Spielbasierte Lernanwendungen für sicheren Umgang mit IT-Systemen und dem Internet

René Röpke[1]

Abstract: Dieser Beitrag präsentiert ein Forschungsvorhaben zum spielbasierten Lernen zu Themen der IT-Sicherheit. Es widmet sich der Frage, wie spielbasiertes Lernen eingesetzt werden kann, um die Lernmotivation von Nutzerinnen und Nutzern ohne Vorkenntnisse in IT-Sicherheit und Informatik zu fördern. Dabei sollen Spielmechaniken und -elemente auf ihre Effektivität mittels systematisch gestalteter Forschungsprototypen untersucht werden. Die Zielgruppe bilden Kinder im Alter von neun bis zwölf Jahren.

Keywords: Spielbasiertes Lernen, Lernanwendungen, Lernspiele, IT-Sicherheit, Phishing

1 Problemstellung und Motivation

Wenn es um die sichere Interaktion mit IT-Systemen und dem Internet geht, werden Sicherheitspraktiken nur mehr oder weniger gewissenhaft angewandt [Io15]. Informationsquellen für solche Praktiken sind oftmals sehr unterschiedlich und qualitativ fragwürdig. Diese Quellen bestehen in nur informellem Wissen, welches durch Familie oder den Freundeskreis geteilt wird oder Empfehlungen aus Blogs, Zeitschriften und Nachrichten. Gerade bei Nutzerinnen und Nutzer, welche technisch nicht versiert sind, oder auch erst anfangen, digitale Technologien selbstständig zu verwenden, z. B. Kinder im Alter von neun bis zwölf Jahren, kann von einem angemessenen Kompetenzniveau nicht ausgegangen werden. Nutzerinnen und Nutzer können Risiken nicht richtig einschätzen, gehen womöglich nicht vorsichtig mit sensiblen Daten von sich selbst oder anderen um. Außerdem wird oft davon ausgegangen, dass man selbst kein interessantes Ziel darstellt, und daher weniger Risiken ausgesetzt ist. Schlussendlich wissen Nutzerinnen und Nutzer nicht, sich sicher zu verhalten, interagieren jedoch trotzdem mit IT-Systemen und dem Internet. Hierdurch werden nicht nur die Nutzerinnen und Nutzer selbst gefährdet, sondern auch andere, sich womöglich sicher verhaltene Nutzerinnen und Nutzer.

Auch unter Experten unterscheiden sich die Meinungen, welche Praktiken zu befolgen sind und wie man sich sicher verhält. Zumal sind online verfügbare Informationen inkonsistent, bereits veraltet oder schlichtweg falsch. Diese Unterschiede bei den Sicherheitspraktiken entmutigen die Nutzerinnen und Nutzer häufig und das langfristige Interesse an angemessenen Sicherheitspraktiken sinkt.

[1] RWTH Aachen, Informatik 9 (Learning Technologies), Ahornstr. 55, 52704 Aachen, roepke@informatik.rwth-aachen.de

In Bildungskontexten werden Sicherheit, Privatsphäre und verwandte Themen im Informatikunterricht oder integriert in anderen Unterrichtsfächern behandelt. Lehrplanempfehlungen und andere Handreichungen, z.B. die Bildungsstandards der GI [Br08], enthalten relevante Praktiken und Wissen, aber die Art der Vermittlung ist die Verantwortung der Lehrkraft. Im Informatikunterricht werden bspw. Datensicherheit durch Verschlüsselungsverfahren behandelt. Unterschiedliche Konzepte zur Medienkompetenz greifen ebenfalls den sicheren, souveränen Umgang mit Technologie auf, z. B. der Medienkompetenzrahmen NRW[2] und die KMK-Strategie zu „Bildung in der digitalen Welt“[3].

Ein wichtiger Aspekt bei der Vermittlung von Sicherheitspraktiken ist es, die Motivation und das Interesse der Nutzerinnen und Nutzer aufrechtzuerhalten und gleichzeitig ausreichend Informationen bereitzustellen, sodass sie ihr eigenes Verhalten anpassen und reflektieren können. Es reicht nicht, Handlungsanweisungen ohne Hintergrundwissen zu vermitteln, da sich sonst bei sich ändernden Systemen kaum ein Transfer realisieren lässt. Auch der Transfer zu neuen Technologien mit der Entwicklung von Smart-Home-Geräten und modernen Kommunikationstechnologien ist ein wichtiges Ziel. Durch die Interaktion mit diesen neuen Technologien, entstehen weitere, oftmals unbekannte Angriffspunkte für Nutzerinnen und Nutzer.

Es stellt sich also die Frage, wie Nutzerinnen und Nutzer motiviert werden können, sich mit den relevanten Themen der Informatik und IT-Sicherheit auseinanderzusetzen, um angemessene Sicherheitspraktiken für den Umgang mit IT-Systemen und dem Internet zu lernen. Der gewählte Ansatz für dieses Vorhaben ist spielbasiertes Lernen, welches versucht die Motivation und das Interesse am Spielen auf Lernprozesse zu übertragen. Gestützt durch interaktive Technologien können Lernende emotional gebunden werden und einen regelbasierten, virtuellen Raum versetzt werden, indem es möglich ist, Fehler zu machen, Konsequenzen und Reaktionen zu erleben und auch in die Rolle des Angreifers versetzt zu werden [Ga15]. Die Zielgruppe sind Kinder im Alter von neun bis zwölf Jahren, welche selbstgetrieben und ohne Supervision im Internet aktiv sind und eigene IT-Systeme mit Internetzugang besitzen [FPR18].

2 Forschungsvorhaben

Nach Darlegung der Problemstellung und Motivation widmet sich das Vorhaben also der Frage, wie spielbasierte Lernanwendungen eingesetzt werden können, um Nutzerinnen und Nutzer ohne Vorkenntnisse in IT-Sicherheit und Informatik nachhaltig zu schulen. Das Vorhaben versucht spielbasiertes Lernen auf einen Lerngegenstand der IT-Sicherheit, z. B. Phishing anzuwenden. Hierbei wird der Fokus auf die Lern- und Spielmechaniken gelegt. Es soll beforscht werden, welche Spielmechaniken sich für die Förderung der

[2] https://medienkompetenzrahmen.nrw/, zuletzt abgerufen am 31.05.2019
[3] https://www.kmk.org/fileadmin/Dateien/veroeffentlichungen_beschluesse/2016/2016_12_08-Bildung-in-der-digitalen-Welt.pdf, zuletzt abgerufen am 31.05.2019

Kenntnisse und Fähigkeiten zum sicheren Umgang mit IT-Systemen und dem Internet positiv auf die Lernmotivation und das Interesse der Nutzerinnen und Nutzer auswirkt.

Spielbasiertes Lernen oder im Englischen „(Digital) Game-based Learning“ kann intuitiv definiert werden als Lernen durch Spielen. Weitere in diesem Kontext relevante Begriffe sind „Serious Games“ oder Lernspiel. Während es keine genaue Abgrenzung der unterschiedlichen Begriffe gibt, werden diese Konzepte durch die Idee des „ernsthaften“ Einsatzes von Spielen, also zum Wissenserwerb bzw. zu Bildungszwecken verbunden. Spielbasiertes Lernen zeichnet sich vor allem durch in pädagogischer Absicht gestalteten Inhalte und Strukturen aus, welche mit zentralen Spielelementen verbunden werden. Die Anwendungsbereiche und Spielgenre sind dabei sehr vielfältig. [Ga15] Spielbasiertes Lernen erlangte aufgrund seines Potenzials, die Motivation und das Engagement der Lernenden zu verbessern, in den letzten Jahren zunehmende Aufmerksamkeit [Ga15].

Das Vorhaben zur Beforschung von spielbasiertem Lernen zum Lerngegenstand der IT-Sicherheit teilt sich im Wesentlichen in drei Schritte auf.

- Der erste Schritt umfasst die Aufarbeitung des aktuellen Forschungsstandes und der Einarbeitung in die Grundlagen des Spielbasierten Lernens und der Lernspielgestaltung. Zudem soll eine systematische Literatur- und Produktrecherche die aktuellen spielbasierten Lernanwendungen und Lernspiele im Bereich der IT-Sicherheit zusammentragen. Die Analyse der verfügbaren Produkte und Forschungsarbeiten in diesem Bereich ermöglicht die Verfeinerung und Abgrenzung der Problemstellung. Außerdem können Implikationen für die anschließende Gestaltung und Entwicklung eigener Forschungsprototypen erfasst werden.
- Im nächsten Schritt soll auf Grundlage der unzureichenden Verfügbarkeit geeigneter spielbasierter Lernanwendungen die systematische Gestaltung und Entwicklung von prototypischen Anwendungen folgen. Hierbei soll auf Basis von Gestaltungsprinzipien für Lernspiele [Le03] sowie eines Modells zum optimierten Einsatz von Lernmechaniken und Spielmechaniken [Ar15] ein oder mehrere Forschungsprototypen entstehen, welche die gezielte Untersuchung verschiedener Spielmechaniken ermöglichen.
  Die Umsetzung der spielbasierten Anwendungen soll mithilfe des an der RWTH Aachen entwickelten MTLG Frameworks (Multitouch Learning Games) [ELS17, ERS18] durchgeführt werden. Dieses web-basierte Framework ermöglicht die Anwendungsentwicklung für verschiedene Single- und Multitouch-Geräte. Die Entwicklung erfolgt in JavaScript und nutzt das HTML5-Canvas-Element. Alle Anwendungen sollen quelloffen entwickelt und veröffentlicht werden.
- Im letzten Schritt sollen die entwickelten Prototypen zur Beforschung mit der Zielgruppe dienen. Hierbei soll vor und nach der Intervention unterschiedliche Merkmale der Zielgruppe erfasst werden, sodass die Wirksamkeit validiert werden kann. Interessante Merkmale sind die Selbstwirksamkeitserwartung, die Lernmotivation, sowie der Lernstand in Hinblick auf Kenntnisse und Fähigkeiten der Zielgruppe.

Die Forschungsmethodik basiert auf Design-based Research (DBR). Grundlegend für Design-based Research ist das Ziel, die Entwicklung innovativer Lösungen für praktische Bildungsprobleme mit der Gewinnung wissenschaftlicher Erkenntnisse zu verknüpfen. Ausgangspunkt ist dabei die Frage, wie ein erstrebenswertes Bildungsziel (in diesem Fall der sichere Umgang mit IT-Systemen und dem Internet) in einem gegebenen Kontext am besten zu erreichen ist. Design-based Research unterscheidet sich von anderen Forschungsmethoden dadurch, dass prospektive und reflektierende Komponenten des Forschungsdesigns nicht voneinander getrennt sind. [Co03]

Ziel des Vorhabens ist die Gestaltung und Entwicklung zielgruppengerechter spiel-basierter Lernanwendungen für IT-Sicherheit und die Ermittlung effektiver Spielmechaniken zur Förderung der Lernmotivation.

3 Aktueller Stand und nächste Schritte

Im ersten Schritt des Forschungsvorhabens erfolgte eine Erarbeitung des aktuellen Stands der Forschung und Technik. Hierzu wurden im Rahmen einer systematischen Literatur- und Produktrecherche existierende spielbasierte Lernanwendungen und Serious Games gesichtet und unter Betrachtung zweier Hypothesen klassifiziert und analysiert. Zuerst wurde davon ausgegangen, dass nur wenige spielbasierte Lernanwendungen und Serious Games für die Zielgruppe der Nutzerinnen und Nutzer ohne informatische Vorbildung existieren (H1). Während diese Hypothese zwar widerlegt wurde, zeigten jedoch die untersuchten Produkte, dass nur selten angemessen Lernziele und Lerninhalte formuliert sind, um nachhaltige Kenntnisse und Fähigkeiten im sicheren Umgang mit IT-Systemen und dem Internet zu fördern (H2). Außerdem zeigte sich, dass bei vielversprechenden Anwendungen, welche auch in formalen Bildungskontexten Einsatz finden, der Zugang für Nutzerinnen und Nutzer erschwert ist [RS19].

Aufbauend auf der Datenerhebung der Literatur- und Produktrecherche lassen sich weitere Analysevorhaben durchführen. So wurden die Anwendungen mithilfe des G/P/S-Modells, ein Klassifikationsmodell für Serious Games, analysiert [DAJ11]. Hierbei zeigte sich, dass mehr als 75% der Anwendungen für Bildungskontexte geeignet sind und dabei der Fokus auf der Vermittlung von Inhalten und dem Training von Handlungsabläufen liegt, z. B. der Einordnung von Phishing URLs oder die Bewertung von Passwörtern.

Mit der Einarbeitung in existierende Literatur und verfügbare Anwendungen soll im nächsten Schritt die systematische Gestaltung vom spielbasierten Lernanwendungen folgen. Hierfür soll auf existierende Methoden bzw. Frameworks zur Gestaltung und Entwicklung von Lernspielen aufgebaut werden. Ein eben solches Modell ist das LM-GM Model (Learning Mechanics-Game Mechanics Model). Es ist ein deskriptives Modell zur Analyse und Gestaltung von Lernspielen. Das LM-GM Model erlaubt die Reflexion von didaktischen Elementen in Kombination mit verwendeten Spielelementen und unterstützt

somit die systematische Entwicklung von spielbasierten Lernanwendungen und Lernspielen. [Ar15]

Als technische Grundlage wurde mithilfe des MTLG Frameworks eine simulierte Browserumgebung implementiert, welche die Einbindung von Lerninhalten in Form von einem oder mehreren Lernspielen ermöglicht.

4 Fazit

Das Forschungsvorhaben widmet sich der Frage, wie mithilfe von spielbasiertem Lernen die Lernmotivation von Nutzerinnen und Nutzern ohne Vorkenntnisse zu IT-Sicherheit und Informatik gefördert werden kann. Im Fokus stehen dabei die unterschiedlichen Spielmechaniken und ihre Effektivität. Die Zielgruppe bilden Kinder im Alter von neun bis zwölf Jahren. Im ersten Schritt des Vorhabens wurde der aktuelle Forschungsstand aufgearbeitet und verfügbare Anwendungen zum Lernen über Themen der IT-Sicherheit analysiert. Als Nächstes soll die systematische Gestaltung und Implementierung von spielbasierten Lernanwendungen folgen.

Literaturverzeichnis

[Ar15] Arnab, S. et al.: Mapping Learning and Game Mechanics for Serious Games Analysis. British Journal of Educational Technology, 46(2), S. 391-411, 2015.

[Br08] Brinda, T. et al.: Grundsätze und Standards für die Informatik in der Schule. Bildungsstandards Informatik für die Sekundarstufe I. Beilage zu LOG IN, 150(151), S.28, 2008.

[Co03] Cobb, P. et al.: Design experiments in educational research. In: Educational Researcher 32 (1), S. 9–13, 2003.

[DAJ11] Djaouti, D.; Alvarez, J.; Jessel, J.: Classifying serious games: the G/P/S model. In: Handbook of research on improving learning and motivation through educational games: Multidisciplinary approaches, ICI Global, S. 118–136, 2011.

[ELS17] Ehlenz, M.; Leonhardt, L.; Schroeder, U.: Spielend leicht Lernspiele entwickeln - Ein Framework für Multitouch-Lernspiele. In Igel, C. et al. (eds.): Bildungsräume 2017. Gesellschaft für Informatik, Bonn, S. 297–302, 2017.

[ERS18] Ehlenz, M.; Roepke, R.; Schroeder, U.: Towards Multi-touch Learning Applications in Collaborative Education. In: Proc. 7th ACM Int. Symposium on Pervasive Displays, ACM, S. 35, 2018.

[FPR18] Feierabend, S.; Plankenhorn, T.; Rathgeb, T.: KIM-Studie. Kindheit, Internet, Medien. Medienpädagogischer Forschungsverband Südwest (mfps), 2018.

[Ga15] Game-based Learning – e-teaching.org, https://www.e-teaching.org/didaktik/konzeption/methoden/lernspiele/game_based_learning, 09.06.2019

[Io15] Ion, I.; Reeder, R.; Consolvo, S.: "… no one can hack my mind": Comparing Expert and Non-Expert Security Practices. In (Cranor, L. F.; Biddle, R.; Consolvo, S.): SOUPS '15

Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security, Ottawa, S. 327-346, 2015.

[Le03] Lee, J. P.: What Video Games Have to Teach Us about Learning and Literacy, Palgrave Macmillan, New York, 2003.

[Re05] Reinmann, G.: Innovation ohne Forschung? Ein Plädoyer für den Design-Based Research-Ansatz in der Lehr-Lernforschung. Unterrichtswissenschaft, 33. Jg., Nr. 1, S. 52-69.

[RS19] Roepke, R.; Schroeder, U.: The Problem with Teaching Defence against the Dark Arts: A Review of Game-based Learning Applications and Serious Games for Cyber Security Education. In: Proc. 11th Int. Conf. on Computer Supported Education - Volume 2: CSEDU, S. 58-66, 2019.