Wie IT-Security Matchplays als Awarenessmaßnahme die IT-Sicherheit verbessern können

Andreas Rieb[1], Marko Hofmann[1], Alexander Laux[1], Steffi Rudel[1] und Ulrike Lechner[1]

[1] Universität der Bundeswehr München,
Professur für Wirtschaftsinformatik, München, Deutschland
{andreas.rieb,marko.hofmann,alexander.laux,steffi.rudel,
ulrike.lechner}@unibw.de

Abstract. „Operation Digitales Chamäleon" ist eine IT-Security Schulung in Form eines Serious Games. Zielgruppe des Spiels sind IT-Sicherheitsprofessionals. Teams entwerfen Angriffs- und Verteidigungsstrategien – eingebettet in einen Prozess von Schulung und Debriefing. Die vorliegende Arbeit adressiert die Frage, wie „Operation Digitales Chamäleon" die IT-Security Awareness bei IT-Sicherheitsprofessionals beeinflusst. Hierzu wird im ersten Teil das Design vorgestellt, welches im zweiten Teil um ausgewählte Ergebnisse der Evaluation von sieben Spielen zu Spielerlebnis, Wahrnehmung, Wissensgewinn und geplanten Verhaltensveränderungen ergänzt wird. „Operation Digitales Chamäleon" ist ein Format der IT-Security Matchplays, die im Rahmen des Forschungsprojekts VeSiKi entwickelt und validiert werden.

Keywords: IT-Sicherheit, Sensibilisierung, IT-Security Awareness, IT-Security Matchplay, Serious Game

13th International Conference on Wirtschaftsinformatik,
February 12-15, 2017, St. Gallen, Switzerland

Rieb, A.; Hofmann, M.; Laux, A.; Rudel, S.; Lechner, U. (2017): Wie IT-Security Matchplays als Awarenessmaßnahme die IT-Sicherheit verbessern können, in Leimeister, J.M.; Brenner, W. (Hrsg.): Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017), St. Gallen, S. 867-881

1 Einführung

Smartphone-Sticker, Kaffeetassen, Poster, Schulungen und Trainings – die Liste der Maßnahmen, die Anwender oder Mitarbeiter für das Thema IT-Sicherheit sensibilisieren sollen, ist lang. Spaß macht das Thema IT-Sicherheit meistens nicht. IT-Sicherheit Kritischer Infrastrukturen (KRITIS) ist ein neues Thema in der IT-Sicherheit, das die Absicherung von Produktionsanlagen, Logistikketten o.a. thematisiert. Stuxnet hat das Thema IT-Sicherheit für Kritische Infrastrukturen bekannt gemacht. So ist es notwendig, dass sich Mitarbeiter mit dem Thema IT-Sicherheit auseinandersetzen, die bisher die IT lediglich als Enabler im Rahmen der Unternehmensprozesse genutzt haben. Ebenso müssen sich IT-Professionals über IT-Sicherheit von Anlagen Gedanken machen, die bisher nicht als IT-Sicherheitsrisiko betrachtet wurden. Im Spannungsfeld von unpopulärer IT-Sicherheit und drängender Notwendigkeit Kritische Infrastrukturen abzusichern, soll „Operation Digitales Chamäleon“ Mitarbeiter sensibilisieren und befähigen, adäquat auf Bedrohungen der IT-Sicherheit zu reagieren.

„Operation Digitales Chamäleon“ ist eine IT-Sicherheitsschulung, die als ein Serious Game konzipiert und im Rahmen des Forschungsprojektes „Vernetzte IT-Sicherheit Kritischer Infrastrukturen” (VeSiKi) als Teil der IT-Security Matchplay Serie entwickelt und validiert wird. Das Serious Game basiert auf dem Format Wargaming und integriert Elemente der IT-Risiko- und IT-Bedrohungsanalyse. Ziel ist es, IT-Sicherheitsverantwortliche und IT-Sicherheitsprofessionals im Umgang mit Advanced Persistent Threats (APTs) zu schulen, wie sie typisch sind für KRITIS. APTs sind ausgeklügelte, dauerhafte und verschleierte Cyber-Bedrohungen [1]. Symantec beschreibt dies als “An advanced persistent threat (APT) uses multiple phases to break into a network, avoid detection, and harvest valuable information over the long term.“ und vermutet dass „Betrug – oder Schlimmeres“ Teil von APTs sind [2][3]. Zudem modifizieren die Angreifer während ihrer APT-Attacken regelmäßig ihre Angriffsvektoren und ihren Schadcode, um eine Entdeckung zu erschweren [4].

Dieser Artikel erweitert erste Publikationen zum Serious Game „Operation Digitales Chamäleon“. In [5] wurde „Operation Digitales Chamäleon“ als Instrument der Open Innovation mit einer Analyse des Innovationsgrads der APTs aus Spielergebnissen präsentiert. Das Spiel mit ausgewählten Spielergebnissen sind in einem Short Paper dargestellt [6].

2 State of the Art – IT-Security Awarenessmaßnahmen

„Operation Digitales Chamäleon“ wurde als IT-Security Awarenessmaßnahme konzipert. Im ersten Abschnitt wird der State of the Art in IT-Sicherheitsmaßnahmen vor allem in der Praxis zusammengefasst, während im zweiten Abschnitt vor allem der Stand der wissenschaftlichen Literatur zu Awareness dargestellt ist. In beiden Abschnitten sind die Verbindung von (passivem) „Wissen” zu (aktivem) „richtigen Handeln” sowie die Evaluation des Erfolgs besonders berücksichtigt. Der dritte Abschnitt ist „Serious Games” als Methode im Themenfeld IT-Sicherheit gewidmet.

2.1 IT-Security Awareness und Sensibilisierung in der Praxis

Maßnahmen zur Sensibilisierung für das Thema IT-Sicherheit (auch bezeichnet als IT-Security Awareness) sind in der Praxis weit verbreitet. So werden international bspw. in [7] und [8] verschiedene Maßnahmen inkl. Vor- und Nachteilen beschrieben. In einer Studie aus dem Jahr 2007 wurde u.a. untersucht, welche Maßnahmen in der Praxis eingesetzt und wie der Erfolg dieser Maßnahmen gemessen wird [9]. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bzw. die Allianz für Cyber-Sicherheit zu IT-Security Awareness stellt in ihrer Studie von 2015 [10] fest, dass 63% der Befragten angeben, dass IT-Security Awarenessmaßnahmen in der Organisation durchgeführt werden und dass Awarenessmaßnahmen überwiegend eine Präventivmaßnahme aufgrund wachsender Risiken sind. Als Maßnahmen werden angeführt (in absteigender Reihenfolge der Nennung): Dienstanweisungen/Vorschriften/Policies, Schulungen/Seminare in Gruppen, Informationskampagnen (z.B. Flyer, Poster), Mitarbeiterveranstaltungen (z.B. Roadshow), Einzelunterricht/E-Learning, Testszenarien zur Prüfung des Mitarbeiterverhaltens und andere; wobei als wesentliche Medien Intranet, E-Mail, Folienpräsentationen und Broschüren/Flyer, Poster und Mitarbeiterzeitschriften sowie Videos genannt werden. (Gewinn-)Spiele spielen nur eine untergeordnete Rolle. Diese Maßnahmen werden überwiegend nur sporadisch durchgeführt und eine Erfolgsmessung bleibt meistens aus. Nur ein kleiner Prozentsatz der befragten Unternehmen wertet die Sicherheitsvorfälle zur Erfolgsmessung der Awarenessmaßnahmen aus. Diese Zahlen und Daten decken sich mit der Erfahrung der Autoren dieses Artikels – interaktive Formate für IT-Security Awarenessmaßnahmen werden nur selten verwendet und der Nutzen für die IT-Sicherheit kaum evaluiert.

Für die IT-Sicherheit Kritischer Infrastrukturen stellt das BSI als maßgebliche staatliche Organisation in Deutschland Referenzwerke der Informationssicherheit bereit. Je nach Quelle ist auch von „IT-Sicherheit“ die Rede, jedoch wird derzeit dieser Begriff durch den Begriff „Informationssicherheit“ ersetzt. Grund dafür ist, dass sich IT-Sicherheit primär mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung beschäftigt, während Informationssicherheit als umfassender zu betrachten ist [11]. Innerhalb der o.a. Referenzwerke beschreibt das BSI auch Maßnahmen zur Sensibilisierung für das Thema Informationssicherheit und motiviert wie folgt: „Aufgrund der Entwicklung, dass inzwischen weder technische noch organisatorische Schutzmaßnahmen allein wirkungsvoll gegen Cyber-Bedrohungen schützen, rückt der Nutzer zunehmend in den Fokus. Er ist bei vielen Arten von Cyber-Angriffen noch häufig als das schwächste Glied in der Angriffskette zu sehen. […] Die kontinuierliche Sensibilisierung von Mitarbeitern für die bestehenden Risiken ist daher unerlässlich.“ [12]. Als Ziel wird genannt, die „Informationssicherheit in unser tägliches Handeln zu überführen“. Als Aufgaben werden bspw. angeführt: „Vermittlung der Ziele der Informationssicherheit“, „Empowerment, d.h. Vermittlung (praktischer) Kompetenzen hinsichtlich der Umsetzung von Regelungen“ oder „Positionierung von Informationssicherheit durch Kommunikation von Security-Themen,-Aufgaben, -Tools und -Protagonisten mit dem

Ziel, Bekanntheit und Akzeptanz zu steigern bzw. in der Unternehmenskultur als Teil der Sicherheitskultur zu etablieren.“ [12].

Im Baustein der IT-Grundschutzkataloge zu „Sensibilisierung und Schulung zur Informationssicherheit“ (B 1.13) [13] wird motiviert „alle Mitarbeiter erkennen und akzeptieren, dass [die Informationssicherheit] ein bedeutender und notwendiger Faktor für den Erfolg der Institution ist und [die Mitarbeiter] bereit sind, Sicherheitsmaßnahmen wirkungsvoll zu unterstützen“. Die Akzeptanz von Sicherheitsmaßnahmen zielt auf „langfristige Verhaltensänderungen“ ab, besonders wenn Informationssicherheit mit Komfort- oder Funktionseinbußen verbunden ist [13]. Planspiele werden als eine Maßnahme (M 3.47; [14]) empfohlen, um die Sensibilisierung und Schulung zur Informationssicherheit erfolgreich zu gestalten. Es ist wichtig, „eine positive und konstruktive Grundstimmung“ in Planspielen zu haben – denn „Ständige Angst vor Sicherheitsvorfällen kann einerseits zur Verdrängung von Sicherheitsproblemen und andererseits zu Panikreaktionen verleiten.“ [14]. Das BSI sieht in seinen Referenzwerken der IT-Sicherheit Sensibilisierung der Mitarbeiter als wichtiges Element einer IT-Sicherheitsstrategie an und zeigt auf, dass Planspiele oder Rollenspiele ein geeignetes Instrument wären, Mitarbeiter in einer positiven Atmosphäre zu schulen – im Baustein Planspiele jedoch gibt es außer drei Themen wenig Konkretes zu Planspielen für IT-Sicherheit.

An dieser Stelle soll erwähnt werden, dass sowohl Planspiele als auch Rollenspiele Formen von Serious Games sind [15]. In der Praxis, wie auch in der Literatur werden diese Begrifflichkeiten jedoch häufig synonym verwendet [16].

2.2 IT-Security Awareness aus Sicht der Wissenschaft

Die ausgezeichnete Literaturübersicht von Hänsch und Benenson systematisiert die Definitionen der IT-Security Awareness in Wahrnehmung (Perception), Schutz (Protection) und Verhalten (Behavior) mit den Fähigkeiten Bedrohungen zu erkennen (recognize threat), Wissen über Lösungen zu haben (know solutions) und richtig zu handeln (act right) [17]. Betrachtet werden in dieser Übersicht auch Messkriterien für IT-Security Awareness. Während Wahrnehmung und Schutz – entsprechend dieser Literaturübersicht – in verschiedenen Ansätzen gemessen werden kann, finden sich zu IT-Security Awareness für „richtiges Handeln“ nur wenige Methoden.

Die Forschung von Bulgurcu et al. illustriert die zentrale Rolle von IT-Security Awareness: Awareness beeinflusst mittelbar Nutzen von Compliance genau wie wahrgenommene Kosten von Compliance und von Non-Compliance [18]. Nach Johnston und Warketing genügen Wissen über Bedrohungen und Verwundbarkeiten nicht, sondern reduzieren Wirksamkeit und Selbstvertrauen (Response, Self Efficacy) und damit die Bereitschaft (richtig) zu handeln [19].

Das Konzept von IT-Security Literacy schlägt ähnlich wie IT-Security Awareness den Bogen zwischen „Wissen“ und „Wahrnehmung“ zu „richtigem Handeln“ in der IT-Sicherheit speziell in Schulungen und Trainings (vgl. bspw. [20]).

2.3 Serious Games in der IT-Sicherheit

„Operation Digitales Chamäleon“ wurde unter anderem entwickelt, um IT-Sicherheitsverantwortliche und IT-Sicherheitsprofessionals in spielerischer Art und Weise zu sensibilisieren. Die Methode Wargaming, die wir für „Operation Digitales Chamäleon“ adaptieren, hat eine lange Tradition: In der Literatur hat Wargaming seinen Ursprung im 19. Jahrhundert, als Baron von Reisswitz diese Methode nutzte, um Kommandostäbe in ihrer Entscheidungsfindung „besonders in dynamischen und unvorhersehbaren Situationen zu schulen“ [21]. Charakteristisches Element des Wargamings ist die durch Regeln gesteuerte und von Schiedsrichtern bewertete Auseinandersetzung der Ideen und Pläne zumindest zweier Teams (Rot und Blau). Die Methode wird vor allem für effektives Training von Kommandostäben verwendet, seltener auch zum Erforschen komplett neuer Bedrohungen. Jedoch ist Wargaming in der Domäne IT-Sicherheit eher neu.

2012 gab ENISA einen Überblick über 85 IT-Security Übungen [22]. Die meisten davon waren theoretische Übungen “to validate plans and integration of procedures prior to moving on to more complex, team-based activities” [22]. Ziele dieser IT-Security Übungen waren u.a. die Steigerung von IT-Security Awareness bzgl. Cyber-Bedrohungen, Rollenidentifikation, Klärung von Verantwortlichkeiten und zuständigen Behörden, Entscheidungsfindung, Überprüfung des Incident Managements oder Vertrauensbildung zwischen Staaten [22]. 2015 wurde der ENISA-Bericht um mehr als 200 Übungen erweitert [23]. Hier hebt ENISA Methoden wie Red Teaming, Diskussionsbasierte Spiele, Capture the Flag, Seminare und weitere hervor. Gemäß ENISA [23] wird nur ein Bruchteil (11%) der Übungen mit gegenüberstehenden Teams durchgeführt.

Weitere Serious Games für IT-Sicherheit sind beispielsweise „Friend Inspector“ – ein softwarebasiertes Serious Game zur Steigerung der IT-Security Awareness unter Facebook-Nutzern [24][25]. Das Kartenspiel „Elevation of Privilege“ dient ebenfalls der Steigerung von IT-Security Awareness, jedoch stehen hier Softwareentwickler im Vordergrund [26]. Die Zielgruppe „Mitarbeiter eines Unternehmens“ adressiert das Kartenspiel von Beckers und Pape zu Gefahren und Methoden des Social Engineerings [27]. „Game of Threats“ adressiert das Management [28].

3 Methode

In der Forschung orientiert sich dieser Beitrag am Paradigma der gestaltungs-orientierten Forschung (Design Science) von Hevner et al. [29]. Wir verwenden einen iterativen Ansatz in Design und Evaluation mit einem kreativen Designprozess – so wie es bspw. Baskerville und Pries-Heje beschreiben [30]. Dieser kreative Designprozess bezieht insbesondere die mehr als 10 jährige Erfahrung des ersten Autors als IT-Security und IT-Security Awareness Spezialist mit ein.

In der Datengenerierung hat der erste Autor des vorliegenden Artikels als Spiel-leiter die Daten gesammelt, Umfragen durchgeführt und Beobachtungen protokolliert. In einem Fall wurde er von einem Beobachter in der Datensammlung unterstützt.

4 Das Spieldesign von „Operation Digitales Chamäleon”

„Operation Digitales Chamäleon“ ist als IT-Security Awarenessmaßnahme konzipiert und speziell entwickelt für die Schulung zum Thema IT-Sicherheit Kritischer Infrastrukturen. Diese Schulung umfasst neben der eigentlichen Spielphase eine Phase der Wissensvermittlung zu aktuellen IT-Sicherheitstechnologien und -bedrohungen mit ggf. Live-Hackings sowie eine Phase des Debriefings, die u.a. auch eine Umfrage beinhaltet. „Operation Digitales Chamäleon“ ist ein Planspiel und verwendet „traditionelle“, also nicht IT-gestützten Spielmaterialien.

4.1 Teams und Zielgruppe

„Operation Digitales Chamäleon“ ist als IT-Security Awarenessmaßnahme für IT-Sicherheitsverantwortliche und IT-Sicherheitsprofessionals als Zielgruppe konzipiert. Spielteilnehmer füllen in ihren Organisationen IT-Sicherheitsfunktionen aus oder haben berufliche Erfahrung im Themenfeld IT-Sicherheit (bspw. IT-Sicherheitsadministratoren auf operativer Ebene, IT-Security Manager). „Operation Digitales Chamäleon“ wird mit einer Gruppe von 8 bis 20 Personen durchgeführt.

Im Serious Game tritt diese Zielgruppe in Teams gegeneinander an: Team Rot als Angreifer gegen Team Blau als Verteidiger – ein weißes Team übernimmt Spielleitung und Schiedsrichterfunktion. Typischerweise haben Team Rot und Team Blau jeweils drei bis sieben Mitglieder.

Zu Beginn wählt Team Rot eine von fünf vorgegebenen Angreiferrollen (Threat Actors). Die Angreiferrolle beschreibt die Motivation und die Fähigkeiten des Threat Actors, die Grundlage für die zu planenden Angriffsstrategien bilden. In „Operation Digitales Chamäleon“ stehen insgesamt fünf verschiedene Angreiferrollen bzw. Threat Actors zur Verfügung: Script Kiddies, Cyber Criminals, Employees, Nation States und Hacktivists. Die Rolle „Hacktivists“ ist bspw. auf der Basis von Hald und Petersen [31] in den Spielunterlagen beschrieben: Ruhm, Ehre oder ein „moralischer Grund” sind die Motivationen, die finanziellen Ressourcen sind limitiert, jedoch sind die technischen Fähigkeiten „gut“.

Team Blau verteidigt die Kritische Infrastruktur und dem Team ist bekannt, welcher Threat Actor sie angreifen wird. So hat Team Blau die Aufgabe, sich in die Rolle des Angreifers hineinzuversetzen, die kritischen Assets (z.B. Personen, Netzwerkkomponenten, IT-Systeme u.a. Vermögenswerte) zu identifizieren und die IT-Sicherheitsmaßnahmen spezifisch auf zu erwartenden Angriffe auszurichten. Team Blau etabliert Schutzmaßnahmen zu den Faktoren Organisation, Technik und Mensch und erstellt ein IT-Sicherheitskonzept.

Team Weiß trifft als Spielleitung die Entscheidungen über den Spielablauf und überwacht die Einhaltung der Regeln. Beobachter oder Experten dokumentieren Spielverlauf und Ergebnisse und wirken bei der Ermittlung des Siegerteams mit.

Team Rot und Team Blau haben je einen Teamleiter, der durch Losverfahren bestimmt wird. Die Teamleitung organisiert die Teamarbeit, präsentiert die Ergebnisse und wählt (im Fall Rot) die Angreiferrolle.

4.2 Spielbrett und Spielmaterialien

„Operation Digitales Chamäleon“ verwendet konventionelle, nicht-digitale Spielmaterialien. Dazu gehören u.a. ein Spielbrett, auf dem ein Netzplan mit IT-Infrastrukturkomponenten abgebildet ist, wie sie für Kritische Infrastrukturen typisch sind (siehe Abbildung 1). Assets dieses Netzplans sind u.a. eine Industrieanlage sowie Windows PCs mit verschiedenen älteren, teilweise nicht mehr unterstützten Betriebssystemen. Zudem beinhaltet der Netzplan einen Fernwartungszugang, mobile Clients und ein Office-Teilnetz mit aktuelleren Betriebssystemen, Servern und Druckern. Die Teilnetze werden zu Beginn des Serious Games nur durch Router geschützt.

Abbildung 1: Das Spielbrett zu „Operation Digitales Chamäleon“

Mit Karten wird markiert, welches Asset der IT-Infrastruktur angegriffen bzw. verteidigt wird. Auf Post-Its werden Ideen zu Angriffsvektoren oder Schutzmaßnahmen notiert. Das Spielmaterial beinhaltet (pro Team) Karten, die die Rollen beschreiben, einen Satz Spielregeln, sowie Stifte für Notizen auf dem Spielbrett. Spielleibchen in den Farben Rot, Blau oder Weiß markieren die Teamzugehörigkeit. Dem Spielleiter bzw. dem weißen Team stehen für die Unterstützung der Entscheidung über die Machbarkeit diverser Angriffe oder Schutzmaßnahmen Zufallskarten mit unterschiedlichen Wahrscheinlichkeiten zur Verfügung.

4.3 Spielregeln, Spielablauf und Spielmissionen

Zu Beginn der Spielphase wird die Rahmenlage durch die Spielleitung präsentiert. Team Rot wird vorgegeben, dass der Angriff entsprechend der gewählten Spielerrolle eine Wirkung entfalten muss, die es notwendig macht, das BSI entsprechend den Meldepflichten – so wie sie im IT-Sicherheitsgesetz festgelegt sind – zu informieren [32].

Die Teams werden im Briefing ermuntert kreativ zu sein. Somit sind der Phantasie im Spiel nur wenig Grenzen gesetzt – es limitieren Spielzeit und Plausibilität.

Team Rot nimmt die Sicht des gewählten Threat Actors ein und soll einen Angriffspfad entwickeln, der für diese Angreiferrolle hinsichtlich Absichten, Ressourcen und Methoden typisch ist. Dieser Angriffspfad besteht aus voneinander abhängigen und ggf. alternativen Angriffsvektoren. In den weiteren Spielmissionen

bekommt Team Rot die Aufgabe, Alternativen zu den einzelnen Angriffsvektoren zu definieren und den Angriffsbaum auch zu präsentieren.

Das blaue Team verfolgt das Ziel, die bevorstehenden Cyberangriffe erfolgreich abzuwehren. Team Blau entwickelt ein IT-Sicherheitskonzept sowie Schutzmaßnahmen zu den Faktoren Organisation, Technik und Mensch. Die Regeln des Spiels legen fest, dass die IT-Sicherheitsstrategie von Team Blau jedoch nicht zu Lasten der Verfügbarkeit und Nutzerfreundlichkeit der IT der KRITIS gehen darf. Die Regeln geben ebenfalls vor, dass die Mitarbeiter (der KRITIS) die Internetanbindung auch für Internetdienste wie Facebook nutzen. Ferner dürfen Netzverbindungen und Fernwartungszugänge nicht aus Gründen der IT-Sicherheit gekappt werden. Solche und andere der Realität entsprechenden Prämissen verhindern, dass Team Blau die „sicherste“ Lösung – das dauerhafte Trennen sämtlicher Internetverbindungen – wählt. Team Blau ist so gefordert, kreative Lösungen zu entwickeln, um die Angriffe von Team Rot zu antizipieren und abzuwehren.

In der Ermittlung des siegreichen Teams sind Nachvollziehbarkeit in der Argumentation und Transparenz der Entscheidungsfindung wichtig. Die Teams präsentieren die erarbeiteten Lösungen. Die Spielleitung geht Angriffsvektor um Angriffsvektor durch und bezieht die Teams in die Diskussion mit ein. In dieser Bewertung finden drei Kriterien Anwendung: (Technische) Machbarkeit (1), Plausibilität (2) und Erfolg im Hinblick auf Schutzmaßnahmen, die von Team Blau festgelegt wurden (3). Für Fälle, in denen keine eindeutige Entscheidung in der Diskussion getroffen werden kann, hilft „der Zufall“, implementiert als Spielkarten.

Die Teams erhalten einen Ordner mit Informationen über den Spielablauf und den Spielregeln. Diese legen beispielsweise fest, dass außerhalb der Spielzeiten nicht an der Weiterentwicklung der Strategie im Team gearbeitet werden darf. Zudem dürfen die Teams keine IT-Unterstützung in Form von Laptops, Smartphones o.ä. nutzen.

4.4 Das Debriefing

Ein Debriefing gibt den Teilnehmern die Möglichkeit, ihre persönlichen Erkenntnisse zu reflektieren und gibt Anregungen, das im Spiel Erfahrene in den Arbeitsalltag zu übernehmen. Hier folgt das Spiel den Anregungen von Kriz [33]. Wesentliche Ergebnisse, die im Rahmen dieser Debriefings gewonnen wurden, werden im nächsten Abschnitt vorgestellt.

5 Ergebnisse der „Operation Digitales Chamäleon“

Der nachfolgende Abschnitt stellt wesentliche Ergebnisse der gespielten Serious Games „Operation Digitales Chamäleon“ vor. Hierbei stützt sich die Empirie auf sieben Spiele, die in Tabelle 1 gelistet sind.

Tabelle 1. Durchgeführte Spiele „Operation Digitales Chamäleon"

#	Datum	Dauer Training	Dauer Spiel	Teil-nehmer	Anzahl rote Teams	Anzahl blaue Teams	Sektor	Länder-code
1	10/2015	3d	6h	11	1	1	Staat und Verwaltung (Polizei, Justiz)	DEU
2	01/2016	5d	9h	9	1	1	Transport und Verkehr (Luftfahrt)	FRA
3	03/2016	2d	6h	10	1	1	Staat und Verwaltung (Polizei)	DEU
4	03/2016	2d	10.5h	19	3	1	Staat und Verwaltung (Militär)	DEU
5	05/2016	2d	10h	18	2	1	Staat und Verwaltung (Militär)	DEU
6	05/2016	2d	10h	20	3	1	Staat und Verwaltung (Militär)	DEU
7	07/2016	2d	10.5h	17	3	1	Staat und Verwaltung (Militär)	DEU

Es ist zu beachten, dass in dem iterativen Vorgehen beim Design des Serious Games auch die Evaluation weiterentwickelt wird. So wurde der Fragebogen zur Evaluation des Spiels erst ab Spiel #4 eingesetzt. Ergebnisse wurden in den Spielen #2 und #3 mittels Post-Its im Rahmen einer moderierten Gruppendiskussion erhoben. Spiel #1 diente als Pretest mit Fokus auf die Spieldurchführung – hier wurden Notizen des Spielleiters während des Debriefings angefertigt.

5.1 Spielerlebnis

Spielerisches Lernen wird mit Spaß assoziiert und eine positive, angstfreie Atmosphäre ist entsprechend den Empfehlungen des BSI und den empirischen Resultaten (vgl. Kap. 2.1 und 2.2) wichtig für den Erfolg von Schulungen und speziell Sensibilisierungsmaßnahmen. Dies steht in Einklang mit den Empfehlungen zur Entwicklung von Serious Games (z.B. [34]). Gemäß McConigal ist Spaß während des Spielens eine wichtige Voraussetzung zur Steigerung der Motivation der Teilnehmer und der Qualität der Spielergebnisse [35]. Killmeyer definiert den Faktor Spaß ebenfalls als wichtige Voraussetzung für eine erfolgreiche IT-Sicherheitssensibilisierung [36]. Tabelle 2 zeigt die Ergebnisse der Spielevaluation per Fragebogen zur Aussage „Das Cyberwargame hat mir Spaß gemacht".

Tabelle 2. Spaßfaktor in Spiel #4 bis #7

Aussage	*Trifft nicht zu*	*Trifft eher nicht zu*	*Neutral*	*Trifft teilweise zu*	*Trifft voll zu*
Das Cyberwargame hat mir Spaß gemacht.	0	3	4	41	26

„Operation Digitales Chamäleon" hat den meisten Spielteilnehmern Spaß gemacht. Beobachtungen seitens des Spielleiters bestätigen dieses Ergebnis: Während der Durchführungen konnten des Öfteren Reaktionen wie „lautes Lachen" beobachtet werden. In allen Spielen herrschte eine konzentrierte, aber lockere Atmosphäre – keiner der 104 Spielteilnehmer der ersten sieben Spiele ist vorzeitig ausgestiegen. Eine positive Arbeitsstimmung ist wesentliche Voraussetzung für den (langfristigen) Erfolg der Sensibilisierungsmaßnahme und damit für die Verbesserung der IT-Sicherheit wie in den folgenden Kapiteln dargestellt.

5.2 Wahrnehmung

IT-Security Awareness beinhaltet die Wahrnehmung (Definitionen Awareness Kap. 2.2) von Gefahren und Risiken. Im Debriefing von Spiel #4 bis #7 wurde ermittelt, ob „Operation Digitales Chamäleon“ die Wahrnehmung verbessert.

Tabelle 3. Risikobewusstsein / Bedrohungseinschätzung in Spiel #4 bis #7

Aussage	*Trifft nicht zu*	*Trifft eher nicht zu*	*Neutral*	*Trifft teilweise zu*	*Trifft voll zu*
Ich stelle für mich eine Steigerung meines IT-Risikobewusstseins fest.	1	3	9	34	27
Ich kann die Komplexität von Bedrohungen auf die IT-Infrastruktur besser einschätzen.	0	4	9	46	15

Tabelle 3 stellt dar, dass „Operation Digitales Chamäleon“ sowohl das IT-Risikobewusstsein, als auch die Fähigkeit, die Komplexität von Bedrohungen auf die IT-Infrastruktur einschätzen zu können, positiv beeinflusst. Der Selbsteinschätzung der Teilnehmer nach, ist das Spiel nicht nur geeignet (Fakten-) Wissen zu vermitteln, sondern schlägt die Brücke zu Wahrnehmung und richtigem Handeln (vgl. Kap. 2.2).

5.3 Wissensgewinn

Im Debriefing von Spiel #4 bis #7 wird im Fragebogen nach dem Wissenszuwachs gefragt und die Mehrheit stellt einen Wissenszuwachs für sich fest (vgl. Tabelle 4).

Tabelle 4. Wissensgewinn in Spiel #4 bis #7

Aussage	*Trifft nicht zu*	*Trifft eher nicht zu*	*Neutral*	*Trifft teilweise zu*	*Trifft voll zu*
Ich stelle für mich einen Wissenszuwachs am Ende der Veranstaltung fest.	0	1	4	28	41

In einer zweiten, offenen Frage (Durchführung #4 bis #7) oder in einem Debriefing über Post-Its werden die Spielteilnehmer nach dem Wissensgewinn gefragt. Nach sieben Durchführungen stehen 144 Aussagen zur Auswertung zur Verfügung. In einer qualitativen Inhaltsanalyse nach Mayring [37] werden diese 144 Aussagen in die drei Hauptkategorien „Wissen über Angriffe“, „Wissen über Schutzmaßnahmen“ und „Sonstiges Wissen“ einsortiert.

Die beiden Kategorien „Wissen über Angriffe“ mit 57 Aussagen sowie „Wissen über Schutzmaßnahmen“ mit 66 Aussagen sind in etwa gleich stark ausgeprägt („Sonstiges Wissen“ mit 21 Aussagen). Dieses Ergebnis ist bemerkenswert: Die „böse Seite“ – also das rote Team – hat die kreativere Rolle und so wäre eine intensivere Auseinandersetzung mit Angriffen, also mehr Nennungen in der Kategorie „Wissen über Angriffe“ zu erwarten. Zudem sind in den sieben Spielen mehr rote als blaue Teams angetreten und zusätzlich werden in der Wissensvermittlung bspw. in Live-Hackings Angriffe plastischer behandelt als Schutzmaßnahmen. Dies illustriert, dass

„Operation Digitales Chamäleon“ zur Auseinandersetzung mit Schutzmaßnahmen anregt – entsprechend dem Forschungsziel, IT-Sicherheit für KRITIS zu verbessern.

Eine zweite Inhaltsanalyse der Aussagen zu „Technik“, „Organisation“, „Mensch“, und „Übergreifend“ lässt erkennen, dass die Spielteilnehmer auf Angreiferseite mehr „übergreifendes Wissen“ gewinnen konnten. Exemplarisch ist hier die Aussage „Arbeitsweise von Nation States“ zu nennen. Auf der Seite der Schutzmaßnahmen werden mehr spezifische Einzelmaßnahmen genannt. Genannte Beispiele sind das PAP-Prinzip des BSI (vgl. [38]) oder die Funktionsweise einer Datendiode (vgl. [39]).

Spielteilnehmer stellen interessanterweise nicht nur neueste Bedrohungen oder Schutztechnologien sondern auch ältere Angriffsvektoren oder etablierte Sicherheitstechnologien als Wissenszuwachs dar. So wurden als „Neues Wissen“ referernziert: der seit Jahrzehnten bekannte Angriffsvektor „Man-in-the-Middle“, der „Unterschied zwischen IDS / IPS“ , Angriffsvektoren wie „Man-in-the-Cloud“ [40] aus dem Jahr 2015 oder „Watering hole attack“ [41] von 2012. Das illustriert die Notwendigkeit für Sensibilisierungsmaßnahmen – auch für Funktionsträger.

„Operation Digitales Chamäleon“ vermag also neues Wissen zu vermitteln und sensibilisiert besonders im Themenfeld der Schutzmaßnahmen.

5.4 Verhaltensänderung

Im Debriefing reflektieren die Teilnehmer ihre Erfahrungen der Spielphase und leiten daraus individuell Vorsätze für ihre berufliche Tätigkeit ab. Die empirische Basis umfasst 208 Vorsätze (aus Spiel #1-#7), die mittels Fragebogen und in Diskussionen erhoben und in qualitativer Inhaltsanalyse nach Mayring [37] analysiert wurden. Jeder Vorsatz wird einer Kategorie (Individuum, Organisation, IT-Infrastruktur) zugeordnet, abhängig worauf sich ein Vorsatz auswirkt (siehe Tabelle 5).

Tabelle 5. Ausgewählte Vorsätze der Spielteilnehmer im Hinblick auf eine Verhaltensänderung

Individuum	*Organisation*	*IT-Infrastruktur*
Büros nicht unverschlossen lassen; Mehr Berichte / TecBlogs zum Thema IT-Sicherheit / Cyberwar lesen; Mehr Zeit in IT-Sicherheit investieren; Bewusster auf potentielle Gefahren achten;	Transparenz in der IT-Sicherheit; Sensibilisierung der Mitarbeiter intensivieren; Mit den anderen Administratoren Angriffsszenarien ausdenken und dann checken, ob man safe ist; Kompetenzen auf mehrere Schultern verteilen;	Öfter eigenes Netzwerk penetrieren; Regelmäßige Schwachstellenanalyse; Datenabfluss über Web-Schnittstellen (Cloud, Email, …) verhindern / eindämmen; Testumgebung für kommende Updates nutzen (Office, Windows 7, Java etc.);

Auffällig ist, dass viele Vorsätze genannt werden, die die Organisation betreffen: Organisation (117 Vorsätze), Individuum (78 Vorsätze), IT-Infrastruktur (13 Vorsätze). Das zeigt, dass „Operation Digitales Chamäleon“ eher organisatorische IT-Sicherheit als technischen Schutz der IT-Infrastruktur adressiert. Gerade vor dem Hintergrund, dass sich im Themenfeld IT-Sicherheit Kritischer Infrastrukturen IT-Professionals um die Sicherheit von bspw. Industrieanlagen Gedanken machen müssen, die bisher nicht als IT-Sicherheitsrisiko eingeschätzt wurden, kann ein solcher Impuls die notwendigen organisatorischen Änderungen anregen.

Tabelle 6. Kategorien und Anzahl der Vorsätze für Verhaltensänderung

Kategorie	*Anzahl der Vorsätze*
(Organisatorisches) IT-Security Awarenesstraining	55
(Individuelles) IT-Security Awarenesstraining	27
Operative IT-Security-Vorgänge	19
Monitoring	18
Bestehende IT-Security-Konzepte	15
Aufgeschlossene Denkansätze	14
Cross-Functional IT-Security-Teams	13
Aufmerksamkeit	11
Informationsverteilung	10
Informationsbeschaffung	6
Auditing	5
Penetration Testing	5
Abschreckung	3
Personalmanagement	3
Resignation	2
Keine Verhaltensänderung	1
Keine Auswertung möglich	1

In einer qualitativen Inhaltsanalyse wurden die 208 Vorsätze in 17 Kategorien systematisiert (vgl. Tabelle 6). 55 Vorsätze werden der Kategorie „(Organisatorisches) IT-Security Awarenesstraining“ zugeordnet: Spielteilnehmer möchten die Mitarbeiter der Organisation besser sensibilisieren. 27 Vorsätze umfasst die Kategorie „(Individuelles) IT-Security Awarenesstraining“, mit Vorsätzen wie „Erhöhte Weiterbildung im Bereich IT-Sicherheit“. Kategorie „Operative IT-Security-Vorgänge“ beinhaltet 19 Vorsätze – ein Beispiel ist, zu prüfen, „Dass keine unbekannte Person sich alleine im Raum aufhält“. Auch dies illustriert, dass das Spiel Impulse setzt, IT-Sicherheit als Organisationsaufgabe zu begreifen.

In den Spieldurchführungen konnte beobachtet werden, dass interdisziplinäre Teams gute Resultate erzielen, also Teams mit Mitgliedern entweder verschiedener Hierarchiestufen von der strategischen bis hin zur operativen Ebene oder mit Mitgliedern aus den Kernthemen der IT-Sicherheit zusammen mit Vertretern angrenzender Domänen wie Arbeitsschutz oder bauliche Sicherheit. So nutzte bspw. ein blaues (interdisziplinäres) Team Motivatoren zur Steigerung der Mitarbeiterzufriedenheit um die Bereitschaft der Mitarbeiter, Innentäter zu werden zu reduzieren. Die Notwendigkeit für Interdisziplinarität spiegelt sich auch in den Vorsätzen wieder. So beinhaltet Kategorie „Cross-Functional IT-Security-Teams“ 13 Vorsätze, von denen ein Vorsatz lautet: „Zusammenarbeit mit anderen (Admins, User, SiBe, Brandschutzbeauftragter)“.

Nur vergleichsweise wenige Spielteilnehmer planen als Vorsatz die IT-Sicherheitstechnologie zu verbessern oder zu erneuern. Spielteilnehmer gaben an, sie wollen bspw. häufiger nach Schwachstellen oder Fehlkonfigurationen in der IT-Infrastruktur suchen und diese beheben („Penetration Testing“ (5 Vorsätze)).

Zusammenfassend lässt sich feststellen, dass „Operation Digitales Chamäleon“ zu Verhaltensänderungen motiviert, also nicht alleine Faktenwissen vermittelt und vor allem zur Auseinandersetzung mit organisatorischen Aspekten anregt.

6 Zusammenfassung und Ausblick

In diesem Artikel präsentierten wir unsere IT-Security Awarenessmaßnahme „Operation Digitales Chamäleon“ mit ausgewählten Ergebnissen der ersten sieben Durchführungen. Die APTs als Spielergebnisse zeigen, dass die Spielteilnehmer APTs und IT-Sicherheitsmaßnahmen realistischer Komplexität erarbeiten und so „Operation Digitales Chamäleon“ geeignet ist, als IT-Security Awarenessmaßnahme für IT-Sicherheitsverantwortliche und IT-Sicherheitsprofessionals im KRITIS Kontext eingesetzt zu werden (vgl. [5] [6]). Die Auswahl der Ergebnisse liegt in diesem Beitrag auf dem Spielerlebnis, der Wahrnehmung, dem Wissensgewinn und der Verhaltensänderung. Das Spiel macht Spaß und erfüllt damit ein wichtiges Erfolgsmerkmal von Serious Games. „Operation Digitales Chamäleon“ motiviert die Spielteilnehmer zu Verhaltensänderungen, und vermittelt nicht alleine Faktenwissen. Diese Verhaltensänderungen betreffen eher organisatorische als individuelle oder technische Aspekte. „Operation Digitales Chamäleon“ adressiert also die wichtigen Themen der IT-Sicherheit Kritischer Infrastrukturen. Das deckt sich mit den Empfehlungen des BSI: Langfristige Verhaltensänderungen sind wesentlich für ein langfristig erfolgreiches IT-Sicherheitsmanagement – neue IT-Sicherheitstechnologie anzuschaffen genügt nicht. Die Evaluation des Erfolgs solcher IT-Sicherheitsawarenessmaßnahmen ist inhärent schwierig zu evaluieren – das zeigen der State of the Art von Praxis und wissenschaftlicher Literatur und so ist die Evaluation des Spieles dem Spielgegenstand angemessen.

„Operation Digitale Schlange“ und „Operation Digitale Eule“ sind zusammen mit „Operation Digitales Chamäleon“ die ersten Spielformate der IT-Security Matchplay Serie. Für alle drei Formate sind weitere Spiele und Weiterentwicklungen geplant.

7 Danksagung

Hiermit bedanken wir uns beim BMBF als Fördergeber des Projekts „Vernetzte IT-Sicherheit Kritischer Infrastrukturen“ (FKZ 16KIS0213). Ebenso möchten wir allen Spielteilnehmern für die guten Spielergebnisse und das Engagement danken. Dem Associate Editor und den Gutachtern sind wir für hilfreiche und konstruktive Kommentare dankbar.

Literaturverzeichnis

1. McAfee: Combating Advanced Persistent Threats. , Santa Clara (2011).
2. Symantec: Advanced Persistent Threats: How They Work, http://www.symantec.com/theme.jsp?themeid=apt-infographic-1.
3. Rowney, K.: What We Talk About When We Talk About APT, http://www.symantec.com/connect/blogs/what-we-talk-about-when-we-talk-about-apt#!
4. Rouse, M.: advanced persistent threat (APT), http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT.
5. Rieb, A., Lechner, U.: Operation Digital Chameleon – Towards an Open Cybersecurity Method. In: Proceedings of the 12th International Symposium on Open Collaboration

(OpenSym 2016). pp. 1–10. , Berlin (2016).
6. Rieb, A., Lechner, U.: Towards Operation Digital Chameleon. In: Havârneanu, G., Setola, R., Nassopoulos, H., and Wolthusen, S. (eds.) CRITIS 2016 - The 11th International Conference on Critical Information Infrastructures Security (to appear). pp. 1–6. , Paris (2016).
7. Wilson, M., Hash, J.: NIST Special Publication 800-50: Building an Information Technology Security Awareness and Training Program. , Gaithersburg (2003).
8. ENISA: Der neue Leitfaden für die Praxis: Wege zu mehr Bewusstsein für Informationssicherheit. Europäische Agentur für Netz- und Informationssicherheit (ENISA) (2008).
9. ENISA: Information security awareness initiatives: Current practice and the measurement of success. (2007).
10. BSI: Awareness-Umfrage 2015, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/awareness-umfrage-2015.pdf?__blob=publicationFile&v=5, (2016).
11. BSI: IT-Grundschutz: Glossar und Begriffsdefinitionen, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html.
12. BSI: ERFA-Kreis Awareness, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Erfahrungsaustausch/ERFA-Kreise/Awareness/awareness.html.
13. BSI: IT-Grundschutz - B 1.13 Sensibilisierung und Schulung zur Informationssicherheit, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b01/b01013.html.
14. BSI: IT-Grundschutz - M 3.47 Durchführung von Planspielen zur Informationssicherheit, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m03/m03047.html.
15. Blötz, U.: Planspiele und Serious Games in der beruflichen Bildung: Auswahl, Konzepte, Lernarrangements, Erfahrungen - Aktueller Katalog für Planspiele und Serious Games (Berichte zur beruflichen Bildung). W. Bertelsmann Verlag GmbH & Co. KG, Bielefeld (2015).
16. Schwägele, S.: Planspiel - Lernen - Lerntransfer. Eine subjektorientierte Analyse von Einflussfaktoren, file:///home/arieb/Downloads/SchwaegeleDissopusse_A3a.pdf.
17. Hansch, N., Benenson, Z.: Specifying IT security awareness. In: Proceedings - International Workshop on Database and Expert Systems Applications, DEXA. pp. 326–330. , München (2014).
18. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Q. 34, 523–548 (2011).
19. Johnston, A.C., Warkentin, M.: Fear Appeals and information Security Behaviors: An Empirical Study. MISQ. 34, 549–566 (2010).
20. Furnell, S., Moore, L.: Security literacy: The missing link in today's online society? Comput. Fraud Secur. 2014, 12–18 (2014).
21. Perla, P.P.: The Art of Wargaming: A Guide for Professionals and Hobbyists. US Naval Institute Press (1990).
22. ENISA: On National and International Cyber Security Exercises. Europäische Agentur für Netz- und Informationssicherheit (ENISA), Heraklion (2012).
23. ENISA: The 2015 Report on National and International Cyber Security Exercises. Europäische Agentur für Netz- und Informationssicherheit (ENISA), Athen (2015).
24. Cetto, A., Netter, M., Pernul, G.: Friend Inspector: A Serious Game to Enhance Privacy

Awareness in Social Networks. Proc. 2nd Int. Work. Intell. Digit. Games Empower. Incl. (IDGEI '13). 1–8 (2014).
25. Netter, M., Pernul, G., Richthammer, C., Riesner, M.: Privacy in Social Networks: Existing Challenges and Proposals for Solutions. Commun. Comput. Inf. Sci. 576, 16–27 (2015).
26. Shostack, A.: Elevation of Privilege: Drawing Developers into Threat Modeling. USENIX Summit Gaming, Games, Gamification Secur. Educ. 1–15 (2014).
27. Beckers, K., Pape, S.: A Serious Game for Eliciting Social Engineering Security Requirements. Presented at the (2016).
28. PWC: Game of ThreatsTM – Cybersecurity-Simulation für Manager, http://www.pwc.de/de/digitale-transformation/game-of-threats-cybersecurity-simulation-fuer-manager.html.
29. Hevner, A.R., March, S.T., Park, J., Ram, S.: Design Science in Information Systems Research. MIS Q. 28, 75–105 (2004).
30. Baskerville, R., Pries-Heje, J.: Explanatory Design Theory. Bus. Inf. Syst. Eng. 2, 271–282 (2010).
31. Hald, S., Pedersen, J.: An updated taxonomy for characterizing hackers according to their threat properties. Adv. Commun. Technol. (ICACT), 2012 14th Int. Conf. 81–86 (2012).
32. BSI: Industrie und Kritische Infrastrukturen: Meldepflicht, https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/IT-SiG/Neuregelungen_KRITIS/Meldepflicht/meldepflicht_node.html.
33. Kriz, W.C., Nöbauer, B.: Den Lernerfolg mit Debriefing von Planspielen sichern, http://www.bibb.de/dokumente/pdf/1_08a.pdf.
34. Kriz, W.C., Hense, J.: Qualitätskriterien von Planspielprodukten. In: Blötz, U. (ed.) Planspiele und Serious Games in der beruflichen Bildung2. pp. 222–223. W. Bertelsmann Verlag GmbH & Co. KG, Bielefeld (2015).
35. McConigal, J.: Besser als die Wirklichkeit!: Warum wir von Computerspielen profitieren und wie sie die Welt verändern. Heyne Verlag, München (2012).
36. Killmeyer, J.: Information Security Architecture: An Integrated Approach to Security in the Organization. Auerbach Publications, Boca Raton, New York (2006).
37. Mayring, P.: Qualitative Inhaltsanalyse. Grundlagen und Techniken. (2008).
38. BSI: IT-Grundschutz - M 2.73 Auswahl geeigneter Grundstrukturen für Sicherheitsgateways, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02073.html.
39. heise: Datendiode gegen Datendiebe, http://www.heise.de/newsticker/meldung/Datendiode-gegen-Datendiebe-2139499.html.
40. Shulman, A., Dulce, S.: Man in the Cloud (MITC) Attacks. (2015).
41. Gragido, W.: Lions At The Watering Hole - The "VOHO" Affair, http://blogs.rsa.com/lions-at-the-watering-hole-the-voho-affair/.