Serious Games als Lernmethode zur Steigerung der Informationssicherheit

Frauke Prott[1], Ulrike Küchler[2], Regina Schuktomow[3] und Margit Scholl[4]

Abstract: Sensibilisierung für Informationssicherheit und die Förderung entsprechender Kenntnisse sind essentiell für eine gelungene Digitalisierung. Im vorliegenden Projekt werden dafür u. a. digitale Serious Games entwickelt und erprobt. Serious Games bieten in der Nachbildung realistischer Alltagssituationen einen geschützten Raum, in dem Fehler gemacht, Konsequenzen von getroffenen Entscheidungen ohne Folgen für das wahre Leben erlebt und verschiedene Wege ausprobiert werden können. So kann sicherheitsbewusstes Verhalten im Falle eines Angriffs auf die Informationssicherheit eingeübt werden. Die Ergebnisse eines Usertests zeigen, dass narratives Lernen mit Serious Games zum Thema Informationssicherheit positiv angenommen wird und zum Lernerfolg beiträgt.

Keywords: Serious Game, digitale Lernszenarien, Informationssicherheit, Sensibilisierung, KMU

1 Einleitung

Erfolgreiche Digitalisierung benötigt ein hohes Niveau an Informationssicherheit [BMI21]. Da Informationssicherheits-Vorfälle häufig durch Unwissenheit und/oder aktives Handeln ermöglicht werden (z. B. Klicken eines Links, Öffnen eines Anhangs), ist die Sensibilisierung von Nutzenden für ein sicheres Verhalten im digitalen Umfeld unerlässlich [BMI21]. Insbesondere kleine und mittlere Unternehmen (KMU) sind aufgrund mangelnden Bewusstseins für die Risiken des Einsatzes von Informationstechnologie, knapper Ressourcen und fehlenden Wissens besonders gefährdet [BMI21] [BSI21].

Daher verfolgt das Projekt „Awareness Labor KMU (ALARM) Informationssicherheit“, gefördert vom Bundesministerium für Wirtschaft und Klimaschutz, das Ziel, ein innovatives Gesamtszenario zur Unterstützung von KMU zur Erhöhung ihrer Informationssicherheit und zur Etablierung einer nachhaltigen Sicherheitskultur zu entwickeln und zu erproben. Das Gesamtszenario umfasst analoge und digitale Lernszenarien (Serious Games) sowie „Vor-Ort-Angriffe“ (z. B. Phishing-Simulation) zur Sensibilisierung für Informa-

1 Technische Hochschule Wildau (TH Wildau), Fachbereich Wirtschaft, Informatik, Recht (WIR), Hochschulring 1, 15745 Wildau, frauke.prott@th-wildau.de
2 Gamebook Studio HQ GmbH, Wilhelm-Kabus-Straße 77, 10829 Berlin, ulrike.kuechler@gamebook.studio
3 TH Wildau, Fachbereich WIR, Hochschulring 1, 15745 Wildau, regina.schuktomow@th-wildau.de
4 TH Wildau, Fachbereich WIR, Hochschulring 1, 15745 Wildau, margit.scholl@th-wildau.de

https://doi.org/10.30844/AKWI_2022_23

tionssicherheit sowie Befragungen, Wissenstests, Awareness-Messungen und Reifegradaussagen. Informationssicherheit soll (be-)greifbar und emotional erlebbar werden. Der vorliegende Beitrag widmet sich den digitalen Serious Games in diesem Projekt.

2 Literaturüberblick

2.1 Game-based Learning

Game-based Learning (GBL) wird als unterhaltsame und motivierende Form des Lernens beschrieben [LA09]. Lernförderliche Eigenschaften von Spielen sind klare Zielvorgaben und direktes Feedback [FZC13]. Die Teilnehmenden arbeiten auf ein Ziel hin, wählen und führen Aktionen aus und erleben unmittelbar die daraus resultierenden Konsequenzen. GBL ermöglicht, in einem geschützten Raum Fehler zu machen sowie zu experimentieren [Tr14]. Die gemachten Erfahrungen sind gut von der simulierten in die reale Welt zu übertragen [Tr14]. Game-based Learning ermöglicht statt einer passiven Informationsaufnahme (Vortrag, Video, Lesen) eine aktive Auseinandersetzung mit den Lerninhalten.

Aufgrund dieser Eigenschaften belegen zahlreiche Studien positive Wirkungen des Einsatzes von Spielen und Spielelementen: GBL-Umfelder sind hoch involvierend und unterstützen daher effektiv den Lernprozess [Bu15]. Spiele als Lernmethode verbessern kurzfristige und langfristige Lernergebnisse [Wo13]. Spielebasierte Lernszenarien erhöhen die Motivation und fördern Verhaltensänderungen [BK11] [Hs08]. Wichtig ist die spezifische Ausrichtung an der Alltagswirklichkeit der Zielgruppen, da die Verbindung zu realen Situationen und Herausforderungen den Lernerfolg verbessert [Lo07].

2.2 Serious Games

Serious Games nutzen (Computer-)Spiele, um für ein Thema zu sensibilisieren sowie Wissen und Fähigkeiten zu entwickeln, indem sie den Lernenden ermöglichen, in Situationen einzutauchen, die sonst schwer oder selten erlebt werden können [Yp14]. Im Gegensatz zu Unterhaltungsspielen zielen Serious Games neben Unterhaltung auf die Vermittlung von Lerninhalten [MM16]. Serious Games fördern den Lernerfolg durch die Ansprache mehrerer Sinne (z. B. visuell, auditiv) und somit verschiedener Lerntypen sowie durch die aktive Einbindung der Spielenden, die dadurch relevante Bezüge zu realen Situationen herstellen können [Yp14].

Narrative – sinnstiftende Erzählungen – fördern das Eintauchen in ein Serious Game, was entscheidend für den Lernerfolg ist. Narrative laden die Spielenden ein, an der Geschichte teilzuhaben sowie ihren Verlauf mitzubestimmen, und fördern die intrinsische Motivation

zu lernen. Dabei sollten die Geschichten unter anderem die Fantasie anregen und empathische Charaktere beinalten [NL20].

2.3 Sensibilisierung für Informationssicherheit

Klassische Lernmethoden, bei denen Fachpersonen in z. B. Vorträgen Lerninhalte an Lernende vermitteln, scheinen eher ineffektiv und passiv im Vergleich zu moderneren Methoden, die auf „learning by doing“ oder experimentellem Lernen basieren [Yp14]. Gleichwohl erfolgen die Sensibilisierung für Informationssicherheit und die Schulung entsprechender Kenntnisse in der Praxis oftmals nach diesem Prinzip durch die Bereitstellung von Web-Based-Trainings (WBT) oder durch Vorträge [Al16].

Gerade ein oftmals abstraktes und komplexes Thema wie Informationssicherheit erfordert eine aktive Auseinandersetzung mit Lerninhalten, wie es Game-based Learning ermöglicht. Im Ernstfall eines Angriffsversuchs auf die Informationssicherheit sollten Nutzende fähig sein, richtig zu handeln. Um das richtige Verhalten für den Ernstfall, bei Bedarf auch wiederholend, einzuüben, empfehlen sich Serious Games. Sie bieten in der Nachbildung realistischer Alltagssituationen einen geschützten Raum, in dem Fehler gemacht, Konsequenzen von getroffenen Entscheidungen ohne Folgen für das wahre Leben erlebt und verschiedene Wege ausprobiert werden können [Tr14]. Im Gegensatz zu kognitiven Informationsvermittlungen ermöglichen Serious Games ein stärkeres Involvement der Teilnehmenden, mehr Lebendigkeit sowie Interaktion und Lernen gemäß der von Pestalozzi geprägte Formel mit „Kopf, Herz und Hand“ [BroJ].

Daher haben in den vergangenen Jahren vermehrt Forschungsprojekte [Ha20] [HAB16] und kommerzielle Anbieter [Ka22] [FaoJ] Serious Games zur Sensibilisierung für Informationssicherheit und Vermittlung entsprechender Kenntnisse entwickelt, um Schulungen mit reiner Wissensvermittlung zu ergänzen. Sowohl analogen als auch digitalen Serious Games werden positive Wirkungen auf die Beteiligung der Teilnehmenden und den Lernerfolg zugeschrieben [Ha20] [Ya19] [GS18].

3 Entwicklung von digitalen Serious Games zur Steigerung der Informationssicherheit

3.1 Storykonzept

Die digitalen Serious Games im vorliegenden Projekt sind immersive Geschichten, die Alltagssituationen aus dem Berufsleben in KMU darstellen. Die Spielenden erleben die Geschichten in der Ich-Perspektive. Dies ermöglicht eine intensive Auseinandersetzung und Identifikation mit den enthaltenen Lerninhalten – und damit auch eine besondere Effizienz und Nachhaltigkeit in der Wissensvermittlung. Für die Entwicklung der Serious Games wurde das Visual Novel Format gewählt – eine Art interaktives Buch, in dem die Spielenden Entscheidungen treffen und damit den weiteren Verlauf der Geschichte bestimmen [Ch19]. Die Lernszenarien sind von Bildern, geschriebenen Dialogen und Situationsbeschreibungen geprägt. Dreidimensionalität wird durch Ambient-Hintergrundmusik und Soundeffekte (z. B. Räuspern, Telefonklingeln, Türzuschlagen) erzeugt.

Das Storykonzept der insgesamt sieben Serious Games zeichnet sich durch Vielfalt, Individualität und Kontinuität aus. Jedes Lernszenario behandelt schwerpunktmäßig ein anderes informationssicherheitsrelevantes Thema: von Passwörtern, über Datenschutz in der Cloud und CEO Fraud[5], bis zu Informationsklassifizierung. Dabei nehmen die Spielenden wechselnde Rollen ein – einmal agieren sie als Sicherheitsexpertin, ein anderes Mal als Hackende oder Ermittelnde oder sogar als Künstliche Intelligenz. Dies erlaubt nicht nur ein abwechslungsreiches Spiel, sondern ermöglicht, die Themen aus verschiedenen Blickwinkeln kennenzulernen und zu verstehen. Die sieben Serious Games können unabhängig voneinander und in beliebiger Reihenfolge gespielt werden. Jede Geschichte und jeder Lerninhalt sind in sich geschlossen. So können die einzelnen Themen in einer größeren Breite und Tiefe behandelt werden. Gleichwohl sind die einzelnen Geschichten durch eine übergreifende Gesamtstory, die in einem fiktiven Unternehmen spielt, miteinander verknüpft und die Spielenden begegnen in jedem Serious Game denselben Personen (Chef, Disponentin, Auszubildender, Werkstattleiter) und lernen sie immer besser kennen.

5 Betrugsmethode, bei der Kriminelle sich als Führungskraft der Organisation ausgeben und Mitarbeitende auffordern, Geld zu überweisen [LS20]

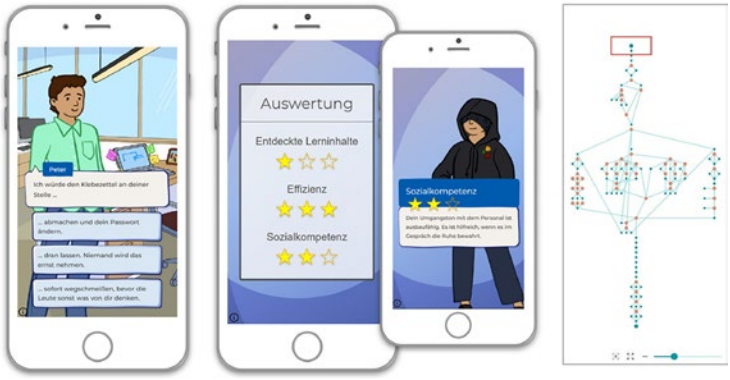

Abb. 1: Beispiele einer Entscheidungsauswahl, eines Feedbacks und eines Entscheidungsbaums

Jedes Lernszenario bietet ein personalisiertes Lernerlebnis. Zu Beginn wählen die Spielenden ihren Charakter und ihren Namen. Mit jeder Entscheidung, die echte Konsequenzen im Spielverlauf mit sich bringt, begeben sich die Spielenden auf ihre ganz persönliche Lernreise, die von ihrem Wissen und ihren Präferenzen bestimmt wird. Jedes Serious Game enthält zwei bis drei Lernpfade, die die Spielenden durch ihre Entscheidungen einschlagen. Die gewählten Wege bestimmen, wie viele Lerninhalte den Spielenden begegnen und welche Schwierigkeiten sie zu bewältigen haben. In jedem Serious Game können die Spielenden unterschiedliche Fähigkeiten (z. B. Sozialkompetenz) stärken und Kenntnisse (z. B. Sicherheitsverständnis) vertiefen, die für Informationssicherheit wichtig sind.

Die Spielenden werden stets von einem Charakter der Gesamtstory begrüßt und darauf aufmerksam gemacht, worum es im vorliegenden Spiel geht, was konkret bewertet wird und worauf sich die Spielenden konzentrieren sollten. Am Ende gibt derselbe Charakter Feedback zu den erzielten Punkten. Dieses beinhaltet zum einen Erläuterungen, wie die Punkteanzahl zustande kommt, und zum anderen Vorschläge und Aufforderungen an die Spielenden. Auch bereits im Laufe des Spiels werden Feedbacknachrichten eingeblendet, die auf vorteilhafte oder nachteilige Entscheidungen und Verhaltensweisen aufmerksam machen. Zudem bietet ein Lexikonmodul die Möglichkeit, wichtige Begriffe der Informationssicherheit vor und nach dem Spiel nachzulesen. Die Spielenden werden nicht alleine gelassen, sondern auch in diesem digitalen Format beim Lernen begleitet.

3.2 Technische Anforderungen

Die Serious Games wurden mit der Gamebook Technologie von Gamebook Studio erstellt. Die Gamebook Technologie ist ein Werkzeug zur vereinfachten und schnellen Produktion von interaktiven seriellen Inhalten. Sie verbindet klassische Erzähltechniken aus Literatur und Film mit modernen digitalen Produktionsmethoden und ermöglicht, aus einem analogen Drehbuch eine interaktive Sequenz zu erstellen. Die Lernszenarien werden als statische Inhalte in einer abgeschlossenen HTML5 Webapplikation bereitgestellt und können per iFrame in die Projektwebseite eingebunden werden und sind dort über den Browser abspielbar. Aufgrund der Allgegenwärtigkeit des Smartphones sind die Zielplattform mobile Endgeräte. Somit können Nutzende auf die Serious Games direkt über die Webseite des Projekts zugreifen.

3.3 Usertest

Mitarbeitende der Pilot- und kooperierenden Unternehmen des Projekts evaluieren die Serious Games aus Sicht der Praxis. Die Rückmeldungen aus den Usertests sind die Grundlage für die finale Erstellung der Serious Games. Die Usertests werden von kurzen, standardisierten, schriftlichen Vorher- und Nachher-Befragungen begleitet, die deskriptiv ausgewertet werden. Die Teilnehmenden werden gebeten, auf einer fünf-Punkte-Likert-Skala zu verschiedenen Aspekten (z. B. Inhalt, realistische Darstellung, Spielzeit, Schwierigkeitsgrad) ihre Zustimmung mitzuteilen. Zur Messung des Lernerfolgs dienen Selbsteinschätzungen zur Erfahrung mit dem Thema Informationssicherheit sowie zum Wissenserwerb. Im Folgenden sind die Ergebnisse des Usertests zum Serious Game „Der Hackerangriff“ dargestellt. Hier nehmen die Spielenden die Rolle eines Hackenden ein und versuchen, sich auf dem Firmenserver des fiktiven Unternehmens einzuloggen. Beurteilt werden die Spielenden nach Effizienz – gelingt ihnen der Hack – und Variabilität – wie viele Wege sind die Spielenden zur Erreichung ihres Ziels gegangen.

An dem Usertest nahmen mehrheitlich Männer (65%, N=26)[6] im Alter von 25 bis 50 Jahren teil (69%, N=26). Die Testpersonen arbeiten hauptsächlich im Vertrieb/Außendienst (23%), in der IT (19%) und im Personalwesen (19%) (N=26). Im Durchschnitt benötigten sie zehn Minuten für das Serious Game (N=22). Diese Spielzeit wurde im Mittel als „genau richtig“ beurteilt (N=31). Auch der Schwierigkeitsgrad tendiert mit einem Mittel von 2,81 zu „genau richtig“ (Skala 1=zu einfach, 3=genau richtig, 5=zu schwer, N=31).

6 Die unterschiedliche Stichprobengröße N ist dadurch bedingt, dass nicht alle Befragten an der Vorher- und Nachher-Befragung teilnahmen bzw. nicht zu allen Fragen Angaben machten.

Abb. 2: Beurteilung des Serious Games „Der Hackerangriff“ im Usertest

Abbildung zwei zeigt eine gute Bewertung des Serious Games „Der Hackerangriff“, da die Testpersonen nahezu allen Aussagen im Durchschnitt mit größer drei zustimmen (Skala 1=überhaupt nicht bis 5=sehr). Wir interpretieren Mittelwerte über dem Skalenmittelpunkt (=3) als zufriedenstellend in der Beurteilung der Nutzenden aufgrund der Heterogenität der Testpersonen im Hinblick auf Branchen, Tätigkeiten und Präferenzen in Bezug auf (digitale) Spiele sowie der Tatsache, dass das linke Ende einer Antwortskala häufiger als das rechte Ende gewählt wird [MB15]. Die geringe Zustimmung zur Aussage „Das Lernszenario möchte ich erneut spielen“ wird relativiert durch die höhere Zustimmung zur Aussage „Das Lernszenario macht Lust, weitere Lernszenarien dieser Art zu spielen“. Gleichwohl wurden im Feedback im betreffenden Serious Game Formulierungsänderungen vorgenommen, um Spielende stärker zu motivieren, das Lernszenario erneut zu spielen. Zudem attestieren die Testpersonen dem Serious Game eine lernförderliche Wirkung. Teilweise wurde neues Wissen erworben und/oder bestehendes vertieft (jeweils M=3,17, N=30). Die eigene Erfahrung mit dem Thema Informationssicherheit wurde nach dem Serious Game leicht höher wahrgenommen (M_{vorher}=3,12, $M_{nachher}$=3,32, N=25).

4 Mehrwert für Wirtschaft und Gesellschaft

Gleichwohl die Serious Games für Mitarbeitende in KMU entwickelt wurden, ist die Sensibilisierung für die behandelten Informationssicherheits-Themen für das Berufsleben insgesamt als auch für das Privatleben (z. B. Passwörter, Telefonbetrug) relevant. Somit besteht der Mehrwert darin, dass die Serious Games für alle interessierten Personen sukzessive auf der Projektwebseite kostenfrei zur Verfügung stehen. Organisationen können damit ihre Mitarbeitenden mit nur geringem Einsatz eigener Ressourcen sensibilisieren und schulen. Ferner können die Serious Games in die Ausbildung von jungen Menschen integriert werden, sodass Auszubildende als auch Studierende bereits mit einem Bewusstsein für Informationssicherheit in die Arbeitswelt starten.

5 Ausblick

Es wird angestrebt, Lernenden auf Basis ihrer erzielten Ergebnisse in den Serious Games einerseits Empfehlungen für das Spielen weiterer Serious Games zu geben, die, im Falle einer geringen Punktzahl, dieselben oder, im Falle einer hohen Punktzahl, andere Fähigkeiten stärken. Andererseits sollen die Teilnehmenden an einen Wissenstest verwiesen werden, in dem sie ihre Kenntnisse zu den im Serious Game behandelten Thema ausbauen können. Aufgrund begrenzter Ressourcen im vorliegen Projekt konnten nicht alle gewünschten Features in den Serious Games umgesetzt werden. In zukünftigen Projekten sollen weitere Ansätze zur Erhöhung der Interaktivität entwickelt und erprobt werden.

Literaturverzeichnis

[Al16] Allianz für Cyber-Sicherheit: Awareness-Umfrage 2015. Ergebnisse, Stand 5.4.2016. Bonn.

[BfV22] Bundesamt für Verfassungsschutz: Sicherheitshinweis für die Wirtschaft, 02/2022, 23. März 2022, Betreff Krieg in der Ukraine. 2022.

[BK11] Bösche, W.; Kattner, F.: Fear of (Serious) Digital Games and Game-based Learning? Causes, Consequences and a Possible Countermeasure. International Journal of Game-Based Learning, 1/3, S. 1–15, 2011.

[BMI21] Bundesministerium des Innern, für Bau und Heimat (BMI): Cybersicherheitsstrategie für Deutschland 2021. Berlin, 2021.

[BroJ] Brühlmeier, A.: Heinrich Pestalozzi: Grundgedanken: Erziehung / Bildung. https://www.heinrich-pestalozzi.de/grundgedanken/erziehung-bildung, Stand: 8.7.2022

[BSI21] Bundesamt für Sicherheit in der Informationstechnik (BSI): Die Lage der IT-Sicherheit in Deutschland 2021. Bonn, 2021.

[Bu15] Buffum, P. S.; Boyer, K. E.; Wiebe, E. N.; Mott, B. W.; Lester, J. C.: Mind the Gap: Improving Gender Equity in Game-Based Learning Environments with Learning Companions. AIED: International Conferences on Artificial Intelligence in Education, 2015.

[Ch19] Choi, C.: Bigger on the Inside: A History of Visual Novels. https://medium.com/@cecilchoi/bigger-on-the-inside-a-history-of-visual-novels-981e42f43608, 22. Februar 2019, Stand: 25.4.2022.

[FaoJ] Fabula Games: Security Games. https://fabula-games.de, Stand: 28.6.2022.

[FZC13] Fang, X.; Zhang, J.; Chan, S.S.: Development of an Instrument for Studying Flow in Computer Game Play. International Journal of Human-Computer Interaction, 29/7, S. 456–470, 2013.

[GS18] Ghazvini, A.; Shukur, Z.: A Serious Game for Healthcare Industry: Information Security Awareness Training Program for Hospital Universiti Kebangsaan Malaysia. International Journal of Advanced Computer Science and Application, 9/9, S. 236–245, 2018.

[Ha20] Hart, S. et al.: Riskio: A Serious Game for Cyber Security Awareness and Education. Computer & Security, 95/August 2020, Artikel 101827, 2020.

[HAB16] Hendrix, M.; Al-Sherbaz, A.; Bloom, V.: Game Based Cyber Security Training: Are Serious Games suitable for cyber security training? International Journal of Serious Games, 3/1, S. 53–61, 2016.

[Hs08] Hsu, S. H.; Wu, P. H.; Huang, T. C.; Jeng, Y. L.; Huang, Y. M.: From Traditional to Digital: Factors to Integrate Traditional Game-based Learning into Digital Game-based Learning Environment. Proceedings 2nd IEEE International Conference on Digital Game and Intelligent Toy Enhanced Learning, DIGITEL, S. 83–89, 2008.

[Ka22] Kaspersky: [Dis]connected. A mobile cybersecurity quest.

https://media.kaspersky.com/en/business-security/enterprise/Kaspersky_[dis]connected_datasheet_0121EN_Gl.pdf, 2022, Stand: 28.6.2022.

[LA09] Linek, S. B.; Albert, D.: Game-based Learning: Gender-Specific Aspects of Parasocial Interaction and Identification. Conference: International Technology, Education and Development Conference (INTED), 2009.

[Lo07] Lombardi, M.: Authentic Learning for the 21st Century: An Overview. 2007.

[LS20] Luber, S.; Schmitz, P.: Definition CEO Fraud / CEO-Betrug – Was ist CEO-Fraud?. Security Insider, 14.12.2020, https://www.security-insider.de/was-ist-ceo-fraud-a-991462/, Stand: 12.4.2022.

[MB15] Menold, N.; Bogner, K.: Gestaltung von Ratingskalen in Fragebögen. Mannheim, GESIS – Leibniz-Institut für Sozialwissenschaften (SDM Survey Guidelines), 2015.

[MM16] Mildner, P.; Mueller, F.: Design of Serious Games. In (Dörner, R.; Göbel, S.; Effelsberg, W.; Wiemeyer, J. Hrsg.): Serious Games: Foundations, Concepts and Practice. Springer International Publishing, Cham, S. 57–82, 2016.

[NL20] Naul, E.; Liu, M.: Why Story Matters: A Review of Narrative in Serious Games. Journal of Educational Computing Research, 58/3, S. 687–707, 2020.

[Tr14] Trybus, J.: Game-Based Learning: What it is, Why it Works, and Where it‘s Going. New Media Institute, 2014.

[Wo13] Wouters, P.; van Nimwegen, C.; van Oostendorp, H.; van der Spek, E. D.: A Meta-analysis of the Cognitive and Motivational Effects of Serious Games. Journal of Educational Psychology, 105/2, S. 249–265, 2013.

[Ya19] Yasin, A. et al.: Improving software security awareness using a serious game. IET Software, 13/2, S. 159–169, 2019.

[Yp14] Ypsilanti, A.; Vivas, A.B.; Räisänen, T.; Viitala, M.; Ijäs, T.; Ropes, D.: Are Serious Video Games Something More than a Game? A Review on the Effectiveness of Serious Games to Facilitate Intergenerational Learning. Education and Information Technologies, 19, S. 515–529, 2014.