



Schutzübung für Computerbasierte Unternehmensübergreifende Disaster Logistik (SCUDO)

Peter Kieseberg, Alexander Szönyi

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



Bundesministerium
für Verkehr,
Innovation und Technologie

FFG

Österreichische
Forschungsförderungsgesellschaft



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 Zertifikat 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
BUNDEMINISTERIUM FÜR INNERES

 ÖSTERREICHS BUNDESHEER



THALES

Kritische Infrastrukturen

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



Demonstrator Ansicht 1 Spielleiter

The screenshot displays the THALES SCUDO TRAINING SCUDO MASTER interface. At the top, the title bar reads "THALES SCUDO TRAINING SCUDO MASTER". Below this, the "Scudo Master Board" is visible, featuring a navigation bar with buttons for "Sortieren", "Neues Spiel", "Importieren", "Messages", "Load Contacts", "Load Messages", and "Load Games". The interface shows a list of training modules, each with a play button, a description, address, expected behavior, sender, technique, format, and schedule. The selected module is "10_00_A_video_scudonymus", which is currently playing in a video player. The video shows a person in a pirate costume holding a sign that reads "BESCHREIBUNG ADRESSAT ERW. VERHALTEN ABSENDER TECHN. HTML ZETPLAN: 10:00 PUBLISH". The video player includes a progress bar and a volume control. The interface also shows the date and time as "Mar 3, 2015 12:48:11 PM" and a language selector for "DE".

Demonstrator Ansicht 2 Spielleiter

THALES SCUDO TRAINING SCUDO MASTER

Scudo Master Board

scudomaster [Sortieren](#) [Neues Spiel](#) [Importieren](#) [Messages](#) [load Contacts](#) [load Messages](#) [load Games](#)

Mar 3, 2015 12:52:28 PM

Aliases: LIEFERANT1 | LIEFERANT2 | LIEFERANT3 | LIEFERANT10 |

ID	Beschreibung	Adressat	Emp. Verhalten	Absender	Technik	email	Zeitplan	publish
09_15_A_cerf_sst_waechle	Beschreibung	Adressat	Emp. Verhalten	Absender	Technik	email	09:15	publish
09_20_A_zb_video	Beschreibung	Adressat	Emp. Verhalten	Absender	Technik	html	09:20	publish
09_25_A_of_scudonymus	Beschreibung	Adressat	Emp. Verhalten	Absender	Technik	html	09:25	publish
09_30_A_standard_scudonymus	Beschreibung	Adressat	Emp. Verhalten	Absender	Technik	html	09:30	publish
ATDS	Beobachtetes Verhalten	Kommunikation	IT-Systeme/Dienste	Kommentar	Erfuhr	Zeit	default	x
KAV	Beobachtetes Verhalten	Kommunikation	IT-Systeme/Dienste	Kommentar	Erfuhr	Zeit	default	x
MA14	Beobachtetes Verhalten	Kommunikation	IT-Systeme/Dienste	Kommentar	Erfuhr	Zeit	default	x
QEBB	Beobachtetes Verhalten	Kommunikation	IT-Systeme/Dienste	Kommentar	Erfuhr	Zeit	default	x
QESD	Beobachtetes Verhalten	Kommunikation	IT-Systeme/Dienste	Kommentar	Erfuhr	Zeit	default	x
QBSO	Beobachtetes Verhalten	Kommunikation	IT-Systeme/Dienste	Kommentar	Erfuhr	Zeit	default	x
THALES	Beobachtetes Verhalten	Kommunikation	IT-Systeme/Dienste	Kommentar	Erfuhr	Zeit	default	x
T-SYSTEM	Beobachtetes Verhalten	Kommunikation	IT-Systeme/Dienste	Kommentar	Erfuhr	Zeit	default	x
Alle								

SCUDO/Einigen/09_30_A_standard_scudonymus post [toggle chat](#)

ID	Beschreibung	Adressat	Emp. Verhalten	Absender	Technik	email	Zeitplan	publish
09_35_A_mitarbeiter_scudonymus	Beschreibung	Adressat	Emp. Verhalten	Absender	Technik	email	09:35	publish
09_45_A_hesse_fedstar	Beschreibung	Adressat	Emp. Verhalten	Absender	Technik	html	09:45	publish
09_55_A_kaspersky_ssl	Beschreibung	Adressat	Emp. Verhalten	Absender	Technik	html	09:55	publish
10_00_A_video_scudonymus	Beschreibung	Adressat	Emp. Verhalten	Absender	Technik	html	10:00	publish
14_25_S_Toysims_Registrar_Aud	Beschreibung	Adressat	Emp. Verhalten	Absender	Technik	email	10:00	publish

Demonstrator Ansicht 3 Spielleiter

The screenshot displays the THALES SCUDO TRAINING SCUDO MASTER interface. At the top, it shows the 'Scudo Master Board' with navigation buttons for 'Sortieren', 'Neues Spiel', 'Importieren', 'Messages', 'load Contacts', 'load Messages', and 'load Games'. The date and time are shown as 'Mar 3, 2015 12:57:09 PM'. Below this, there are several game entries, each with a play button, description, address, sender, recipient, technique, and scheduled time. The entry '09_35_A_mitarbeiter_scudonymus' is selected and expanded, showing a list of participants with columns for 'Beobachtetes Verhalten', 'Kommunikation', 'IT-Systeme/Dienste', 'Kommentar', 'Erkennung', 'Zeit', and 'Status'. The participants listed are KAV, MA14, OEBB, OESD, SBG, THALES, T-SYSTEM, and Alle. At the bottom, there is a 'login chat' button.

Demonstrator Ansicht Spieler

The screenshot displays the THALES SCUDO - Player interface. At the top, it shows the logo 'THALES SCUDO - Player' and the user role 'SPIELER'. The interface is titled 'Spieler Interface' and includes navigation buttons for 'Sortieren', 'Default', 'Medien', and 'Simulate insert'. A date and time indicator shows 'Die, 1. 2014 4:27:01 PM' with a German flag.

Below the navigation, there is a list of three games: 'Game-ABC-01', 'Game-ABC-02', and 'Game-ABC-03'. Each game entry has a play button and buttons for 'Beschreibung' and 'Aktion'.

The main content area features a news article titled '"Masque Attack": Neue iOS-Sicherheitslücke entdeckt' dated 11.11.14, 16:18. The article includes an image of a hand holding an iPhone and a 'FEATURED' badge. The text discusses a security vulnerability in the FireEye app, stating that 95% of iPhones and iPads are affected. A 'KOMMENTARE III' section is visible below the article.

To the right of the article, there is a comment section with a date '15.00 28.11.2014 | Spieler1' and a text area containing Latin placeholder text. Below this is a 'Test Kommentar' field and a 'Comment' button.

Demonstrator Ansicht Spielbeobachter

THALES SCUDO - Observer SPIELBEOBACHTER

Spielbeobachter Interface

Spielbeobachter: **Sortieren**

Die 3.  
2014 4:33:27 PM

Game-ABC-01 Beschreibung Erw. Verhalten Absender Technik (html) Zeitplan: 12:00 Beobachtetes Verhalten Kommunikation IT-Systeme/Dienste Kommentar Erfüllt: Zeit: Respond

Game-ABC-02 Beschreibung Erw. Verhalten Absender Technik (html) Zeitplan: 12:15 Beobachtetes Verhalten Kommunikation IT-Systeme/Dienste Kommentar Erfüllt: Zeit: Respond

Game-ABC-03 Beschreibung Erw. Verhalten Absender Technik (html) Zeitplan: 12:30 Beobachtetes Verhalten Kommunikation IT-Systeme/Dienste Kommentar Erfüllt: Zeit: Respond [archive](#)

Game-ABC-04 Beschreibung Erw. Verhalten Absender Technik (email) Zeitplan: 12:45 Beobachtetes Verhalten Kommunikation IT-Systeme/Dienste Kommentar Erfüllt: Zeit: Respond

Player called with Customer

CYBER SECURITY AUSTRIA DAS BOSE TRÜMPHERT ALLEN DADURCH DASS QUTE MENSCHEN NICHTS UNTERNEHMEN (Edward Bernik, 1976)

HOME VEREIN AKTIVITÄTEN PUBLIKATIONEN BLOGG SUCHE LINKS KONTAKT

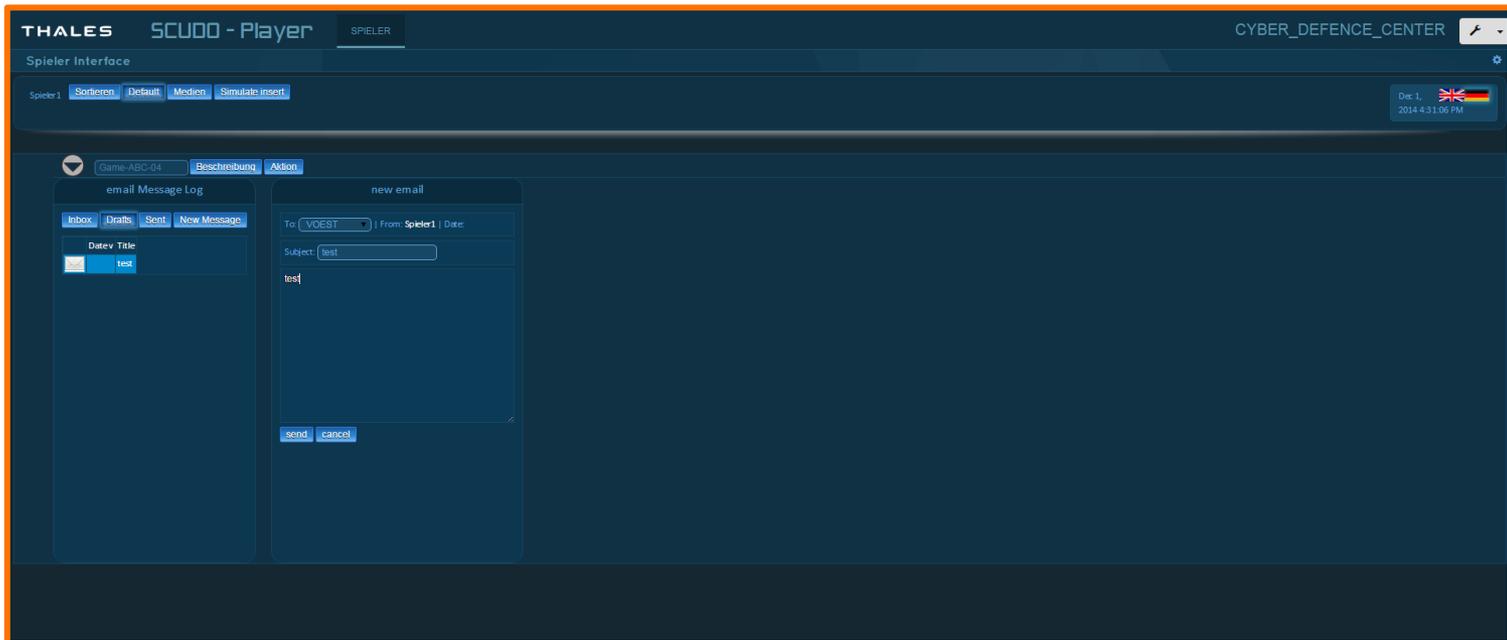
Aktivitäten

Die von "Cyber Security Austria" ist die beste öffentliche Vermittlung von gemeinsamen Erkenntnissen. Dies wird im Rahmen von verschiedenen Aktivitäten durchgeführt. Die Aufzählung stellt einen Teil dieser Aktivitäten dar.

Art	Vermittlung	Thema	Durchführung
Vortrag	Software Quality Days	Security of Legacy Systems	Holger Dörflinger, Florian Brunner

Art	Vermittlung	Thema	Durchführung
Bericht	CSA	CS User Security Challenge Austria 2014	CSA
Bericht	CSA	European Cyber Security Challenge 2014	CSA
Vollendung	Masterstudium „Sicherheitstechnologien“ des OÖH Linz	CS Security	Holger Dörflinger
Vortrag	Expert Cyber Intelligence Masterclass	Vermittlung und Konzeption - sind sie darauf vorbereitet?	Holger Dörflinger
Vortrag	ICT Skills November 2014	Wahr in Industrie 4.0 - Industrie 4.0 and Internet of Things	Holger Dörflinger
Vortrag	CSA Security Awareness in der 9th Fachforum 2014	Phishing Backlist	Holger Dörflinger
Live Hacken	Security Awareness in der 9th Fachforum 2014	On-Demand Live Marking	Eric Bock, Dörflinger, Jürgen Brunner
Vortrag	Security Awareness in der 9th Fachforum 2014	Equipment Industrie 4.0	Holger Dörflinger
Vereinbarung	European Cyber Security Month	Cyber Security Austria Red CyberWeek 19th September Awareness Day with the Austrian Police and local private industry	CSA/Police/Brunner
Live Hacken	2. Sicherheitsforum Österreich	In 1000 Live Marking 100 zeigen wie es geht - nicht so ungenügend!	Holger Dörflinger, Peter Rausch
Konferenz	SECURE - Tagung 11	CS versus Business IT	Holger Klauer
Vortrag	SECURE - Tagung 12	Equipment Industrie 4.0	Holger Dörflinger

Demonstrator Ansicht Kommunikation





Gruppenfoto Abschluss Übung

Kontakt Daten

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

Alexander Szönyi
Thales Austria GmbH
Alexander.szoenyi@thal.esgroup.com