbeitenden der Cegid Cloud-Teams wird eine Sicherheitsrichtlinie für Wechselmedien eingeführt und verwaltet. Diese Richtlinie wird durch Endpoint-Software oder GPO implementiert, die die Nutzung von Wechselmedien nicht einschränken.

10.5.4. Updates, Antivirus, Verschlüsselung von Medien

Die IT-Abteilung ist verantwortlich für die System- und Applikationsaktualisierungen von Cegid (Office Updates, interne Applikationen), die Aktualisierung des Malware-Schutzes sowie die Verschlüsselung von Datenträgern (interne und Wechseldatenträger). Indikatoren werden regelmäßig erstellt und vom Sicherheitsteam analysiert.

11. Richtlinie zur Sicherung von Betriebssystemen

Cegid hat strenge Richtlinien eingeführt, die darauf abzielen, die Betriebssysteme zu sichern. Dabei geht es darum, die potenzielle Angriffsfläche zu verringern, indem nicht essenzielle Objekte (Dienste, Applikationen, Funktionen usw.) deaktiviert oder entfernt werden. Dazu gehört es, besondere Sicherheitsoptionen einzurichten und für Software-Updates zu sorgen.

11.1. Betriebssystem der Server

Die Maßnahmen an den Server-Betriebssystemen betreffen:

- Updates
- Kontostrategie
- Benutzer- und Netzwerkrechte
- Protokollierung
- Schutz vor Malware
- Rollen- und Funktionsservice
- Benutzerbereich
- Speicherplatz auf der Festplatte

Diese Abläufe orientieren sich an den Leitfäden des CIS (Center for Internet Security), der ANSSI und des NIST (National Institute of Standards and Technology).

12. ZUGANGSKONTROLLE

12.1. Passwort-Richtlinie

Jeder Cegid-Benutzer wird mit einer eindeutigen Benutzerkennung und einem starken Passwort authentifiziert.

Die Passwörter der Benutzer werden nicht als Klartext im Informationssystem von Cegid gespeichert.

Die Standardregel für unseren Anwendungsbereich ist die Verwendung von nicht umkehrbaren Verschlüsselungsfunktionen des Typs „Hash“ mit sicheren Algorithmen.

Für die AS400-Perimeter wurde eine Vigenère-Verschlüsselung mit einem X-OR-Schlüssel eingerichtet.

12.1.1. Richtlinie für technische Administratoren von Cegid

Die Verwaltung der Passwörter für die technischen Administratoren von Cegid unterliegt einer strengen Sicherheitsrichtlinie:

- Mindestlänge: 10 Zeichen
- Komplexität: Groß,- und Kleinbuchstaben, Zahl und Symbol
- Häufigkeit der Änderungen: alle 60 Tage
- Keine Wiederverwendung der letzten 24 Passwörter
- Sperrung nach fünf Versuchen (Entsperrung durch einen Cegid-Administrator)

12.1.2. Richtlinien für Cegid-Kunden

Die Standard-Passwortrichtlinie für Benutzer von Cegid-Kunden lautet wie folgt:

- Mindestlänge: 8 Zeichen
- Komplexität: Groß,- und Kleinbuchstaben, Zahl und Symbol
- Häufigkeit der Änderungen: alle 90 Tage
- Keine Wiederverwendung der letzten 24 Passwörter
- Sperrung nach fünf Versuchen (Entsperrung durch einen Cegid-Administrator oder durch den Benutzer über ein Online-Tool zur Verwaltung von Passwörtern)

Einige Applikationen ermöglichen es, die Verwaltung der Benutzerkennungen an den Kunden zu delegieren. Wenn diese Identitätsföderation aktiviert ist, ist der Kunde bei der Verwaltung und Durchsetzung seiner eigenen Passwortpolitik autonom. Cegid empfiehlt seinen Kunden, diese Option zu nutzen und dabei die mit der DSGVO verbundenen Anforderungen zu beachten.

12.2. Rechteverwaltung

Die Rechteverwaltung für Cegid-Teams basiert auf dem Prinzip der minimalen Privilegien. Jedes Team besitzt lediglich die notwendigen Rollen, Rechten und Autorisierungen, sodass Nutzer ausschließlich auf Daten und Funktionen in ihrem Zuständigkeits- und Aufgabenbereich zugreifen können.

Regelmäßige Zugangskontrollen werden von Cegid Security Team durchgeführt.

Die Beantragung von Rechten (Hinzufügen, Ändern, Löschen) bei den wichtigsten Applikationen und Domänen erfolgt über Workflows.

Aus Gründen der Vertraulichkeit werden keine persönlichen Daten von Cegid-Mitarbeitenden weitergegeben.

12.3. Verwaltung des Serverzugriffs

Nur Personen mit entsprechender Berechtigung können auf Server mit Kundendaten zugreifen. Cegid verfügt über spezifische Verzeichnisse für die Produktionsperimeter, die vom internen Informationssystem getrennt sind.

12.4. Zugriff löschen

Die Aufhebung des Zugriffs für Cegid-Personal ist mit dem HR-Prozess zur Verwaltung von Austritten oder interner Mobilität verbunden. Diese Aktionen werden mithilfe interner Workflow-Tools verfolgt und zurückverfolgt.

Bei externen Mitarbeitenden liegt die Verantwortung für die Änderung oder Aufhebung von Rechten bei der Führungskraft.

12.5. Überprüfung der Rechte

Die Überprüfung der Rechte der Anwendungsbereiche wird durch das Sicherheitsteam organisiert. Auf der Grundlage einer Risikoanalyse werden regelmäßig Zugangsüberprüfungen durchgeführt.

13. VERSCHLÜSSELUNG

13.1. Weiterleitung von Daten an öffentliche Netzwerke

Die Daten werden bei der Übertragung in öffentliche Netzwerke mit sicheren Protokollen (HTTPS, TLS, SFTP, SSH usw.) verschlüsselt.

13.2. Daten auf andere Medien übertragen

Bei Wechselmedien (z. B. USB-Sticks oder -Disketten) müssen die Medien vom Kunden oder bei Bedarf mit Hilfe der Support-Teams verschlüsselt werden, bevor sie an Cegid gehen. Ist dies nicht der Fall, ist der Kunde für die Sicherheit der Daten während des Transports und des Empfangs bei Cegid verantwortlich. Die Medien werden nach der Integration der Daten gelöscht, bevor sie wieder zum Kunden gehen.

13.3. Zertifikate

Um das höchste Sicherheitsniveau zu gewährleisten, stammen die von Cegid verwendeten HTTPS-Zertifikate von öffentlichen und anerkannten Zertifizierungsstellen. Die Verwaltung dieser Zertifikate wird durch Verfahren geregelt, die ihren Lebenszyklus abdecken.

13.4. Verschlüsselungen

Die Regeln für die Länge von Chiffrierschlüsseln sind:

- Asymmetrische Verschlüsselung: größer oder gleich 2048 Bit
- Symmetrische Verschlüsselung: größer oder gleich 256 Bit

Cegid verwendet Verschlüsselungssoftware, die sich auf AES256 stützt, um sichere Archive zu erstellen.

Was die Verschlüsselung betrifft, so sind die Verbindungsprotokolle für unsere externen Sites mindestens TLS 1.2.

13.5. Mobilität

Die Administratorenteams von Cegid verwenden ihre Laptops nur, um sich remote anzumelden.

14. PHYSISCHE SICHERHEIT

14.1. Lokalisierung

Die von Cegid genutzten Rechenzentren befinden sich auf der ganzen Welt, um den regulatorischen und lokalen Anforderungen unserer Kunden gerecht zu werden. Cegid stellt sicher, dass seine Lieferanten sowohl in technischer als auch in sicherheitsrelevanter Hinsicht die Anforderungen erfüllen. Die Wahl des Rechenzentrums erfolgt vor der Aufnahme in die Produktion und in Abhängigkeit von den Cegid-Angeboten.

14.2. Rechenzentren

14.2.1. Physische Sicherheit der Standorte und Zugangskontrolle

Um ein optimales Sicherheitsniveau zu bieten, sind alle von Cegid genutzten Rechenzentren nach ISO 27001 zertifiziert. Der Zutritt zu den Rechenzentren ist ausschließlich befugten Personen gestattet.

14.2.2. Hardware-Sicherheit

Bei der Gestaltung der Infrastruktur wurden eine Reihe von Maßnahmen und Grundsätzen ergriffen, um die optimale Verfügbarkeit und Integrität der Cegid-Dienste zu gewährleisten.

Die wichtigste Regel ist die Vermeidung eines einzelnen Ausfallpunkts (‚Single Point Of Failure') auf Hardware- und Netzwerk-Ebene.

Beispiele:

- Redundanz auf der Ebene der physischen Server
- Redundanz auf Netzwerkebene
- Auf der Ebene der Speicherung
- Virtualisierung

14.3. Cegid

14.3.1. Sicherheit der Standorte

Die Räumlichkeiten von Cegid unterliegen denselben Regeln wie der Rest der Räumlichkeiten von Cegid Lyon Vaise, die hauptsächlich in Folgendem bestehen:

- Energielieferung mit Sondervertrag + Wechselrichter
- Feuermelder, Feuerlöscher
- Erbringung von CCV-Dienstleistungen (Klimaanlagen, Heizung, Lüftung)

14.3.2. Zugangskontrolle

Der Zugang zu den Räumlichkeiten ist durch Ausweisleser gesichert. Jeder Mitarbeitende hat einen programmierten Ausweis, der ihm den vollständigen oder teilweisen Zugang zu bestimmten Teilen des Gebäudes ermöglicht.

Physische Zugangskontrollen sind Teil der Rechteverwaltung, wie in Absatz 12.2 beschrieben wird.

14.3.3. Clean Desk-Richtlinie

In den Räumlichkeiten der Cegid-Teams gilt eine „Clean Desk"-Richtlinie. Dokumente, Medien oder andere Materialien, die vertrauliche Informationen enthalten könnten, werden sicher verstaut, wenn diese nicht in Gebrauch sind.

15. SICHERHEIT IM ZUSAMMENHANG MIT DEM BETRIEB

15.1. Daten

15.1.1. Klassifizierung von Daten

Die ISO-Norm 27001 schreibt eine Klassifizierung der wesentlichen Güter und Informationen vor. Diese Klassifizierung wird auf mindestens drei Ebenen vorgenommen:

- Öffentlich
- Begrenzt
- Vertraulich

In diesem Rahmen werden die Kundendaten als „vertraulich" eingestuft.

15.1.2. Sicherheit auf Dateien

Die Datendateien werden in dedizierten Verzeichnissen für jeden unserer Kunden gespeichert. Diese Verzeichnisse werden mit den Sicherheitsmechanismen geschützt, die von den zugrunde liegenden Betriebssystemen bereitgestellt werden.

Dadurch wird die Sicherheit, Abschottung und Abdichtung zwischen den einzelnen Klienten gewährleistet.

15.1.3. Sicherheit auf Datenbanken

Cegid verwendet für seine Datenbanken standardmäßige und bekannte Systeme des Typs Microsoft SQL, Oracle, MySQL, MongoDB, DB2 etc.

Die Auswahl der wichtigsten Akteure auf diesem Gebiet ermöglicht es Cegid, sich auf bewährte Herausgeber und eine sehr aktive Gemeinschaft zu stützen, um seine Datenbankverwaltungssysteme immer auf einem optimalen Niveau zu halten.

15.1.4. Verschlüsselung von Daten

Daten werden bei der Übertragung zwischen den Arbeitsplätzen der Kunden und dem Informationssystem von Cegid durch die Verwendung von Verschlüsselungsprotokollen gesichert, die in Absatz 13.1 beschrieben werden.

15.1.5. Datenintegrität

Cegid verpflichtet sich zu sicheren Verfahren, technischen Maßnahmen und Protokollen zur Übertragung und Aufbewahrung der Daten seiner Kunden, um sich gegen (absichtliche oder versehentliche) Manipulation zu schützen.

15.1.6. Vertragsende

Die Aufbewahrung und Löschung von Kundendaten nach der Beendigung eines Vertrags ist in den Vertragsunterlagen detailliert geregelt.

15.2. Change Management

Änderungen werden basierend auf den unten aufgeführten Verfahren durchgeführt:

Änderungen der Applikation:

- Standardmäßige und normale Änderungen sind nach Bestätigung durch den Ausschuss erlaubt. Zu diesen Änderungen gehören zum Beispiel: Standard-Portalaktualisierungen, Steueraktualisierungen, Weiterentwicklungen von Einstellungen, Korrekturen von Fehlern und Schwachstellen usw.

Änderungen an Infrastrukturen und Systemen:

- Genehmigt nach Freigabe durch den Ausschuss: Infrastrukturänderungen mit direkten Auswirkungen auf die Produktion, Behebung von Incidents, Kapazitätsmanagement, Sicherheit
- Ohne Freigabe durch das Komitee genehmigt: laufende Betriebsmaßnahmen, die dazu dienen, die Produktion in einem betriebsbereiten Zustand zu halten

Besondere Zeiträume:

- Je nach Abhängigkeit der Produkte und Geschäftstätigkeiten unserer Kunden sind Änderungen auf bestimmte Zeiträume beschränkt, die allgemein als „Freeze Periods" bezeichnet werden

DRINGENDE Änderungen:

- Dringende Änderungen sind schnell umzusetzen und können nicht bis zum nächsten Validierungszyklus warten
- Diese Kategorie von Änderungen ist für die Behebung einer Krise oder eines unmittelbar bevorstehenden kritischen Risikos (z. B. Sicherheitslücke, größerer Incident) reserviert
- Diese Kategorie von Änderungen wird in einem Ausschuss behandelt, der in einer Notfallsituation einberufen wird (z. B. eCAB/Emergency CAB)

15.3. Schutz vor Malware

Die gesamte Server-Infrastruktur wird durch zentrale Antivirus- und Antimalware-Lösungen geschützt. Die Server prüfen mindestens täglich, ob beim Herausgeber eine Aktualisierung vorliegt. Sie werden dann auf allen Servern gestreamt.

Eine Antivirus-Überwachung ist in die Überwachung des Informationssystems von Cegid integriert und ist Gegenstand von Indikatoren, die bei den mit der Informationssicherheit verbundenen Komitees überprüft werden.

15.4. Datensicherung (Backup)

15.4.1. Backup Richtlinie

Die Kundendaten stehen im Mittelpunkt der Aufmerksamkeit der Cegid-Teams. Um die Integrität und Verfügbarkeit der Daten zu gewährleisten, betreibt Cegid ein leistungsstarkes Backup-System.

Das von Cegid gewählte Prinzip ist das der doppelten Sicherung:

- Ein erstes Backup wird von den Produktionssystemen auf einer ersten dedizierten Infrastruktur erstellt
- Anschließend erfolgt eine Vervielfältigung auf einer zweiten, dedizierten Infrastruktur

Die Infrastruktur für die Datensicherung befindet sich nicht im selben Rechenzentrum wie die Produktionssysteme. Diese Organisation ermöglicht es, ein optimales Maß an Verfügbarkeit und Integrität zu gewährleisten und gleichzeitig unsere RTO- und RPO-Anforderungen zu erfüllen (siehe dazu Kapitel 20.3).

Die Häufigkeit der Backups und die Dauer der Speicherung ist für jedes Angebot spezifisch und wird im Service-Handbuch des jeweiligen Angebots detailliert beschrieben.

15.4.2. Kontrollen und Wiederherstellung

Eine Kontrolle der Backups erfolgt über Reporting-Werkzeuge. Bei einem eventuellen Incident während eines Backups wird automatisch eine Warnung ausgegeben, die von den Cegid-Teams bearbeitet wird.

Im Rahmen der regulären Betriebstätigkeit führt Cegid täglich Restaurationen durch. Diese ermöglichen es, die ordnungsgemäße Funktion der Backups sowie die damit verbundenen Wiederherstellungsprozesse zu validieren.

15.4.3. Aufbewahrungsprinzipien

Als spezialisierter Herausgeber kennt Cegid das Geschäft und Bedürfnisse seiner Kunden sehr gut. Dank dieser Eigenschaft konnten für jedes angebotene Angebot spezifische Aufbewahrungsfristen für Backups eingerichtet werden.

Die Aufbewahrungsprinzipien sind im Service-Handbuch des jeweiligen Angebots detailliert beschrieben.

15.5. Log Management

15.5.1. Sammeln von Logs

Die Rückverfolgbarkeit des Informationssystems von Cegid wird durch Tools zur Konzentration und Korrelation von Ereignisprotokollen (Logs) gewährleistet. Diese werden zu technischen und betrieblichen Zwecken für eine Dauer aufbewahrt, die an die gesetzlichen, vertraglichen und betrieblichen Auflagen angepasst ist.

Diese Tools ermöglichen eine einheitliche Aufbewahrungsdauer für die gesammelten Informationen und sorgen für deren Sicherheit.

Zu den gesammelten Informationen gehören z. B. der Name des Anwenders, die Uhrzeit der Anmeldung bzw. der Abmeldung, die verwendete Applikation, die Quell-IP-Adresse usw.

Die Logs sind für die Cegid-Teams zugänglich und können vom Kunden nicht exportiert werden. Diese Logs können mit dem Kunden nur auf legitime Anfrage wie beispielsweise für die Lösung eines Incidents geteilt werden. Einige Cegid-Lösungen bieten Applikationslogs, die direkt aus der Applikation heraus verfügbar sind.

15.5.2. Richtlinien für den Zugang zu Tools

Auf die Tools können Cegid-Cloud-Mitarbeitende für die spezifischen Bedürfnisse des Betriebs der Plattform und mit Rechten zugreifen, die ihren Funktionen entsprechen (siehe Kapitel 12).

15.5.3. Gebrauch von Logs

Beispiele für die Verwendung der gesammelten Informationen:

- Erfüllung der regulatorischen und vertraglichen Auflagen, die mit den Geschäftsbereichen von Cegid verbunden sind
- Überwachung des Gesundheitszustands der von Cegid Cloud verwalteten Systeme und in der Lage sein, frühzeitig alle Ereignisse zu erkennen, die zu einer Verschlechterung des Service führen könnten
- Erstellung anonymisierter statistischer Informationen über die Bereitstellung des Dienstes

Die Nutzung von Statistiken und Informationen aus Trackern wird durch die Allgemeinen Nutzungsbedingungen geregelt.

15.6. Überwachung

15.6.1. Grundsätze

Alle von Cegid Cloud verwalteten Dienste und Systeme werden überwacht. Die Überwachungstools verwenden entweder das SNMP-Protokoll oder speziell entwickelte PLCs (Programmable Logic Controller), um die Informationen von allen Kontrollpunkten abzurufen.

Ein Fernüberwachungsraum ermöglicht es den Teams von Cegid Cloud, den Gesundheitszustand bestimmter Dienste ständig zu überwachen. Bei Fehlfunktionen werden Echtzeitwarnungen für alle überwachten Dienste ausgelöst.

Die Tools sind mit Systemen gekoppelt, die SMS Nachrichten an Bereitschaftsdienstteams während der arbeitsfreien Zeit versenden.

15.6.2. Bereitschaftsdienst

Der Bereitschaftsdienst übernimmt die Aufgabe, das Informationssystem von Cegid rund um die Uhr 24/7 zu überwachen und bei Bedarf zu intervenieren. Er besteht aus Experten, die alle Kompetenzbereiche von Cegid vertreten.

15.7. Update Management

15.7.1. Verwaltung der installierten Software

Cegid verwendet eine Reihe von Softwareprogrammen, die es ermöglichen, die gesamte Software im Informationssystem und auf den Verwaltungsstationen zu inventarisieren und zu kontrollieren.

15.7.2. System-Update

Systemaktualisierungen werden über zentralisierte Konsolen durchgeführt.

Das von Cegid gewählte Prinzip, um sowohl kritische als auch sicherheitsrelevante Updates durchzuführen, ist das Folgende: Updates werden in einem monatlichen Zyklus auf einer Reihe von Kontrollumgebungen bei der Veröffentlichung eines Patches eingesetzt, um sicherzustellen, dass er keine Probleme mit der Integrität und/oder Verfügbarkeit des an die Kunden gelieferten Dienstes verursacht. Wenn keine Probleme festgestellt werden, erfolgt der Einsatz auf der gesamten Produktionsplattform.

Sollte ein Patch nicht verfügbar sein, wird ein Workaround eingerichtet, um die Sicherheit des angebotenen Dienstes nicht zu beeinträchtigen.

15.7.3. Applikations-Update

Cegid implementiert ein Änderungsmanagement (siehe Kapitel 15.2. Change Management), das ermöglicht, Applikationsaktualisierungen gemäß den in den Serviceheften seiner SaaS-Lösungen festgelegten Verpflichtungen zu verwalten.

16. SICHERHEIT DER KOMMUNIKATION

16.1. Technische Architektur

Die Infrastruktur, die die Dienste von Cegid unterstützt, ist abgeschottet und in Sicherheitszonen sowie Applikationszonen organisiert. Dieses Prinzip ermöglicht es, eine Sicherheit in der Tiefe anzubieten, die den aktuellen und zukünftigen Bedürfnissen entspricht.

16.2. Telekom-Zugang

16.2.1. Internet

Cegid besitzt eigene öffentliche IP-Adressen und mehrere Internetzugänge von verschiedenen Anbietern, um den Ausfall eines Anbieters zu kompensieren und seinen Kunden das erwartete Serviceniveau zu bieten.

Die gesamte von Cegid angebotene Kommunikation ist sicher und verwendet die in Kapitel 13.1 aufgeführten Protokolle.

16.2.2. WLAN-Netzwerke

WLAN-Netzwerke sind nach Funktion unterteilt (Gäste-, Mitarbeiter-, Mobil-WLAN usw.) und der Zugang hängt von der Rechteverwaltung ab. WLAN-Zugangspunkte sind geschützt.

In Rechenzentren ist WLAN verboten.

16.3. Sicherheitsausrüstungen

16.3.1. Firewall

Zwischen jeder Sicherheitszone und jeder Applikationszone befinden sich Firewalls.

Von außen kommende Datenströme durchlaufen mehrere Firewall-Schichten, bevor sie den gewünschten Dienst erreichen.

Direkte Datenströme in vertrauliche Zonen sind nicht erlaubt, sie müssen zwingend über die demilitarisierten Zonen (DMZ) laufen.

16.3.2. IDS/IPS

An einigen strategischen Netzwerkstandorten wurden IDS/IPS-Sonden eingerichtet, um die ein- und ausgehenden Datenströme des Informationssystems von Cegid zu analysieren. Ihre Aufgabe ist es, anormale Datenströme und bösartigen Datenverkehr zu erkennen und zu blockieren.

Die Sonden holen sich die Updates der Angriffssignaturen von den Sicherheitsexperten des Anbieters und werden unter der Verantwortung des Cegid-Sicherheitsteams eingesetzt.

Diese Daten werden zu Dashboards und Indikatoren korreliert.

16.3.3. DDoS-Schutz

Alle Plattformen und Infrastrukturen profitieren von einem DDoS-Schutz, der an die verschiedenen betriebenen Technologien angepasst ist.

16.3.4. Hohe Verfügbarkeit und Fehlertoleranz

Die Verfügbarkeit der Cegid-Dienste wird durch redundante Systeme sichergestellt, um Fehlfunktionen, den Ausfall einer Komponente oder eine vorübergehende Nichtverfügbarkeit auszugleichen. Zu den verwendeten Technologien gehören:

- Virtualisierung von Servern
- Redundante Datenspeicherung
- Cluster-Lastenausgleich auf Netzwerk- und Telekomgeräten
- Methode der Kapazitätsplanung mit Erweiterung im laufenden Betrieb (VM und Firewall)
- Ausgleich der Applikationslast auf Serverfarmen

17. Erwerb, Entwicklung und Pflege von Informationssystemen

Bei der Software-Entwicklung spielt die Sicherheit eine wesentliche Rolle für Cegid.

Cegid hat einen Ansatz eingeführt, der darauf abzielt, die Sicherheit während des gesamten Lebenszyklus der entwickelten Applikationen zu integrieren. Diese orientiert sich an den Empfehlungen von OWASP SAMM, OWASP ASVS und BSIMM.

17.1. Lebenszyklus einer sicheren Softwareentwicklung

Ein Governance-Workstream umfasst Aktivitäten im Zusammenhang mit der Organisation des Lebenszyklus einer sicheren Entwicklung mit der Definition von Richtlinien, Zielen und Maßnahmen sowie einem damit verbundenen Schulungs- und Sensibilisierungsprogramm.

Ein Design-Workstream umfasst Aktivitäten im Zusammenhang mit der Sammlung von Sicherheitsanforderungen, High-Level-Architekturspezifikationen und dem detaillierten Design.

Ein Implementierungs-Workstream umfasst die Aktivitäten und Prozesse zum Aufbau und Einsatz von Softwarekomponenten sowie die Aktivitäten und Prozesse im Zusammenhang mit dem Fehlermanagement.

Eine Verifizierungs-Workstream umfasst Aktivitäten im Zusammenhang mit Funktions-, Regressions- und Sicherheitstests, mit welchen die Qualität der entwickelten Software sichergestellt werden kann.

Der gesamte Ansatz zielt darauf ab, die Qualität und Sicherheit der gelieferten Produkte zu verbessern, u. a. mithilfe von:

- einer Gemeinschaft von Entwicklerinnen und Entwicklern, die innerhalb jedes Entwicklungsteams auf Sicherheitsthemen verweisen
- dedizierten Tools für die Sicherheitsüberprüfung des Codes
- einem gemeinsamen Referenzsystem (OWASP), das die Kapitalisierung von Sicherheitsthemen ermöglicht und die Verbreitung und Umsetzung guter Praktiken sicherstellt
- einer speziellen Sicherheitsüberwachung mit Newslettern zu Informationen, Aktualisierungen und Verbesserungen, die an die Teams gesendet werden

17.2. Abschottung der Umgebungen

Die Netzwerke und Infrastrukturen von Cegid sind physisch und logisch je nach angebotenen Service voneinander getrennt.

Die Plattform wendet zudem eine Trennung der verschiedenen Applikationsumgebungen (Entwicklung, Test, Vorproduktion und Produktion) an. Die Entwicklungsumgebung ist ausschließlich für Entwickler zugänglich und enthält keine Produktionsdaten, es sei denn, es wurde eine besondere vertragliche Vereinbarung mit dem Kunden getroffen.

Der Zugriff auf die Geräte erfolgt über eine Verwaltungsbastion oder eine virtuelle Bounce-Maschine für Teams mit den entsprechenden Privilegien.

17.3. Erwerb

Beim Kauf neuer Systeme werden die Sicherheitsbedürfnisse im Auswahlprozess berücksichtigt.

18. Beziehung zu Lieferanten

Cegid klassifiziert seine Lieferanten nach ihrer Kritikalität in Bezug auf die Bereitstellung von Kundendienstleistungen. Je nach Kritikalität werden verschiedene Kontrollen eingeführt, z. B.:

- Analyse der Sicherheits-Zertifizierungen
- Einrichtung von Überwachungsausschüssen mit Indikatoren für Wirksamkeit und Einhaltung der Sicherheitsmaßnahmen
- technische oder organisatorische Audits
- Einführung und Überwachung von Sicherheits-SLAs
- Einführung spezieller Sicherheitsklauseln in Verträgen
- Klärung der Rollen und Zuständigkeiten bei der Bewältigung von Incidents

19. Umgang mit Schwachstellen und Incidents im Bereich der Informationssicherheit

19.1. Umgang mit Schwachstellen

Die Schwachstellen werden nach CVSS V3.0 klassifiziert und werden standardmäßig gemäß folgender Tabelle behandelt:

Art der Anfälligkeit	CVSS-Score	Verpflichtung zu einem Aktionsplan
Low	0,1–3,9	Best Effort
Medium	4,0–6,9	Best Effort
High	7,0–8,9	7 Tage ab Erkennung
Critical	9,0–10	7 Tage ab Erkennung

Einige Produkte oder Dienstleistungen können höhere Verpflichtungen haben, die in den Serviceheften erwähnt werden.

19.2. Scanner für Schwachstellen

Scans des gesamten Internetperimeters des Informationssystems von Cegid werden regelmäßig, mindestens jedoch monatlich, über einen vom Cegid-Sicherheitsteam verwalteten Schwachstellen-Scanner gestartet.

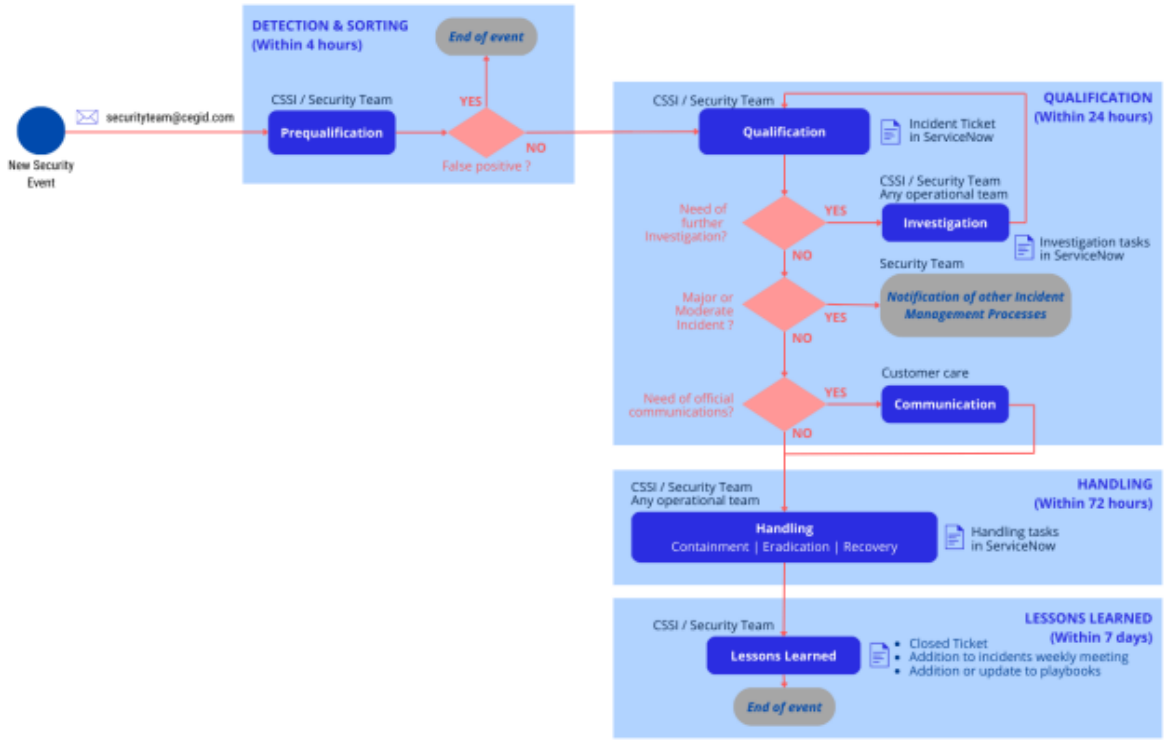
Mithilfe dieser Scans wird die korrekte Konfiguration von Hardware und Software überprüft, um das Auftreten von Schwachstellen zu erkennen.

Die Ergebnisse werden überprüft und sind Gegenstand spezifischer Aktionspläne.

19.3. Verwaltung von Incidents

Die Bearbeitung von Sicherheitsvorfällen wird durch einen Workflow in den ITSM-Tools von Cegid betrieben. Das Prinzip orientiert sich an den guten Praktiken, die in den Normen ISO 27001 und ISO 27002 zu finden sind.

Er wird wie folgt festgelegt:



Eine Mitteilung erfolgt innerhalb von höchstens 72 Stunden an die betroffenen Kunden und/oder Partner, sobald der betroffene Umfang beurteilt wurde.

Je nach Art des Aktionsplans kann Cegid auch mit den betroffenen Einheiten von Cegid kommunizieren, um die Behandlung des Incidents zu organisieren.

19.4. Krisenmanagement

Spezielle Pläne für das Krisenmanagement sind formalisiert.

Krisenszenarien werden durch eine Organisation und durch Prozesse gerahmt. Ein Verzeichnis für das Krisenmanagement wird beibehalten.

20. VERWALTUNG DER GESCHÄFTSKONTINUITÄT

20.1. Kontinuität der Steuerung

Ein Kontinuitätsplan wird für die Geschäftsführung und zur Steuerung der Dienste (Infrastruktur, Applikationen usw.) für die Cegid-Teams definiert.

Die Kontinuität dieser Aktivitäten beruht sowohl auf der Einrichtung belastbarer Architekturen der Steuerungssysteme als auch auf der Sicherheit der Laptops, die es jedem Mitarbeitenden/Administrator der Cegid-Teams ermöglicht, auf sichere Weise aus der Ferne und in Übereinstimmung mit den jeweils gewährten Rechten auf die Ressourcen und Tools zuzugreifen, die die Erbringung der Dienstleistung ermöglichen.

20.2. Geschäftskontinuitätsplan und Resilienz

Die Geschäftskontinuität wird standardmäßig bereits in der Konzeptionsphase, der von Cegid erbrachten Dienstleistungen berücksichtigt.

Der Business Continuity Plan (BCP) wird ganzheitlich definiert und umfasst eine menschliche, organisatorische und technische Komponente. Es wird auf die Ebene der einzelnen Geschäftsangebote heruntergebrochen und angepasst, um den geschäftlichen Einschränkungen und der technischen Architektur Rechnung zu tragen.

Die kritischen Ressourcen (Humanressourcen, Infrastruktur, Informationssystem, immaterielle Ressourcen) werden für jedes Geschäftsangebot identifiziert.

Der Geschäftskontinuitätsplan ist so konzipiert, dass er den geäußerten Bedarf an Kontinuität in Bezug auf die Verfügbarkeit von Diensten erfüllt.

Über die Konzeption der Widerstandsfähigkeit der technischen und Software-Architektur hinaus werden die operativen und organisatorischen Prozesse des Geschäftskontinuitätsplans definiert und im Hinblick auf kontinuierliche Verbesserung getestet.

20.3. RPO und RTO

20.3.1. RPO

RPO: Recovery Point Objective oder Wiederherstellungspunkt der Daten

Der RPO wird in den Service-Handbuch vermerkt. Standardmäßig beträgt er 24 Stunden.

20.3.2. RTO

RTO: Recovery Time Objective oder Wiederherstellungsdauer des Dienstes

Standardmäßig legt Cegid in den Servicehandbüchern kein RTO fest, aber für bestimmte Spezialangebote wird ein RTO garantiert (siehe Vertrag oder Service-Handbuch).

Bei einer schweren Katastrophe, die zu einer längeren Unterbrechung des Dienstes führt, verpflichtet Cegid sich, den Dienst so schnell wie möglich auf der Grundlage der am besten geeigneten Datensicherung wiederherzustellen.

21. COMPLIANCE

21.1. ISO 27001

Die Teams von Cegid beziehen sich bei der Gestaltung und dem Betrieb der für die Kunden bereitgestellten Dienstleistungen auf ISO 27001:2013. Die abgedeckten Zertifizierungen und Umfänge werden in Kapitel 5 aufgeführt.

Mit dem Ziel, eine Architektur und Infrastruktur anzubieten, die dem neuesten Stand der Sicherheitstechnik entspricht, stützt sich Cegid auf Rechenzentren und zugehörige Dienstleistungen, die nach ISO 27001 zertifiziert sind.

21.2. DSGVO und Schutz personenbezogener Daten

Cegid hat eine Datenschutz- und Cookie-Richtlinie erarbeitet, die auf der Cegid-Website verfügbar ist: https://www.cegid.com/fr/politique-de-confidentialite/

21.3. Audit

21.3.1. Internes Audit

Die Überwachung der Sicherheitsaktivitäten in den Zertifizierungsperimetern von Cegid wird von qualifizierten Beratern unter der Aufsicht der Sicherheitsabteilung durchgeführt.

Diese führen in geplanten Abständen eine Überprüfung der Elemente durch, die mit den zertifizierten Umfängen gemäß dem Auditplan von Cegid in Zusammenhang stehen.

Dokumente, die interne Prüfungen betreffen, sind vertraulich und dürfen nicht weitergegeben werden. Cegid verpflichtet sich, bei einer Nichtkonformität, die zu einer Verletzung der Sicherheit führt, mit dem/den betroffenen Kunden innerhalb des betroffenen Bereichs zu kommunizieren (siehe Kapitel 19.3).

21.3.2. Externes Audit

Im Rahmen der in Kapitel 5 aufgeführten Zertifizierungen wird Cegid jährlich von den Zertifizierungsstellen auf den Umfang der einzelnen Zertifizierungen geprüft.

21.3.3. Technisches Audit

Cegid lässt außerdem regelmäßig technische Audits des Informationssystems durch qualifizierte Experten durchführen.

Eine regelmäßige Planung dieser technischen Audits ist effektiv und ermöglicht es, jede strategische Applikation in einem Dreijahreszyklus zu testen.

21.3.4. Audit durch den Kunden

Kunden können unter den im Vertrag festgelegten Bedingungen auf die von ihnen genutzten Dienste Pentests vornehmen.

Organisatorische Audits können auch auf Initiative der Kunden durchgeführt werden. Sie unterliegen bestimmten Anspruchsvoraussetzungen und erfordern die Unterzeichnung besonderer Vertragsklauseln.