Cloud CERT

Testumgebung-Rahmen für die Ausübung zum Schutz kritischer Infrastrukturen

indra

CNPIC
CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

EUROPE *for business*

INTECO Instituto Nacional de Tecnologías de la Comunicación

Fondazione ICSA

Zanasi & Partners

KONTAKTDAT

http://cloudcert.european-project.eu
info@cloudcert.european-project.eu
http://en.wikipedia.org/wiki/CloudCERT

ERGEBNISSE FÜR CLOUDCERT TESTUMGEBUNG-RAHMEN FÜR DIE AUSÜBUNG ZUM SCHUTZ KRITISCHER INFRASTRUKTUREN

Bearbeitung:
Nationale Institution für Kommunikationstechnologie. S.A.
INTECO
Avenida José Aguado, 41- 24005 León
987 877 189
www.inteco.es

Bearbeitung 2013

Die elektronische Version verfügbar unter:
http://cloudcert.european-project.eu/

INDEX

HINTERGRUND und MOTIVATION

PROGRAMMÜBERSICHT

Die Sicherheit und Wirtschaft der Europäischen Union, sowie das Wohlleben ihrer Bürgern sind abhängig von bestimmten Infrastrukturen und Dienste, die von der anbietet sind. Der Zerstörung oder Störung der wichtigen Infrastrukturen und zentralen Dienstleistungen kann den Verlust von Menschenleben, den Verlust von Eigentum und den Zusammenbruch des öffentlichen und moralischen Vertrauens in die EU zur Folge haben.

2004 Zur Vermeidung dieser potentiellen Schwachstellen forderte der Europäischer Rat in 2004 die Entwicklung des Europäischen Programm zum Schutz kritischer Infrastrukturen (EPCIP). Seitdem wurde eine umfassende Arbeitsvorbereitung ausgeführt, die die Organisation von entsprechenden Seminare, die Vorlage eines Grünbuchs und Diskussionen mit den öffentlichen als auch privaten Projektbeteiligten und die Finanzierung eines Pilotprojekts einbezogen hat.

2006 In diesem Sinne hat die Kommission am Dezember 2006 eine Mitteilung über angenommen, die ein horizontaler Rahmen für die Maßnahmen zum Schutz kritischer Infrastrukturen auf EU-ebene geboten hat. Das vorgeschlagene EUProgramm "Prävention, Abwehrbereitschaft und Folgenbewältigung im Zusammenhang mit Terrorakten und anderen sicherheitsbezogenen Risiken" wurde am 12 Februar 2007 angenommen.

2008 Die Richtlinie des Rates 2008/114/EC zur Identifikation und Ausweisung Europäischer kritischer Infrastrukturen sowie zur Bewertung der Notwendigkeit, ihren Schutz zu verbessern hat das erforderliche Verfahren zur Ermittlung und Ausweisung kritischer europäischer Infrastrukturen (ECIs) eingeführt. Zugleich bietet sie einen gemeinsamen Ansatz für die Bewertung dieser Infrastrukturen, mit Blick darauf, sie zu entwickeln zum besseren Schutz des Bedarfs von Bürgern.

2009 Schließlich hat die Kommission am 30 Märtz 2009 eine Mitteilung über (Schutz kritischer Informations infrastrukturen) angenommen, sie berichtet über die wichtigsten Herausforderungen, die haben, und schlägt einen Plan vor, der darauf abzielt, ihr schutz zu verbessern.

HOME/2010/CIPS/AG/20

Das vorgeschlagene EUProgramm "Prävention, Abwehrbereitschaft und Folgenbewältigung im Zusammenhang mit Terrorakten und anderen sicherheitsbezogenen Risiken" fördert den Austausch von Fachwissen und bewährten Praktiken zwischen den verschiedenen Akteuren im Bereich der Durchführung von Krisenbewältigung maßnahmen sowie die Durchführung gemeinsamer Übungen, um die Koordinierung der zuständigen Stellen zu intensivieren.

Die Europäische Kommission arbeitet Jahresarbeitsprogramm aus, um die Prioritäten jedes Jahres abzudecken. Diese beinhalten Aufforderungen zur Einreichung von Vorschlägen um die Zuschussmaßnahmen zu bestimmen, die an transnationale und/oder nationale Projekte vergegeben werden, die einen Beitrag zur Leistung der allgemeinen als auch spezifischen Ziele der Programms sollen.

Als Folge dieses Programms 2010 Aufforderungen zur Einreichung von Vorschlägen, wurde das Projekt “**CloudCERT**” ausgewählt, als eins der vergebenen Projekte.

MOTIVATION

Wie in EPCIP festgestellt, die Projektbeteiligte müssen Informationen über (CIP) teilen, insbesondere über die Maßnahmen der Sicherheit kritischer Infrastrukturen und geschützter Systeme, Studien über gegenseitige Abhängigkeiten und CIP-bezogene Schwachstellen, Bedrohungen und Risikobewertungen. Gleichzeitig muss sichergestellt werden, dass die geschützte, "sensible" oder persönliche Informationen, nicht veröffentlicht werden. und dass die Verarbeitung von Verschlusssachen eine angemessene Sicherheitsüberprüfung von dem Mitgliedstaat haben wirden.

Um diese wirkliche Notwendigkeit zu lösen, zielt CloudCERT Projekt darauf, der sichere Informationsaustausch mit einem Testumgebung-Rahmen anzubieten. Um einheitliche Koordination zu üben, damit die gleiche Kommunikationsprotokoll-Standards zu verwenden, um Verbesserung der Sichtbarkeit des gemeinsamen Gefahrenbewusstsein, der Schwachstellen, Sicherheitshinweise und Warnung CIP-spizifisch.

Um dieses Ziel zu erreichen, muss eine wichtige Arbeit eingeführt werden; die Definition von sicheren Informationsaustausch, Informationsstandards und Protokolldefinition; Design der Testumgebung-Plattform und Umsetzung; zum Schluss, Einsetzen eines Piloten, um zu überprüfen, dass die Wirklichkeit beruhend auf Benutzer-Case-Szenarien ist.

Der Bereich dieses Projekts ist beschränkt auf die Kreation der CloudCERT Pilot-Plattform um die CIP Informationen auszutauschen, deshalb deckt er nur die erste Stufe der Roadmap in der langfristigen Exposition ab.

Die letzte Plattform ist einer Operativer Pilot mit Kommunität von Benutzer und Informationen, die nützlich genug ist, um ihre Funktionalität zu testen und Simulationsübungen für den CIP Informationsaustausch auszuführen.

Die Plattform ermöglicht den Austausch von CIP operativen Maßnahmen, Methoden, Erfahrungen und Know-how zwischen den Benutzer, die als Repository für Information handelnd, diese Information sind:

- Vulnerabilität.
- Notizen, Kündigungen und Warnung.
- Gefahrenbewusstsein.
- Nachrichten.
- CIP beste Praktiken.
  CIP Erfahrungen.

Die CloudCERT Plattform ist technisch in Web-Anwendungen ansässig mit Benutzerverwltung und beinhaltend starker Authentifikation und sicheres Informationsaustausch nach interperabelen Standards

PROJEKT BESCHREIBUNG

BETEILIGTE

KOORDINATOR

- INTECO - Nationale Institution für Kommunikationstechnologie.

MITBEGÜNSTIGTEN

- CNPIC - Nationalzentrum für den Schutz kritischer Infrastrukturen.
- Europe for business.
- Fondazione Intelligenz-Kultur und strategische Analysen (ICSA).
- Indra Systems, Inc.
- INTECO - Nationale Institution für Kommunikationstechnologie.
- Zanasi & Partners.

ANWENDERPARTNERN

- INTECO - Nationale Institution für Kommunikationstechnologie.
- CNPIC - Nationalzentrum für den Schutz kritischer Infrastrukturen.

INTECO Instituto Nacional de Tecnologías de la Comunicación

CNPIC
CENTRO NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

EUROPE for business

Fondazione ICSA
Intelligence Culture and Strategic Analysis
Cultura dell'Intelligence e Analisi Strategica

indra

Zanasi & Partners

ZIELE

- Anbieten eines **Testumgebung-Rahmens** um die Mechanismen der Koordinierung der Anstrengungen von Partnerschaften und Aktionäre zu integrieren. Damit Informationen zu CIP und ihre Sicherheitsaspekte wirksam ausgetauscht werden.
- Um **die EU Infrastrukturen zu sichern**, Verbesserung des Verständniss der Beziehungen zwischen ihren Elementen und der Verbindungen zwischen Risikomanagement und Infrastrukturschutz.
- Anbieten der benötigen Kapazität **um die Potentielle Schwachstellen der kritischen Infrastrukturen zu vermeiden**, wobei Austausch der Schwachstelleninformationen .
- **Verwaltung der Sicherheit** im Ganzen mit Hilfe von vereinigtem Prozess für Informationsasutausch. in dessen Verlauf Gefahren erkannt werden und Maßnahmen zur Minderung der Gefahr auf ein bestimmtes, annehmbares Ausmaß zu einem akzeptablen Preis beschlossen und durchgeführt werden sollen.
- **Um einen Wert u erhalten**, der von ihrem Informationsautausch abgeleitet wird, durch Ausübung der Durchführung. Dieser Wert wird nach Wirksamkeit der Verhinderung, Bekämpfung und die Reaktion auf Cyber-Angriffe auf Kontrollsysteme innerhalb der kritischen Infrastrukturen abgemessen.
- **Eine gemeinsame Berichts-und Informationsaustausch** über die sechs Phasen des CIP-Lebenszyklus, um eine umfassende Lösung zu erstellen.

VORTEILE

Die **erwartete kurzzeitige Wirkung** ist die CIP-Körper mit einer Testumgebung-Plattform anzubieten, um die CIP Informationsaustausch, Koordinierung und die Aufsicht der Mitgliedsstaaten zu unterstützen.

Mittelfristig wird CloudCERT die Zusammenarbeit durch Umsetzungs-Plattform in einer realen Produktionsumgebung verbessern. Es wird auch zu Minimierung der Zusammenarbeitshindernisse für CIP-Betreiber und Schutzbehörden in verschiedenen Ländern in Europa beitragen.

Langfristig soll diese Zusammenarbeit zur Einrichtung einer Europäischen inneren Sicherheitsumgebung für den Schutz der europäischen CIs beitragen.

ZIELGRUPPEN

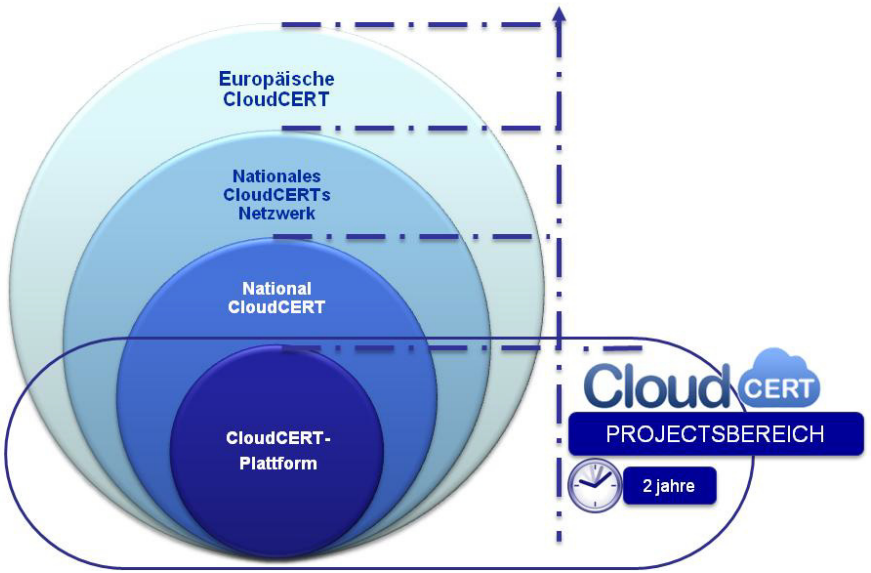
Die wichtigste Zielgruppen und Nutznießer dieses Projekts sind:

- Mitgliedstatten der Schutz kritischer Infrastrukturen zuständigen nationalen Behörden.
- CERTs or CSIRTS kompetent in CIP.
- Betreiber oder Besitzer der kritischen Infrastruktur (CI).

CloudCERT

Testbed Framework to Exercise
Critical Infrastructure Protection

EUROPÄISCHE DIMENSION UND ROADMAP



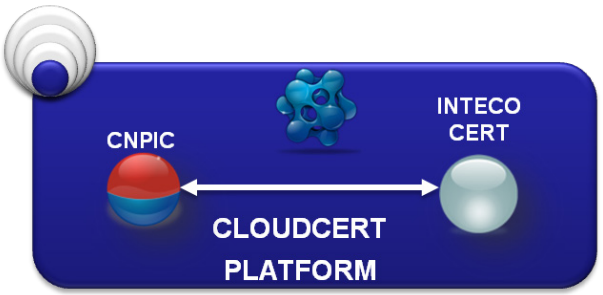
CloudCERT ist ein **transnationales projekt**, das Partner partners in mindestens zwei Mitgliedstaaten umfasst.

Der Ansatz des Langfristigen Projekts kann die fogende Roadmap mit der folgenden Stufen berücksichtigt werden:

- CloudCERT- Plattform.
- National CloudCERT.
- Nationaesl CloudCERT- Netzwerk.
- Europäische CloudCERT.

Um ein paneuropäisches Kollaborationsnetzwerk aufzubauen, schlagen wir eine Methodologie vor, die auf aufeinanderfolgenden inkrementalen Ansätze, erzeugenden Produkte in Phasen basiert, die in jeder Interaktion verbessert werden. Während der Laufzeit des Projekts (2 Jahre) wird nur die Pilot-Plattform, mit dem Ziel vor Augen ein National CloudCERT aufzubauen, erstellt.

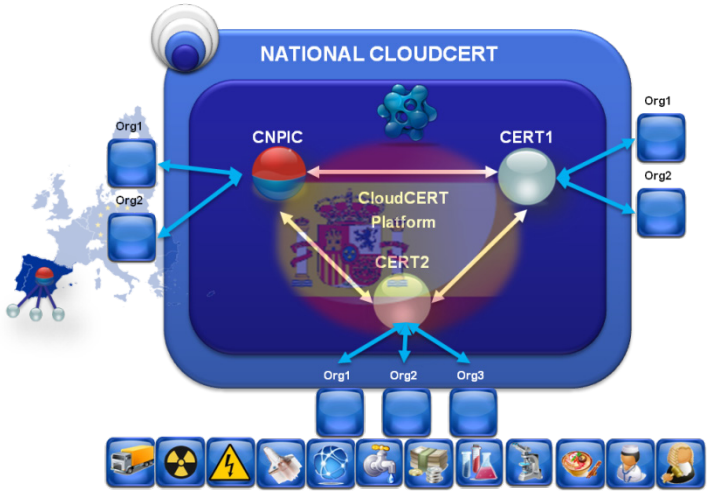
PHASE 1 – CLOUDCERT-PILOT (ZURZEIT VON EU GEWÄHRT)



In der erste Roadmap-Phase ist die Ziel Erstellug der Pilot-Plattform, um sie als Benutzer der Plattform, CIP Akteure innerhalb eines Landes addiert zu werden

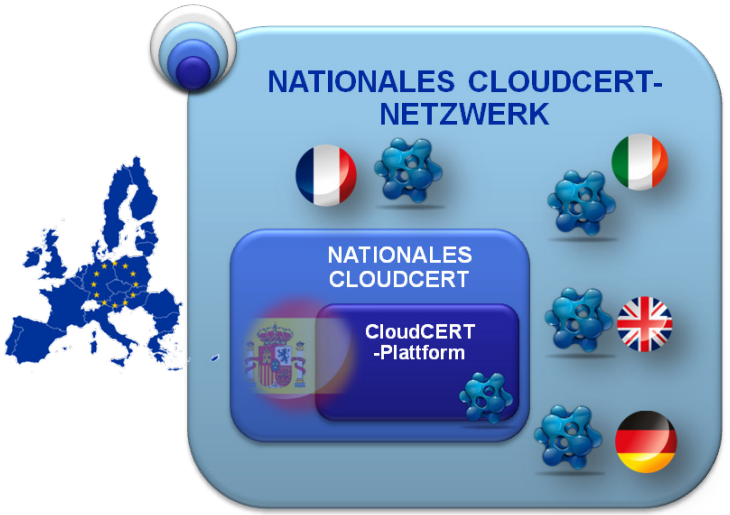
Aufgrund der Einschränkungen des Projekts werden die Benutzer dieser Plattform die CERTS- Beteiligte des (INTECO-CERT) Projekts sowie der teilnehmenden nationalen PIC Zentren (CNPIC) sein.

PHASE 2 - NATIONAL CLOUDCERT (GELEGENHEIT)



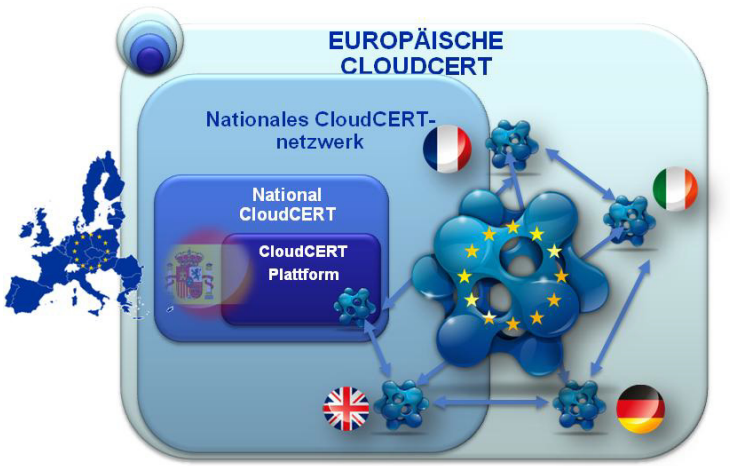
Wenn Pilot freigegeben wird, würde dies zur Exploitation der Plattform-Stufe führen. Dieser abschnitt kann in dieser Stufe beginnen, dabei mit dem Einsatz der Plattform in einer realen Produktionsumgebung mit dem Ziel der Gründung eines Nationalen CloudCERT, die das nationales CIP Zentrum sowie Haupt-CERTS mit CIP-Möglichkeiten und andern möglichen Akteuren der Interrese und Relevanz integriert.

PHASE 3 – CLOUDCERT-KNOTEN (GELEGENHEIT)



Die nächste Roadmap-Stuffe könnte die Replication ohne Schwierigkeiten in anderen Mitgliedsländern sein, um nationale CloudCERT-Knoten zu erstellen. Die Differenzen des Regelungsrahmens in dem einzelnen Staat können den Informationsaustauch bestimmen. Es wäre wünschenswert, kleine Qualifikationen oder Bedingungen

PHASE 4 - EUROPÄISCHE CLOUDCERT (GELEGENHEIT)

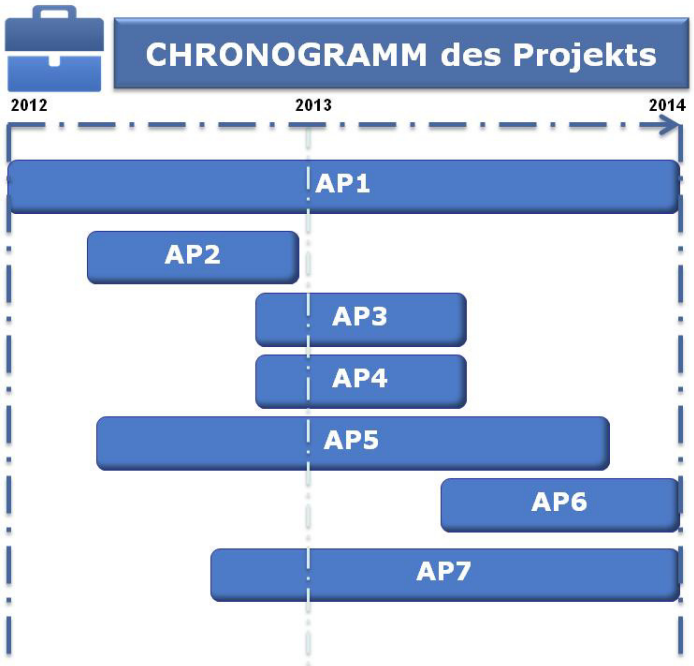


Wenn diese Roadmap-Stufen den Erfolg haben, könnte eine finale Phase die Verbindung der nationalen CloudCERT Knoten, Bildung des Europäischen CloudCERT mit der Summe aller nationalen Mitglieder, oder paneuropäisches CloudCERT mit dem Nationalen CIP-Zentrum repräsentieren.

hinzufügen, um die Plattform zu verbessern, aber nicht dramatische Änderung ihres Hauptzwecks.

ARBEITSPAKETE

ARBEITSPAKETE-ÜBERSICHT



AP1: PROJEKTMANAGEMENT

- Koordinierung der Partner und ihrer Arbeit.
- Risikomanagement.
- Finanzmanagement.

AP2: KONZEPTIONELLE MODELLIERUNG UND ARCHITEKTUR

- Die Systemarchitektur auf Basis des Systems der konzeptionellen Definition der CloudCERT-Plattform zu entwickeln.

AP3: INFORMATIONS UND KOMMUNICATIONSTANDARDS

- Die Definition des Inhalts und das Format der information werden ausgetauscht.
- Definition des Protokolls zum Informationsaustausch

AP4: DEFINITION DES SICHEREN RAHMENS

- Um die derzeitige Arbeitsmethoden des sicheren Managements und den Austausch der sensitiven Informationen zu untersuchen und endlich wird eine Liste von erforderlichen Funktionen gemacht.

AP5: PLATTFORMENTWICKLUNG

- Um eine sichere Teilung des sensitiven informationsaustauschs, Katalogs und der Datenbank der CIP-Schwachstellen zu entwickeln.

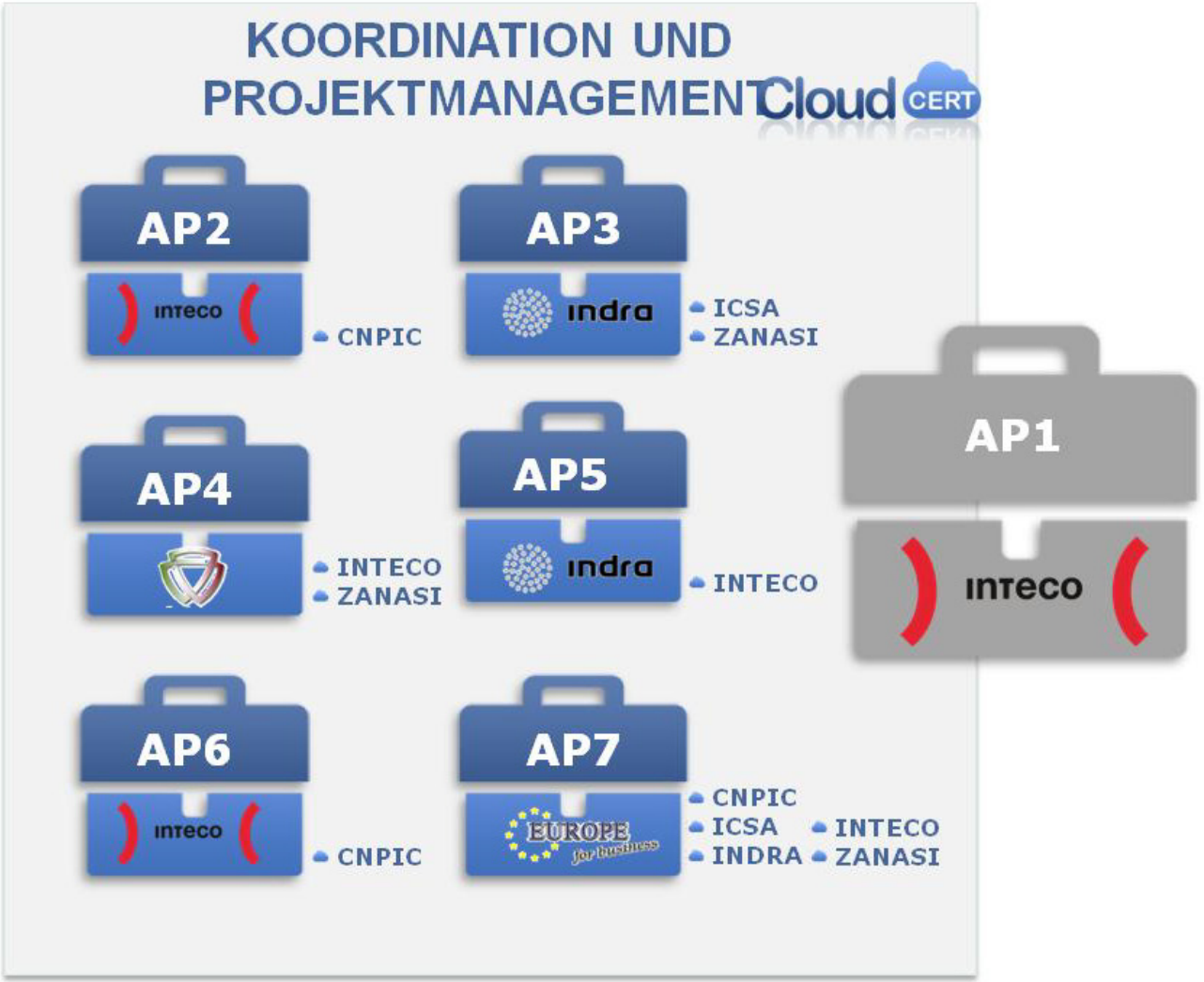
AP6: PILOTVERSUCH

- Um das Plattform-Tool auf Basis der Integration der Benutzersfälle zu testen.

AP7: VERBREITUNG DER PROJEKTERGEBNISSE

- Verbreitung der Projektergebnisse durch Publikationen, Konferenzen und Seminare.

AP1. PROJEKTMANAGEMENT



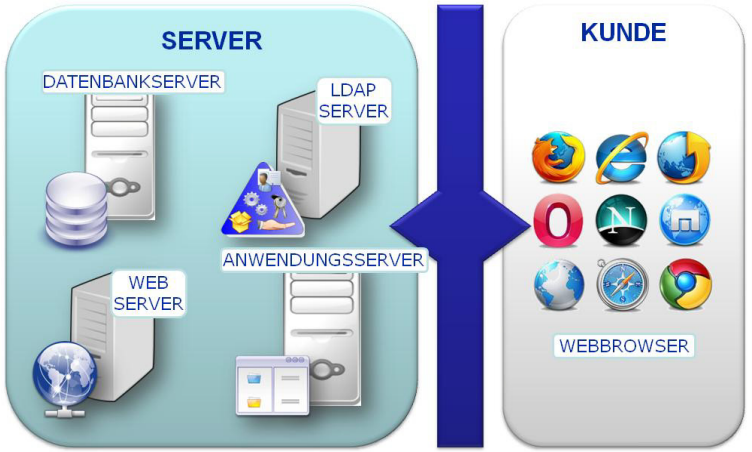
INTECO, als einer Koordinator des CloudCERT Projekts, ist verantwörtlich für die vollendung aller anderen Arbeitspakete und leitung der Projektmanagement-Aktivitäten.

AP2. PLATTFORM-DESIGN

ARCHITEKTURMODELL

CloudCERT basiert auf Kunde- / Server-Architektur. Das Modell der unterschiedlichen Komponenten der CloudCERT- Plattform basiert auf den J2EE-standard.

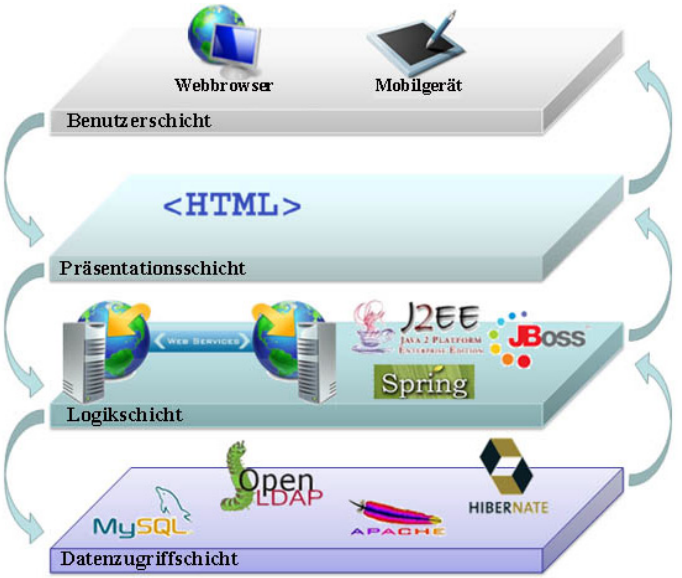
ARCHITEKTURMODELLS



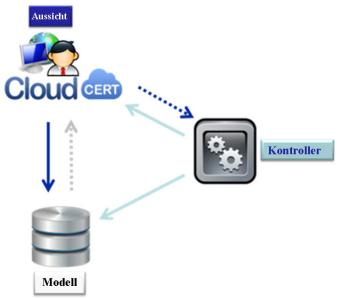
LOGISCHES MODELL

Die Komponenten des logischen Modells sind in der folgenden Typen gegliedert:

- **Daten-Persistenz.** CloudCERT hat ein komplexes Datenmodell. Um mit diesem Modell umzugehen, werden manche Rahmen benutzt, um das Modell in einer effizienten Weise zu verwalten.
- **Anwendungssicherheit.** Alle Arbeitsschritte der Anwendungssicherheit basierten auf die LDAP-Informationen.
- **Flusskontrollmanagement der Anwendung**. CloudCERT verwendet den Struts-Rahmen. Struts sind ein Support Tool für die Entwicklung der Web-Anwendungen nach MVC Standard nach J2EE-plattform.
- **Web-Services**. Sie werden in AXIS CloudCERT eingesetzt. AXIS ist eine SOAP Implementation, die von Apache entwickelt wird, und OASIS and W3C Standards entspricht.
- **Darstellungsschicht**. Die basiert auf der Verwendung der Rahmen: Struts und DWR.



MVC ÜBERSICHT

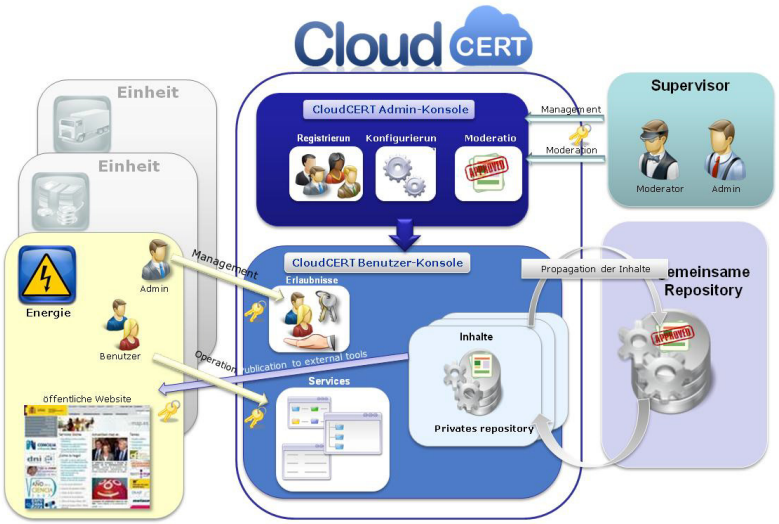


In Folge der überwiegenden Mehrheit der bestehenden J2EE-Anwendungen, der MCV wurde in der CloudCERT-Plattform adoptiert.

FUNKTIONELLER AUFBAU

Die Anwendungen und Module der CloudCERT-Plattform enthalten:

- **CloudCERT-Authentifizierungsmodule**: Zentraler Authentifizierungsdienst (CAS).
- **Passwort-Management-Module**: Ein Module für die Verwaltung der Passwortänderung und die Aktivierung der Benutzerkonton.
- **CloudCERT-Benutzer-Konsole**: Anwendung der Verwaltungskonsole für verschiedene Einheiten.
- **CloudCERT-Administrationskonsole**: Anwendungsmanagement für CloudCERT-Plattform (Services, Web-Services, Einheiten, and Inhalte).
- **CloudCERT-WEB-Services.**



SICHERHEIT

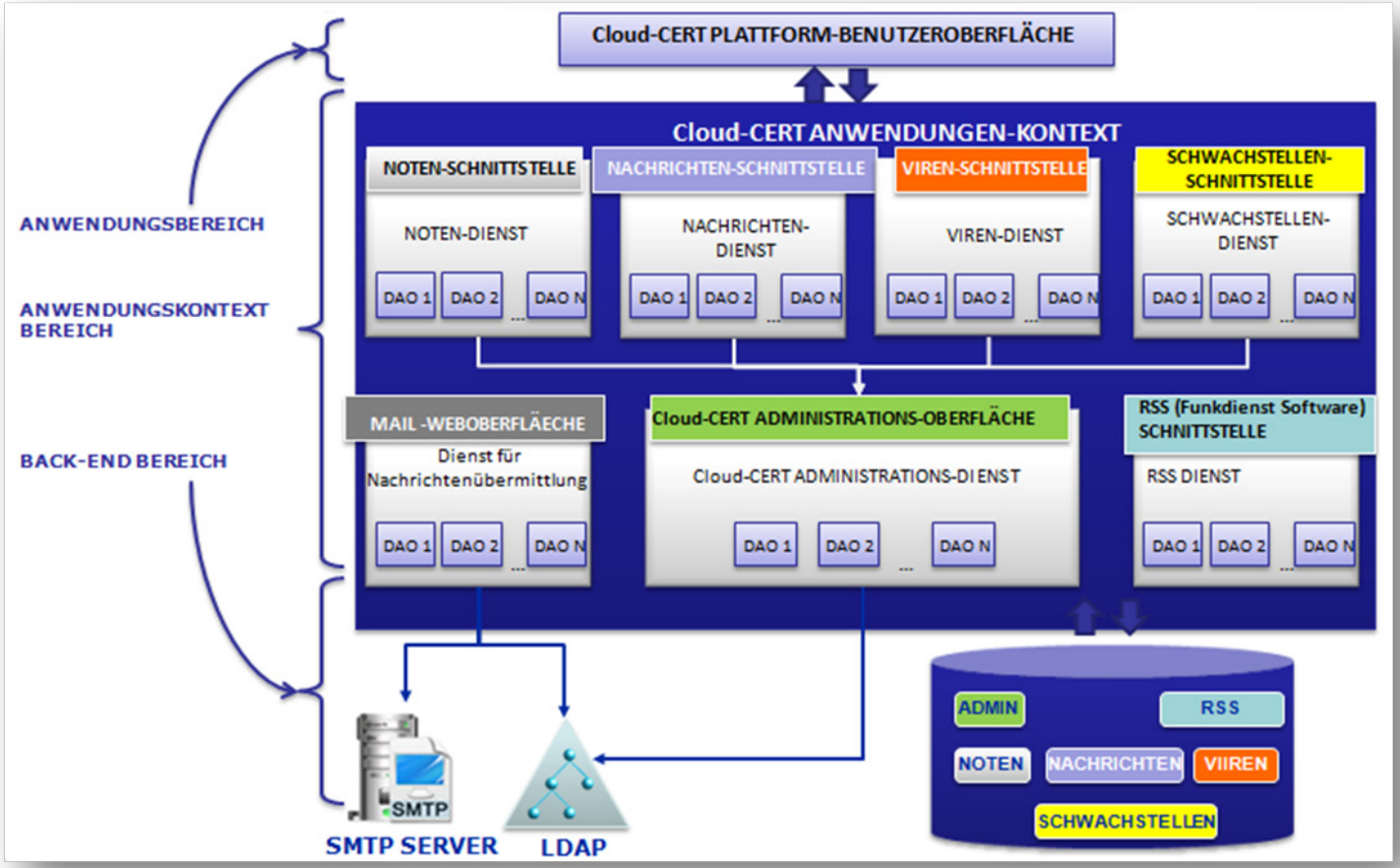
Alle Fragen bezüglich der **Sicherheitsanwendung** basierten auf LDAP-Information. Die folgende Rahmen wurden benutzet, um die CloudCERT-Sicherheit zu verwalten:

- **Spring Security.** ein Module, das zum Spring-Rahmen gehörend ist, es ermöglicht die Anwendungslogik Sicherheitscode zu erhalten, Authentifikation und Autorisierungsmechanismen für J2EE-Anwendungen anzubieten. Außerdem ünterstützt Spring Security die Authentifikation beim zentralen Authentifizierungsdienst (CAS), bietet dem Kunden API an, um mit dem CAS-Server zu interagieren.

- **Spring LDAP.** ein Module, das zum Spring-Rahmen gehörend ist, es bietet Interaktionsmechanismen an, um die Operationen beim jeden Typ vom LDAP-Server zu erleichtern .

GESAMTKONTEXT-DESIGN

Mit der Verwendung der Persistenz der Datenbank LDAP, hat CloudCERT einen globalen Kontext definiert, der von verschiedenen Anwendungen zugänglich ist.



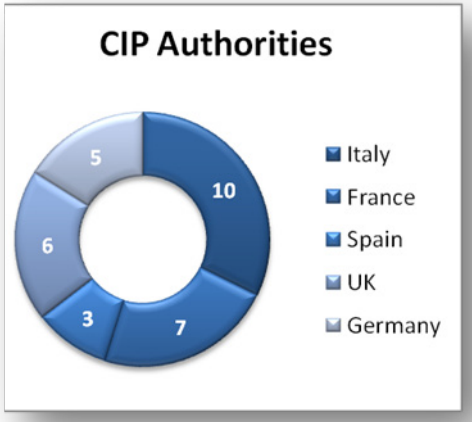
- **Anwendungsbereich.** Wo alle Präsentationslogik und Flusskontrolle inbegriffen sind .
- **Anwendungskontext-Bereich.** Der Kontext, der die verschiedene Services zu den Anwendungen, die sie unterstützt, oder anderen Services definiert. Diese Services sind von öffentlichen Schnittstelle angeboten.
- **Back-End Bereich.**
  - CloudCERT-Datenbankplattform.
  - CloudCERT-LDAP.
  - SMTP-Server.

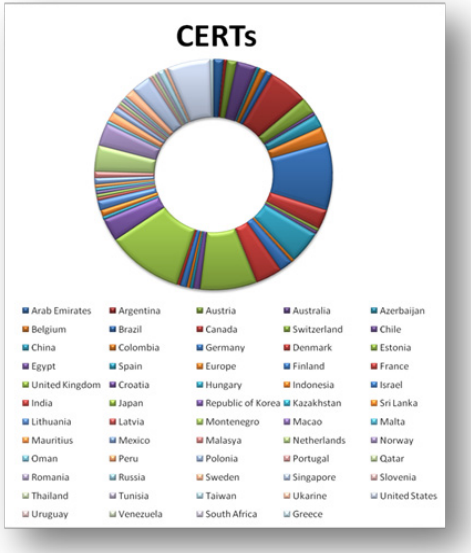
AP3. INFORMATIONS UND KOMMUNICATIONSTANDARDS

INFORMATIONSINHALTE -ONTOLOGIE

- **Notizen:** Verwalten und Teilen aller Informationen, die mit institutionellen Ereignissen der allgemeinen Interesse von CERT verbunden sind, in der Netzwerk der CloudCERT-Plattform.
- **Nachrichten:** Einführen, Verwalten und Teilen aller öffentlichen Nachrichten, die als allgemeine Interesse betrachtet werden.
- **Warnungen:** Einführen, Verwalten und Teilen aller Fälle, die als Alarmsignale mit besonderer Interesse betrachtet warden.
- **Viren:** Einführen, Verwalten und Teilen aller Viren, die besondere Interesse haben.
- **Schwachstellen/ Vulnerabilität:** Einführen, Verwalten und Teilen aller Schwachstellen, die besondere Interesse haben.
- **RSS ITEMS:** Konsultieren aller RSS items, die als besondere Interesse betrachtet werden.

POTENZIELLE BENUTZER FÜR CLOUDCERT





PROTOKOLLE FÜR INFORMATIONSAUSTAUCH- UND INFORMATIONSBESCHREIBUNG-STANDARDS

Allgemeine Zwecke- Technologien für Informationsaustauch

Unter dem breiten Spektrum an den **Protokollen des Informationsaustauschs**, die im Laufe der Jahre entwickelt wurden, wurden 3 Protokolle ausgewählt, aufgrund ihrer breiten Nutzung verschiedener Arten der Orginationen, und auch ihrer Flexibilität. Diese Protokolle können erfolgreich mit dem CloudCERT-Kontext genutzt werden:

- EDI (Elektronischer Datenaustausch).
- XML (Erweiterbare Auszeichnungssprache).
- SOAP (Einfaches Objekt- Zugriffsprotokoll).

Informationsaustauschs- Standards spezifisch für Sicherheitszwecke

Das CloudCERT- Projekt konzentriert sich besonders auf Helfen der Administratoren der kritischen Infrastrukturen und kritischen Informationsinfrastrukturen, um sich besser gegenüber der Androhungen der cyber-Sicherheit zu schützen. Die Sicherheitsmängel sind (und werden in der Zukunft) eine Drohung für die Operation der IT-Infrastrukturen.

Sobald werden neue Mändel erkennt. Informierung der Benutzer und Administratoren über die erkennte Fälle ist eine wichtige Aufgabe für IT-Anbieter und Sicherheit-Teams.Die allgemeine Weise dieser Informationen zu verbreiten ist durch Sicherheitswarnungen, technische Dokumente, die detailliert die Eigenschaften der Fälle ihre potentielle Auswirkungen zu beschreiben und auch eine Liste von möglichen Lösungen anzubieten.

Dieser Teil konzentriert sich auf die beliebteste **Standardformaten für die Sicherheitswarnungen**:

- **CAIF** (Austauchformat der allgemeinen Ankündigung).
- **EISPP** (Europäisches Programm der Informationssicherheit-Promotion) das allgemeine Warnungsformat.
- **DAF** (Deutsches Advisory Format).
- OpenIOC (offene Ausgleich-Indikatoren).
- **IODEF** (Incident Object Description Exchange Format).
- **VERIS** (Vokabeln für Eventaufnahme und Incident - Teilung).
- **STIX** (Informationsausdruck für strukturierte Drohung).

ALTERNATIVE LÖSUNGSPLAN

Auswertung des Inhaltsaustauschs

Inhalte, die würdige information über Alarmsignale enthalten, sind ausreichend, um mit **SOAP** (Einfaches Objekt- Zugriffsprotokoll) über **HTTPs** (Hypertext-Übertragungsprotokoll) übertragen zu werden:

- Warnungen.
- Viren.
- Schwachstellen.

Die folgende Inthalte sind jedoch nicht ausreichend, um teilen zu werden:

- **Notizen**. Dieser Inhalt wird von CloudCERT-Benutzer verwendet, um die Information , die auf CERTs-institutionellen Events bezogen sind, in die eigene Netzwerk-Plattform zu teilen.
- **Nachrichten**. Dieser Inhalt wird von CloudCERT-Benutzer verwendet, um URL links, die auf CERT-öffentlichen Nachrichten bezogen sind, besondere Interesse außerhalb der eigenen Netzwerk-Plattform zu teilen.
- **RSS Items**. Dieser Inhalt wird von CloudCERT-Benutzer verwendet, um RSS items aus verschiedenen öffentlichen feeds zu teilen.

Indikatoren

Es ist wichtig alle teilende mit anderen Orginationen Inhalte vorsichtig zu verwalten. Für diesen Zweck wäre Dashboard-Module erforderlich in der CloudCERT-Plattform zu integrieren. Das ermöglicht den Administrator, ein Zahl von Indikatoren zu patrouillieren.

Die Indikatoren waren:

- Anzahl der Elemente, die in einem bestimmten Zeitraum hergestellt werden.
- Anzahl der Elemente, die in einem bestimmten Zeitraum gelesen werden.
- Die Top N meistgelesene Inhalte.
- Die Top N der aktivsten-Hersteller Organisationen.
- Die Top N der aktivsten-Leser Organisationen.
- Die Top N der aktivsten-Importinhalten Organisationen. (von gemeinsamen Repository nach eigenen Repository)
- Monatliche Distribution der aktivsten Tage der Herstellung/ Verbrauchen der Inhalten.

AP4. DEFINITION DES SICHEREN RAHMENS

DIE ARBEITSMETHODEN DES SICHEREN MANAGEMENTS UND DEN AUSTAUSCH DER SENSITIVEN INFORMATIONEN

Die CloudCERT-plattform soll den Austausch der sensitiven Informationen betreffend CIP durch verschiedene Arten von Stakeholder mit Sicherheitsgarantien zu erleichtern. Daher ist die erste Aktivität der Arbeitspakete eine Umfrage, um die Arbeitsmethoden für sichere Bedienung und Teilung der sensitiven Informationen zu untersuchen.

INFORMATIONSSICHERHEIT

In diesem Teil wird die Domain der Informationssicherheit und ihre wichtige verbundene Fälle mit einem besonderen Fokus auf Informationssysteme eingeführt.

- **Vertraulichkeit**: die missbräuchliche Offenbarung sollte aufgedeckt und verhindert werden.
- **Integrität**: Die Informationen sollten nicht durch unautorisierte Subjekte modifiziert werden.
- **Availability**: Die Informationen sollten verfügbar für die autorisierte Subjekte werden, immer wenn sie verlangt werden.

INFORMATIONSAUSTAUSCH FÜR CIP

Dieses Kapital überprüft, was getan wurde, um effektive Informationsautauch im Kontext des CIP von den Regierungen der zwei wichtigsten Länder in der welt (Vereinigte Staaten, Vereinigtes Königreich) zu ermöglichen.

Schutz kritischer Infrastrukturen

Zwei Länder wurden als Beispiel genommen und ihre CIP-Pläne detailliert beschriebt und analysiert.: Die Policen sind elaboriert von der Vereinigten Staaten und Italien:

- Nationale Strategie des Heimatschutzes.
- Der Italienische Nationale Strategische Rahmen für die Sicherheit des cyber-spaces.

CLOUDCERT-SICHERHEITSANFORDERUNGEN

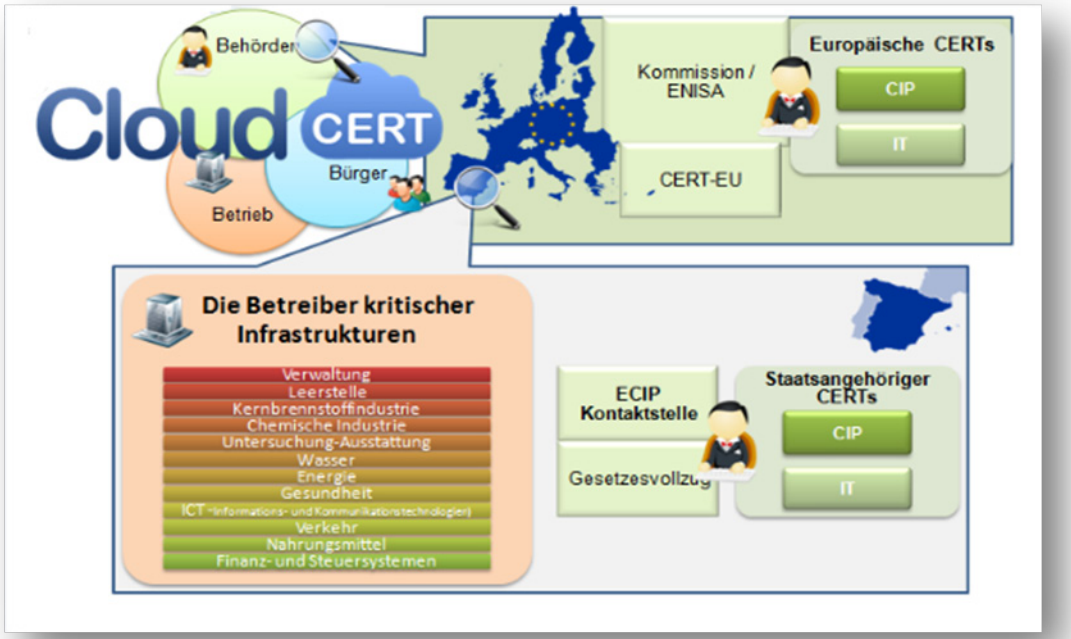
Hauptziele dieses Arbeitsergebnisses sind:

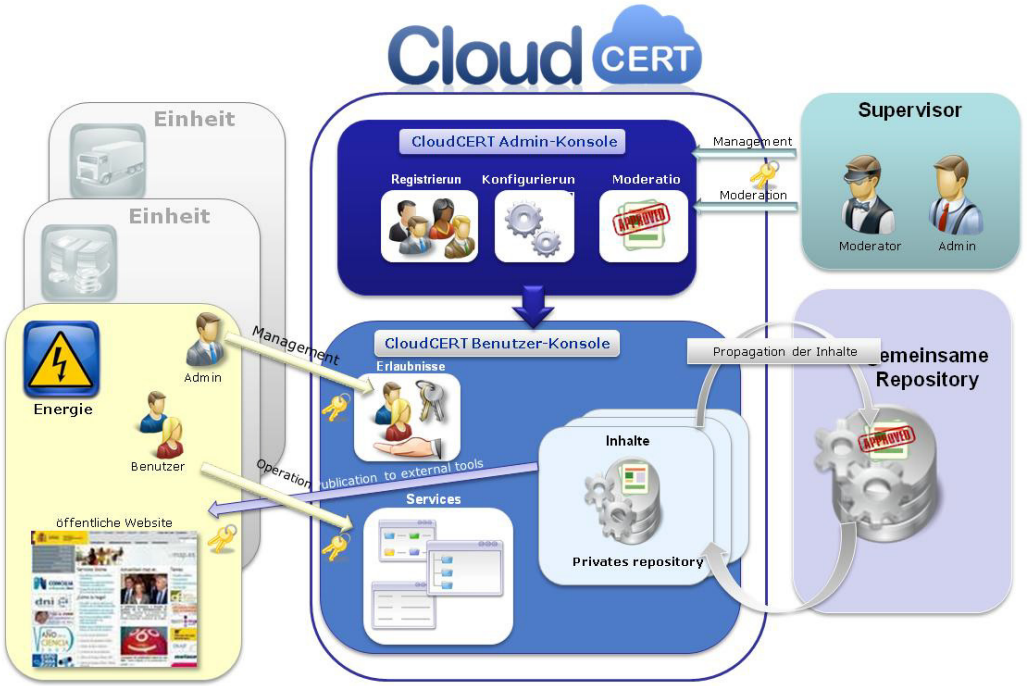
- Identifizierung der wichtigsten wissenschaftlichen Quellen auf dem Gebiet der PIC.
- Identifizierung der hypothetischen Methoden und Prozeduren um kollaborative Prozessen des systems zu erweitern und verstärken.
- Identifizierung der hypothetischen Methoden und Prozeduren um die Koordinierungskapazität zwischen den System-Stakeholders während des Lebenszykluses des IC zu erweitern und verstärken.

Alle mit dem Endziel dem Ausbau des Betriebsmodells der Regierung um die Rollen, Verantwortlichkeiten und Ziele des System-Stakeholders zu bestimmen.

The CloudCERT-Stakeholders werden in drei Hauptkategorien unterteilt:

- **Autoritäten** (öffentlicher Sektor): Die Autoritäten sind kompetent in der Informationssicherheit und den Schutz kritischer Infrastruktur einschließlich der rechtlichen operativen Ebene. Hierin beinhaltet die politische Entscheidungsträger und Regulierer sowie die Strafverfolgungsteam.
- **Industrie** (öffentlicher Sektor): Die Schutz kritischer Infrastrukturen einschließlich ihrer wichtigsten Anbieter (Produkthersteller und Diensteentwickler).
- **Bürger** (Zielgruppe): Konsumenten der Services, die von der kritischen Infrastrukturen angeboten sind.





Diese Stakeholders interagieren mit der CloudCERT-Plattform, die basierend auf Model der Regierung reguliert sind, wie unten dargestellt ist:

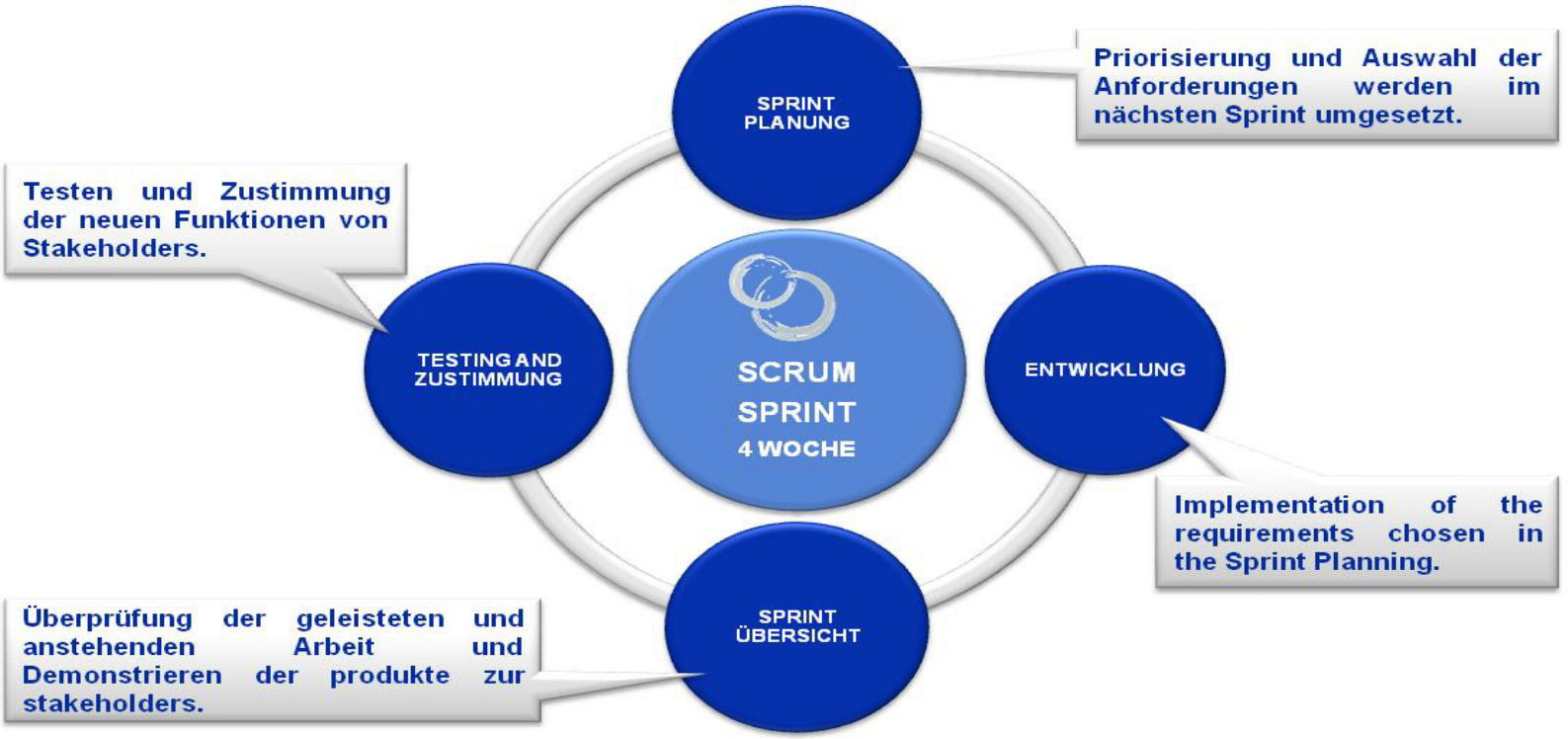
- Verschiedene Einheiten können die Plattform zugreifen: CERTs, Strafverfolgungsteams, und Betreiber der kritischen Infrastrukturen . Jede Einheit hat ihr eigene Space um die Inhalte zu ordnen und die Inhalte aus dem geteilten Repository importieren zu können. Sie können automatisch die Inhalte zu externen Tools wie ihre eigene interne Website exportieren.

- Einer **Organisation-Supervisor**:
  - **Verwaltet** die Plattform durch Registrierung der Organisation und ihres Administrator-Benutzers sowie durch Konfigurierung und Verwaltung der verfügbaren Services. Supervisor Konfiguriert die Einheitenberichtigung zu Inhalten und Services.
  - Bietet **moderation an**. Alle Inhalte, die ein Teil des geteilten Repository sind, müssen gegen Moderator-Aufsicht verbreitet werden. Die Moderation enthält auch Publikationen in Tools wie Foren, wiki, usw.

- Jede Einheit hat einen **Administrationsbenutzer**, wer die Benutzer erstellen und die Berichtigungen seiner/ ihrer Einheit bestimmen können.Die Inhalte des privatn Repositorys der Enheit können in einem geteilten Repository mit der Zustimmung des supervisors veröffentlicht werden..
- **Benutzer** können mit den Inhalten und Plattform-Services interagieren**.**

AP5. PLATTFORMENTWICKLUNG

Während der Phase des Pilotprojekts umgesetzt wird, werden die Folgende Aufgaben geschafft:



ANFORDERUNGEN UND ANALYSEN

Die Softwareanforderungsspezifikation darauf zielen:

- Bestimmung der Anforderungen und Funktionalitäten der CloudCERT-Plattform.
- Verbindung der Anforderungen des Sicheheitsrahmens und Austauschs der sensitiven Informationen.
- Difinieren Und Priorisierung der Anforderungen der CloudCERT-Plattform.

ENTWICKLUNG

Nach des Agil-Methodik-Scrums, umfasst die Entwicklungsphase:

- Umsetzung der vorherige gennante Anforderungen, um funktionallen Pilot zu erstellen.
- Erstellung der Benutzers- und Administrationsdokumentation des entwickelten Pilots.

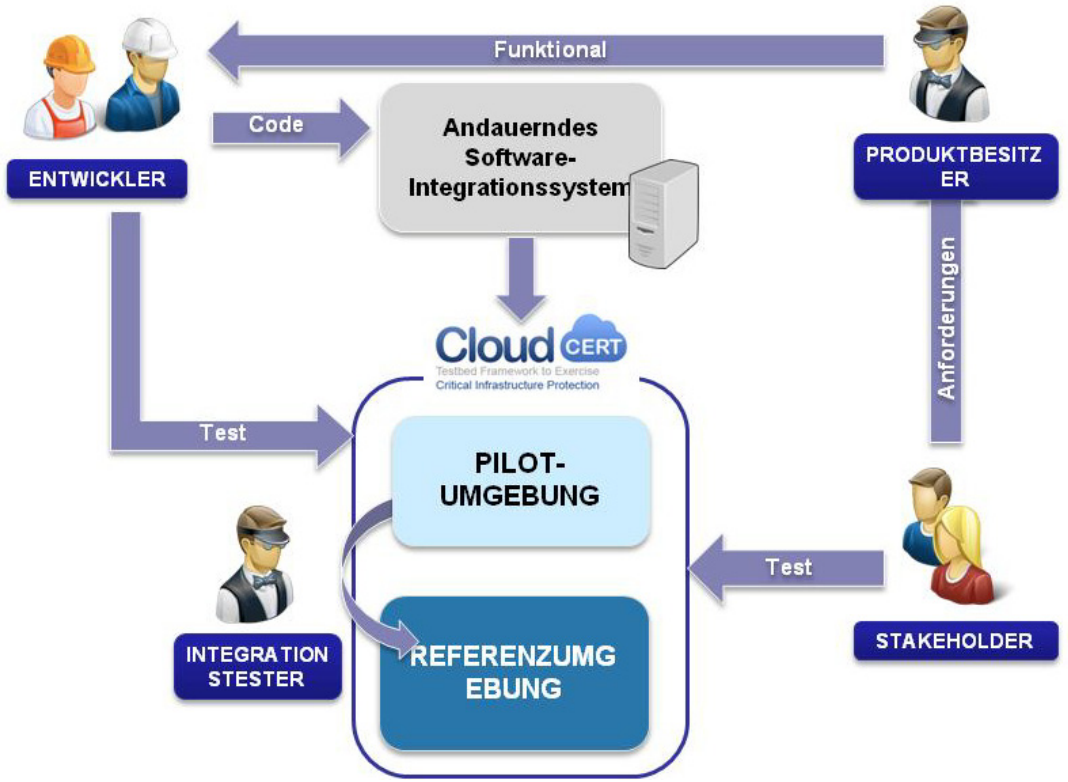
PLATTFORM-SETUP UND KONFIGURIERUNG

Während dieser Phase sind die Entwicklungs- und Überprüfungsumgebungen angeboten und die Installations und Konfigurationshanbuch erstellt.

UMGEBUNGEN

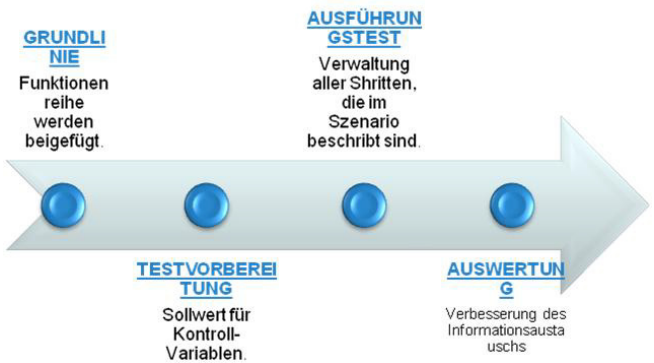
Die **Pilot-Umgebungen** wird benutzt, um neue Entwicklungen einzustellen und sie nach jeder Sprint zu prüfen.

Wenn die Testphase vorbei ist und alles überprüft werden, wird die neue Version in der **Referenz-Umgebung** installiert. umfassend einer stabileren Version der CloudCERT-Plattform.



AP6. PILOT - EXPERIMENTIEREN

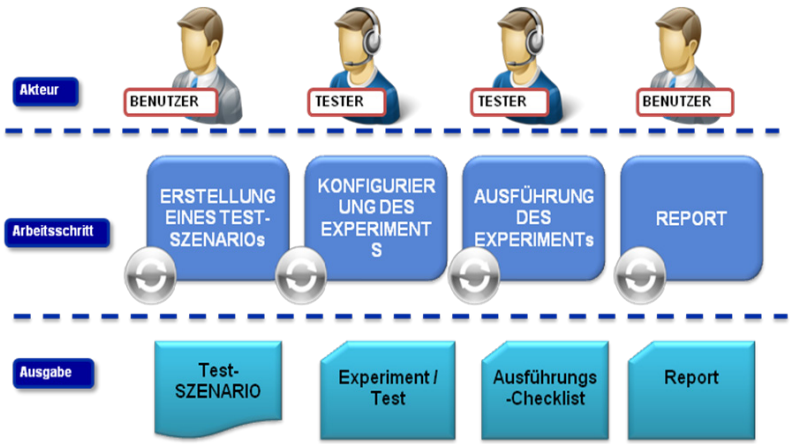
Die Aktivitäten der AP6 sind auf Experimentieren und Auswertung konzentriert, aufgrund der Integration der Benutzer-Fälle, über die Pilot-Plattform, die entwickelt und installiert in der vorherigen Arbeitpakete. Die Aktivitäten enthalten Funktionsprüfung, Produktakzeptanz sowie Simulationsübungen zum Informationsaustausch zwischen den Benutzern der Plattform, um zu experimentieren und Informationen über Entdeckung der Schwachstelle, Sicherheitswarnungen und auszutauschen.

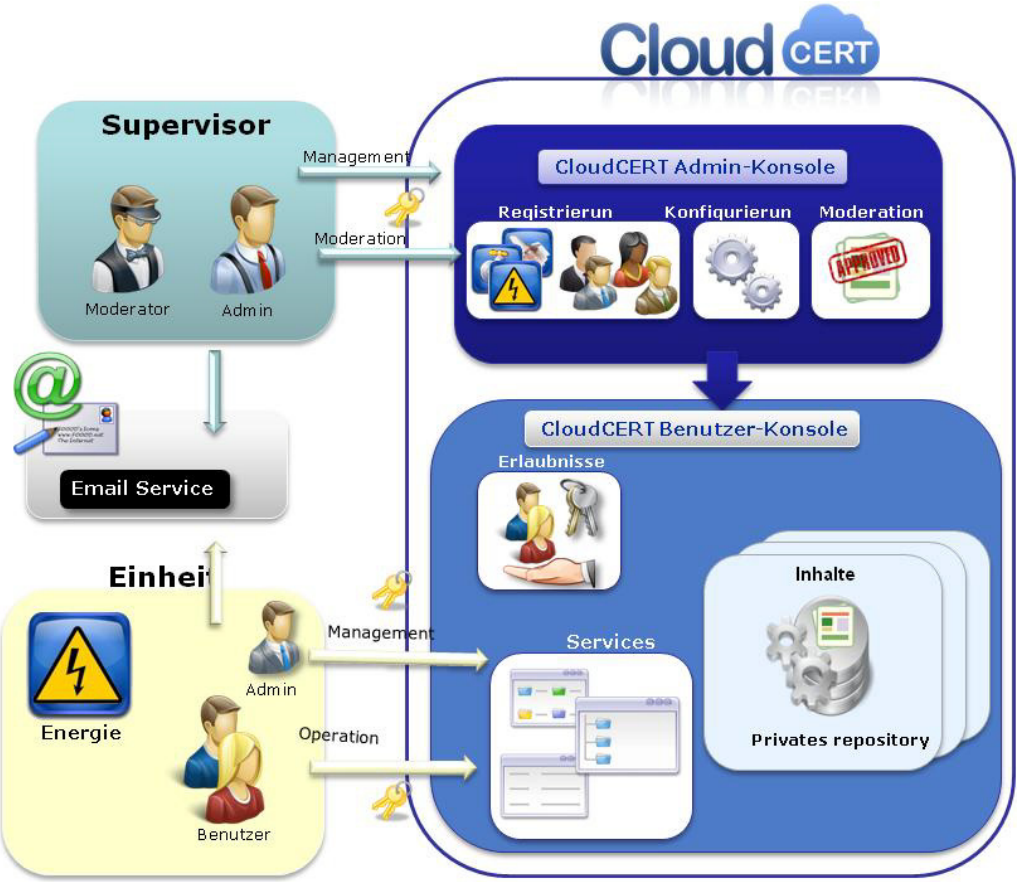


Die Ziele der Auswertung und Experimentieren ist Verwendung der Szenario-Experimentieren als eine Grundlage für Auswertung der Beteiligung der CloudCERT-Plattform-Lösung um die Zusammenarbeit zwischen der CIP-Darsteller in dem Austauch der Sicherheitsinformation zu verbessern, dabei werden die Testfunktionalität und die verfügbare Arbeitsabläufe der Kommunikation abgehalten

Die Ziele der Auswertung, die auf der Ergebnissen der Experimentieren basiert ist, sind:

- CloudCERT zu testen (ob die Prozesse der Informationsaustausch richtig unterstützt werden);
- Überzuprüfen, wie viel CloudCERT Herausforderungen und auf den Bedarfe der Domain in Bezug auf Zusammenarbeit und Kooperation angeht;
- Und die mögliche Verbesserung in CIP auszuwerten, die von CloudCERT ermöglicht ist.





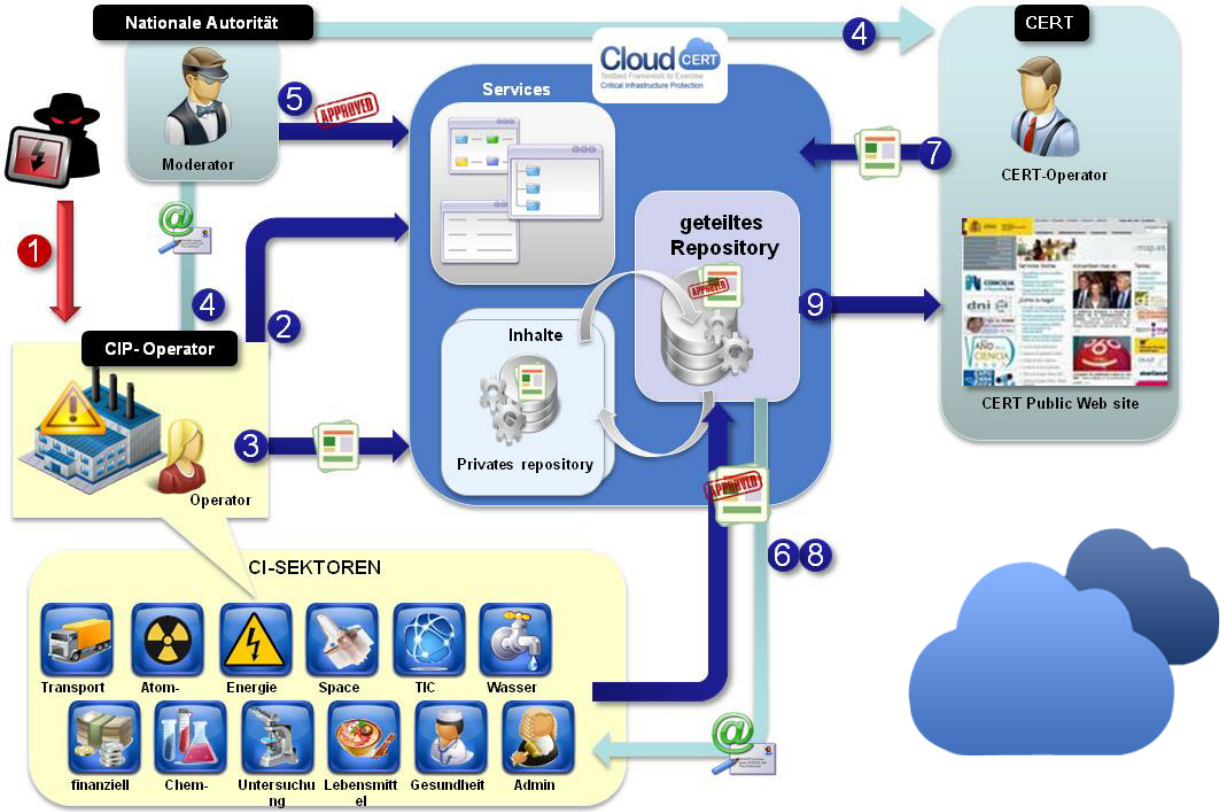
TOOLS FÜR EXPERIMENTIEREN

- **CloudCERT-Administrationskonsole.** lässt die gesamte verwaltung der Funktionalitäten der CloudCERT-Plattform.
- **CloudCERT- Benutzerskonsole**. Erleichtert die Erstellung, Anwendung und Betriebe der neuen Einheiten um auf Sicherheitsvorfällen zu reagieren.
- **Email-Client-Tool.**

AKTEURE

- Benutzer – CI Operator.
- Administrator – CI Operator.
- Moderator. – CERT / Autorität
- Administrator.- Autorität

VERWENDEN SIE SZENARIENFALLBEISPIEL

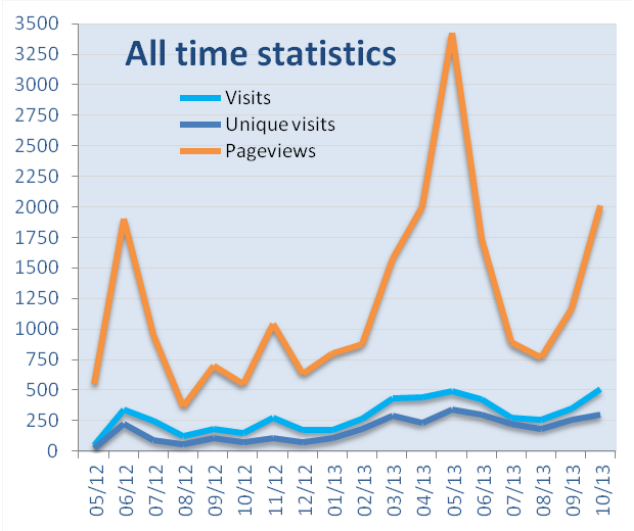


1. Operator **erkennt Schwachstelle** in einem Produkt und Eingriff im Internen Netzwerk.
2. Sucht nach Informationen und liest **Vorfallbehandlungs-Prozeduren** inwikiCIP.
3. Erstellt eine **Warnung** und **Beiträge** im Forum.
4. Öffentliche **Zwischenfallerfassung**.
5. CNPIC **überprüft** die Warnung.
6. **and 8.** Warnung sichtbar in CloudCERT und per E-Mail durch den Bulletin
7. CERT **löst** die Warnung and schließt einen Forumeintrag bei der Problemumgehung .
9. Warning wird in **externer Website** veröffentlicht.

AP7. VERBREITUNG DER PROJEKTERGEBNISSE

Die wichtigste Indikatoren derCloudCERT-ProjektWebsite **http://cloudcert.european-project.eu/** :

- Mehr als **200** Nachrichten veröffentlicht.
- Mehr als **5.000** Besuche (angesammelt).
- Mehr als **40** Quellen geteilt..
- Mehr als **22.000** Seitenabrufe (angesammelt).



WIKIPEDIA

- Englisch: http://en.wikipedia.org/wiki/CloudCERT
- Spanisch: http://es.wikipedia.org/wiki/CloudCERT
- Italienisch: http://it.wikipedia.org/wiki/CloudCERT

EVENTS

2012

- CRITIS12 Konferenz über Schutz kritischer Informationsinfrastrukturen. http://critis12.hig.no/

2013

- Junge Forscher Innovationswoche
- ENISA 8th CERT workshop.
- Protezione delle Infrastrutture Critiche – Telecomunicazioni.

CloudCERT

Testbed Framework to Exercise Critical Infrastructure Protection

Cloud CERT
Testbed Framework to Exercise
Critical Infrastructure Protection

Keywords	CERT, CSIRT, Critical Infrastructure Protection (CIP), Critical Infrastructure (CI), Information Sharing, Infrastructure Security
Funding Agency	European Union
Project Type	4rth Annual Work Programme adopted under the Council Decision No 2007/124/EC, Euratom, of Specific Programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security related Risks for the Period 2007–2013" as part of the General Programme on "Security and Safeguarding Liberties".
Reference	HOME/2010/CIPS/AG/20

FINANCIADO POR LA UE

Innova.- Inteco publica la web del proyecto 'Cloud Cert' sobre protección de infraestructuras críticas

LEÓN, 14 Jun. (EUROPA PRESS) -

El INTECO presenta la web de un consorcio europeo en defensa de las infraestructuras críticas

15 de septiembre de 2012 | 18:29 CET

PROYECTOS

Cloud CERT de INTECO: innovación internacional para la seguridad de las Infraestructuras Críticas

La Comisión Europea seleccionó el proyecto Cloud CERT del Instituto Nacional de Tecnologías de la Comunicación (INTECO), dirigido a desarrollar una plataforma para ejercicios específicos de cooperación en la seguridad de las infraestructuras críticas en la Unión Europea. El Instituto pondrá en valor la experiencia de INTECO CERT en esta materia, los estándares de comunicación segura, y otros desarrollos que ha llevado a cabo relacionados con la seguridad en las infraestructuras críticas. INTECO será el líder del proyecto, que tendrá una duración de dos años y un presupuesto estimado de 454.952,73 euros. Del consorcio también forman parte CNPIC (ES), Indra (ES), Zanasi Alessandro Srl. (IT), Europe for Bussiness Ltd (UK), ICSA (IT), y como asociado Theodore Puckas Foundation (HU).

Raúl Rivero / Ignacio Cobo

FINALE KONFERENZ

CloudCERT -Finale Konferenz um die Ergebnisse des Europäischen Projekts zu der Zielgruppe zu verbreiten.

- **Datum:** 22 November 2013.
- **Ort:**
  - Spanischer Außenminister der Telekommunikation und Informationsgesellschaft (SETSI). Madrid (Spain)
- **Zielgruppe:**
  - CloudCERT Projekts- stakeholders.
  - Spanishe Betreiber kritischer Infrastrukturen einschließlich Hauptlieferant.
  - Andere Europäische CERTs und Strafverfolgungs-Teams, die an CIP beteiligt sind.
- **Eintritt:**
  - Freier Eintritt mit Einladung und per video streaming übertragt http://www.cloudcert.webcastlive.es.


Cloud CERT

Publication date: 28.10.13
Subject: CloudCERT final conference

Final Conference of CloudCERT European Project to Present Results Achieved

The CloudCERT European Project, which is co-financed by the European Union (E.U.) and whose project consortium is co-ordinated by INTECO, is holding its **Final Conference on 22 November at the Spanish Secretariat of State for Telecommunications and the Information Society (SETSI) in Madrid.** The conference will present the results obtained during the execution of the project (2012 to 2013), demonstrating the CloudCERT platform for sharing cyber-security information that it has produced, as well as the various other deliverables generated by the project.

The CloudCERT Project provides a test-bed environment for the exchange of information on Critical Infrastructure Protection (CIP) and its security aspects, enabling co-operation and co-ordination of the agents involved so as to manage cyber-risk-critical assets effectively.

The EU has supported this project financially through the specific programme entitled "Prevention, Preparedness and Consequence Management of Terrorism and Other Security-Related Risks", falling within the "Security and Safeguarding Liberties" framework programme.

The project consortium is made up of the National Institute for Communication Technologies (INTECO), a company dependent upon the Ministry of Industry, Energy and Tourism (MINETUR) through the Secretariat of State for Telecommunications and the Information Society (SETSI) (Spain) **as project co-ordinator**, together with the National Centre for Critical Infrastructure Protection (CNPIC) of the Ministry of the Interior (Spain), Indra (Spain), ZANASI and Partners (Italy) , Europe for Business Ltd. (United Kingdom) and the ICSA Foundation (Italy).

TECHNOLOGISCHE LÖSUNG

KORPORATIVE PLATTFORM

IST CLOUDCERT INTERESSANT FÜR SIE?

- Wenn Ihre Organisation einer **CERT oder CI Operator** ist, dann können Sie dise Plattform verwenden, um mit Vorfällen der kritischen Infrastrukturen umzugehen und cyber-Sicherheitsinformation zu teilen.
- Wenn der Kundenkreis ihrer Organisation als **CERT oder Autorität ist,** die Operatoren kritischer Infrastrukturen enthält, dann können Sie anpassene Plattform, um ihren Kundenkreis mit Services und Tools anzubieten (forum, wiki, etc).
- Wenn Ihre Organisation mit **Nationalen Autoritäten für den schutz kritischer Infrastrukturen** interagieren muss, und von ihren nationalen Firmen abhängig ist, dann können Sie innerhalb der Plattform die wichtigste Funktion bestimmen: Koordinierung, Supervision, Beteiligung, usw.

INHALTE

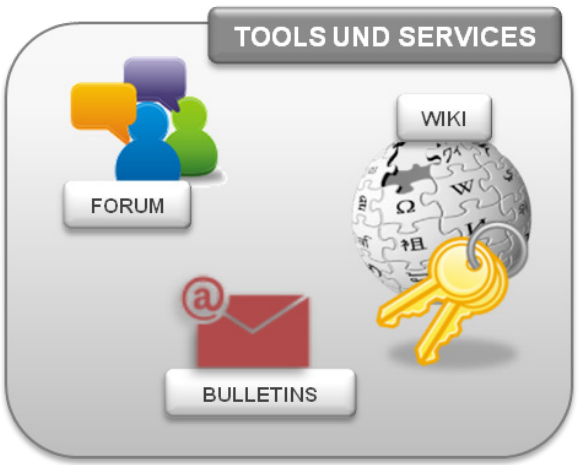
CloudCERT-Plattform lässt Sie, sicherheitsinhalte zu erstellen und propagieren wie:

- Notizen.
- Nachrichten.
- Warnungen.
- Viren.
- Schwachstellen.
- RSS-Items.

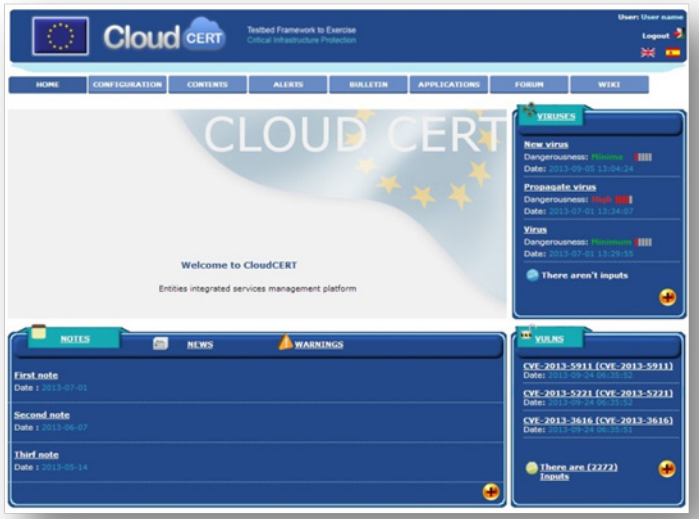
SERVICES UND TOOLS

CloudCERT-Platform Lässt die Benutzer, Information auszutauschen, um Sicherheitsvorfälle durch ihre Services zu verhindern :

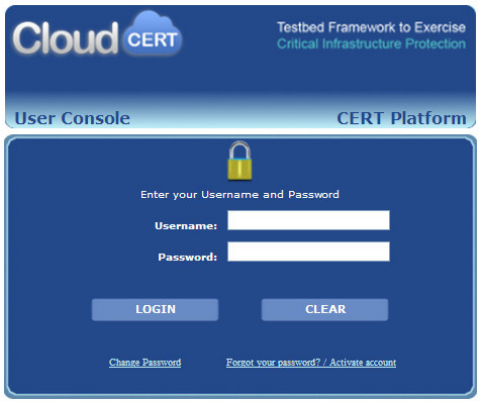
- Forum.
- WikiCIP.
- Bulletins-Service.



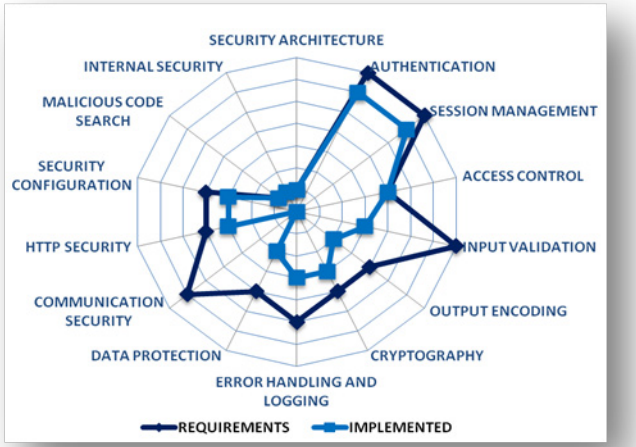
PRODUKTBESCHREIBUNG



- **Kollaborative Plattform** um die Zusammenarbeit des geteilten Repository der cyber-Sicherheitsinformation in einer wirksamen weise zu verwalten.

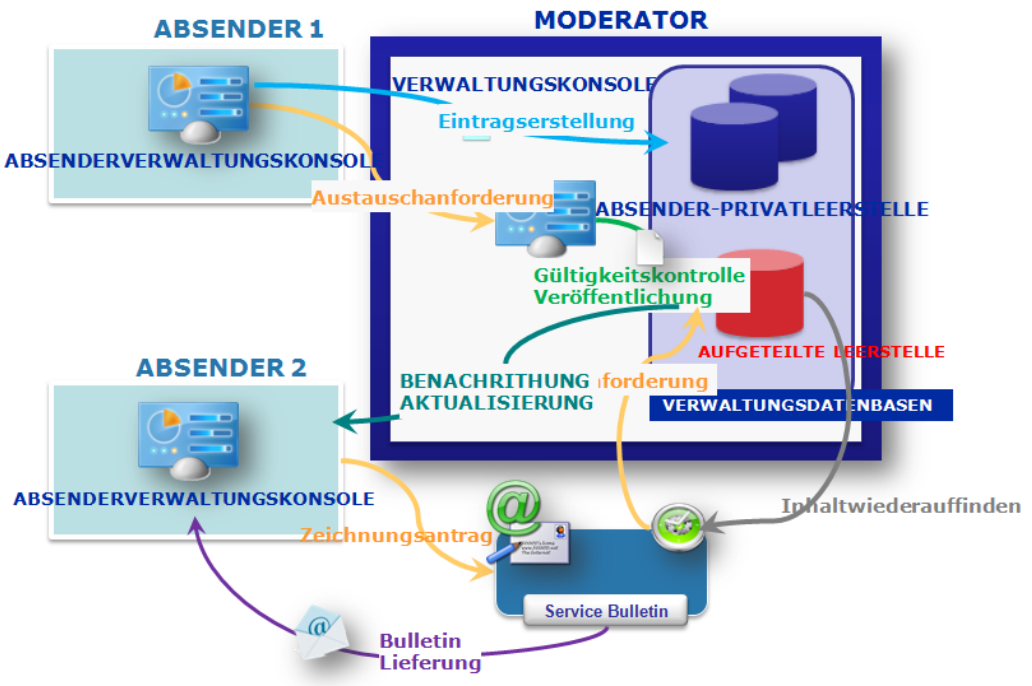


- **Cloud Paradigma**, das auf privaten und geteilten Repositorien basiert ist.
- **Mehrsprachige** Anwendung und Übersetzungsinterface der Inhalten.
- Personalisierte **Services** (beschränkt).
- **skalierbare** Plattform, die neue Inhalte, Services, Tools und Workflows ermöglicht.
- **Sichere Umgebung**:
  - Authentifizierungsmechanismen, die auf Benutzername and Passwort bassieren: zentraler Authentifizierungsdienst (CAS).
  - Autorisierung, die auf Berechtigungen und Rollen basiert.
  - Sichere Sitzungsverwaltung.
  - Vertraulichkeit und Datenschutz sind garantiert.



INHALTSLEBENSZYKLUS

- CloudCERT ermöglicht die Erstellung und das Update von Inhalten in einer kooperativen Weise.
- Jede Einheit speichert die inhalte in ihrer privaten Stelle und es könnte um den Austausch bitten werden.
- Einer Moderator überprüft die Inhalte, die in dem gemeinsamen Repository veröffentlich werden.
- Die Einheit können ihre Inhalte abrufen, um in einem Außentool (wie Intranets) veröffentlicht zu werden.



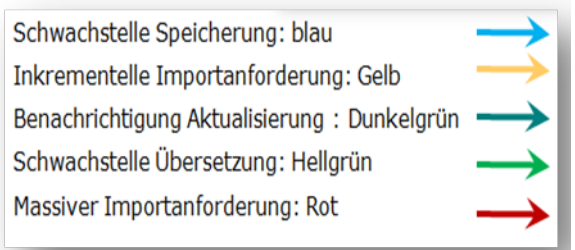
Erstellung von Dekumenten: Blua
Anträge: Gelb
Update-Benachrichtigung: Dunkelgrün
Überprüfung des Antrags: Hellgrün
Antrag des massiven imports: Rot
Abruf von Inhalten für Erstellung von Bulletin: Grey.
Lieferung von Bulletin: Purpur

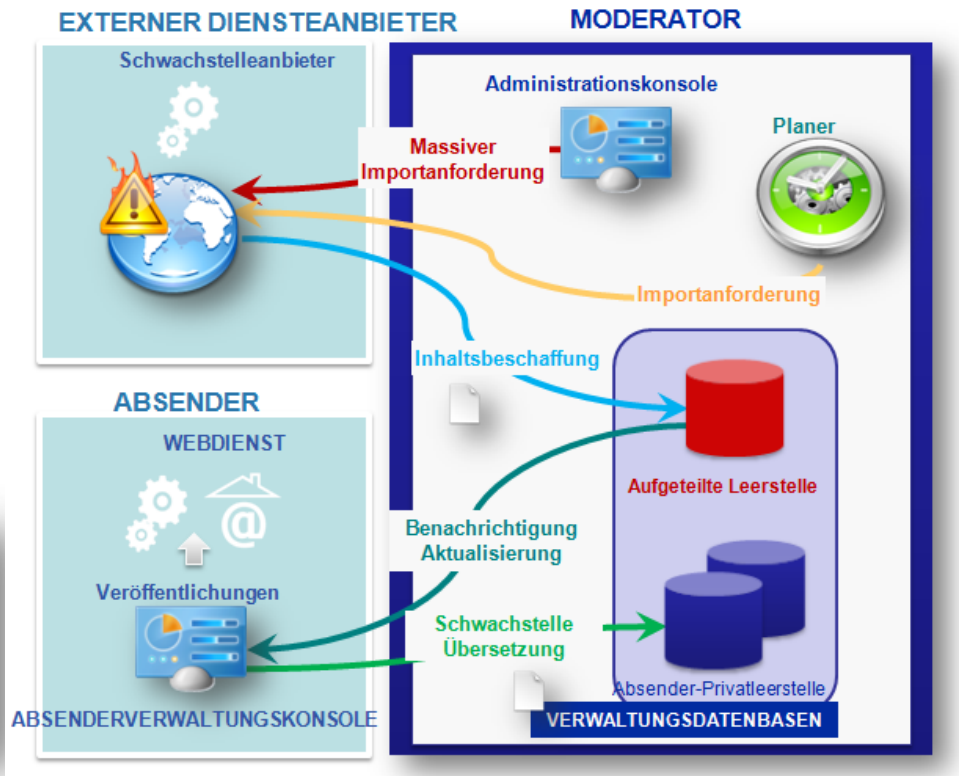
In den folgenden Ständen werden die Inhalte währen ihres Lebenszykluses:

- Erstellen.
- Modifiziert
- Geteilt.
- aktualisiert.
- Bestätigt.
- Abgelehnt.

LEBENSZYKLUS DER SCHWACHSTELLEN

- Die Schwachstellen werden von externen Quellen (wie NIST) angeboten.
- Ein geplanter Job importiert automatisch die Schwachstellen im System.
- Moderator kann auch um einen massiven Import (für einen Zeitraum) in das System bitten.
- Einheiten können die Schwachstellen auf ihre eigene private Stelle verschieben.





Die Schwachstelle werden in der folgenden Ständen während ihres Lebenszykluses:

- importiert.
- notifiziert (update).
- Übersetzt.

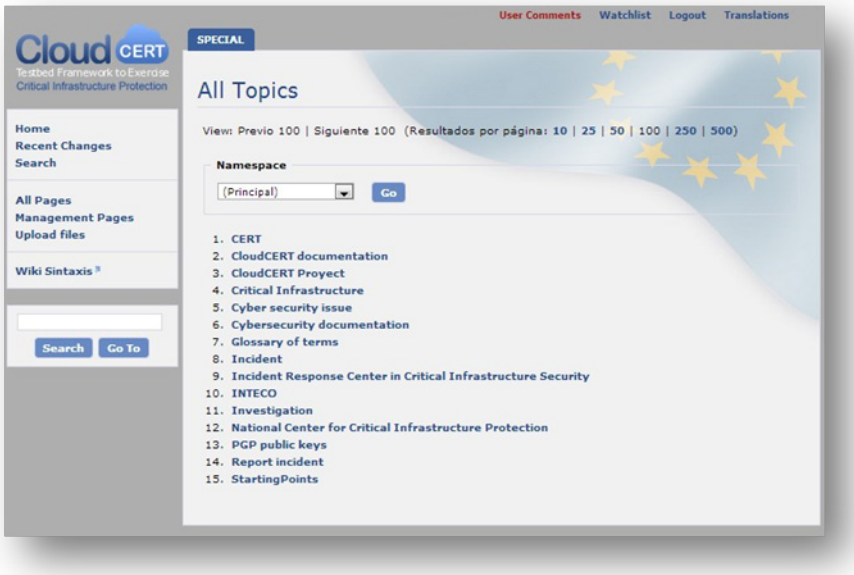
WIKICIP

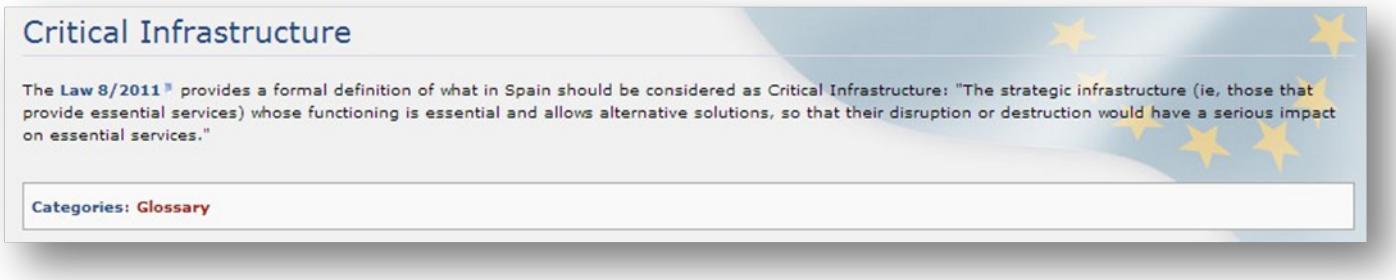
Wiki ist ein flexibeles System, erlaubt den Administrator jeder Seite-Hierarchie zu bestimmen. WikiCIP erlaubt **die unstrukturierte Inhalte** in einer kollaborativen Weise mit folgenden Strukturelementen zu halten.:

- **Index** – Index- Seite, die Links zu verschiedenen Wiki-Seiten mit einem ähnlichen Thema zeigt.
  - **Seite**- Einzelne Seiten zu einem bestimmten Thema.

WikiCIP hat die folgende Strukturthemen:

- **CloudCERT -Dokumentation**:
  - Allgemeine Präsentation des Projekts und der Hauptquellen.
    - Benutzerhandbuch.
    - Administratorhandbuch.
    - Entwicklerhandbuch.
- **Cyber-Sicherheit-Dokumentation**:
  - Bedienablauf für cyber-Sicherheitsvorfälle.
  - Rechtlicher Rahmen.
  - interessante CIP-Links.
- **Glossar.** Hauptbedingungen bezogen auf den Schutz kritischer Infrastrukturen**.**

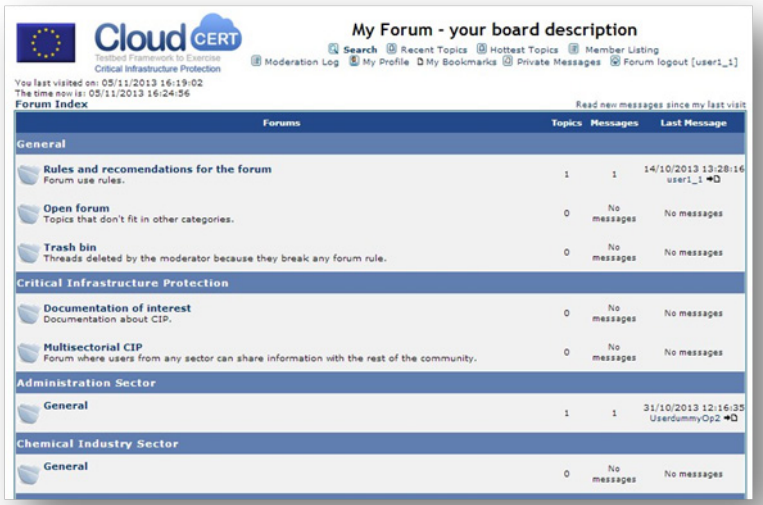




FORUM

Das Forum-Service erlaubt den unstrukturierten Informationsaustausch mit folgenden Gruppierungselementen:

- **Kategorie.** Sie ist das obere Element der Hierarchie, und wird normalerweise benutzt, um mehrere verwandte Foren zu gruppieren. Sie ist eine logische Gruppe, und jedes Forum hat seinen eigenen Lebenszyklus in der Kategorie.
  - **Forum.** Ein Forum ist eine Gruppe von Drohungen oder Diskussionen über das gleiche Thema**.**
    - **Drohnung oder Thema.** Es ist die Diskussion selbst, die Mitteilungen von den Benutzern, in den über ein bestimmtes Thema sprechen.



CloudCERT-Forum hat die folgenden Kategorien:

- **Allgemeine** Foren für allgemeine Information.
- **Schutz kritischer Infrastrukturen.** Wo die Benutzer diskutieren und allgemeine Informationen über den Schutz kritischer Infrastrukturen mit dem Rest der Gemeinschaft teilen können.
- Jeder Operator kritischer Infrastrukur hat ein reserviertes Forum für seinen **Sektor** (nach CIP-spanische Klassifizierung des nationalen Recht), wo die Benutzer Informationen mit passenden Akteure in dem Sektor.
  - Administration.
  - Space.
  - Atomwirtschaft.
  - Chemieindustrie.
  - Erleichterungen der Untrsuchung.
  - Wasser.
  - Energie.
  - Gesundheit.
  - Informations- und Kommunikationstechnologie (ICT).
  - Transport.
  - Lebensmittel.
  - Finanz- und Steuersystem.

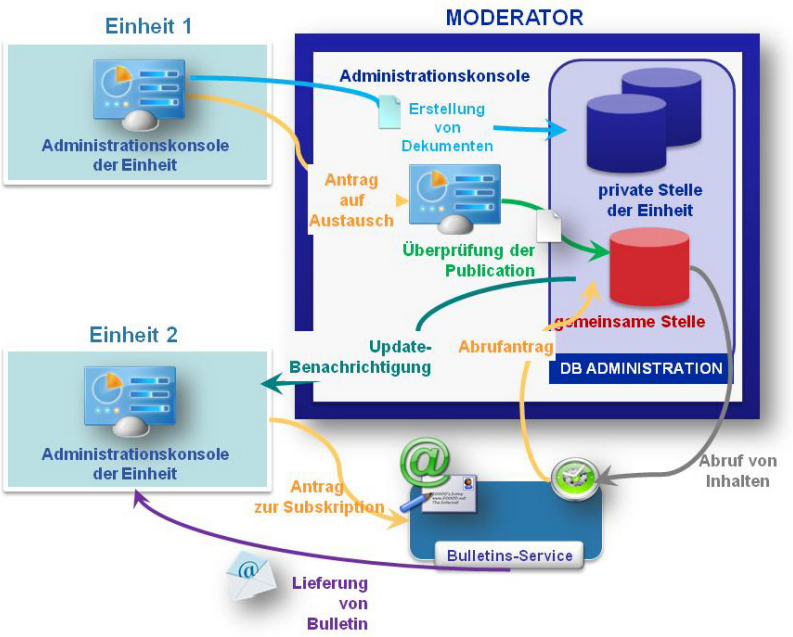
BULLETINS-SERVICE

Das Bulletins-Service ist ein externes Service, das der CloudCERT-Plattform kommuniziert, um **die Subskriptionen der Benutzern zu erhalten**, und auch **die Sicherheitsinhalte in CloudCERT-Datenbanken zu speichern**, um Bulletins zu erstellen. Das Bulletins-Service ist verantwortlich für Erstellung der Bulletins und Lieferung der Bulletins zu den finalen Benutzer nach ihren Einstellungen.

Die Benutzer (registrierte oder externe Benutzer) können verschiedene Sicherheits-Bulletins (Zeitungen) abonnieren, um Bulletins regelmäßig in ihrem Posteingangsordner zu empfangen.

Die Subskription kann vom Administrator der Einheit oder vom finale Benutzer abgearbeiten werden.

- Bulletins-service erlaubt es, dass die Benutzer über Update-Inhalte per Email informiert werden.
  .
- A Subskriptionsprozess ist erforderlich, um Typ und Inhalte von Bulletin auszuwählen
- Das Bulletins-Service sammelt Inhalte, erstellt die bulletins und liefert sie jedem finalen Benutzer.



Erstellung von Dokumenten: Blua
Anträge: Gelb
Update-Benachrichtigung: Dunkelgrün
Überprüfung des Antrags: Hellgrün
Antrag des massiven imports: Rot
Abruf von Inhalten für Erstellung von Bulletin: Grey.
Lieferung von Bulletin: Purpur

CloudCERT

Testumgebung-Rahmen für die Ausübung
zum Schutz kritischer Infrastrukturen

CloudCERT Testumgebung-Rahmen für die Ausübung zum Schutz kritischer Infrastrukturen.

HOME/2010/CIPS/AG/20.

Mithilfe der Finanziellen Unterstützung des Programm "Prävention, Abwehrbereitschaft und Folgenbewältigung im Zusammenhang mit Terrorakten und anderen sicherheitsbezogenen Risiken"

Die Europäische Kommission - die Generaldirektion Justiz, Freiheit und Sicherheit