MedienPädagogik
Zeitschrift für Theorie und Praxis der Medienbildung
www.medienpaed.com
ISSN 1424-3636

Themenheft Nr. 36: Teilhabe in einer durch digitale Medien geprägten Welt – Perspektiven des wissenschaftlichen Nachwuchses
Herausgegeben von Tim Riplinger, Jan Hellriegel und Ricarda Bolten

Spielerisch sichere Teilhabe

Ein Review spiel-basierter Lernanwendungen über IT-Sicherheit und Sicherheitspraktiken

René Röpke

Zusammenfassung
Die Interaktion mit IT-Systemen und dem Internet ist in der durch digitale Medien geprägten Welt für manche ein Kinderspiel, für andere eine grosse Herausforderung. Doch was intuitiv erscheint, ist es nicht zugleich richtig – oder sicher. In Bezug auf sicheren Umgang sind es grundlegende Kenntnisse und Fähigkeiten über IT-Sicherheit und Informatik, die vielen fehlen. Spiel-basierte Ansätze zur Vermittlung der notwendigen Kenntnisse und Fähigkeiten soll sichere Teilhaber ermöglichen. In diesem Beitrag wird ein zweitteiliges Review spiel-basierter Lernanwendungen und Serious Games über IT-Sicherheit und Sicherheitspraktiken präsentiert, das anhand von zwei Hypothesen Publikationen und verfügbare Anwendungen analysiert und bewertet. Während es zwar viele Publikationen aus dem Bereich der Forschung gibt, die auch für Endnutzerinnen und -nutzer ohne Vorkenntnisse geeignet sind, sind es nur wenige Spiele, die wirklich verfügbar sind. Online verfügbare Spiele vermitteln zudem keine nachhaltigen Kenntnisse und Fähigkeiten, die sichere Teilhabe ermöglichen. Es bedarf der Vermittlung von Kontext und Relevanz, um sicheren Umgang mit IT-Systemen und dem Internet zu lehren. Mit der Entwicklung neuer Spiele, die eben diese Aspekte berücksichtigen, können Endnutzerinnen und -nutzer einen motivierenden Einstieg in IT-Sicherheit erfahren.

Playful Secure Participation. A Review of Game-based Learning Applications on IT Security and Security Practices

Abstract
In a world dominated by digital media, interaction with IT systems and the Internet is child's play for some and a major challenge for others. But what seems intuitive is not immediately right – or safe. In terms of secure practices, many lack basic knowledge and skills about IT security and information technology. Game-based approaches to imparting the necessary knowledge and skills should enable secure participation in this digitalized world. This paper presents a two-fold review of game-based learning applications and serious games on IT security and security practices that analyzes and evaluates publications and available applications based on two hypotheses. While there are

Röpke, Réne. 2019. «Spielerisch sichere Teilhabe. Ein Review spiel-basierter Lernanwendungen über IT-Sicherheit und Sicherheitspraktiken». *MedienPädagogik* 36, (November), 170–185. https://doi.org/10.21240/mpaed/36/2019.11.21.X.

many publications from the field of research that are also suitable for end users without previous knowledge, there are only a few games that are actually available. Moreover, games available online do not provide sustainable knowledge and skills that enable safe participation. It takes context and relevance to teach secure practices for the use of IT systems and the Internet. With the development of new games that take these aspects into account, end users can experience a motivating introduction to IT security.

Einleitung

Wenn es um den sicheren Umgang mit IT-Systemen und dem Internet geht, wenden heutige Nutzende verschiedene Sicherheitspraktiken mehr oder weniger gewissenhaft an. Gerade wenn sie technisch nicht versiert sind, kann von einem angemessenen Wissens- und Kompetenzniveau nicht ausgegangen werden. Selbst unter Expertinnen und Experten unterscheiden sich die Meinungen darüber, welche Praktiken zu befolgen sind und wie man sich verhalten soll. Diese Unterschiede bei den Sicherheitspraktiken entmutigen die Nutzenden häufig und das langfristige Interesse an guten Sicherheitspraktiken ist nicht ausreichend, um sich weiter damit zu beschäftigen (Ion, Reeder und Consolvo 2015). Dies führt dazu, dass Nutzende Sicherheitspraktiken nicht angemessen befolgen und eine *sichere* Teilhabe an der durch digitale Medien geprägten Welt nur schwer möglich ist.

Ein wichtiger Aspekt bei der Vermittlung von Sicherheitspraktiken ist, die Motivation und das Interesse der Nutzenden aufrecht zu erhalten und gleichzeitig ausreichend Wissen zu vermitteln, so dass sie ihr eigenes Verhalten anpassen und reflektieren können. Auch der Transfer zu neuen Technologien ist eine Herausforderung.

In den letzten 15 Jahren wurden verschiedene Spielprototypen für das Lernen über IT-Sicherheit entwickelt und evaluiert. Als spiel-basierte Lernanwendungen oder so genannte Serious Games versuchen diese Spiele, die Spielenden über Phishing, Malware, Verschlüsselung und andere wichtige Themen der IT-Sicherheit aufzuklären.

Der Begriff «Serious Game» wurde ursprünglich 1970 von Clark Abt definiert (Abt 1970) und 2005 von Mike Zyda aktualisiert (Zyda 2005). Nach unserem Verständnis sind es Spiele, die einen anderen Zweck als reine Unterhaltung verfolgen (Hendrix, Al-Sherbaz & Victoria 2016). Ein Synonym ist der Begriff des Lernspiels. Dazu gehört auch der von Wolf et al. 2016 definierte Begriff «Competence Developing Game» (Wolf & König 2017). Spiel-basiertes Lernen wird in diesem Beitrag definiert, als das Lernen durch Spielen. Oft wird das Präfix «digital» hinzugefügt, um die Verwendung digitaler Lernspiele hervorzuheben, aber in seinem Ursprung geht es nur um Spass und Entertainment, verbunden mit der ernsthaften Aktivität des Lernens (Prensky 2001).

Während Serious Games meist Teil von Forschungsprojekten sind und systematisch entwickelt werden, verschwinden sie nach ihrer Erprobung und Beforschung oft und sind selten der Öffentlichkeit zugänglich.

Ein weiterer Nachteil dieser Spiele ist die Zielgruppe. Bekannte Beispiele richten sich an Studierende der Informatik und Ingenieurswissenschaften auf Universitätsniveau oder Beschäftigte in ähnlichen Berufsfeldern. Diese Zielgruppen suchen aufgrund ihrer Interessen und ihres Studien- oder Arbeitsbereichs nach Lernmöglichkeiten im Bereich der IT-Sicherheit. Häufig werden entsprechende Spiele in Universitätskursen oder als Weiterbildungsmassnahme am Arbeitsplatz eingesetzt, um spiel-basiertes Lernen zu fördern und als explorative Lernmöglichkeit zu dienen.

Wenn es um Endnutzende ohne starkes Interesse an IT-Sicherheit geht, sind die Ziele verschieden. Serious Games für IT-Sicherheit sollten Endnutzende motivieren, sich über ein recht schwieriges Thema zu informieren, auch wenn ihnen grundlegende Kenntnisse über Informatik fehlen. Sie werden verwendet, um Endnutzende zu begeistern und sie zu unterhalten, während sie über ein Thema lernen, das kompliziert und zu schwer zu erlernen erscheint. Ohne entsprechende Kenntnisse ist es für Endnutzende sehr schwierig, die mit der Nutzung des Internets und IT-Systemen verbundenen Risiken einzuschätzen. Sie wissen nicht, wie man sich *sicher* verhält. Dieses Problem kann nach Meinung des Autors dazu führen, dass die Endnutzenden weiterhin die heutige Technologie und das Internet nutzen, sich aber der potenziellen Risiken und Massnahmen zur Sicherung nicht bewusst sind.

Im Rahmen des ERBSE Projekts, das für «Enable Risk-Aware Behavior to Secure End-users» steht, werden spiel-basierte Ansätze zum Lernen über IT-Sicherheit untersucht[1]. Dabei liegt der Fokus auf dem Spannungsfeld der hohen Komplexität der IT-Sicherheit und Endnutzenden ohne informatische Grundbildung. Ziel des Projekts ist es, spiel-basierte Ansätze (z.B. Serious Games) zu implementieren und zu evaluieren.

In diesem Beitrag wird ein systematischer Überblick über spiel-basierte Lernanwendungen und Serious Games für das Lernen über IT-Sicherheit präsentiert. Die zugrunde liegende Hypothese ist, dass es nicht viele spiel-basierte Lernanwendungen und Serious Games zur IT-Sicherheit gibt, die sich an Endnutzende ohne Vorkenntnisse in Informatik richten. Darüber hinaus wird davon ausgegangen, dass die verfügbaren Spiele für Endnutzende keine nachhaltigen, informatischen Fähigkeiten und Kenntnisse vermitteln, um sich sicher zu verhalten und Risiken angemessen einzuschätzen.

Es gibt ein reges Forschungsinteressen an Serious Games über IT-Sicherheit, aber es ist zu erwarten, dass die meisten Arbeiten nach der Evaluation von Forschungsprototypen abgeschlossen wurden. Wenn sich ein Spielprototyp als wirksam erwiesen hat, scheint er danach zu verschwinden und schafft es nicht, die Zielgruppe der Endnutzenden zu erreichen.

Der Beitrag ist wie folgt strukturiert: Zunächst werden die verwandten Arbeiten und die darin gewonnenen Erkenntnisse vorgestellt. Anschliessend wird die Methodik

1 https://nerd.nrw/forschungstandems/erbse/

der Literaturrecherche einschliesslich der schrittweisen Filterung erläutert und die Ergebnisse werden vorgestellt. Abschliessend folgt eine Diskussion der Ergebnisse und Schlussfolgerungen mit Fokus auf die nächsten Schritte und offene Fragen.

Verwandte Arbeiten

Verschiedene Autorinnen und Autoren haben Ansätze des Lernens über IT-Sicherheit untersucht. Einige konzentrierten sich auf das spiel-basierte Lernen und verglichen es mit traditionellen Trainingsansätzen. Andere verglichen verschiedene Serious Games oder spiel-basierte Ansätze, um einen Überblick über den Stand der Forschung und Technik zu geben.

Tioh et al. stellen einen Vergleich von traditionellem Training und angewandten «Hands-on» Training vor und betonen, dass spiel-basiertes Lernen die Eigenschaften beider Trainingsmethoden kombinieren kann, um die Nutzenden effektiver zu qualifizieren. Im nächsten Schritt identifizieren sie eine Reihe von akademischen Prototypen sowie Produkten, die auf dem Markt erhältlich sind. Für jedes Ergebnis identifizieren sie den Spieltyp und das Thema. Tioh et al. stellen fest, dass die Wirksamkeit spiel-basierter Ansätze noch nicht ausreichend empirisch nachgewiesen wurde. (Tioh, Mina & Jacobson 2017)

Eine ähnliche Analyse durch Hendrix et al. bestätigt den gleichen Bedarf an Weiterbildungsmöglichkeiten für die Öffentlichkeit und Unternehmen. Während die Ergebnisse der analysierten Studien positive Effekte zeigen, waren die jeweiligen Stichprobengrössen klein und Effektgrössen wurden nicht angemessen diskutiert (Hendrix, Al-Sherbaz, und Victoria 2016). Darüber hinaus wurden die Stichproben aus verschiedenen Zielgruppen gezogen, was beobachtete Effekte schwächen kann. Hendrix et al. stellen fest, dass Forschungsprototypen entweder schwer zu finden oder gar nicht verfügbar sind.

Compte et al. analysieren einige Serious Games zur Informationssicherheit und präsentieren Beobachtungen und Vorschläge zur Gestaltung von Serious Games zu IT-Sicherheit. Ein Serious Game versucht, als immersives Erlebnis zu dienen, und oft werden Simulationen gewählt, um den Spielinhalt zu präsentieren (Le Compte, Elizondo & Watson 2015). Da die meisten Spiele in Bildungseinrichtungen wie Universitäten oder Schulen eingesetzt werden, schränken Zeitdruck und andere Rahmenbedingungen die Verwendungsmöglichkeiten solcher Spiele ein, obwohl Pastor et al. argumentieren, dass die Spielenden in der Lage sein sollten, ein Serious Game in ihrer eigenen Umgebung/Lebenswelt zu spielen (Pastor, Díaz, und Castro 2010) und dann Zeitbeschränkungen nicht existieren (Le Compte, Elizondo, und Watson 2015).

In einem weiteren Review zu Spieltechnologien für das Lernen über IT-Sicherheit von Alotaibi et al. wurden verschiedene Studien verglichen. Alotaibi et al. stellen fest, dass der Ansatz des Spielens zur Sensibilisierung relativ neu ist und einer

umfangreicheren Forschung bedarf. Im nächsten Schritt analysierten sie zehn Spiele zu IT-Sicherheit auf Aspekte wie Spieltyp, Zielgruppe und Lernziel. Laut ihrer Bewertung zielen die meisten Spiele auf Studierende oder Teenager ab. Je nach Inhalt können sie auch für Fachleute oder Berufstätige in bestimmten Arbeitsbereichen geeignet sein. (Alotaibi et al. 2016)

Während sich die meisten Reviews auf digitale Spiele mit Hilfe von Simulationen, 2D- oder 3D-Umgebungen konzentrieren, haben Dewey und Shaffer auch verfügbare Gesellschaftsspiele wie [d0x3D!] oder Control-Alt-Hack® hervorgehoben (Dewey & Schaffer 2016). Beide Spiele zeigen Sicherheitskonzepte im Zusammenhang mit der Netzwerk- und Computersicherheit für Endnutzende, z.B. jüngere Erwachsene (Gondree, Peterson, und Denning 2013). Zu den Vorteilen von Gesellschaftsspielen gehören die Zugänglichkeit, die Veränderbarkeit sowie das Potenzial für soziale Interaktion. Sie sind zudem günstig und einfach zu beziehen. (Gondree, Peterson, und Pusey 2016)

Ein weiteres Konzept, das dem starken Trend der Simulationen zu Grunde liegt, sind virtuelle Labore. Mit ihnen können Lernende praktische Erfahrungen sammeln und die Theorie mit der Praxis verbinden (Dewey und Shaffer 2016; Son, Irrechukwu, und Fitzgibbons 2012).

Noch mehr Übungsmöglichkeiten bieten IT-Sicherheitswettbewerbe wie «Capture The Flag» (CTF) Events oder Hack-a-thons. Sie werden meist als «offene Herausforderungen» formuliert, bei denen am Ende keine Lösung offenbart wird, sondern die Herausforderung weiterhin bestehen bleibt. CTFtime berichtet von mehr als 155 CTFs im Jahr 2018. Mehr als 70% davon sind online verfügbar und offen für alle Interessenten. (CTFtime.org 2018)

Aufgrund des Wettbewerbscharakters von CTFs ziehen sie oft Spielende mit Hintergrundwissen in IT-Sicherheit an, z.B. Informatikstudierende oder Fortgeschrittene im privaten oder beruflichen Bereich. Im Allgemeinen sind sie zwar für die Öffentlichkeit zugänglich, aber die Herausforderungen können für Spielende ohne Anleitungen oder entsprechendes Hintergrundwissen einfach zu schwer und folglich demotivierend sein.

Obwohl alle Reviews versuchen, verfügbare Spiele basierend auf ihrer Zielgruppe, der verwendeten Technologie, dem Spieltyp oder den Inhalten zu klassifizieren, ähneln sie sich alle in ihrem Vorgehen. Während die meisten Forschungsprototypen ausgewertet wurden und positive Effekte zeigen, waren die Stichprobengrössen eher klein und bestanden aus verschiedenen Zielgruppen (Hendrix, Al-Sherbaz, und Victoria 2016; Tioh, Mina, und Jacobson 2017). Ausserdem sind viele Forschungsprototypen nicht mehr verfügbar oder sehr schwer zu finden (Hendrix, Al-Sherbaz, und Victoria 2016).

Im Folgenden stellen wir einen ganzheitlicheren Review-Ansatz vor, bei dem alle Beiträge nach Typen, Zielgruppen und Bildungskontexten gegliedert werden.

Methodik

Aufgrund des rasanten Fortschritts in der Informatik und folglich auch der Welt der digitalen Spiele, getrieben durch akademische und kommerzielle Akteure, deckt eine systematische Literaturrecherche allein möglicherweise nicht alle verfügbaren Serious Games und spiel-basierten Lernanwendungen über IT-Sicherheit ab. Daher ist ein zweiteiliger Rechercheprozess notwendig, bei dem einerseits eine systematische Literaturrecherche zu wissenschaftlichen Publikationen und andererseits eine Produktsuche mithilfe einer etablierten Suchmaschine durchgeführt wird.

Für die Recherche wurden zunächst zwei Schlüsselwort-Sets ausgewählt, eines mit Begriffen zur IT-Sicherheit und ein anderes mit Begriffen zum spiel-basierten Lernen und Serious Games. Diese Schlüsselwort-Sets enthalten die passendsten Schlüsselwörter in ihrer Kategorie, werden aber voraussichtlich trotzdem nicht alle Ansätze finden können.

Die Schlüsselwort-Sets sind wie folgt definiert[2]:

- *ITsec = {IT security, cyber security, risk awareness, security awareness, security education, cyber education, security}*
- *LearnTech = {game based learning, gamification, serious game, learning game, edugame, teaching game, competence developing game}*

Alle Kombinationen von zwei Schlüsselwörtern, eines aus jedem Set, werden für Suchanfragen verwendet. Für den Suchprozess werden die folgenden drei digitalen Bibliotheken und/oder Suchmaschinen verwendet: IEEE Xplore[3], Google Scholar[4] und ACM Digital Library[5]. Bei jeder Anfrage wurden die ersten 100 Ergebnisse zur weiteren Analyse extrahiert (im Falle weniger Suchergebnisse, werden alle Ergebnisse verwendet). Es wird sich auf die ersten 100 Ergebnisse beschränkt, da Ergebnisse mit noch niedrigeren Rängen weniger wahrscheinlich zur Suchanfrage passen und nicht für die weitere Analyse geeignet sind.

Mit allen erfassten Ergebnissen wurde ein mehrstufiger Filter- und Klassifizierungsprozess durchgeführt, um alle extrahierten Ergebnisse systematisch zu überprüfen.

Im ersten Schritt wurden alle Duplikate entfernt, um die Ergebnismenge zu reduzieren. Anschliessend wurde die Online-Verfügbarkeit und Zugänglichkeit (über Universitätsbibliothek oder Open Access) ermittelt und alle Ergebnisse, die nicht zugänglich sind, ausgeschlossen.

Der dritte Schritt ist die Filterung aller Ergebnisse basierend auf der Leitfrage, ob es sich bei einer Publikation um eine Massnahme zum Lernen über IT-Sicherheit

2 Um Beiträge mit internationaler Reichweite zu finden, basieren die Schlüsselwort-Sets sowie Kategorien in der späteren Analyse auf englischsprachigen Begriffen.

3 https://ieeexplore.ieee.org/

4 https://scholar.google.de/

5 https://dl.acm.org/

handelt oder nicht. Mit der reduzierten Ergebnismenge wurde anschliessend eine Kategorisierung angewandt. Alle Ergebnisse wurden in die folgenden Kategorien unterteilt: «Competition», «Game», «Gamification», «Review» und «Sonstige». Unter «Sonstige» wurden alle Publikationen zu Frameworks, Tools und weiteren Inhalten des Lernens über IT-Sicherheit zusammengefasst, die in keine andere Kategorie passen.

Im nächsten Schritt wurden alle als Review kategorisierten Ergebnisse betrachtet und alle genannten Serious Games oder spiel-basierten Lernanwendungen zur weiteren Verarbeitung in die Ergebnismenge aufgenommen. Diese Massnahme garantiert, dass Spiele, die bereits von anderen Autoren betrachtet wurden, aber durch die Schlüsselwortsuche nicht gefunden, dennoch im weiteren Prozess betrachtet werden.

Alle Ergebnisse, die als «Game», «Competition» oder «Gamification» kategorisiert wurden sowie für alle Spiele, die im vorherigen Schritt aus Reviews hinzugefügt wurden, wurden im nächsten Schritt weiter analysiert. Für jede Publikation bestimmen wir das Thema in Bezug auf IT-Sicherheit, den Spielnamen (falls zutreffend), die jeweilige Zielgruppe und den vorgesehenen Bildungskontext.

Schliesslich wurde für alle identifizierten Spiele die Online-Verfügbarkeit überprüft. Da Brettspiele oder Kartenspiele von Grund auf nur offline verfügbar sind, bezieht sich die Online-Verfügbarkeit auf online verfügbare Informationen über diese Spiele.

Als nächstes wurde die Produktsuche nach Serious Games und spiel-basierten Lernanwendungen zu IT-Sicherheit mithilfe der Google-Suche durchgeführt.

Alle über die Produktsuche gefundenen Spiele wurden in die Ergebnismenge aufgenommen und es wurde das Thema, die Zielgruppe und der Bildungskontext zur Vervollständigung der Analyse ermittelt.

Ergebnisse

Nach dem Rechercheprozess mit beiden Schlüsselwort-Sets wurden 2636 Ergebnisse ermittelt. Diese Menge wurde durch die Eliminierung von Duplikaten auf 1277 Ergebnisse reduziert. Als nächstes wurden alle verfügbaren Ergebnisse anhand der Frage gefiltert, ob es sich um einen Ansatz zum Lernen über IT-Sicherheit handelt. Die Ergebnismenge wurde auf 183 Publikationen reduziert.

Einschliesslich der in anderen Reviews erwähnten Spiele sowie der Produktsuche wurde die Ergebnismenge auf 216 Ergebnisse erweitert. Innerhalb dieser Menge sind 181 Ergebnisse vom Typ «Game», «Gamification» oder «Competition» (s. Tab. 1).

Typ	# Ergebnisse
Game	133
Gamification	24
Competition	24
	Σ = 181
Review	14
Sonstige	21

Tab. 1.: Kumulierter Überblick über Ergebnisse.

Da es sich bei «Competition» höchstwahrscheinlich um CTFs oder andere IT-Sicherheit-Wettbewerbe handelt, die oft Spielmechaniken beinhalten, sich aber eher von spiel-basierten Lernanwendungen und Serious Games unterscheiden, ist anzunehmen, dass kein repräsentativer Teil der verfügbaren Wettbewerbe ermittelt wurde und weitere Analysen nicht aussagekräftig und generalisierbar sind. Unser Schlüsselwort-Set *LearnTech* legte den Fokus auf Serious Games, Lernspiele und spiel-basiertes Lernen und nicht auf Herausforderungen oder Wettbewerbe.

Das Grundprinzip von CTFs und anderen IT-Sicherheits-Wettbewerben ist zudem kompetitiver als Serious Games. Die Teilnehmenden solcher Wettbewerbe sind hoch motiviert zu gewinnen und betreiben daher eine umfassende Vorbereitung und Recherche auf diesem Gebiet. Es ist womöglich auch ein Preis zu gewinnen, der extrinsisch motiviert.

Im Vergleich zu Serious Games, bei denen die Lernenden zur Unterhaltung spielen und spielerisch lernen, lehren sich die Teilnehmenden, um in einem Wettbewerb erfolgreich zu sein, z.B. sichere Systeme aufzubauen, ihre Gegner mit komplexen Techniken anzugreifen und sich vor Angriffen zu verteidigen. Endnutzende ohne gesondertes Interesse werden ermutigt, ein tieferes Verständnis über IT-Sicherheit zu erlangen, das über das erwartete Bildungsniveau in diesem Bereich hinausgeht.

Bei der Betrachtung der 24 Ergebnisse, welche als «Competition» markiert wurden, konnte festgestellt werden, dass fast 2/3 der Ergebnisse auf Informatikstudierende oder fortgeschrittene Nutzende ausgerichtet sind. Während 1/3 für andere Studierende, Lernende oder Endnutzende mit weniger Erfahrung geeignet ist, sind sie für Teilnehmende, die sich für Informatik und IT-Sicherheit interessieren, dennoch attraktiver. Es wird angenommen, dass Endnutzende ohne informatische Grundbildung oder formales Lernszenario (z.B. Schule, Fortbildung) nicht an solchen Wettbewerben teilnehmen. Daher werden in den weiteren Analysen alle als Wettbewerbe eingestuften Ergebnisse ausgeschlossen. Ein Interesse für zukünftige Forschung liegt in der Untersuchung der verwendeten Spieltechnologien und die Übertragbarkeit auf Spiele für Endnutzende.

24 Ergebnisse wurden aufgrund ihrer Verknüpfung von Spielelementen im Lernprozess als «Gamification» kategorisiert. Das Konzept von Gamifizierung und spielbasiertes Lernen sind aber zu differenzieren. Gamifizierung ist die Verwendung von Spielelementen (z.B. Punktesysteme, Rankings oder Avatare) in einem eher traditionellen Lernkontext (Deterding et al. 2011).

Folglich wurden alle als «Gamification» kategorisierten Ergebnisse ausgeschlossen und sich stattdessen ausschliesslich auf Spiele konzentriert. Es verblieben 133 Ergebnisse zu spiel-basierten Ansätzen in der IT-Sicherheitserziehung.

Für alle als «Game» kategorisierten Ergebnisse wurde die Analyse fortgesetzt und die jeweiligen Themen der IT-Sicherheit, der Name des Spiels, die Zielgruppen und der vorgesehene Bildungskontext ermittelt.

Es wurden 99 verschiedene Serious Games oder spiel-basierte Lernanwendungen identifiziert. Mögliche Zielgruppen sind Informatikstudierende/-schüler, Berufstätige, Endnutzende, Eltern, Lehrkräfte sowie andere Studierende und Schüler.

Während die Anzahl der identifizierten Spiele aufgrund der Publikationen gross erscheint, ist die Online-Verfügbarkeit ein entscheidendes Kriterium für die weitere Interpretation der Ergebnisse. Spiele, die nicht online (web-basiert oder zum Download) verfügbar sind, sind für die jeweilige Zielgruppe überhaupt nicht verfügbar. Wie Tabelle 2 zeigt, sind 48 von 99 Spielen online verfügbar (inkl. Brett- und Kartenspiele).

Zielgruppe	# Spiele	Online verfügbar
Informatikstudierende und -schüler	19	5
Berufstätige	12	7
Endnutzende	26	12
Eltern und Lehrkräfte	1	1
Experten	9	5
Andere Studierende, Schüler	32	18
	Σ = 99	Σ = 48

Tab. 2.: Verteilung der Zielgruppen.

Im Hinblick auf den Bildungskontext treten verschiedene Kontexte auf. Es wurde zwischen Primarstufe, Mittelstufe, Oberstufe, Hochschule, beruflichem und non-formalem Kontext unterschieden (s. Tab. 3). Da einige Spiele in mehr als einem Kontext einsetzbar sind, wurde eine Klassifizierung mit mehreren Labels angewendet, d.h. ein Beitrag kann mehrere Kontexte bedienen.

Die meisten Spiele sind für Hochschulen, Universitäten sowie berufliche und non-formale Kontexte konzipiert. Dies ist nicht verwunderlich, da es keine vollständige Abdeckung des Schulfachs Informatik von Primar- bis Oberstufe gibt und daher die Unterrichtsthemen zu IT-Sicherheit noch weniger vorhanden sind.

Bildungskontext	# Spiele
Primarstufe	4
Mittelstufe	9
Oberstufe	10
Hochschule	26
Beruflich	20
Non-formaler Kontext	38

Tab. 3.: Überblick über Bildungskontexte nach Multi-Label-Klassifikation.

Da viele Spiele als Forschungsprototypen konzipiert sind, sind sie oft für Studierende an Hochschulen oder Universitäten gedacht. Diese Spiele können einem bestimmten Bildungskontext dienen, können aber auch für Endnutzende in non-formalen Lernkontexten geeignet sein.

Spiele für den beruflichen Kontext werden oft professionell entwickelt und können für Trainingszwecke von Mitarbeitenden oder Expertinnen und Expteren verwendet werden. Diese Spiele sind für die Öffentlichkeit weniger geeignet, z.B. simulieren sie Unternehmensumgebungen, um ein authentisches Lernerlebnis zu schaffen. Sie sind auch oft mit den IT-Sicherheitsregelungen in Unternehmen verbunden und unterscheiden sich daher von der Sicherheit für Endnutzende in Privatleben.

Bei der Analyse von Spielthemen gibt es kein klares Ergebnis, sondern eine Vielzahl von Themen, die identifiziert wurden. Die Themen reichen von Forensik, Hacking und Netzwerksicherheit bis hin zu Phishing, Social Engineering und Online-Sicherheit und meist behandeln Spiele mehr als ein Thema.

Das Gesamtergebnis des zweiteiligen Reviews zur Erfassung von spiel-basierten Lernanwendungen und Serious Games im Bereich der IT-Sicherheit enthält 99 Spielen, die entweder in wissenschaftlichen Publikationen oder über eine Produktsuche gefunden wurden.

Diskussion

Nach der Beschreibung der Ergebnisse der systematischen Literaturrecherche und Produktsuche, folgt nun eine Diskussion unter Berücksichtigung der zu Anfang formulieren Hypothesen. Die erste Hypothese lautet, dass es nicht viele spiel-basierte Lernanwendungen und Serious Games zu IT-Sicherheit gibt, die sich an Endnutzende ohne informatische Grundbildung richten.

Wie in Tabelle 2 dargestellt, adressieren die ermittelten Spiele unterschiedliche Zielgruppen. Was die Vorkenntnisse in Informatik betrifft, so richtet sich ein grosser Teil der Spiele an Endnutzende ohne explizite Vorkenntnisse. Es konnte festgestellt werden, dass 58 Spiele auf «Endnutzende» (26 Ergebnisse) und «Andere Studierende, Schüler» (32 Ergebnisse) ausgerichtet sind. Da nicht alle von ihnen derzeit online verfügbar sind, verbleiben nur 30 Spiele für die entsprechenden Zielgruppen.

Dieses Ergebnis scheint zunächst unsere Hypothese widerlegen. Mehr als 60% der verfügbaren spiel-basierten Lernanwendungen und Serious Games zu IT-Sicherheit richten sich an Endnutzende, die keine Vorkenntnisse oder Fähigkeiten im Bereich Informatik vorweisen.

Im Hinblick auf unsere zweite Hypothese ist ein genauerer Blick auf die verfügbaren Ergebnisse nötig. Es werden Spiele gesucht, die nachhaltige, informatische Fähigkeiten und Kenntnisse vermitteln, um Endnutzende nachhaltig zu qualifizieren, sich sicher zu verhalten und Risiken angemessen zu bewerten. Im Weiteren werden einzelne Spiele aus der Ergebnismenge verfügbarer Spiele für die entsprechende Zielgruppe der Endnutzenden vorgestellt und unter Berücksichtigung der zweiten Hypothese geprüft. Das Spiel «The Internet Safety Game»[6], das auf der Plattform «NetSmartKidz» des National Center for Missing & Exploited Children erhältlich ist, ist ein webbasiertes Spiel zur Sicherheit im Internet und richtet sich an jüngere Kinder in non-formalen Lernkontexten. Das Spiel besteht aus einer Spielumgebung, die an ein Brettspiel erinnert. Gespielt wird mit einem Charakter, der durch Würfeln schrittweise bewegt werden kann (s. Abb. 1). Die Aufgabe besteht darin, verschiedene Gegenstände auf dem Spielfeld zu sammeln. Diese sind Informationen, die Fakten über das Internet vermitteln. Es gibt insgesamt sechs Gegenstände zu finden und danach endet das Spiel. Basierend auf dem Schwierigkeitsgrad steht eine optionale Multiple-Choice-Befragung zur Verfügung, um die Spielenden bzgl. der gesammelten Fakten zu testen. Zu den Fakten gehört unter anderem die Empfehlung, keine personenbezogenen Daten (z.B. Name, Alter oder Adresse) online weiterzugeben. Obwohl dies ein vernünftiger Vorschlag zu sein scheint, gibt es keine Erklärung dafür, welche Risiken versucht werden zu unterbinden.

Abb. 1.: Screenshot aus «The Internet Safety Game».

6 https://www.netsmartzkids.org/AdventureGames/TheInternetSafetyGame

Als nächstes wird das Spiel «PASDJO»[7], von Seitz und Hussmann betrachtet. In diesem Spiel bewertet der Spieler eine Reihe von Passwörtern und erhält ein entsprechendes Feedback über die Qualität der Passwörter (Seitz & Hussmann 2017). Das Spiel ist sehr kurz und die Spiellogik ist einfach. Obwohl Feedback zu Passwörtern und deren Qualität gegeben wird, wird das gesamte Thema der Passwortsicherheit nicht ausführlich behandelt. Mögliche Angreifermodelle und Risiken schlechter Passwörter werden nicht angesprochen, weshalb dieses Spiel keine nachhaltigen Fähigkeiten und Kenntnisse zu Passwortsicherheit vermittelt.

Das dritte Beispiel ist die Plattform «Safe Online Surfing» des Federal Bureau of Investigation (FBI). Es handelt sich um eine Reihe von Minispielen für verschiedene Altersgruppen (sortiert für dritte bis achte Klasse). Das Spiel behandelt Themen wie Online-Sicherheit und Internet. Während diese Plattform verschiedene Spielmechanismen zur interaktiven Einbindung der Spielenden nutzt, sind die in den Spielen vermittelten Fähigkeiten und Kenntnisse eher willkürlich und nicht richtig motiviert. Auch hier fehlen inhaltliche Aspekte wie Risiko- und Angreifermodelle und es wird die Relevanz bestimmter Themen nicht herausgearbeitet. Das gewonnene Wissen ist nur Faktenwissen und daher aufgrund der sich schnell verändernden Risiken nicht nachhaltig.

Ein weiteres Spiel ist CyberCIEGE, ein Forschungsprototyp der Naval Postgraduate School. Er ist online frei verfügbar und steht allen Interessierten zum Download zur Verfügung[8]. CyberCIEGE ist als 3D-Simulation implementiert, in der die Spielenden etwas über Computer- und Netzwerksicherheit lernen. Die Spielenden agieren als Angestellte eines Unternehmens und sind für die Konfiguration von Firewalls, VPNs und anderen sicherheitsrelevanten Systemen verantwortlich (s. Abb. 2). Das Spiel ist komplexer als die zuvor vorgestellten Spiele. Es bietet verschiedene Szenarien. Die Angriffsszenarien umfassen Viren, Trojaner, bösartige E-Mail-Anhänge und mehr. CyberCIEGE vermittelt zudem deutlich umfassendere Fähigkeiten und Kenntnisse zu IT-Sicherheit und Informatik. Das Spiel wurde in verschiedenen Studien auf seine Wirksamkeit evaluiert (Ariffin, Ahmad, und Sulaiman 2016; Irvine, Thompson, und Allen 2005; Raman, Lal, und Achuthan 2014).

7 https://password-game.firebaseapp.com/
8 https://my.nps.edu/web/c3o/cyberciege

Tab. 4.: Screenshot von CyberCIEGE.

Auf den ersten Blick wirkt es, als vermittle CyberCIEGE nachhaltige Fähigkeiten und Kenntnisse zu IT-Sicherheit und Informatik vermittelt, um Endnutzenden ein risikobewusstes Verhalten zu ermöglichen, aber die Verfügbarkeit verschiedener Szenarien erschwert den Einstieg in das Spiel. Es wurde in verschiedenen Bildungskontexten eingesetzt, aber immer von einer Lehr- oder Ausbildungsperson unterstützt. Die Entwickler von CyberCIEGE stellen auch unterstützende Materialien zur Verfügung, um das Spiel in Einführungskurse zur IT-Sicherheit einzubeziehen, z.B. einen Lehrplan, der Szenarien zu möglichen Kursthemen abgleicht.

Im Vergleich zu Plattformen wie NetSmartKidz oder «Safe Online Surfing» mag CyberCIEGE inhaltlich ein geeigneter Ansatz sein, aber seine Einstiegspunkte können seinen Erfolg bei den Endnutzenden in non-formalen Lernkontexten behindern. Für Spielende in nicht-formalen Lernkontexten erfordert ein Spiel über IT-Sicherheit einen einfachen Zugang. Es sollte keinen Aufwand geben, wie die Einrichtung einer komplexen Umgebung, um das Spiel zu spielen.

Nachdem vier verschiedene Spiele für Endnutzende vorgestellt und auf ihre Qualität untersucht wurden, liegen Indikatoren vor, die die zweite Hypothese verifizieren können. Spiele wie «The Internet Safety Game» oder die Plattform «Safe Online Surfing» sind für jüngere Kinder in non-formalen Lernkontexten konzipiert, während PASDJO oder CyberCIEGE für erwachsenere Zielgruppen besser geeignet sind. Alle Spiele sind zwar für Endnutzende ohne Vorkenntnisse und Fähigkeiten in IT-Sicherheit und Informatik, aber ihr Potential zur Qualifizierung ist stark limitiert.

Spiele wie PASDJO und «The Internet Safety Game» stellen Informationen der IT-Sicherheitsdomäne, z.B. Passwörter, ohne Kontext dar. Sie beantworten nicht, warum die jeweiligen Themen wichtig sind und erläutern keinerlei Risiken oder Angreifermodelle. Ohne Relevanz zu schaffen, bleibt das Sachwissen in diesen Spielen unbedeutsam und motiviert nicht, sich sicher zu verhalten.

Ein weiterer Nachteil dieser Spiele ist die Art der Präsentation. Beispielsweise präsentiert PASDJO nur Passwörter und fordert Spielende auf sie zu bewerten. Nach der Bewertung der ersten Passwörter wird das Spiel repetitiv und langweilig. Minispiele auf der Plattform «Safe Online Surfing» implementieren verschiedene Spielmodi, schaffen aber keinerlei Kontext und Relevanz.

In Bezug auf die zweite Hypothese, dass verfügbare Spiele für Endnutzende kein nachhaltiges Wissen oder Fähigkeiten in IT-Sicherheit und Informatik vermitteln, scheinen erste Indikatoren die Hypothese zu bestätigen. Zum einen fehlt in den präsentierten Spielen Kontext und Informationen über Risiken, Angreifermodelle und Qualität der vermittelten Sicherheitsmassnahmen. Sie sind zudem sehr begrenzt, da die meisten von ihnen nur Faktenwissen vermitteln. Während man sich mit CyberCIEGE auch auf konzeptionelles oder prozedurales Wissen konzentriert, sind die Einstiegspunkte und seine hohe Komplexität Nachteile für die eigentliche Zielgruppe.

Um tatsächlich nachhaltigere Kenntnisse oder Fähigkeiten in IT-Sicherheit und Informatik zu vermitteln, muss eine Kombination aus sachlichem, konzeptionellem und prozeduralem Wissen vermittelt werden. Spiel-basierte Ansätze müssen Relevanz für die Inhalte schaffen und Fragen beantworten, wie warum man sich über ein Thema der IT-Sicherheit informieren sollte und was die Risiken für die Endnutzende sind.

Aufgrund des ständigen Wandels im Feld der IT-Sicherheit, d.h. die Entwicklung neuer Angriffstechniken, der Nutzung versteckter Hintertüren oder das Ausnutzen von ungebildeten Nutzenden, muss die Vermittlung von IT-Sicherheit nachhaltig gestaltet sein. Nachhaltigkeit ist wichtig, damit die Nutzenden die erworbenen Kenntnisse und Fähigkeiten anwenden und sich an neue Herausforderungen in der IT-Sicherheit leicht anpassen können. Es muss zudem die Selbstwirksamkeit der Lernenden gesteigert werden, sodass sie sich im Internet sicher bewegen. Natürlich müssen Sie weiterhin über neue Risiken lernen, aber mit grundlegenden Fähigkeiten und Kenntnissen aus früheren Lernmöglichkeiten sollte dies weniger schwierig sein als zuvor.

Fazit und Ausblick

Nach der Vorstellung eines zweiteiligen Ansatzes zum systematischen Review spielbasierter Lernanwendungen und Serious Games zu IT-Sicherheit wurden 216 Ergebnisse klassifiziert. Es wurden 181 Ergebnisse als Spiele, Wettbewerbe und Massnahmen der Gamifizierung identifiziert. Anschliessend wurden alle Spiele auf Aspekte wie Themen, Zielgruppe und Bildungskontext analysiert. Ausserdem wurde die Online-Verfügbarkeit ermittelt. Schliesslich wurden 48 verfügbare Spiele für verschiedene Zielgruppen (s. Tab. 2) und Bildungskontexte (s. Tab. 3) identifiziert.

Im nächsten Schritt wurden die zu anfangs aufgestellten Hypothesen unter Berücksichtigung der Ergebnisse diskutiert. Zuerst konnte die erste Hypothese, dass es nicht viele Spiele für Endnutzende ohne Vorkenntnisse oder Fähigkeiten in IT-Sicherheit und Informatik gibt, widerlegt werden. Mehr als 2/3 der verfügbaren Spiele richten sich an die entsprechende Zielgruppe.

Weiterhin wurde angenommen, dass verfügbare Spiele für Endnutzende kein nachhaltiges Wissen und Fähigkeiten in IT-Sicherheit und Informatik vermitteln. Es konnten Indikatoren gefunden werden, die die Hypothese bestätigen. Zum einen basieren die Spiele meist auf der Vermittlung von Faktenwissen ohne motivierten Kontext. Oft fehlt die Relevanz, warum dieses Wissen wertvoll ist. Auch werden Risiken, Angreifermodelle und die Qualität der Sicherheitsmassnahmen nicht berücksichtigt.

Als nächstes kann die Ergebnismenge der präsentierten systematischen Recherche weiter analysiert werden. Ein Blick auf Studienergebnisse könnte Einblick über die Qualität und erzielten Lerneffekte der Spiele geben. Weitere interessante Aspekte sind die verwendeten Spielmechanismen und behandelten Themen.

Zudem können mit den Ergebnissen dieser Arbeit neue Spielprototypen für Endnutzende entworfen werden, welche nachhaltiges, relevantes Wissen an die Spielenden vermittelt.

Eingebunden in das Projekt ERBSE sollen spiel-basierte Ansätze für die IT-Sicherheitserziehung implementiert und evaluiert werden, um Endnutzenden zu befähigen, sich sicher im Umgang mit IT-Systemen und dem Internet zu verhalten und Risiken angemessen einzuschätzen. Wie bereits festgestellt, sollten der entsprechende Kontext, die Relevanz und Informationen über Risiken, potentielle Angreifend und die Qualität der Sicherheitsmassnahmen in die Spiele integriert werden, um nachhaltige Kenntnisse und Fähigkeiten zu vermitteln. Mit eben solchen spiel-basierten Ansätzen kann dann von einer Möglichkeit zur spielerisch sicheren Teilhabe gesprochen werden.

Literatur

Abt, Clark. 1970. «Serious Games.» Viking Press, Inc., Nueva York.

Alotaibi, Faisal, Steven Furnell, Ingo Stengel, und Maria Papadaki. 2016. «A Review of Using Gaming Technology for Cyber-Security Awareness.»

Ariffin, Mazeyanti M, Wan Fatimah Wan Ahmad, und Suziah Sulaiman. 2016. «Investigating the Educational Effectiveness of Gamebased Learning for IT Education.» In *Computer and Information Sciences (ICCOINS), 2016 3rd International Conference on*, 570–73.

Compte, Alexis Le, David Elizondo, und Tim Watson. 2015. «A Renewed Approach to Serious Games for Cyber Security.» In *Cyber Conflict: Architectures in Cyberspace (CyCon), 2015 7th International Conference on*, 203–16.

CTFtime.org. 2018. «All about CTF (Capture The Flag).» 2018.

Deterding, Sebastian, Rilla Khaled, Lennart E Nacke, und Dan Dixon. 2011. «Gamification: Toward a Definition.» In *CHI 2011 Gamification Workshop Proceedings*. Vol. 12.

Dewey, Chad M, und Chad Shaffer. 2016. «Advances in Information SEcurity EDucation.» In *Electro Information Technology (EIT), 2016 IEEE International Conference on*, 133–38.

Gondree, Mark, Zachary N J Peterson, und Tamara Denning. 2013. «Security through Play.» *IEEE Security & Privacy*, no. 3. IEEE: 64–67.

Gondree, Mark, Zachary N J Peterson, und Portia Pusey. 2016. «Talking about Talking about Cybersecurity Games.»

Hendrix, Maurice, Ali Al-Sherbaz, und Bloom Victoria. 2016. «Game Based Cyber Security Training: Are Serious Games Suitable for Cyber Security Training?» *International Journal of Serious Games* 3 (1): 53–61.

Ion, Iulia, Rob Reeder, und Sunny Consolvo. 2015. «'... No One Can Hack My Mind': Comparing Expert and Non-Expert Security Practices.» In *SOUPS*, 15:1–20.

Irvine, Cynthia E, Michael F Thompson, und Ken Allen. 2005. «CyberCIEGE: Gaming for Information Assurance.» *IEEE Security & Privacy* 3 (3). IEEE: 61–64.

Pastor, Vicente, Gabriel Díaz, und Manuel Castro. 2010. «State-of-the-Art Simulation Systems for Information Security Education, Training and Awareness.» In *Education Engineering (EDUCON), 2010 IEEE*, 1907–16.

Prensky, M. 2001. «Digital Game-Based Learning, McGraw-Hill & Paragon House, New York.»

Raman, Raghu, Athira Lal, und Krishnashree Achuthan. 2014. «Serious Games Based Approach to Cyber Security Concept Learning: Indian Context.» In *Green Computing Communication and Electrical Engineering (ICGCCEE), 2014 International Conference on*, 1–5.

Seitz, Tobias, und Heinrich Hussmann. 2017. «PASDJO: Quantifying Password Strength Perceptions with an Online Game.» In *Proceedings of the 29th Australian Conference on Computer-Human Interaction*, 117–25.

Son, Joon, Chinedum Irrechukwu, und Patrick Fitzgibbons. 2012. «Virtual Lab for Online Cyber Security Education.» *Communications of the IIMA* 12 (4): 5.

Tioh, Jin-Ning, Mani Mina, und Douglas W Jacobson. 2017. «Cyber Security Training a Survey of Serious Games in Cyber Security.» In *Frontiers in Education Conference (FIE)*, 1–5. IEEE.

Wolf, Martin R, und Johannes A König. 2017. «Competence Developing Games.» *INFORMATIK 2017*. Gesellschaft für Informatik, Bonn.

Zyda, Michael. 2005. «From Visual Simulation to Virtual Reality to Games.» *Computer* 38 (9). IEEE: 25–32.