Schutzübung für Computerbasierte Unternehmensübergreifende Desaster Logistik (SCUDO)

Peter Kieseberg, Alexander Szönyi

October 1st, 2012

THALES

Ziele

- Erstens wurde ein auf österreichische **Unternehmen und Bedarfsträger zugeschnittener**, optimierter **Übungsprozess entwickelt** und getestet
- Zweitens wurden daraus **Empfehlungen abgeleitet**
- Drittens wurden **Visualisierungsdemonstratoren**, sowohl im Bereich des Krisenmanagements, als auch als Unterstützung zur Durchführung von Planspielen **entwickelt**.

Projektpartner

- Thales Austria GmbH
- Infraprotect GmbH
- SBA Research GmbH
- nic.at Internet Verwaltungs- und Betriebsgesellschaft m.b.H.
- Zentraler Informatikdienst der Universität Wien
- Universität Wien Arbeitsgruppe Rechtsinformatik
- REPUCO Unternehmensberatung GmbH

- Bundeskanzleramt
- Bundesministerium für Landesverteidigung und Sport
- Bundesministerium für Inneres

Projektinformationen

- Österreichisches Sicherheitsforschungsprogramm KIRAS

  Das österreichische Sicherheitsforschungsprogramm KIRAS ist ein nationales Programm zur Förderung der Sicherheitsforschung in Österreich. KIRAS unterstützt nationale Forschungsvorhaben mit dem Ziel der Erhöhung der Sicherheit Österreichs und seiner Bevölkerung.

- Projektbeginn: 09/2012
- Projektende: 02/2015
- Projektinformationen: KIRAS www.kiras.at

bmvit
Bundesministerium für Verkehr, Innovation und Technologie

FFG
Österreichische Forschungsförderungsgesellschaft

KIRAS Sicherheitsforschung

THALES

Technische Schwerpunkte

- DNS, DNSSEC, Zertifikate in einer PKI, Schwachstellen in weit verbreiteten Komponenten analysieren und kontrollieren
- Prüfung der nationalen IKT Struktur und potentielle Angriffsflächen
- Prüfung des Zusammenspiels von öffentlichen Sicherheitsstrukturen, Erstellung von Verbesserungsvorschlägen
- Überprüfung internationaler Standards, Standardprozesse und Vorgehensweisen
- Analyse der Ergebnisse der Schutzübungen auf Effektivität der Notfallmaßnahmen

Szenarien und Störungsklassen

- Im Rahmen des Projektes werden **drei Szenarien** zu **drei Störungsklassen** erstellt, die **realistische** und gleichzeitig herausfordernde **Cyber Security Bedrohungen darstellen** sollen.

Szenario / Störungsklasse 1

- Anonymous Austria führt einen erfolgreichen Angriff auf österreichische Infrastruktur durch. Langsam werden Probleme durch interne (Mitarbeiter) und externe (Kunden) Personen gemeldet. Nach Bekanntgabe von Anonymous Austria ist es ersichtlich, dass **Domain-Delegationen** verändert wurden. Neben den bereits bekannten Service-Ausfällen wird die Organisation mit der Problematik konfrontiert, dass falsche Webseiten im Internet abrufbar sind, die als Ziel haben, dass Kunden-Informationen bzw. –zugänge gestohlen werden (Phishing Angriff).

- Schreckensmitteilungen, dass „alle“ Kundeninformationen gestohlen wurden, müssen durch analytisches Denken kritisch hinterfragt werden und auf die Phishing Attacken zurückgeführt werden. Neben technischen und organisatorischen Herausforderungen wird auch ein grundsätzliches juristisches Bewusstsein zur Diskussion gestellt

Szenario / Störungsklasse 2

- Anonymous Austria führt einen erfolgreichen Angriff auf österreichische Infrastruktur durch. Langsam werden Probleme durch interne (Mitarbeiter) und externe (Kunden) Personen gemeldet. Als Ursache dieser Probleme stellt sich heraus, dass eine **Certification Authority** kompromittiert wurde und das Stammzertifikat von dieser Authority zurückgezogen wurde. Die eigenen SSL etc. Zertifikate, die von der CA signiert wurden, stellen ab diesem Zeitpunkt keine Sicherheit mehr dar und es muss davon ausgegangen werden, dass bereits im Vorhinein Angriffe auf Kunden geschehen sind.

- Betriebssystem- und Browser-Hersteller reagieren indem sie aktuelle Sicherheitsupdates veröffentlichen. Spätestens ab diesem Zeitpunkt erfahren alle Nutzer, dass das Zeritfikat zurückgezogen worden ist. Dies bedeutet, dass die Vertraulichkeit bei der Kommunikation mit den angebotenen Onlineservices, nicht mehr sichergestellt werden kann.

Szenario / Störungsklasse 3

- Durch Bekanntmachung, dass in einem Standard-Produkt eines **Hardwareherstellers** ein **Backdoor** vorhanden ist, muss davon ausgegangen werden, dass die organisationsweite Infrastruktur kompromittiert ist.

- Nutzer sind gesperrt, firmeninterne Dokumente sind scheinbar im Netz, der Support meldet sich (viele Kunden haben Probleme bei der Authentisierung), etc. Die Behebung des Problems ist abhängig von einem Firmwareupdate des Hardwareherstellers, das nicht rasch verfügbar ist. Soll die Hardware deaktiviert werden oder muss sie in Betrieb bleiben, obwohl das Backdoor vermutlich bereits ausgenutzt wird?

Arbeitspakete

- AP1 – Projektmanagement
- AP2 – Projektgrundlagen
- AP3 - Resilienz- und Handlungsempfehlungen
- AP4 - Resilienzumsetzung und Validierung
- AP5 - Nachbereitungs- und Analysephase
- AP6 - Recht, Grundrechtsschutz, Datenschutz und Compliance
- AP7 - Unterstützungswerkzeuge

AP2 – Projektgrundlagen

- Analyse- und Studienphase
- Anforderung und Wege zur Erstellung von Kommunikationsplänen bei Ausfällen / Störungen von informationstechnischer Infrastruktur
- technische Auswirkungen auf existierende Systeme bei Ausfällen / Störungen von informationstechnischer Infrastruktur
- Detailanalyse der möglichen Bedrohungsszenarien und deren Langzeitauswirkungen auf die Businessprozesse von Unternehmen.
- Deren Langzeitauswirkungen auf die Businessprozesse von Unternehmen.

AP3 - Resilienz- und Handlungsempfehlungen

- Technischer Umgang mit Störungen
- Organisatorische Anforderungen und österreichweite Umsetzung von Kommunikations- und Bewältigungsplänen
- Personelle Anforderungen
- Grundlage Drehbücher

AP4 - Resilienzumsetzung und Validierung

- Teststellung1 Schwerpunkt trimodale Kommunikation
- Evaluierung technischer Einzelszenarien
- Teststellung2 Schwerpunkt multimodale Kommunikation

AP5 - Nachbereitungs- und Analysephase

- Zusammenfassung der Studien und Analyse der Probleme
- „Lessons Learned“ und Maßnahmenkatalog erstellen
- Workshop zur Nachbesprechung des SCUDO Projekts

AP6 - Recht, Grundrechtsschutz, Datenschutz und Compliance

- Das Arbeitspaket soll sicherstellen, dass die Anforderungen des Datenschutzrechts und der Grundrechte in allen Phasen des Projekts insbesondere auch im Hinblick auf die aktuellen Entwicklungen in Europa berücksichtigt werden.

AP7 - Unterstützungswerkzeuge

- Einbindung Infrastruktur
- Integration der Workflows
- Customer Übung 1 (Kommunikation)
- Customer Übung 2 (Kleinübung)
- Customer Übung 3 (Großübung)
- Erstellen der Dokumentation

Großübung

- Spielleitung

  Standort: Landesverteidigungsakademie (LVAk)

- Lagezentrum

  Standort: Landesverteidigungsakademie (LVAk)

- Kritische Infrastrukturen (Spieler)

  Standort: Vor Ort bei den Spielern

Spielleitung und Spielbeobachter

- Thales Austria GmbH
- Infraprotect GmbH
- SBA Research GmbH
- nic.at Internet Verwaltungs- und Betriebsgesellschaft m.b.H.
- Zentraler Informatikdienst der Universität Wien
- Universität Wien Arbeitsgruppe Rechtsinformatik
- REPUCO Unternehmensberatung GmbH

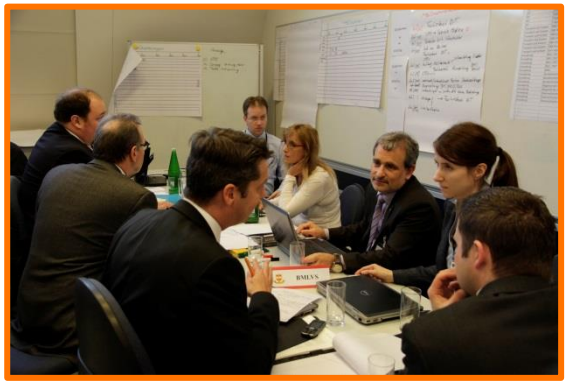
Lagezentrum

- Bundeskanzleramt (Gov Cert)
- Bundesministerium für Inneres
- Bundesministerium für Landesverteidigung und Sport

BUNDESKANZLERAMT ÖSTERREICH

BM.I REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR INNERES

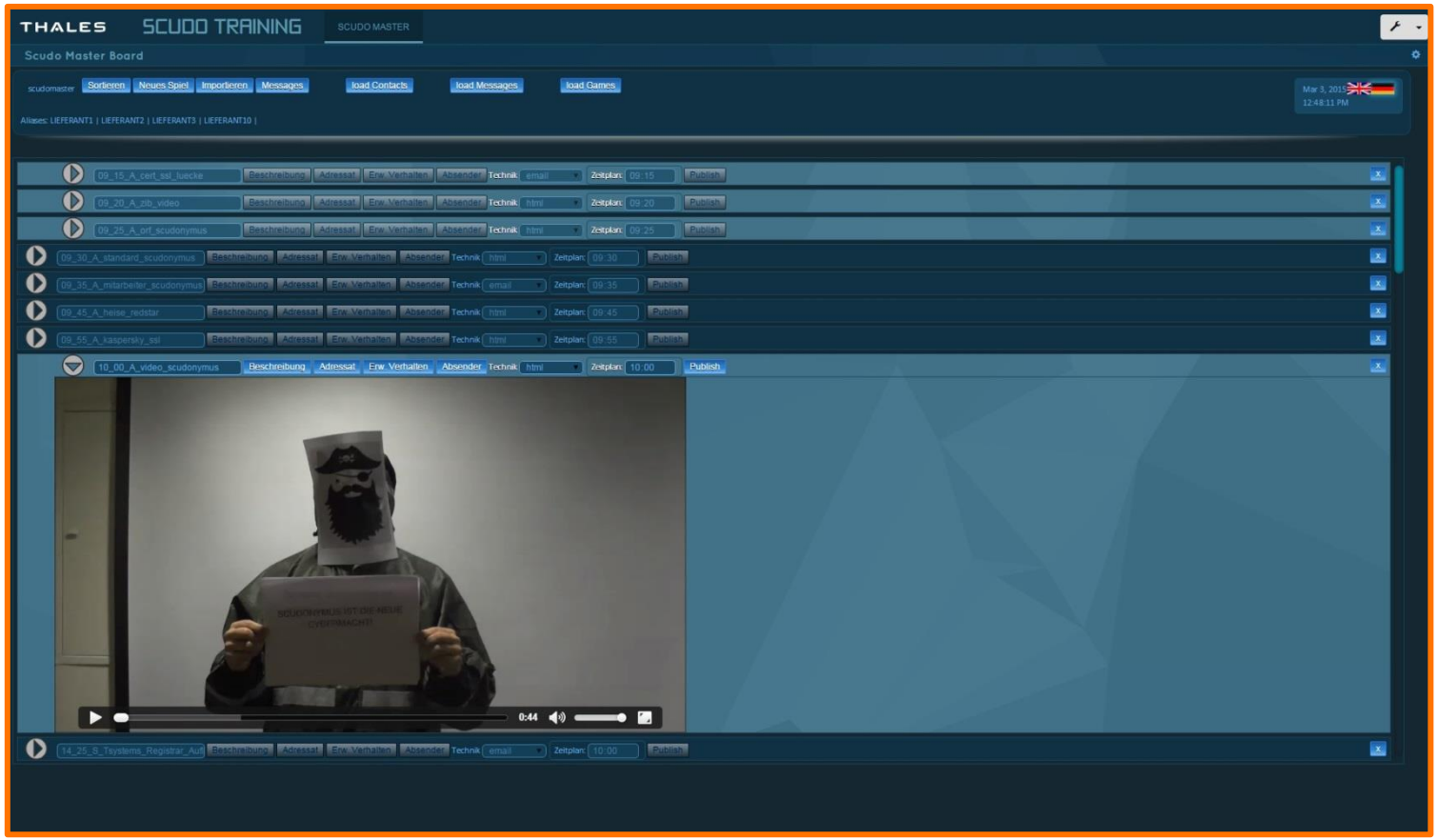
ÖSTERREICHS BUNDESHEER



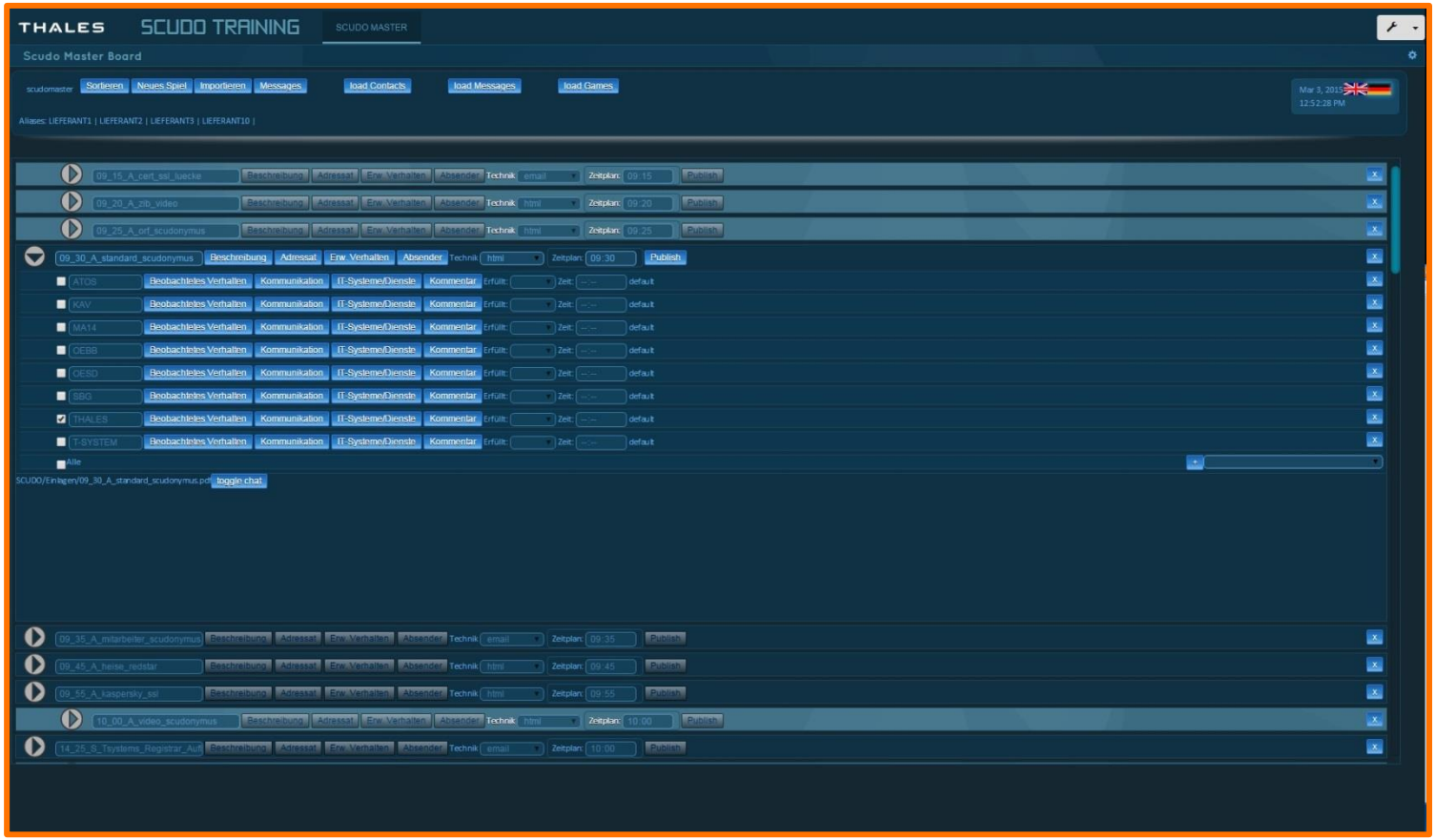
Kritische Infrastrukturen

- Gespag
- Krankenanstalten Verbund Wien
- MA 14
- ÖBB
- Österreichische Staatsdruckerei
- Salzburg AG
- Thales
- T-Systems

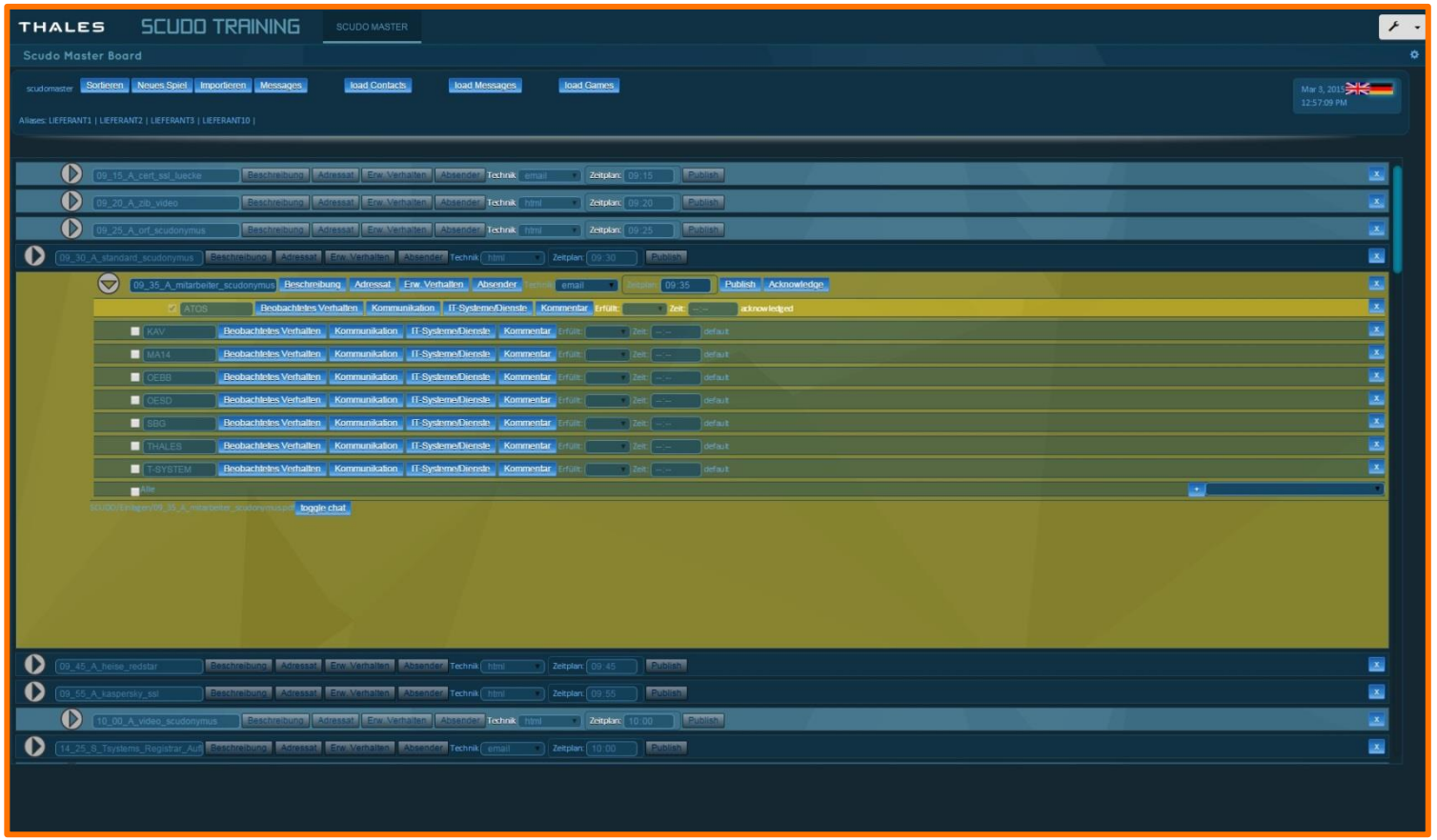
Demonstrator Ansicht 1 Spielleiter



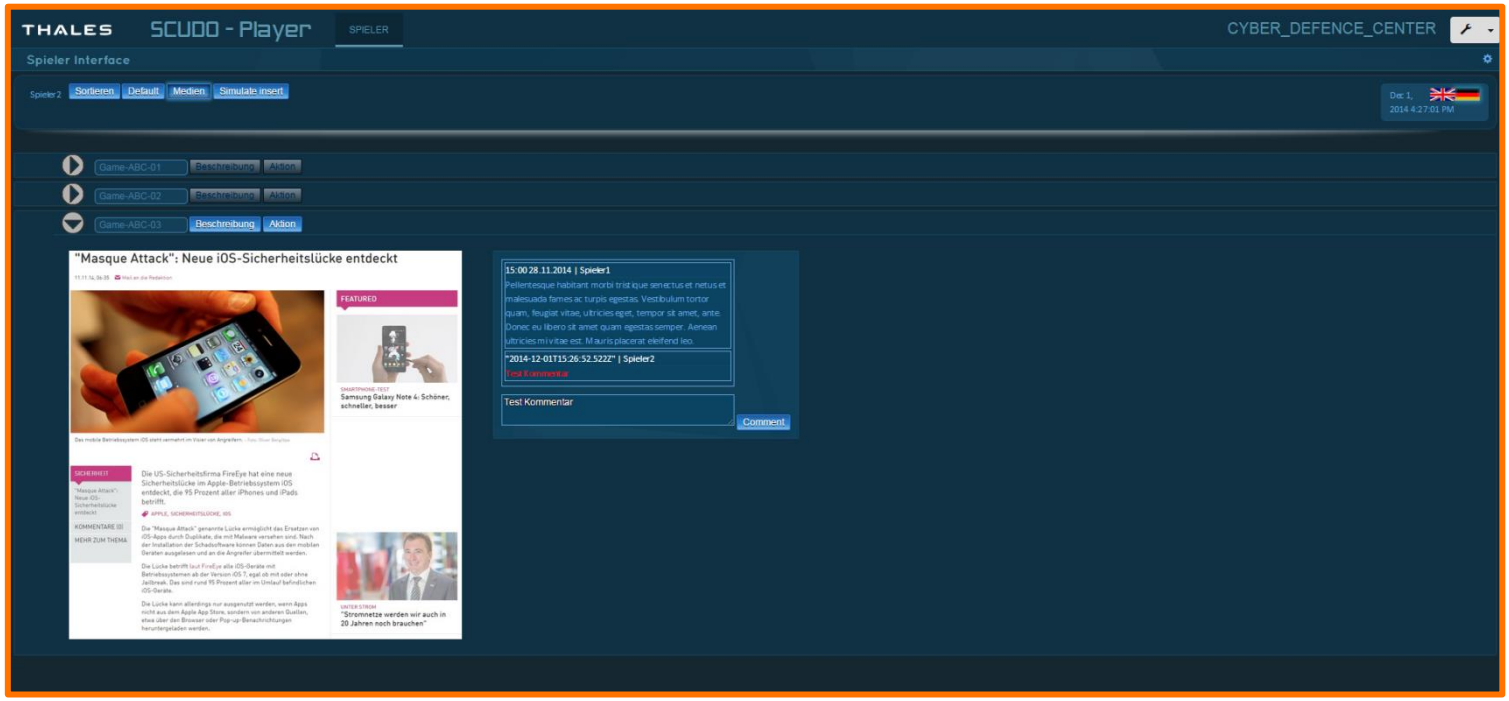
Demonstrator Ansicht 2 Spielleiter



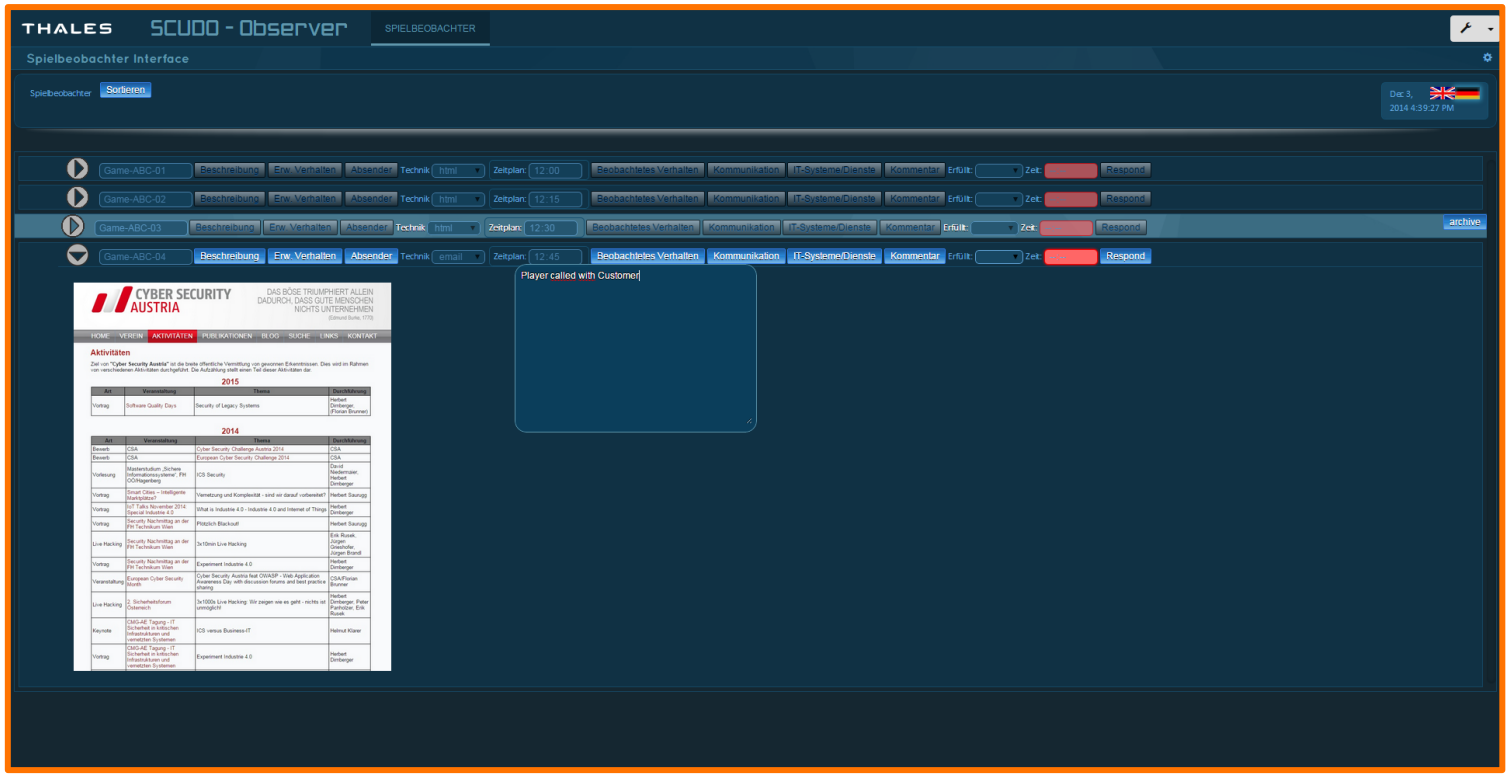
Demonstrator Ansicht 3 Spielleiter



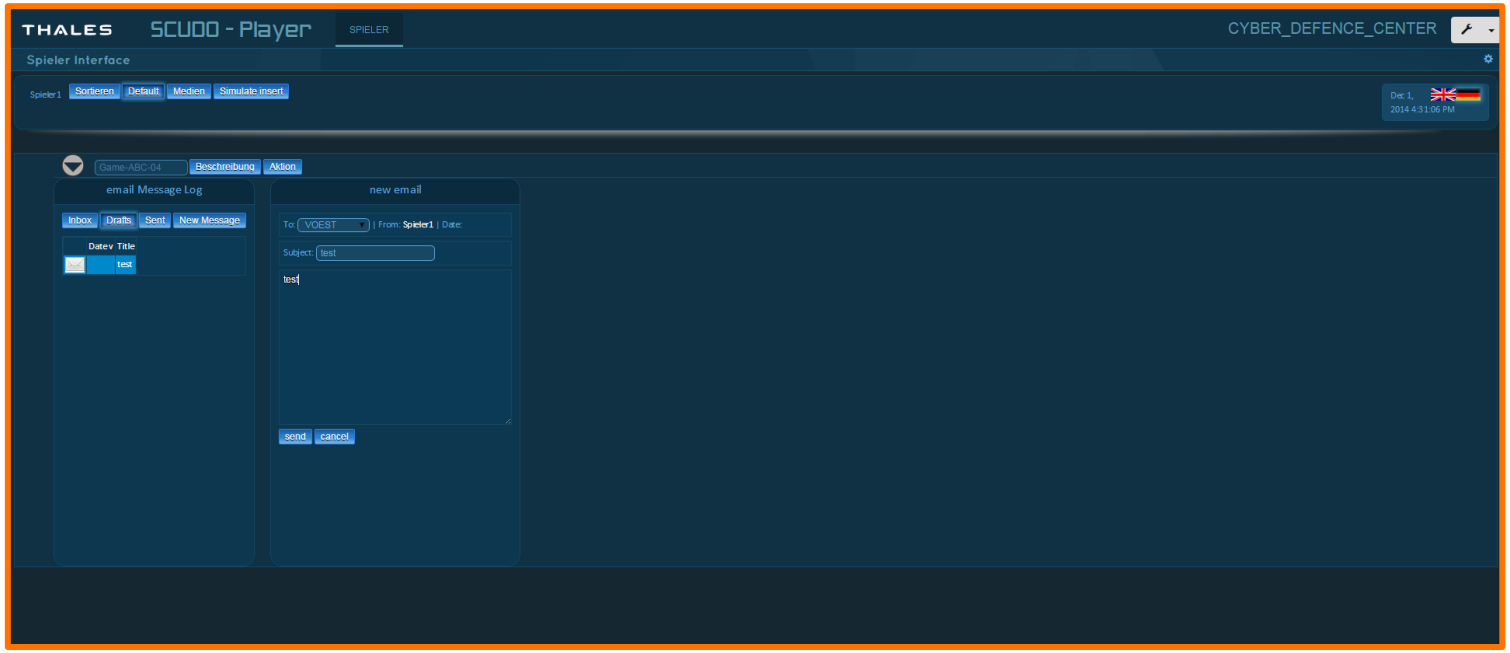
Demonstrator Ansicht Spieler



Demonstrator Ansicht Spielbeobachter



Demonstrator Ansicht Kommunikation



Gruppenfoto Abschluss Übung

Kontaktdaten

Peter Kieseberg
SBA Research GmbH
pkieseberg@sba-research.org

Alexander Szönyi
Thales Austria GmbH
Alexander.szoenyi@thalesgroup.com