

communicated by:
Lehr- und Forschungsgebiet Informatik 9

Prof Dr. Ulrik Schroeder



Diese Arbeit wurde vorgelegt am Lehr- und Forschungsgebiet Informatik 9

The present work was submitted to Learning Technologies Research Group

Phishing Academy:

Entwicklung und Umsetzung eines digitalen Lernspiels zu Website-URLs und Phishing

Phishing Academy:

Developing a Digital Educational Game on Website-URLs and Phishing

Bachelorarbeit

Bachelor-Thesis

von / presented by

Schöbel, Sven

Erstprüfer: Prof. Dr. Ulrik Schroeder

Zweitprüfer: Prof. Dr. Ulrike Meyer

Aachen, 05.02.2019

Inhaltsverzeichnis

I	Einleitung und Einführung	2
1.	Einleitung	3
1.1.	Motivation	3
1.2.	Zielsetzung	4
1.3.	Aufbau der Arbeit	5
II	Related Work	6
2.	Fachlicher Hintergrund	7
2.1.	Uniform Resource Locator in Bezug auf Websites	7
2.2.	Phishing	9
3.	Einordnung innerhalb der Fachdidaktik Informatik	12
3.1.	Bildungsstandards Sekundarstufe I der Gesellschaft für Informatik	12
3.2.	Dagstuhl-Erklärung der Gesellschaft für Informatik	13
4.	Entwicklung eines digitalen Lernspiels	15
4.1.	Definition eines digitalen (Lern-)Spiels	15
4.2.	Design eines digitalen (Lern-)Spiels	17
5.	Lernspiele im Themenbereich Phishing	19
5.1.	Anti-Phishing Phil	19
5.2.	NoPhish	22
5.3.	Schlussfolgerungen für die Konzeption	24
III	Konzeption und Umsetzung des Lernspiels	25
6.	Konzeption des Lernspiels	26
6.1.	Lernziele	26
6.2.	Didaktisches Konzept zur Vermittlung	29
6.3.	Spielaufbau und Story	31
6.3.1.	Trainingscenter – Levelboard	33
6.3.2.	Kriminalfälle – Rahmenbedingungen	35
6.3.3.	Grafische Konzepte zur Umsetzung	36
6.4.	Analyse bezüglich (Design-)Merkmale von Computerspielen	37
6.5.	Anwendungsfälle des Lernspiels	38

7. Umsetzung des Lernspiels	39
7.1. Werkzeuge und technische Gegebenheiten	39
7.1.1. Multitouch-Learning-Game-Framework	39
7.1.2. Herausforderung von Cross-Platform-Development	40
7.2. Umsetzung der konzeptionellen Spielstruktur	40
7.3. Umsetzung der Detektivdialoge	41
7.4. Umsetzung von Einführung und Spielermenü	42
7.5. Umsetzungen der Interaktionsmöglichkeiten	44
7.6. Umsetzung der Level des Trainingscenters	47
7.7. Umsetzung der Kriminalfälle	47
7.8. Umsetzung von informativem Feedback	48
7.9. Speichermöglichkeit des Spielfortschritts	50
7.10. Offene Umsetzungspunkte und zukünftige Erweiterungen	51
 IV Fazit und Ausblick	 53
8. Fazit	54
9. Ausblick	55
Anhänge	56
A. Literaturverzeichnis	56
B. Abbildungsverzeichnis	59
C. Konzipierte Level	60

Zusammenfassung

Ein Großteil der Kinder und Jugendlichen zwischen zehn und achtzehn Jahren besitzen ein digitales Endgerät, über das frei verfügt werden kann. Der freie Zugriff auf das Internet stellt aber gleichzeitig für unerfahrene Kinder und Jugendliche auch eine Gefahr dar. Aufgrund fehlender Lernangebote findet keine Sensibilisierung für mögliche Gefahren wie Phishing statt. Im Rahmen dieser Bachelorarbeit wurde daher ein digitales Lernspiel erstellt, in welchem Kindern und Jugendlichen im Alter der Erprobungsstufe einer weiterführenden Schule fundierte Kenntnisse zum Aufbau einer Website-URL und Phishing vermittelt werden. Auf Basis des fachlichen Inhalts und bisher vorhandener Lernspiele wurde unter der Berücksichtigung unterschiedlicher (Design-)Merkmale für Computerspiele das digitale Lernspiel konzipiert und implementiert. Neben dem fachlichen Inhalt stehen dabei vor allem die Erstellung von interaktiven Vermittlungssituationen und das Einbinden des Lernspiels in eine Story im Vordergrund, um eine persönliche Einbindung der zukünftigen Nutzerinnen und Nutzer in das Lernspiel zu ermöglichen. Die Implementation wurde mit Hilfe eines JavaScripts-Frameworks umgesetzt, welches bereits umfassende Funktionen für das Erstellen von browserbasierten Lernspielen mitbringt. Das implementierte Lernspiel kann daher auf unterschiedlichen Geräteklassen (Laptops, Desktop-Computer und Tablets) ohne Einschränkung im Browser gespielt werden. Schlussendlich werden mögliche Erweiterungen zur Implementierung vorgestellt und Umsetzungsmöglichkeiten für eine spätere Evaluation beleuchtet.

Teil I

EINLEITUNG UND EINFÜHRUNG

Kapitel 1 Einleitung

Der erste Abschnitt des Kapitels beinhaltet die Motivation des Themas. Der zweite Abschnitt enthält die Zielsetzung dieser Bachelorarbeit. Im dritten Abschnitt wird der weitere Aufbau der Bachelorarbeit dargestellt und kurz inhaltlich beschrieben.

1.1. Motivation

Phishing ist bis heute eine weitverbreitete Angriffsmethode im Bereich der Internetkriminalität und die Täter werden immer professioneller in der Ausführung von Phishing-Angriffen. Um den Nutzerinnen und Nutzern (NuN) in der Umsetzung Seriosität vorzutäuschen, besitzen mittlerweile ca. die Hälfte aller Phishing-Seiten eine Transportverschlüsselung [Ant18]. Zudem fokussieren sich die Täter immer mehr auf eine Kundengruppe (z. B. einer bestimmten Bank). Falls es sich um Inlandstäter handelt, sind die Angriffsversuche aufgrund sprachlich korrekter Texte noch schwerer zu erkennen. Neben privaten NuN werden aber auch gezielt Unternehmen angegriffen (Spear-Phishing), bei denen beispielsweise gezielt falsche Bewerbungen mit schadhaftem Inhalt durch die Täter eingehen. Der Schaden der von Phishing-Angriffen ausgeht, kann materieller aber auch informeller Natur sein. Im Wahlkampf zur Präsidentschaftswahl der Vereinigten Staaten im November 2016 schoben beispielsweise Angreifer Hillary Clintons Wahlkampfmanager John Podesta eine Phishing-Website unter, die ihn zum Zurücksetzen seines Mailkonto-Passworts aufforderte. Durch den fremden Zugriff gelangten in Folge dessen über die Plattform WikiLeaks¹ private E-Mails zwischen Podesta und Clinton an die Öffentlichkeit, die der Wahlkampagne von Clinton schaden [Hol18]. Clinton verlor im Anschluss die Präsidentschaftswahl und öffentliche Meinungen sehen die Veröffentlichung der E-Mails als Mitgrund für die Niederlage an [Ent16].

Eine Schwierigkeit das Thema Phishing in seiner Gesamtheit zu erfassen, liegt an der hohen Anzahl an verschiedenen Phishing-Arten. Es ist jedoch möglich mehrere Arten zusammenzufassen, für die sich nur der Einstiegspunkt (z. B. eine E-Mail oder ein Link auf einer Website) ändert, aber das Ziel, den Nutzer zum Eingeben von privaten Informationen auf Phishing-Websites zu bringen, sich nicht ändert. Obwohl Phishing-Angriffe eine hohe Relevanz besitzen, existieren nur wenige frei verfügbare Lernspiele zum Thema Phishing. Existierende Lernspiele können zudem nicht plattformübergreifend genutzt werden, da entweder alte Software genutzt wird oder das Lernspiel nur für ein bestimmtes Betriebssystem veröffentlicht wurde. Plattformübergreifende Weiterbildungsmöglichkeiten sind vor allem durch Informationsartikel oder auch Informationsvideos gegeben (vgl. [Bun], [Möh18] und [Ver18]). Für die Vermittlung von Wissen über Phishing an Kinder zwischen zehn und dreizehn Jahren sind diese Informationsquellen als Konzept aber nur bedingt interessant, da diese nur einen stringenten Ablauf zulassen

*Aktualität des
Themas
Phishing*

*Vorhandene
Lernmaterialien zu
Phishing*

¹ WikiLeaks ist eine Enthüllungsplattform auf der anonym Dokumente veröffentlicht werden, die z. B. als geheim eingestuft werden und dadurch nicht für die Allgemeinheit einsehbar sind.

und individuelle Lerneigenschaften der Kinder nicht berücksichtigt werden. Während bei neunjährigen Kindern nur maximal die Hälfte ein eigenes digitales Endgerät besitzen, steigt dieser Prozentsatz in den nächsten Altersklassen sprunghaft an (10 Jahre: 73% und 13 Jahre: 92%). Ein ähnlicher sprunghafter Anstieg ist in der Nutzung von sozialen Medien belegbar. [Kin18]

Die Kinder besuchen nach der vierten Schulklasse eine weiterführende Schule, sodass der Drang neue Kontakte zu knüpfen zur Nutzung von sozialen Medien beiträgt. Gerade Kinder der genannten Altersklasse sind anfällig für Datendiebstahl, da diese im Verhältnis zu anderen Altersklassen noch unerfahren im korrekten Umgang von privaten Informationen im Internet sind [Brü+17, S. 69f]. Es ist somit umso wichtiger gerade Kindern der genannten Altersklasse passende Lernumgebungen bereitzustellen, um während der Übergangsphase in der digitale Endgeräte an Bedeutung zunehmen, Grundfähigkeiten im Zusammenspiel von Informatiksystemen und der Gesellschaft zu vermitteln. Lernspiele, die Themen der Informatik aufarbeiten und vermitteln, könnten ein Mittel sein, um diesem Anspruch zu genügen. Wichtig ist jedoch auch, dass Hintergrundwissen wie der Aufbau einer Website-URL miteinbezogen wird, um eine generelle Fähigkeit zu schaffen, die über das Maß an genereller Medienkompetenz hinausgeht, damit Lernen auch auf zukünftige Änderungen oder Erweiterungen reagieren können.

*Relevanz von
Phishing für
die Zielgruppe*

1.2. Zielsetzung

Das Ziel dieser Bachelorarbeit ist die Entwicklung eines digitalen Lernspiels, welches unter Berücksichtigung von (Design-)Merkmale und eines didaktischen Konzepts den Aufbau einer Website-URL fundiert einführt, damit zukünftige Phishing-Angriffe sicher durch die NuN erkannt werden können. Das übergeordnete Ziel des Lernspiels ist dabei eine allgemeine Fertigkeit aufzubauen, durch die Phishing auf URL-Basis in allen Kontexten erkannt werden kann und nicht auf beispielsweise Phishing-Angriffe per E-Mail beschränkt ist. Es gilt jedoch auch Grenzen und Möglichkeiten aufzuzeigen, wo weiteres Wissen (u. a. Transportprotokolle oder Cross-Site-Scripting) nötig ist, da heutzutage selbst eine korrekte Website-URL nicht als fälschungssicherer Indikator dienen kann. Als Zielgruppe sind dabei NuN der fünften und sechsten Klassenstufe (Erprobungsstufe) vorgesehen. Das Lernspiel wird dabei als aufrufbares Element in einem emulierten Browser eingebunden, der in Zukunft für alle in diesem Bereich entwickelten Lernspiele als Startpunkt fungieren wird. Das Lernspiel wird dabei den verwendeten *Entdecker*-Modus des emulierten Browsers fortführen, um eine altersgerechte Lernumgebung für die NuN der Zielgruppe bereitstellen zu können. Als Struktur soll ein levelbasiertes Storyboard dienen. Dies kommt auch dem geplanten Einsatz als Einzelspieler-Lernspiel zugute, da so Inhalte unabhängig von einer Gruppe gezielt wiederholt werden können.

1.3. Aufbau der Arbeit

Die vorliegende Bachelorarbeit ist in vier Teile mit insgesamt neun Kapiteln gegliedert.

Der erste Teil enthält das erste Kapitel in welchem einleitend die Motivation des Themas beschrieben und die Zielsetzung der Bachelorarbeit konkretisiert wird. Den Schluss macht der hier gelesene inhaltliche Rahmen.

Der zweite Teil enthält eine Übersicht zu den Inhalten verwandter Arbeiten. Dabei wird in Kapitel 2 zunächst der fachliche Hintergrund geklärt. In Kapitel 3 wird das Thema innerhalb der Fachdidaktik Informatik bezüglich der Bildungsstandards und der Dagstuhl-Erklärung der Gesellschaft für Informatik eingeordnet. Es folgt in Kapitel 4 eine mögliche Definition für digitale Lernspiele und (Design-)Merkmale von Computerspielen. Den Abschluss des zweiten Teils bildet das Kapitel 5, in dem die zwei existierenden Lernspiele *Anti-Phishing Phil* und *NoPhish* bezüglich ihres Spielkonzepts analysiert werden.

Der dritte Teil behandelt die Konzeption und Umsetzung des Lernspiels. In Kapitel 6 wird das Lernspiel basierend auf den Erkenntnissen des zweiten Teils konzipiert. Zudem werden mögliche Anwendungsfälle thematisiert und das konzipierte Lernspiel bezüglich der (Design-)Merkmale für Computerspiele analysiert. In Kapitel 7 wird daraufhin die Umsetzung des konzipierten Lernspiels erläutert. Neben der Umsetzung aller einzelnen Komponenten werden auch bereits zukünftige Erweiterungen und noch offene Umsetzungspunkte beleuchtet.

Der vierte und letzte Teil beinhaltet mit Kapitel 8 und 9 das Fazit und einen Ausblick. Im Fazit werden die Ergebnisse und der Verlauf der Arbeit zusammengefasst. Im folgenden Ausblick werden mögliche Evaluationen und die nächsten Schritte in der Entwicklung des Lernspiels thematisiert.

Teil II

RELATED WORK

Kapitel 2 Fachlicher Hintergrund

Damit für den Aufbau einer Website-URL und Phishing Lernziele entwickelt werden können, wird in diesem Kapitel der fachliche Hintergrund erläutert. Der erste Abschnitt behandelt dabei den Aufbau einer URL und die darin enthaltenen einzelnen Teile, wobei hier der Fokus auch die Möglichkeiten für Websites gelegt wird. Im zweiten Abschnitt werden die Grundlagen des Phishings und mögliche Phishing-Angriffe auf URL-Basis vorgestellt.

2.1. Uniform Resource Locator in Bezug auf Websites

Um per Webbrowser auf Inhalte des World Wide Webs (WWW) als Teil des Internets zugreifen zu können, verwendet man *Uniform Resource Locator* (URL). URLs sind dabei aus technischer Sicht eine Unterklasse der *Uniform Resource Identifier* (URI), durch die eine allgemeine Syntax vorgegeben ist, um „abstrakte oder physikalische Ressourcen zu identifizieren“ [BMF05]. Auf Grundlage der Internetstandards der Internet Engineering Task Force (IETF) werden daher URLs zur Lokalisierung einer Ressource durch Beschreibung des primären Zugangsmechanismus (hier: „Standort“ der Ressource im Netzwerk) benutzt [BMF05]. Die URL kann daher als Wegangabe zu einer gewünschten Website (der gewünschten Ressource) beschrieben werden. Der Aufbau einer URL leitet sich aus der Syntax von URIs ab und besteht aus den Hauptkomponenten Protokoll, Host, Port, Pfad, Query und Fragment (Abb. 2.1)[BMF05].

*Definition und
Einordnung
von URLs*

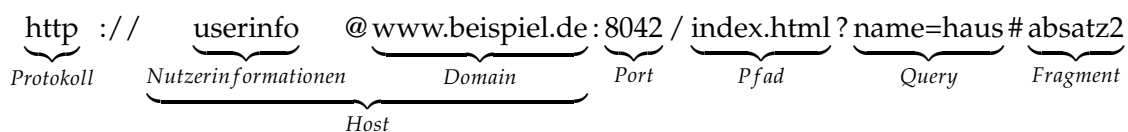


Abbildung 2.1.: Komponenten einer einzelnen URL

Über die Protokoll-Komponente wird festgelegt, durch welches Transportprotokoll die Website übertragen wird. Websites im WWW sind vom Webbrowser dargestellte HTML-Dokumente und können daher durch die Transportprotokolle *http* oder *https* übertragen werden. Dabei werden die Inhalte durch *https* per Transport Layer Security (TLS) verschlüsselt übertragen, während Inhalte durch *http* unverschlüsselt übertragen werden. Auf die Protokoll-Komponente folgt die Zeichenkette `://`, wodurch der Beginn der Host-Komponente signalisiert wird. [BMF05]

*Protokoll-
Komponente
einer URL*

Die Host-Komponente kann mit der Subkomponente Nutzerinformationen beginnen, in welcher beispielsweise Username und Passwort zur Anmeldung am Host mitgesendet werden können. Der Einsatz dieser Komponente ist jedoch ein veralteter Standard, denn

*Host-
Komponente
einer URL*

die Informationen werden unverschlüsselt übermittelt [BMF05]. Da über diese Nutzerinformationen jedoch Phishing-Angriffe verübt worden sind, muss diese Subkomponente auch hier betrachtet werden, obwohl die inhaltliche Relevanz im Allgemeinen nicht mehr gegeben ist. Die Nutzerinformationen werden per @-Symbol abgetrennt.

Mit der Domain folgt der zweite Teile der Host-Komponente und damit die umgangssprachliche Website-Adresse. Der Standort einer Ressource im Internet und damit auch im WWW wird durch das IP-Protokoll eindeutig festgelegt. Die Verwendung von IP-Adressen ist im Alltag aber nicht zielführend, da diese schlecht merkbar ist und durch die Adressknappheit im IPv4-Adressraum mehrere Websites unter einer IP-Adresse beim Internet Service Provider (ISP) abgelegt werden, existiert mit der Domain eine textuelle Repräsentation. Würde die Website durch den ISP eine nicht mehrfach zugewiesene IP-Adresse erhalten, könnte man auch die IP-Adresse anstatt der Domain angeben. Damit eine Ressource gefunden werden kann, wird die Domain mit Hilfe eines Domain Name System (DNS) wieder in eine IP-Adresse übersetzt. Der Aufbau einer Domain und die daraus resultierende Übersetzung sind unter anderem Hauptangriffspunkte für Phishing-Angriffe, sodass eine Erläuterung an dieser Stelle nötig ist. Der Aufbau einer Domain resultiert aus der Speicherung der Einträge des DNS als Wurzelbaum. Die Gesamtheit aller Domains wird daher als DNS-Namensraum bezeichnet. An der Wurzel steht dabei das Root-Level, symbolisiert durch einen Punkt. Darunter folgen die jeweiligen Level-Domains, die ebenfalls Level für Level durch einen Punkt getrennt werden. Die technische Auflösung der Domain erfolgt also durch den Wurzelbaum von rechts nach links entgegen der normalen Leserichtung. Die erste Unterteilung des DNS-Namensraum nach dem Root-Level erfolgt durch die Top-Level-Domains (also Domains des ersten Level). Bekannte Top-Level-Domains sind *de*, *org* oder auch *com*. Es folgen die Second-Level-Domains, wie beispielsweise *wikipedia*. Auf diesem Level können Privatpersonen eigene Domainnamen bei einem ISP registrieren, sofern nicht eine andere Person bereits die gewünschte Domain registriert hat. Domains unter den Second-Level-Domains werden als Subdomains bezeichnet. An eine Second-Level-Domain können durch die Speicherung der Domains als Wurzelbaum mehrere Subdomains angeschlossen werden. Die Standard-Subdomain ist die bekannte Abkürzung *www*. [Moc87] Ein gängiger Host besteht in den meisten Fällen aus Top-Level-Domain, Second-Level-Domain¹ und einer Third-Level-Domain (Abb. 2.2). Die Angabe des Root-Levels durch den einzelnen Punkt kann bei Nutzung moderner Webbrowser vernachlässigt werden. Die Eingabe von beispielsweise *http://www.wikipedia.de* führt aber ebenso wie *http://www.wikipedia.de* auf die Startseite der deutschen Wikipedia. [BMF05]

Bestandteile
der Host-
Komponente
einer URL



Abbildung 2.2.: Beispielhafte Zusammensetzung einer alltäglichen Domain

Im Anschluss an die Host-Komponente folgt die Port-Komponente, getrennt durch einen Doppelpunkt. Die Angabe eines Ports ist nur optional, da durch die Transportprotokolle Standardports definiert wurden. Bei Nichtangabe nutzt *http* den Standardport 80 und *https* den Standardport 443. Die Portangabe kann genutzt werden, um sich über einen

Port- und
Pfadkomponen-
te einer
URL

¹ Der allgemeine Begriff *Domain* wird im Alltag als Synonym für die Second-Level-Domain genutzt.

anderen Port mit einem Server zu verbinden. Ein mögliches Anwendungsszenario stellen beispielsweise Proxies² dar. Im alltäglichen Gebrauch spielen Portangaben kaum eine Rolle. Für Phishing-Angriffe wurden Portangaben jedoch zweckentfremdet, sodass eine Erwähnung und Erklärung notwendig ist. [BMF05]

Nach der Portangabe beziehungsweise in einem Großteil der Fälle nach dem Host wird durch ein Slash der gewünschte Pfad übermittelt. Wichtig ist hier für die spätere Wissensvermittlung, dass ein Wechsel der Leserichtung erfolgt. Ab dem Pfad wird wieder von links nach rechts gelesen.

Weiterhin kann das Trennsymbol als Herleitung einer Regel dienen: *Die Top-Level-Domain ist immer vor dem ersten einzelnen Slash der URL zu finden.* Das Kennen dieser Regel kann Phishing-Angriffe enttarnen. Im Abschnitt 2.3 werden einzelne Anwendungen dieser Regel demonstriert. URLs, die eine Angabe des Ports enthalten, sind immer auf Integrität zu prüfen, da nicht auf Standardports operiert wird. Auf den Pfad können als Schlusskomponenten optional ein Query und ein Fragment folgen. Diese beiden Komponenten haben aber nur eine geringe Bedeutung für Phishing-Angriffe auf URL-Basis. Durch das Query können Phishing-Angriffe per Cross-Site-Scripting durchgeführt werden. Da dieser Fall später aber maximal als Ausblick behandelt werden soll, kann auf eine eingehende Klärung der Begrifflichkeiten verzichtet werden.

Regel für das Finden der Top-Level-Domain einer URL

2.2. Phishing

Um mit dem Begriff *Phishing* arbeiten zu können, ist es notwendig zu Beginn den Begriff zu definieren. Phishing-Angriffe lassen sich in zwei Gruppen aufteilen [Ant18][GAP18]:

Definition des Begriffs Phishing

1. Phishing durch Nutzen eines technischen Tricks oder einer Sicherheitslücke
2. Phishing durch Social Engineering³

Whittaker et al. [WRN10] definieren die Phishing-Variante des Social Engineering als Vorgang, indem die Täter durch Annahme der Identität einer vertrauenswürdigen dritten Partei Zugriff auf private Daten der Opfer erhalten. Das Wort Phishing an sich, ist dabei ein Neologismus in Form einer Wortzusammensetzung der Begriffe *Password* und *Fishing* und kann im Deutschen mit „nach Passwörtern angeln“ angegeben werden. Als Phishing-Angriff wird im Folgenden der Versuch bezeichnet, mit Hilfe einer Website die NuN zur Herausgabe von sensiblen Informationen (u. a. Passwörter, Kreditkartennummern oder TAN-Nummern) zu provozieren. Um einen persönlichen Bezug der NuN zum Angriffsmuster herzustellen, leiten die Täter die NuN auf eine gefälschte Website weiter, die dem Anschein nach zu einem Konzern oder einer Bank gehört [WRN10]. Dabei werden die Websites der Unternehmen oder Banken so detailgetreu wie möglich übernommen, um keinen Verdacht auf Seiten der Opfer zu erwecken. Daher ist das Ziel von Phishing-Angriffen den Opfern durch Identitätsdiebstahl (in den meisten Fällen monetär) zu schaden. [WRN10]

² Proxies sind zwischengeschaltete Komponenten im Netzwerk, die beispielsweise als Vermittler oder als Filter für Anfragen von Clients eines privaten Netzwerks nach außerhalb genutzt werden können. Dabei ist der eigentliche Client hinter dem Proxy verborgen.

³ Als Social Engineering (deutsch: „soziale Manipulation“) bezeichnet man die Beeinflussung von Opfern mit dem Ziel eine gewünschte Verhaltensweise zu provozieren, wie z. B. die Preisgabe von sensiblen privaten Informationen

Um Phishing-Angriffe auf URL-Basis zu verschleiern, verwenden die Täter verschiedene Techniken, die im Folgenden zusammengefasst werden [She+07][ATL15]:

1. Nutzung einer bekannten Domain als Subdomain

Die Angreifer nutzen auf ihrer Seite als Subdomain die Namen von großen Banken oder Marken. Die URL kann dabei beispielsweise die Form <http://www.amazon.de.boeseseite.com/beispiel> annehmen. Nun, die kein Wissen über den Aufbau einer URL haben, können fälschlicherweise annehmen, dass Sie sich auf den Websites von Amazon bewegen. Diese Technik wird oft in Kombination mit langen Zahlenketten als Second-Level-Domain benutzt, um die Übermittlung eines Querys zu simulieren, sodass die Opfer diese Teile der URL ignorieren.

2. Nutzung von ähnlichen Namen als Domain

Durch die De-facto-Standardcodierung in UTF-8⁴ existieren mehrere Möglichkeiten die Opfer durch ähnliche Domainnamen auf gefälschte Websites zu leiten. Da URLs durch die gegebenen Standards nur auf ASCII-Zeichenketten beruhen dürfen, werden URLs mit ASCII-fremden Zeichen zuerst durch das Codierungsverfahren *Punycode* in ASCII-kompatible Zeichenketten umgewandelt [Cos03]. Zum einen werden die Umlaute ö, ä und ü durch UTF-8 anders codiert als oe, ae und ue, sodass die entsprechend mit *Punycode* umgewandelte Zeichenkette der URL auch unterschiedlich ist. Dadurch erreicht man mit <http://www.boese-website.de/beispiel> und <http://www.böse-website.de/beispiel> unterschiedliche Websites. Unternehmen und Institutionen versuchen diesem Einhalt zu gebieten durch die zusätzliche Registrierung dieser Domains, sodass Angreifern möglichst die Basis für einen derartigen Angriff entzogen wird.

Eine weitere Möglichkeit besteht durch das Nutzen ähnlich aussehender Zeichen. Zum Beispiel könnte das Zeichen "l" (klein l) durch die Zahl "1" ersetzt werden. Eine weitere Möglichkeit ist die Nutzung ähnlicher Zeichen aus unterschiedlichen Alphabeten, die im Erscheinungsbild gleich aussehen, aber anders codiert werden wie z. B. das kyrillische und lateinische „a“. Angriffe dieser Art sind durch die Opfer nur schwer zu erkennen. Neben der Nutzung von ähnlichen Zeichen werden auch einfache Ergänzungen genutzt, welche von den Opfern leicht übersehen werden können, wie beispielsweise das zusätzlich eingefügte „i“ in <http://www.wiikipedia.de/beispiel>.

3. Nutzung von IP-Adressen

Mit den Möglichkeiten aus 1. und 2. ist der Name des Unternehmens oder der Institution noch in der URL enthalten. Um unerfahrenen Opfern erst gar nicht die Möglichkeit zu geben eine falsche URL erkennen zu können, wird anstatt der textuellen Repräsentation die IP-Adresse des Webserver angezeigt. Anstatt www.wikipedia.de/beispiel wird dann in der URL-Leiste <http://134.119.24.29/beispiel> angezeigt. Moderne Browser versuchen per *Reverse DNS Lookup* zur IP-Adresse die entsprechende textuelle Repräsentation durch das DNS zu erhalten. Angriffe dieser Art setzen aber voraus, dass die Angreifer eine eindeutige IP erhalten, die nicht wie oben erläutert mehreren Websites durch den ISP zugeordnet wurde.

⁴ Im Februar 2019 nutzen 93% aller Websites UTF-8 zur Codierung [W3T19]. Auch für URLs wird die Codierung in UTF-8 empfohlen [BMF05].

4. Nutzung von bekannten Domains als Pfad

Eine weitere Möglichkeit um unerfahrene Opfer zu täuschen, besteht darin die originale URL im Pfad einer gefälschten URL unterzubringen. Auch hier befinden sich die Opfer auf einer anderen Website als angenommen (z. B. <http://www.boese-website.de/rwth-aachen.de>).

5. Nutzung von Referrern

Durch Kurz-URL-Dienste kann das wahre Ziel eines Links verborgen werden. Für die Opfer ist im ersten Moment nicht ersichtlich, auf welche Website die Weiterleitung durch den Kurz-URL-Dienst erfolgt. Daher erscheinen die Links für unerfahrene Opfer harmlos und eine Kontrolle der finalen URL nach der Weiterleitung erfolgt nicht.

Die fünf genannten Möglichkeiten beziehen sich rein auf das Entdecken eines Angriffs. Durch welchen Umstand das Opfer auf die Website kommt, ist hierbei nicht relevant, da ein didaktisches Konzept erarbeitet wird, um alle Phishing-Angriffe aus allen Einstiegspunkten⁵ heraus rechtzeitig auf Basis der Website-URL zu erkennen, falls der Phishing-Angriff durch eine Phishing-Website erfolgt. Die zweite Gruppe von Phishing-Angriffen nutzen Tricks wie *bösartige E-Mail-Anhänge*⁶ oder *Drive-by-Downloads*⁷. Diese Phishing-Angriffe basieren somit auf anderen Ansätzen oder nutzen Sicherheitslücken in den Webbrowsern aus. Diese Phishing-Angriffe liegen nicht im hier angesetzten Kontext, da diese nicht hauptsächlich auf URL-Basis funktionieren (E-Mail-Anhänge) oder nicht im kontrollierbaren Bereich der Opfer liegen (Drive-by-Downloads).

Es erfolgt daher eine inhaltliche Beschränkung im Lernspiel auf die fünf erörterten Phishing-Techniken auf URL-Basis im Bereich des Social Engineerings. Durch die Synthese des zu vermittelnden Inhalts, ist es nun möglich das fachliche Wissen fachdidaktisch einzuordnen.

*Abgrenzung
von
verschiedenen
Arten des
Phishings*

⁵ zum Beispiel ein Link in einer Phishing-E-Mail

⁶ Malware, als Anhang einer E-Mail und der Nutzer wird dazu genötigt, den Anhang zu öffnen.

⁷ Download von Malware, die allein durch das Aufrufen einer Website heruntergeladen wird.

Kapitel 3 Einordnung innerhalb der Fachdidaktik Informatik

Damit die inhaltliche Relevanz überprüft werden kann, ist eine Einordnung des fachlichen Hintergrunds innerhalb der Fachdidaktik Informatik nötig. Dabei werden zuerst die Bildungsstandards für die Sekundarstufe I (Sek. I) der Gesellschaft für Informatik (GI) herangezogen, da für die Sekundarstufe I momentan noch kein Kernlehrplan für das Unterrichtsfach Informatik festgelegt wurde. Als weitere Einordnungsmöglichkeit wird im zweiten Abschnitt die Dagstuhl-Erklärung der GI verwendet, die drei unterschiedliche Perspektiven der digitalen Bildung betrachtet.

3.1. Bildungsstandards Sekundarstufe I der Gesellschaft für Informatik

Die Bildungsstandards für die Sek. I der GI im Unterrichtsfach Informatik (im Folgenden Bildungsstandards) sind 2008 durch die GI veröffentlicht worden. Die Bildungsstandards stellen dabei eine inhalts- und kompetenzorientierte Empfehlung der GI für den Informatikunterricht der Sekundarstufe I an deutschen Schulen dar. Die inhaltsorientierten Empfehlungen sind strukturiert durch die fünf *Inhaltsbereiche*:

1. Informationen und Daten
2. Algorithmen
3. Sprachen und Automaten
4. Informatiksysteme
5. Informatik, Mensch und Gesellschaft.

Die Einteilung der kompetenzorientierten Empfehlungen erfolgt durch fünf *Prozessbereiche*:

1. Modellieren und Implementieren
2. Begründen und Bewerten
3. Strukturieren und Vernetzen
4. Kommunizieren und Kooperieren
5. Darstellen und Interpretieren.

(vgl. [Ges08])

Innerhalb der Bildungsstandards spiegelt sich der zu vermittelnde Inhalt aus dem zweiten Kapitel vor allem in zwei Bereichen wieder. Im Inhaltsbereich *Sprachen und Automaten* heißt es unter anderem:

„Schülerinnen und Schüler der Jahrgangsstufe 5 bis 7 überprüfen vorgegebene E-Mail und WWW-Adressen auf Korrektheit und geben korrekte E-Mail- und WWW-Adressen an.“ [Ges08, S. 16]

Konkrete
passende
Inhaltspunkte
aus den
Bildungsstan-
dards

Das Überprüfen von WWW-Adressen auf Korrektheit impliziert Kenntnisse zum URL-Aufbau. Laut GI ist damit eine Vermittlung des URL-Aufbaus im Informatikunterricht empfehlenswert. Aus dem Inhaltsbereich *Informatik, Mensch und Gesellschaft* sind weiterhin folgende Inhaltspunkte anzugeben:

„Schülerinnen und Schüler der Jahrgangsstufen 5 bis 7 wissen, dass digitale Daten leicht manipulierbar sind“ und „lernen die potenziellen Gefahren bei der Nutzung digitaler Medien an Beispielen kennen.“ [Ges08, S. 18]

Es ist möglich, diese Punkte mit Phishing in Verbindung zu setzen. Phishing kann dabei explizit als potenzielle Gefahr angegeben werden. Die Opfer können im Falle eines erfolgreichen Phishing-Angriffs geschädigt werden. Eine Manipulation der Daten findet nur indirekt statt. Manipulation muss hier eher im Kontext *Vorspielen falscher Tatsachen* gesehen werden, da die gefälschten Websites in vielen Fällen das Design der Unternehmen und Institutionen nachahmen. Die inhaltliche Relevanz von URL-Aufbau und Phishing für Schülerinnen und Schüler (SuS) der Unterstufe kann damit als gegeben angesehen werden hinsichtlich der Bildungsstandards. Die Bildungsstandards können weiterhin verwendet werden, um mit Hilfe der Prozessbereiche im weiteren Verlauf das didaktische Konzept hinsichtlich der kompetenzorientierten Empfehlungen zu überprüfen. Während die Bildungsstandards nur eine Perspektive bezüglich des Informatikunterrichts liefern, kann durch die Dagstuhl-Erklärung auch die gesamtgesellschaftliche Bedeutung geklärt werden.

3.2. Dagstuhl-Erklärung der Gesellschaft für Informatik

Die Dagstuhl-Erklärung aus 2016 betrachtet Erscheinungsformen der digital vernetzten Welt (Phänomene, Gegenstände und Situationen) aus drei verschiedenen Perspektiven. Um nachhaltige Bildung in der digital vernetzten Welt zu ermöglichen, ist es nach Meinung der Autoren notwendig, die *technologische*, *gesellschaftlich-kulturelle* und die *anwendungsbezogene* Perspektive gemeinsam zu bearbeiten und zu hinterfragen, da sich diese gegenseitig beeinflussen. Den einzelnen Perspektiven ist zudem eine ergänzende Leitfrage zugeordnet worden. Die Verbindung der genannten Punkte führt zum Dagstuhl-Dreieck (siehe Abb. 3.1). [Ges16]

Die hier betrachtete Situation der digital vernetzten Welt ist die (sichere) *Nutzung des Webbrowsers* durch die NuN. Das konkrete Phänomen ist *Phishing*. Die technologische Perspektive kann somit explizit durch den URL-Aufbau und die Funktionsweise von Phishing-Angriffen betrachtet werden. Durch das Verstehen der Funktionsweise von Phishing und des URL-Aufbaus kann durch die NuN mit Hilfe der anwendungsbezogenen Perspektive eine sichere Nutzungsweise entstehen und das bewusste Abwehren von Phishing-Angriffen erfolgen. Innerhalb der gesellschaftlich-kulturellen Perspektive wird den NuN ermöglicht, die Folgen von Phishing-Angriffen zu identifizieren und mit welchem hohen Maß der Schutz von sensiblen Informationen einer jeden einzelnen Person zu bemessen ist.

Das Dagstuhl-Dreieck zeigt damit auf, dass nicht nur der fachliche Inhalt eine Rolle spielen sollte. Ein möglicher Ansatz zur Betrachtung der anderen Perspektiven im Lernspiel ist z. B. die Einbindung dieser in eine mögliche Story. Zur Gewährleistung einer erfolgreichen Vermittlung, wird es aber notwendig zuerst Prinzipien für digitale Lernspiele zur Vermittlung von fachlichem Wissen zu betrachten.

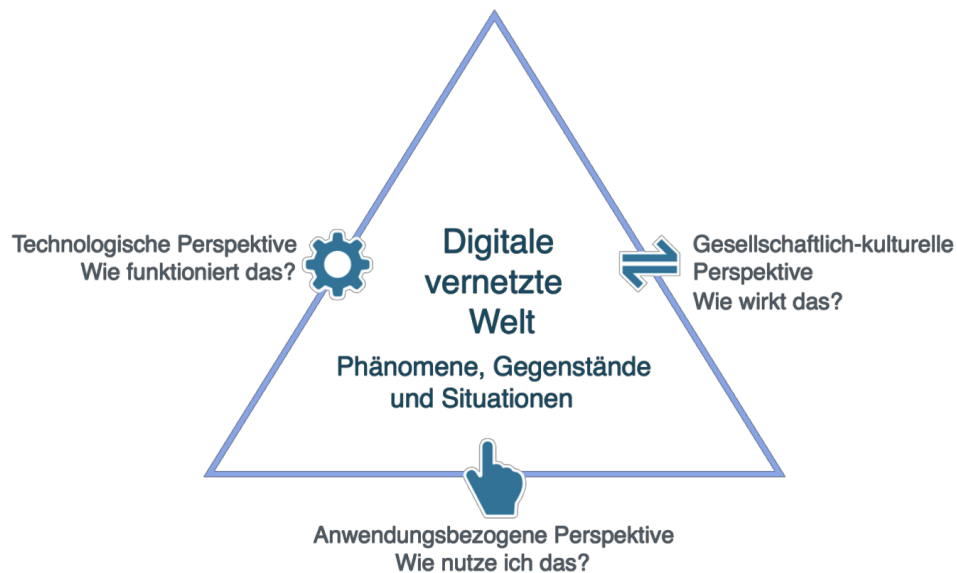


Abbildung 3.1.: Dagstuhl-Dreieck [Ges16]

Kapitel 4 Entwicklung eines digitalen Lernspiels

Durch die fortwährende Entwicklung von digitalen Spielen können Prinzipien und Möglichkeiten für das Design von digitalen Spielen angegeben werden, die zum (Lern-)Erfolg führen können. Im ersten Kapitel wird der Begriff *digitales Lernspiel* definiert, um eine Basis für die Nutzung des Begriffs zu schaffen. Im zweiten Kapitel werden einzelne Prinzipien vorgestellt und hinsichtlich ihrer Umsetzungsmöglichkeit analysiert. Dadurch können Fehler in der Entwicklung des didaktischen Konzepts des Lernspiels vermieden werden.

4.1. Definition eines digitalen (Lern-)Spiels

Um Design-Prinzipien für Lernspiele erörtern zu können, ist es notwendig den Begriff *digitales Lernspiel* genauer zu definieren. Durch die Expansion von digitalen Endgeräten sind diese Geräte auch in den Fokus der Bildung gerückt, woraus verschiedene Einordnungsmöglichkeiten für digitale Lernangebote und damit auch für digitale Lernspiele entstanden sind, die mehr oder weniger strikt den Begriff *digitales Lernspiel* an sich definieren. Als Sammelbegriff oder auch Oberbegriff dient *Entertainment Education*. Dieser Begriff umfasst grob alle Inhalte, die durch Medien eine Einbindung von Unterhaltung in das Lernen fokussieren. Dies müssen nicht unbedingt Lernspiele sein, sondern nur Medien an sich. Für diese Arbeit betrachten wir jedoch Lernspiele, die sich unter dem Begriff *Game-Based Learning* vereinen. Diese Untergruppe der *Entertainment Education* unterteilt sich wiederum in die drei Gruppen *Serious Games*, *E-Learning* und *Digital-Game-Based Learning* (DGBL) (vgl. Abb 4.1). Alle drei Begriffe sind mit einer eigenen Ausrichtung verbunden, weisen aber Schnittmengen auf. Unter dem Begriff *E-Learning* werden digitale Lernspiele versammelt bei denen die Wissensvermittlung klar im Vordergrund steht und spielerische Elemente nachrangig behandelt werden. Der Gegenspieler zum *E-Learning* bezogen auf digitale Lernspiele sind die *Serious Games*. Diese beachten spielerische und inhaltliche Kriterien gleichermaßen, damit sich Wissensvermittlung und reine Unterhaltung die Waage halten, die NuN sich jedoch auch mehr auf den Unterhaltungspart stützen können. Der restriktivste Begriff ist hier nun das DGBL, welches vor allem die spielerischen Komponenten an sich hervorheben möchte.

*Abgrenzung
verschiedener
Gruppen von
digitalen
Lernspielen*

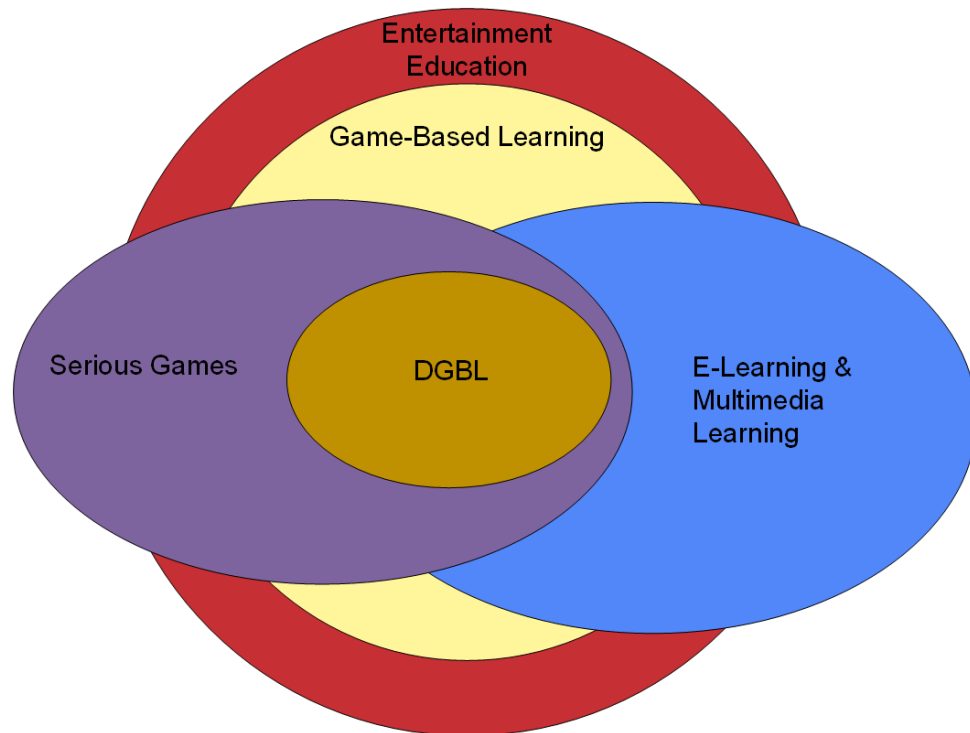


Abbildung 4.1.: Abgrenzung der Begriffe zur Einordnung von Lernspielen (vgl. [Bre10])

Prensky [Pre07] definiert dabei den Begriff *digitales Lernspiel* innerhalb des DGBL als Vereinigung aus Computerspielen und edukativem Inhalt. Zwischen Lernanwendungen, die Prinzipien zum Game-Design¹ umsetzen und digitalen Lernspielen besteht nach Prensky demnach ein Unterschied. Lernanwendungen, die Prinzipien für Computerspiele oder zum Game-Design umsetzen sind nicht als digitales Spiel zu bezeichnen, da diese nicht als Computerspiel mit vorher festgelegten Lernzielen entworfen worden sind und generelle Merkmale von Computerspielen vermissen lassen. Um Computerspiele von der Menge aller Spiele abzugrenzen, gibt Prensky neben sechs Merkmalen aller digitalen und analogen Spiele (vgl. [Pre07, S. 119]) zuerst sechs Merkmale von Computerspielen an:

*Beschreibung
der hier
genutzten
Definition von
digitalen
Lernspielen*

1. a form of fun – enjoyment and pleasure
2. a form of play – intense and passionate involvement
3. interactive – doing
4. adaptive – flow
5. problem solving – creativity
6. win states – ego gratification

(vgl. [Pre07, S. 106])

¹ eine Erläuterung von Prinzipien zum Game-Design folgt im nächsten Unterkapitel 4.2

Prensky hebt neben diesen sechs Merkmalen vor allem die Möglichkeiten des *Storytellings* für digitale Lernspiele hervor (vgl. [Pre07, S. 126f]). Durch diese Eigenschaft grenzt sich das DGBL in beide Richtungen sowohl von den Serious Games, als auch vom E-Learning ab. Unter der Prämisse Prenskys, dass ein digitales Lernspiel „[...] should feel just like a video game or computer game, all the way through“ [Pre07, S. 146], ist die Verwebung von Wissensinhalten in einer Story ein wichtiges Ziel. Durch den Spielkontext kann das Engagement der NuN erhöht werden und eine Anregung zum Lernprozess stattfinden (vgl. [Pre07, S. 147]).

Der Begriff *digitales Lernspiel* wird daher im Folgendem unter Anlehnung an Prenskys Definition benutzt. Die hier erörterten Gesichtspunkte sollen in der Konzeption des entwickelten Lernspiels soweit wie möglich beachtet werden, da diese einen Rahmen

4.2. Design eines digitalen (Lern-)Spiels

Seit Beginn der kommerziellen Spielentwicklung gibt es Spiele, die sich nach ihrer Veröffentlichung zu Klassikern entwickeln oder Meilensteine der Spielgeschichte (z. B. Pac-Man oder Asteroids) darstellen [BM10, S. 204]. Auch heute existieren digitale Spiele, die über mehrere Jahre oder auch Jahrzehnte eine große Anzahl an Spieler/-innen an sich binden (z. B. World of Warcraft oder League of Legends). Über die Jahre haben sich dabei verschiedene Prinzipien etabliert, die einem digitalen Spiel zum Erfolg verhelfen können. Dabei haben sich auch Prinzipien etabliert, die für digitale Lernspiele von Bedeutung sein können. Prensky listet dabei [u. a.] folgende Prinzipien auf, die auch von besonderem Interesse in Bezug auf die Entwicklung von digitalen Lernspielen sein können [Pre07, S. 134ff]:

*Vorstellung
verschiedener
Designmerk-
male für
Computerspiele*

1. Das digitale Spiel ist ausbalanciert

Die NuN werden durch das Spiel gefordert, aber es existieren keine unfairen oder zu leichten Spielsituationen [Pre07]. In Hinsicht auf digitale Lernspiele ist hier auf den fachlichen Inhalt zu achten. Überfordert der fachliche Inhalt die NuN, wenden sich diese vom Spiel ab. Wird Wissen zu kleinschrittig verpackt, kann es zur Ablenkung durch Unterforderung kommen, sodass potenziell neues Wissen nicht vermittelt wird.

2. Das digitale Spiel ist spannend

Die NuN interessieren sich für das Ziel des Spiels, jedoch ist es herausfordernd das Ziel zu erreichen [Pre07]. Für digitale Lernspiele kann daher die reine Vermittlung von Wissen ohne Kontext nicht das Mittel der Wahl sein. Das Lernspiel muss die NuN überzeugen, dass diese durch ihr neues fachliche Wissen etwas erreichen und das Wissen auch realitätsnah anwenden können.

3. Häufiges Belohnung, keine direkten Strafen

Antreibende Belohnungen erhöhen die Motivation bei den NuN ein Spiel weiterzuspielen. Direkte Strafen wie Punktabzüge oder das Wiederholen von Levels vermindern die Spielfreude. Besser sind sinkende Belohnungen oder der Reset an einen Meilenstein im Level selbst [Pre07]. Im Fall von digitalen Lernspielen kann Frust aufkommen, wenn die NuN gewisse fachliche Inhalte nicht verstehen und dafür bestraft werden. Daher kann es ratsam sein, Sprünge innerhalb der Wissensvermittlung zuzulassen, damit zur Fokussierung auf Verständnisschwierigkeiten bereits verinnerlichtes und überprüftes Wissen übersprungen werden kann.

4. Fokus auf das Spielerlebnis

Spielentwickler neigen dazu ein Spiel zu erschaffen, welches sie selbst gerne spielen würde. Dies muss nicht unbedingt von Nachteil sein, jedoch kann der Blick auf das eigentliche Publikum verloren gehen, sodass Spieleinstiege zu schwierig für Neueinsteiger gestaltet werden [Pre07]. Dieser mögliche Problemfall ist für digitale Lernspiele von besonderer Bedeutung. Für die Entwickler ist das zu vermittelnde Wissen trivial, sodass die Möglichkeit eines zu schweren Spieleinstiegs für die NuN entsteht.

5. Erweiterungen und neue Entdeckungen möglich

Spiele, die Möglichkeiten zum weiteren entdecken anbieten, sind interessanter für NuN, da die Ungewissheit hinter den neuen Entdeckungen, die Spannung der NuN hochhält [Pre07]. Die Möglichkeiten hinsichtlich digitalen Lernspielen sind hier aber begrenzt. Neue Gegenstände im Spiel helfen den NuN nicht das vermittelte Fachwissen schneller zu begreifen. Es ist jedoch möglich den NuN die Entdeckung des Wissens zu überlassen, anstatt den Fluss strikt vorzugeben.

6. Spielfortschritt lässt sich speichern

Damit die NuN ihren eigenen Spielfortschritt nach einer Spielunterbrechung nicht verlieren, ist in fortschrittsbasierten Spielen eine Speichermöglichkeit essentiell [Pre07]. Für digitale Lernspiel kann dies beispielsweise das Speichern der Lernfortschritte bedeuten, sodass bei einem neuen Start nicht wieder mit der Vermittlung von bereits vorhandenem Wissen begonnen wird.

7. Leicht lernbar, schwer zu meistern

Damit alle NuN am digitalen Spiel Freude haben, ist ein leichter Einstieg empfehlenswert. Durch größtmögliche Herausforderungen kann aber auch für erfahrene NuN ein Anreiz geschaffen werden, sodass es möglichst schwer wird, ein Spiel in seiner Gesamtheit zu meistern [Pre07]. Der Atari² Gründer Nolan Bushnell prägte diese Design-Philosophie innerhalb der Videospielkultur schon 1971 mit dem Ausdruck „easy to play, hard to master“, heute auch unter *Bushnell's Law* bekannt. Für digitale Lernspiele kann dieser Ansatz ebenfalls möglich sein. Zu berücksichtigen ist jedoch, dass es starke Schwankungen im Vorwissen der NuN geben kann. Es ist nicht möglich immer neues Wissen (innerhalb des Themenkomplexes) zur Verfügung zu stellen, jedoch können kompetitive Komponenten zur Erlangung eines *Highscores* das Lernspiel erweitern. NuN mit Vorwissen können so weiter an das Lernspiel gebunden und NuN ohne Vorwissen währenddessen der Inhalt vermittelt werden.

Anhand der genannten Design-Prinzipien und der vorherigen Definition von digitalen Lernspielen ist es möglich existierende Lernspiele zu analysieren und das Konzept der jeweiligen Lernspiele zu bewerten. In Kombination mit den Analysen kann im Anschluss ein neues (didaktisches) Konzept entwickelt werden.

² Atari war eines der ersten kommerziell erfolgreichen Unternehmen im Bereich der Videospielbranche zu Beginn der Siebziger Jahre des 20. Jahrhunderts und hatte dadurch großen Einfluss auf die Branche.

Kapitel 5 Lernspiele im Themenbereich Phishing

Im letzten Kapitel des zweiten Teils werden das webbasierte Lernspiel *Anti-Phishing Phil* und die Android-App *NoPhish* vorgestellt. Dabei werden beide Phishing-Lernspiele hinsichtlich der vorherigen drei Kapitel des zweiten Teils eingeordnet und analysiert. Danach werden erste Folgerungen für die Konzeption des neuen Lernspiels dargestellt.

5.1. Anti-Phishing Phil

Das Lernspiel *Anti-Phishing Phil*¹ ist 2007 an der Carnegie Mellon University (Pittsburgh, USA) entstanden und basiert auf Flash 8. Im Jahr 2008 wurde das Spiel kommerzialisiert, sodass nur noch eine veraltete Version unter CC-BY-NC Lizenz verfügbar ist. Eine Forschungsgruppe aus Australien hat 2017 zwar eine mobile App-Adaption des Lernspiels unter dem Namen *Phish Phinder* vorgestellt, das Spiel ist jedoch nicht öffentlich verfügbar (Stand: Januar 2019) [MAB17]. Betrachtet wird daher die Flash-Version, die nativ auf 800 x 800 Pixeln ausgegeben wird. Das Lernspiel ist darauf ausgelegt worden, den NuN das Identifizieren von Phishing-URLs zu lehren. Als Hintergrundgeschichte fungiert dabei der junge Fisch *Phil*, der durch das Essen von Würmern wachsen möchte. Diese symbolisieren dabei im Interface die URLs. Dabei kann *Phil* entweder einen Wurm essen oder ablehnen (Abb. 5.1).

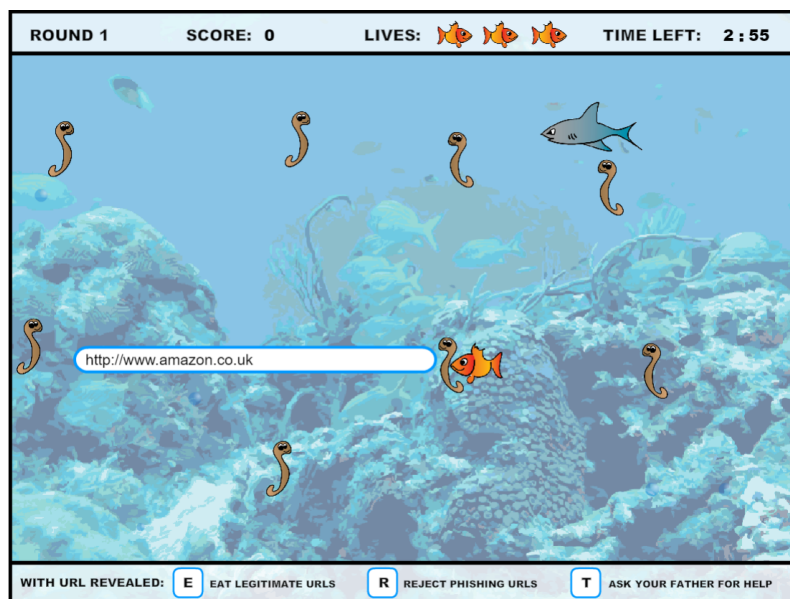


Abbildung 5.1.: User Interface einer Runde im Spiel Anti-Phishing Phil

¹ *Anti-Phishing Phil* ist verfügbar unter <https://www.ucl.ac.uk/cert/antiphishing/>.

Um eine Runde erfolgreich zu beenden sind sieben von zehn Würmern innerhalb dieser Wissensüberprüfung entweder korrekt zu essen oder abzulehnen. Erreichen die NuN diesen Wert nicht, muss die Runde wiederholt werden. Wird ein Wurm gegessen, obwohl es sich um eine Phishing-URL handelt, verlieren die NuN eines von drei Leben. Wird ein Wurm abgelehnt, obwohl es sich um eine seriöse URL handelt, verlieren die NuN innerhalb der Runde zehn Sekunden an Rundenzeit. Bei korrekter Lösung erhalten die NuN 100 Punkte. Trifft der NuN mit Phil auf einen Hai, verlieren die NuN ebenfalls ein Leben. Bei Schwierigkeiten können die NuN den Vater von Phil, um Hilfe bitten. Dieser antwortet, darauf mit einzelnen Hinweisen zur Beurteilung der URL. Sind alle zehn Würmer einmal bearbeitet worden, ist die Zeit abgelaufen oder sind alle drei Leben verbraucht, erscheint eine Feedback-Seite, die zu allen URLs der letzten Runde eine Erklärung plus die korrekte Antwort beschreibt (Abb. 5.2). Der Ablauf des Spiels innerhalb einer Runde wiederholt sich also durch Lerneinheit, gefolgt von einer Wissensüberprüfung und der Feedback-Seite. Der fachliche Inhalt bezüglich der verschiedenen Phishing-Techniken deckt sich dabei mit den im Kapitel 2.2 vorgestellten Möglichkeiten. In der Abbildung 5.2 können die unterschiedlichen Website-URLs passend zu den Möglichkeiten identifiziert werden.

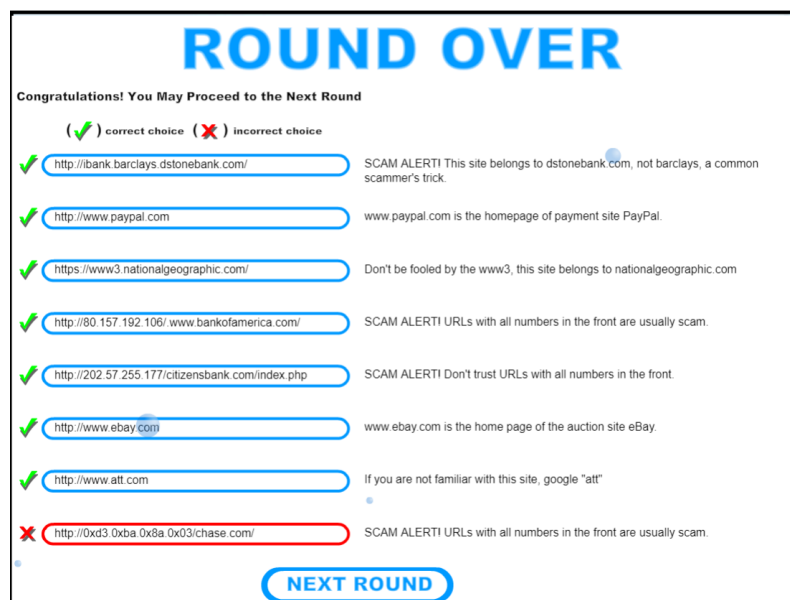


Abbildung 5.2.: Feedback Seite im Spiel Anti-Phishing Phil

Nach der ersten Runde (von vier) und dem Feedback erscheint eine Lerneinheit, die konkretes textuelles Wissen in Bezug auf den URL-Aufbau und in den nachfolgenden Runden zur Erkennung von Phishing-URLs bereitstellt. Dabei werden jedoch keine Fachbegriffe verwendet, sondern allgemeine Wörter wie beispielsweise „Address“ (vgl. Abb. 5.3). Absolvieren die NuN alle vier Runden ist das Spiel beendet. Im Anschluss können sich die NuN die vier Hauptregeln der Lerneinheiten nochmals anschauen und optional das Spiel von vorne beginnen.

Durch die obige Beschreibung wird deutlich, dass die Entwickler zur Einpassung des fachlichen Inhalts eine einfache Story einführen. Durch die begrenzte Anzahl an Leben und die Zeitbegrenzung kann bei unerfahrenen NuN Spannung erzeugt werden. Direkte Strafen in Form von Punktabzügen existieren nicht, es wird lediglich die Rundenzeit verkürzt. Besondere Belohnungen für die NuN sind jedoch ebenfalls nicht vorhanden.

Das Feedback am Ende einer Runde gibt zwar einen Überblick über die eigenen Lösungen, eine weitere Belohnung ist jedoch nicht vorhanden. Werden zu Beginn einfache Beispiele für Phishing-URLs ausgewählt, steigt die Komplexität der URLs im Laufe der vier Runden. Für unerfahrene NuN ist dabei keine unfaire Spielsituation zu erwarten, da das benötigte fachliche Wissen zumindest textuell repräsentiert wird. Die Möglichkeit das Spiel immer weiter und mit mehreren oder noch komplexeren Beispielen zu spielen, ist dabei nicht möglich. Die Punkte, welche die NuN für richtige Antworten erhalten, stehen nicht im Fokus und haben auch für die NuN keinen weiteren Bezugspunkt im Spiel. Weiterhin lässt sich der Spielfortschritt nicht speichern. Neue Entdeckungen sind durch die NuN nicht möglich, da der Spielverlauf stringent durch das Spiel vorgegeben wird und das fachliche Wissen ohne Nutzerinteraktion präsentiert wird. Innerhalb der Runden (also der eigentlichen Wissensüberprüfung) ist die Interaktivität gegeben. Die NuN steuern den Fisch, um die Würmer zu erreichen. Eine Interaktivität innerhalb der Wissensvermittlung der Lerneinheiten ist jedoch nicht vorhanden. Dadurch ist es den NuN möglich, diese Lerneinheiten zu überspringen und direkt in die nächste Runde der Überprüfung zu gelangen. Bei einem dortigen Scheitern wird die Lerneinheit wiederholt, doch für die NuN ist die einzige Interaktion mit dem Spiel in dem Moment das Lesen der Wissenstexte. Die NuN übernehmen somit keine eigene Verantwortung während des Vermittlungsprozess, sodass ein Engagement der NuN nicht gefördert wird.



Abbildung 5.3.: Beispielhafter Inhalt einer Lerneinheit zum URL-Aufbau im Spiel Anti-Phishing Phil

Zusammenfassend ist anzumerken, dass durch das Lernspiel mehrere Design-Prinzipien umgesetzt werden, andere wiederum nicht beachtet worden sind. Insbesondere die fehlende Interaktivität innerhalb des Vermittlungsprozesses, sowie das Fehlen von Elementen, welche die Kreativität und Fähigkeit der NuN zum Problemlösen ansprechen, sind hinsichtlich der Merkmale und Design-Prinzipien kritisierbar. Positiv hervorzuheben ist die Balance des Lernspiels, da unerfahrene NuN während der Wissensüberprüfung nicht verschreckt werden, diese gleichzeitig aber auch durch den Timer und die Lebensbegrenzung nicht auf Antrieb zu meistern ist. Rein spielerische Elemente wie der schwimmende Hai intensivieren das Spielerlebnis, da diese die Dominanz der fachlichen Inhalt eingrenzen. Da der fachliche Inhalt aber noch überwiegt und eine Interaktion mit dem Lernspiel

nur zur Überprüfung stattfindet, ist das Lernspiel eher im E-Learning und weniger im Bereich des DGBL anzusiedeln.

Anti-Phishing Phil wurde nach der Entwicklung evaluiert. Als Testgruppe fungierten vierzehn Angehörige der örtlichen Universität. Dabei konnte eine signifikante Verbesserung der Erkennungsrate von Phishing-URLs festgestellt werden [She+07].

5.2. NoPhish

Die Android-App *NoPhish*² wurde am Karlsruher Institut für Technologie (KIT) im Rahmen einer Masterarbeit entwickelt. Ebenso wie das Lernspiel *Anti-Phishing Phil* ist *NoPhish* darauf ausgerichtet, die NuN für Phishing zu sensibilisieren und durch das Vermitteln der Struktur einer Website-URL das Erkennen von Phishing-Angriffen zu ermöglichen. Die Vermittlung des Inhalts erfolgt über zwei Einführungslevel, acht Level zu verschiedenen Phishing-Möglichkeiten und einem Schlusslevel, das weitere Schlussbemerkungen enthält. Der fachliche Inhalt deckt sich mit den Inhalten des zuvor betrachteten Spiels *Anti-Phishing Phil* und der im Kapitel 2.2 vorgestellten Phishing-Techniken. *NoPhish* besitzt aber im Vergleich zu *Anti-Phishing Phil* längere Vermittlungssequenzen. Im ersten Level sind durch die NuN vor der ersten Interaktion mit dem Spiel neun Bildschirmseiten an Text zu bearbeiten. Dabei ist ein Level spielbar, wenn das vorherige Level erfolgreich absolviert wurde. Ein beispielhaftes Level folgt dabei wie im Lernspiel *Anti-Phishing Phil* dem abwechselnden Schema aus Vermittlung und Überprüfung. Die Vermittlung findet über eine grafische und textuelle Repräsentation des jeweiligen Wissens statt. Als grafische Unterstützung wird zum Beispiel ein Teilelement einer URL farbig unterlegt. Nach der Vermittlung einer neuen Phishing-Möglichkeit ist durch die NuN zu 12 bis 25 nacheinander eingeblendeten Website-URLs die Frage zu beantworten, ob der jeweiligen Website-URL vertraut wird. Bei einer korrekt erkannten Phishing-Website ist je nach Fortschritt des Levels zudem das Anklicken des Hosts gefragt (vgl. Abb 5.4). Hervorzuheben ist dabei, dass die Vermittlungseinheiten wie in *Anti-Phishing Phil* keine technischen Fachbegriffe enthalten, sondern eigens gewählte Synonyme verwendet werden. Der Host wird im Lernspiel beispielsweise als *Wer-Bereich* eingeführt.

Vorstellung
und Spielme-
chanismen von
NoPhish

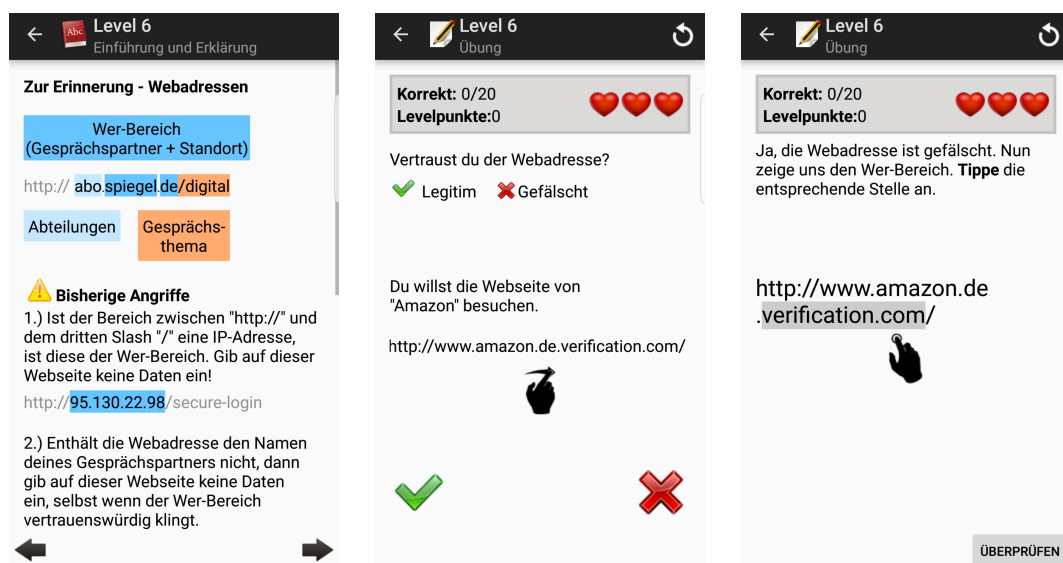


Abbildung 5.4.: Level: Vermittlung, Vertrauensfrage und Anklicken des Hosts im Spiel NoPhish

² *NoPhish* ist verfügbar unter <https://secuso.aifb.kit.edu/521.php>.

Die Leistung eines Nutzers wird im Level bereits bewertet und die NuN erhalten eine Rückmeldung in Form einer Punktzahl, sowie eine Einstufung ebendieser Punkte in ein Raster, durch welches der Nutzer null bis drei Sterne pro Level erhalten kann (Abb. 5.5). Die Sterne haben im weiteren Verlauf des Spiels keine weitere Funktion. Diese geben den NuN aber ein neben den Punkten ein zusätzliches grafisches Feedback. Das Lernspiel enthält kein Storyboard und setzt den Fokus eindeutig auf den zu vermittelnden Inhalt.

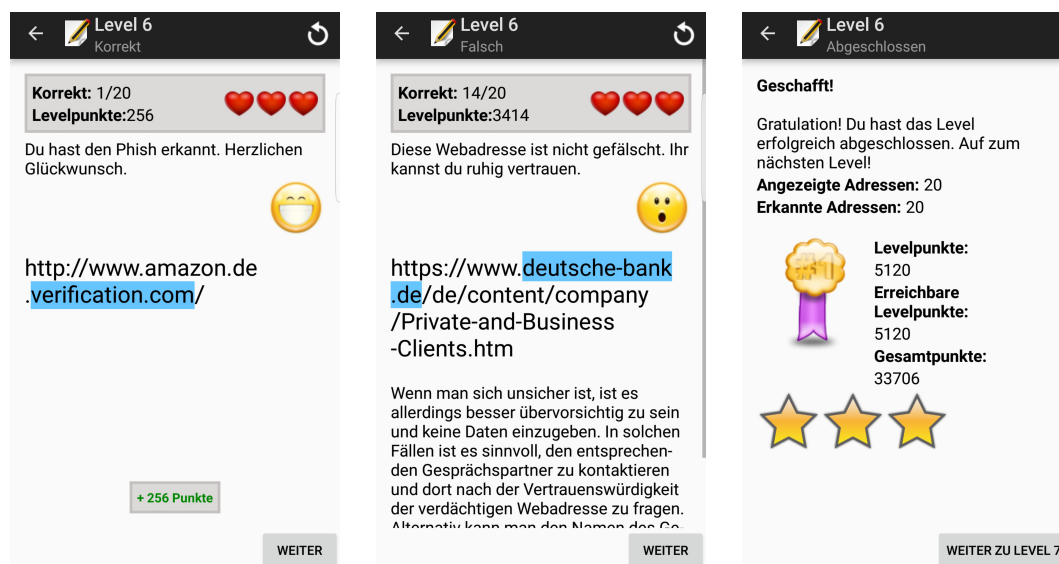


Abbildung 5.5.: Feedback und Bewertung im Spiel NoPhish

Analysiert man die App *NoPhish* bezogen auf die Definition eines Lernspiels nach Prensky ist die Einordnung in das DGBL nicht gegeben. Da die Wissensvermittlung ohne Story oder spielerische Elemente durchgeführt wird, kann eine Einordnung in den Bereich des E-Learnings erfolgen. *NoPhish* erfüllt einzelne Kriterien Prenskys an ein digitales Lernspiel beziehungsweise Computerspiel. Durch die sofortige Bewertung der Leistung der NuN existieren *win states*, da die NuN nach jeder Runde eine Bestätigung ihrer Leistung erhalten. Darüber hinaus ist durch den Überprüfungsmodus mit bis zu 25 Website-URLs zwar nur eine Interaktionsmöglichkeit durchgängig vorgesehen, jedoch kann das Wiederholen dieser Interaktion die NuN in einen *flow* versetzen und ist während der Überprüfung interaktiv gestaltet. Der Vermittlungsprozess ist jedoch nicht interaktiv, da dieser aus dem reinen Lesen der Texte besteht. Situationen zum Lösen von Problemen sind nicht vorhanden. Auch fehlen Elemente zur Steigerung des Engagements der NuN, wie die persönliche Bindung der NuN an das Spiel durch einen die NuN betreffenden Kontext. Ob das Lernspiel den NuN Spaß bereitet unterliegt dem subjektiven Empfinden und kann hier nicht geklärt werden. Neben den Kriterien für Computerspiele sind auch einzelne Designmerkmale vorhanden. So kann der Spielfortschritt durch die Levelstruktur gespeichert werden und eine Erweiterung lässt sich durch das Hinzufügen weiterer Level auch realisieren. Durch die Sternbewertung und die Punktzahl zu jedem Level ist ein häufiges Belohnen der NuN mit visuellen Reizen wie einer fiktiven Medaille zu erkennen. Darüber hinaus ist jedoch durch die fehlende Story kein Spannungsbogen zu erwarten. Ob das Lernspiel ausbalanciert ist, kann wiederum nicht konkret beantwortet werden. Durch die Levelstruktur verteilen sich die neuen Inhalte auf die verschiedenen Vermittlungssituationen, sodass ein leichter Einsteig für die NuN möglich erscheint.

Analyse
bezüglich
(Design)-
Merkmale

5.3. Schlussfolgerungen für die Konzeption

*Gewonnene
Erkenntnisse
für die
Konzeption*

Durch die beiden Lernspiele *NoPhish* und *Anti-Phishing Phil* können bereits mehrere Erkenntnisse in die folgende Konzeption übernommen werden. Zum einen deckt sich der Inhalt beider Lernspiele mit den herausgearbeiteten fachlichen Inhalten aus Kapitel 2, sodass der fachliche Inhalt ohne Änderungen in die Konzeption übernommen werden kann. Beide Lernspiele ließen aber keine Interaktion während der Vermittlungssituationen zu. Hier gilt es in der Konzeption Möglichkeiten zur Einbindung und Steigerung der Interaktivität in den Vermittlungssituationen zu schaffen. Darüber hinaus bieten beide Lernspiele Konzepte, die sich zu einem anderen Zweck übernehmen lassen. Der Überprüfungsmodus beider Lernspiele in Form der sich wiederholenden Abfragen kann ein Instrument zur Evaluation darstellen, da sich die Rahmenbedingungen immer gleichen und sich somit keine weiteren Spieleinflüsse auf die Leistung der NuN auswirken können. Zudem können durch die Levelstruktur aus *NoPhish* bereits mehrere Punkte wie das Speichern des Spielfortschritts oder die einfache Erweiterung des Lernspiels umgesetzt werden.

Bei der sprachlichen Gestaltung der Vermittlungssituationen verfolgen beide Lernspiele den Ansatz Fachbegriffe zu vermeiden. Dieser Ansatz steht jedoch im Widerspruch zu den Bildungsstandards für die Sek. I der GI. In diesen wird die sachgerechte Nutzung von Fachbegriffen sogar als zu erfüllende Fertigkeit für SuS im Prozessbereich „Kommunizieren und Kooperieren“ ausgewiesen:

„Schülerinnen und Schüler der Jahrgangsstufen 5 bis 7 stellen informatische Sachverhalte unter Benutzung von Fachbegriffen mündlich und schriftlich sachgerecht dar.“
[Ges08, S. 21]

Daher werden in der folgenden Konzeption und Umsetzung des Lernspiels die Fachbegriffe aus Kapitel 2.1 und 2.2 explizit genutzt. Es ist jedoch darauf zu achten, dass diese Fachbegriffe dosiert eingeführt werden, um eine Abschreckung der NuN durch die fremden Begriffe zu verhindern.

Teil III

KONZEPTION UND UMSETZUNG DES LERNSPIELS

Kapitel 6 Konzeption des Lernspiels

Zur Erarbeitung eines Konzepts werden zuerst Lernziele definiert, diese entsprechend den Taxonomiestufen nach Bloom¹ eingeordnet und hinsichtlich der SMART-Kriterien² für Lernziele überprüft. Aus den bisherigen Erkenntnisgewinnen zu bereits vorhandenen Lernspielen im Themenbereich Phishing, wird im Anschluss ein didaktisches Konzept erarbeitet (6.2). Zentrale Aspekte des Spielaufbaus und der Story werden auf Basis des didaktischen Konzepts und der Lernziele im Kapitel 6.3 betrachtet. Im Anschluss wird das Spielkonzept bezüglich der Definition eines Lernspiels nach Prensky und der (Design-)Merkmale für Computerspiele analysiert (6.4). Mögliche Anwendungsfälle werden im Unterkapitel 6.5 thematisiert. Insbesondere werden dort die Auswahl der Zielgruppe, Bedingungen zur Nutzung des Lernspiels und aktuelle schulpolitische Entscheidungen miteinbezogen.

6.1. Lernziele

Um Möglichkeiten für Phishing auf Basis von Website-URLs zu verstehen, ist es notwendig sich Hintergrundwissen bezüglich des Aufbaus von Website-URLs anzueignen. Nur so können auch in Zukunft Phishing-Versuche sicher erkannt werden. Ein direkter Einstieg in das Thema Phishing könnte zwar zur Aneignung von Handlungsweisen führen, um nicht auf Phishing hereinzufallen, doch die NuN werden nicht in die Lage versetzt sich fundiert eine eigene Meinung zu bilden und können sich auch zukünftig nicht an geänderte Parameter anpassen, sobald eingeübte Handlungsweisen nicht mehr zielführend sind. Die Lernziele und ihre Teillernziele basieren somit nicht auf der reinen Aneignung von Handlungsweisen, sondern auf dem Erwerb nachhaltiger Fähigkeiten.

Das erste Lernziel ist geprägt durch den fachlichen Hintergrund einer Website-URL. Im Fokus steht hier vor allem die Identifizierung der einzelnen Elemente einer Website-URL. Durch die Forderung nach einer Identifizierung der einzelnen Elemente einer Website-URL kann das erste Lernziel in die vierte Taxonomiestufe (*Analyse*) nach Bloom eingeordnet werden. Die Analyse und Zerlegung einer Website-URL kann nur geschehen, wenn die Struktur sowie die Zusammenhänge einer Website-URL bekannt sind. Damit das erste Lernziel erreicht werden kann, sind vier Teillernziele zu erfüllen und zu verbinden.

*Entwicklung
des ersten
Lernziels*

¹ Mit Hilfe der Taxonomiestufen nach Bloom können Lernziele hierarchisch gegliedert werden, sodass innerhalb einer Lernzielkontrolle gezielt Fähigkeiten überprüft werden können. Als Grundlage dient [BE76].

² Die SMART-Kriterien bieten eine weitere Möglichkeit zur Überprüfung von Lernzielen hinsichtlich ihrer Formulierung und Messbarkeit für eine Lernzielkontrolle. Eine Zusammenfassung ist zu finden unter [Deu].

1. Lernziel:

Die NuN analysieren den Aufbau einer beliebigen Website-URL und können alle einzelnen Bestandteile identifizieren.

Teillernziele zum 1. Lernziel:

Die NuN sollen ...

- 1.1 Top-Level-Domains und Second-Level-Domains innerhalb einer Website-URL erkennen.
- 1.2 eine Subdomain (Third-Level-Domain) erkennen und den Nutzen einer Subdomain erklären. Die NuN deuten weiterhin die Verbindung von Subdomain, Domain und Top-Level-Domain als Host einer Website und bestimmen eben diesen innerhalb einer Website-URL.
- 1.3 die Existenz von Transportprotokollen zur Übertragung von Daten zur Kenntnis nehmen.
- 1.4 die andere Leserichtung von Pfaden und Querys, sowie deren Nutzen einordnen. Die NuN bestimmen darüber hinaus den Beginn von Pfaden und Querys innerhalb einer Website-URL.

Für die einzelnen Teillernziele (TL) sind mehrere inhaltliche Konzepte relevant. Für das TL (1.1) sind das vor allem die Auflösung des Hosts einer URL von rechts nach links, sowie die Merkregel „Die Top-Level-Domain befindet sich vor dem ersten einzelnen Slash“. Darüber hinaus ist die Angabe diverser alltäglicher Top-Level-Domains (.de, .com, .org) relevant. Für die NuN muss außerdem ersichtlich sein, dass durch die Domain die Zielseite eines Website-Aufrufs gegeben ist. Für das TL (1.2) ist besonders die Freiheit in der Vergabe von Subdomains unter einer Domain wichtig, sowie die Verknüpfung einer Subdomain zu ihrer Domain. Durch das TL (1.3) wird die Existenz der Transportprotokolle *http* und *https* betrachtet und welche Konsequenzen sich aus dem jeweilig verwendeten Protokoll ergeben. Das TL (1.4) betrachtet wiederum die Möglichkeiten zur Übermittlung von Anfragen und Daten über die URL. Darüber hinaus ist die Trennung von Host und Pfad beziehungsweise Querys notwendig, um die Top-Level-Domain erkennen zu können.

Das TL (1.1) ist dabei im Bereich der zweiten Taxonomiestufe (*Verständnis*) einzuordnen, da für die Erreichung des Teillernziels die Deutung von Komponenten einer Website-URL von Nöten ist. In die dritten Taxonomiestufe (*Anwendung*) kann das TL (1.2) eingeordnet werden, da hier zur Erfüllung des Teillernziels das Verständnis des Begriffs *Hosts* nötig ist und die Bestimmung des Hosts innerhalb einer Website-URL in verschiedenen Kontexten notwendig ist. Das TL (1.3) genügt der ersten Taxonomiestufe (*Wissen*), da die NuN nur das faktische Wissen über Transportprotokolle erlangen, diese aber in Bezug auf Phishing keine technische Relevanz haben. Wiederum in die dritte Taxonomiestufe kann das TL (1.4) eingeordnet werden, da die Konzepte Pfad und Query später auch im Kontext des Phishings eine Rolle in mehreren Anwendungen spielen (vgl. Kapitel 2.2, Anknüpfungspunkt 4).

In Bezug auf die SMART-Kriterien für Lernziele ist festzustellen, dass eine unmissverständliche Formulierung des ersten Lernziels vorliegt, da bei der Identifizierung von Teilen einer Website-URL kein Spielraum vorhanden ist. Darüber hinaus ist das Lernziel messbar, da durch die NuN entweder alle oder nicht alle Elemente einer Website-URL identifiziert werden können. Durch die Nutzung von „analysieren“ und „identifizieren“

sind die NuN aktiv aufgefordert eine Aufgabe umzusetzen. Daher kann das Lernziel als aktiv bezeichnet werden. Ob das Lernziel von allen NuN als akzeptabel eingestuft wird, kann hier nicht erörtert werden. Das Lernziel an sich ist jedoch realistisch, da der Aufbau einer Website-URL klaren Bildungsregeln (vgl. Unterkapitel 2.1) folgt und somit durch die NuN ein aktives *Entdecken* zu Verständnis führt. Darüber hinaus kann das Lernziel als terminierend angesehen werden, da explizit herausgestellt wird, dass die Erfüllung des Lernziels erst gegeben ist, wenn *alle* Elemente einer Website-URL identifiziert werden können.

Entwicklung
des zweiten
Lernziels

Während das erste Lernziel das Hintergrundwissen und den Umgang mit Website-URLs behandelt, werden durch das zweite Lernziel die Vermittlung und Befähigung der NuN zum aufbauenden Bereich der Phishing-Angriffe betrachtet. Das zweite Lernziel ist ebenfalls in die vierte Taxonomiestufe einzuordnen, da zur Identifizierung von unterschiedlichen Phishing-Angriffen das erste Lernziel erfüllt sein muss. Einen Phishing-Angriff über eine Website-URL zu identifizieren, kann nur durch das Zerlegen der Website-URL in ihre Teilelemente erfolgen. Um die Arbeitsweise von Phishing-Angriffen verstehen zu können ist, muss ebenfalls der Zusammenhang zwischen dem einzelnen Phishing-Angriff und der dahinter stehenden Website-URL erkannt werden. Zur Erfüllung des Lernziels sind wiederum Teillernziele in Verbindung zu bringen, die sich vor allem mit den einzelnen Möglichkeiten für Phishing-Angriffe auseinandersetzen.

2. Lernziel:

Die NuN untersuchen beliebige Website-URLs auf alle vorgestellten Phishing-Angriffe und identifizieren (falls vorhanden) ebendiese Phishing-Angriffe.

Teillernziele zum 2. Lernziel:

Die NuN sollen ...

- 2.1 Angriffe über die Nutzung bekannter Domains als Subdomain erkennen.
- 2.2 Angriffe über die Nutzung ähnlicher Namen für die Phishing-Website erkennen.
- 2.3 Angriffe über die Nutzung gleich aussehender Buchstaben verschiedener Alphabete beschreiben.
- 2.4 Websites, die eine IP als Adresse anzeigen als Phishing-Websites deuten.
- 2.5 Angriffe über die Nutzung bekannter Domains als Pfadangabe erkennen.
- 2.6 präventive Arbeitsweisen benennen, durch die Phishing—Angriffe rechtzeitig erkannt werden können.
- 2.7 Cross-Site-Scripting und @-zeichen in der URL als weitere Missbrauchsmöglichkeiten angeben.

Die Inhalte, die zur Umsetzung der Teillernziele genutzt werden, ergeben sich für die Teillernziele (2.1), (2.2), (2.3), (2.4) und (2.5) direkt aus den zugehörigen Punkten 1. – 5. des Unterkapitels (2.2). Für das Teillernziel (2.6) sind hingegen Handlungsweisen zu betrachten, welche die NuN bei der Analyse einer Website-URL unterstützen, sodass eine Website erst gar nicht geöffnet werden muss. Mögliche Handlungsanweisungen sind

z. B. das Hovern über einen Link auf verschiedenen Betriebssystemen oder die erneute manuelle Eingabe von Website-URLs, um Phishing-Angriffe in Form des TL (2.2) zu vermeiden. Das TL (2.7) wird hier in einer Sonderrolle behandelt, da zum einen Website-URLs, die ein @-Zeichen enthalten, von den gängigen Browsern bereits mit einer Warnung versehen werden und zum anderen nur ein Ausblick auf das Thema Cross-Site-Scripting geschaffen werden soll, damit die NuN weitere potentielle Gefahren nicht verkennen, die auch abseits der Website-URL zu Phishing führen können.

Die TL (2.1), (2.2), (2.4) und (2.5) können der vierten Taxonomiestufe zugeordnet werden, da hier das Verständnis für den Phishing-Angriff und die Fähigkeit zur Erkennung gefragt ist. Der Phishing-Angriff aus TL (2.3) ist ein Spezialfall, da die Browser internationalisierte Domainnamen automatisch umwandeln und somit von außen kein Unterschied innerhalb der Website-URL für die NuN erkennbar ist. Somit ist TL (2.3) der zweiten Taxonomiestufe zuzuordnen, da hier nur das Verständnis möglich ist, aber keine Erkennung. In die erste Taxonomiestufe können die TL (2.6) und (2.7) eingeordnet werden, da hier nur das Wissen, um die jeweiligen Handlungsanweisungen wie in (2.6) gefragt ist oder der Inhalt nur zur Kenntnis genommen werden soll, da ein weiteres Lernspiel diesen Bereich abdecken wird.

Auch das zweite Lernziel ist spezifisch in Bezug auf die SMART-Kriterien, da eine auch hier der Handlungsrahmen der NuN klar abgesteckt ist. Auch ist das Lernziel wieder messbar, da die Untersuchung auf Phishing nur die Antworten Ja und Nein zulässt und ebenso die Identifizierung des spezifischen Phishing-Angriffs objektiv zu beurteilen ist. Da im zweiten Lernziel die gleichen Aktionen durch die NuN durchgeführt werden, kann auch das zweite Lernziel als aktiv bezeichnet werden. Ob das Lernziel für die NuN attraktiv oder akzeptabel ist, kann wiederum nicht beantwortet werden. Durch das aktive Handeln der NuN kann die Erreichung des Lernziels beeinflusst werden, da nur eine begrenzte Anzahl an Phishing-Angriffen vorgestellt werden, sodass die Erreichung des Lernziels durch die NuN machbar und realistisch erscheint. In Kombination mit den Erkenntnissen aus den untersuchten vorhandenen Lernspielen (Kapitel 5) kann nun ein erstes didaktisches Konzept zur Vermittlung der Lernziele konzipiert werden.

6.2. Didaktisches Konzept zur Vermittlung

Die in Kapitel 5 untersuchten Lernspiele nutzen ein sich durchgängig abwechselndes Schema zur Wissensvermittlung, bestehend aus der Vermittlung von Inhalt und der Überprüfung des Inhalts. Dabei wird den NuN das Wissen zwar direkt und in textueller Form präsentiert, aber die NuN agieren während der Vermittlungsphase nicht mit dem Lernspiel, sondern können durch einfaches Durchklicken die Vermittlungsphase überspringen. Das Fehlen ebenjener Interaktivität ist ein entscheidender Punkt, der in dem hier entwickelten Lernspiel vermieden werden soll. Aufgrund der Tatsache, dass es sich um ein Lernspiel handelt, ist eine gewisse textuelle Repräsentation durchaus weiterhin nötig, um den Inhalt verständlich vermitteln zu können. Interaktionsmöglichkeiten geben den NuN aber ein Gefühl der Beteiligung, sodass diese sich in das Spiel eingebunden fühlen und die Anregung eines Lernprozesses möglich ist. Hier bietet sich bereits die Weiterführung des *Entdecker*-Modus des emulierten Browsers³ an. Damit ein

*Entwicklung
eines
didaktischen
Konzepts*

³ Der emulierte Browser ist im Rahmen der Bachelorarbeit von Oleksandr Ratner ebenfalls am LuFg i9 entstanden. Dieser Browser soll in Zukunft als Startpunkt aller weiteren entwickelten Lernspiele mit Bezug zur Browser-Security genutzt werden. Das hier entwickelte Lernspiel wird dabei das erste explizit in den Browser eingebundene Lernspiel sein. Die Bachelorarbeit von Oleksandr Ratner ist verfügbar unter <https://publications.rwth-aachen.de/record/745917/files/745917.pdf>.

Durchklicken nicht möglich ist, werden die NuN erst mit neuem Inhalt konfrontiert, wenn in einer Überprüfung nachgewiesen wurde, dass eine Auseinandersetzung mit dem vorherigen Inhalt stattgefunden hat. Andernfalls soll das Lernspiel die NuN zum vorherigen Inhalt zurückführen. Dadurch kann die Auseinandersetzung mit dem Inhalt forciert werden. Das Schema aus Vermittlung und Überprüfung ist hier ebenfalls zu präferieren, jedoch mit weiteren Interaktionsmöglichkeiten gegenüber NoPhish und Anti-Phishing Phil. Die beiden vorgestellten Lernspiele nutzen maximal zwei Arten der Interaktion. Anti-Phishing Phil und NoPhish nutzen beide Single-Choice Fragen, um die NuN entscheiden zu lassen, ob eine Website-URL Phishing ist oder nicht. NoPhish lässt den Nutzer zusätzlich nach einer Single-Choice Frage mit der Website-URL einer Phishing-Website den Host-Anteil einer Website-URL anklicken. Damit ein Schema aus Vermittlung und Überprüfung nicht ermüdend wird, sind fünf Interaktionsmöglichkeiten zur Vermittlung und Überprüfung des Inhalts geplant:

*Konzipierung
verschiedener
Interaktions-
möglichkeiten*

1. Das Suchen mit einer digitalen Lupe

Verwendet wird hier das bereits vorhandene Konzept aus dem emulierten Browser. Mit einer digitalen Lupe fahren die NuN über den (Touch-)Bildschirm, dabei können mit der Lupe Punkte getroffen werden, hinter denen sich neuer Inhalt befindet, welcher daraufhin angezeigt wird.

2. Surfen auf Phishing-Website und realer Website

Als Grundlage wird wiederum der emulierte Browser genutzt. Dieser zeigt durch zwei geöffnete Tabs zwei Websites an. In einem Tab befindet sich eine Phishing-Website und im zweiten Tab die reale Website. Durch einen Vergleich beider Seiten ist es möglich kleine Unterschiede zu erkennen, welche die jeweilige Phishing-Technik des Levels ausmachen.

3. Drag & Drop von Textelementen

Da eine Website-URL sich explizit in einzelne Elemente zerlegen lässt, bietet es sich an die Elemente einer Website-URL durch Ziehen und Ablegen zu ordnen.

4. Multiple-Choice Fragen

Um im Spiel fortzuschreiten, sind Fragen zum vorherigen Inhalt zu beantworten. In der konkreten Ausführung sind verschiedene Versionen wie beispielsweise Single-Choice Fragen denkbar. Multiple-Choice Fragen erweitern hier explizit die in Anti-Phishing Phil und NoPhish verwendeten Entscheidungsfragen, um Variationen der Fragestellungen zu ermöglichen.

5. Markieren und Anklicken von Textelementen

Das in NoPhish verwendete Prinzip des Markierens von Elementen ist eine sinnvolle Art der Überprüfung. Es entsteht die Möglichkeit individuelles Feedback durch das Markieren der Lösung der NuN und der realen Lösung zu geben, sollten die Elemente nicht übereinstimmen. Dadurch können die NuN explizit etwaige eigene Fehler erfassen und mit Hilfe der korrekten Lösung über den Lösungsweg nachdenken.

Die ersten beiden Interaktionsmöglichkeiten fördern die Interaktivität innerhalb der Vermittlung, da diese aktiv zur Entdeckung von Inhalten durch die NuN genutzt werden können. Die weiteren Interaktionsmöglichkeiten dienen zur Abwechslung innerhalb einer Überprüfung. Durch die konzeptionellen Unterschiede wie beispielsweise zwischen Multiple-Choice Fragen und dem Drag & Drop von Textelementen kann einer Überprüfung mehr Flexibilität⁴ zu Teil werden, um nicht ermüdend auf die NuN zu wirken.

Während die beiden vorgestellten Lernspiele im Kapitel 5 direkt zu Beginn des Lernspiels in der Überprüfung von Lerninhalten eine quantitative Bewertung der Leistung der NuN vornehmen, wird hier eine rein qualitative Bewertung im Rahmen von *ausreichender* und *nicht ausreichender* Leistung im Lernprozess angestrebt. Dies geschieht unter dem Aspekt, in Vermittlungsphasen keine unnötigen kompetitiven Elemente zu fördern. Durch eine allzu kompetitive Ausrichtung kann es zum Verschrecken von weniger leistungsstarken NuN kommen, die sich dadurch einem Lernprozess verweigern könnten. Eine quantitative Bewertung ist daher erst nach Abschluss des intendierten Lernprozesses bezüglich der Lernziele zur konkreten Messung der Leistung der NuN geplant.

Das Lernspiel NoPhish organisiert den Lernprozess mit Hilfe mehrerer Level zu den einzelnen inhaltlichen Komponenten. Diese Lösung wird übernommen, da eine Trennung von Inhalten möglich ist und gezielt Inhalte wiederholt werden können. Ebenso übernommen wird die automatische Speicherung des Spielfortschritts, so kann das Lernspiel beliebig fortgesetzt werden und vermeidet Frust im Fall von technischen Problem (z. B. Absturz des Browsers).

Mit Hilfe des erörterten didaktischen Konzepts kann nun der generelle Spielaufbau und ein Storyboard festgelegt werden.

6.3. Spielaufbau und Story

Um der Prämisse Prenskys⁵ gerecht zu werden, ist das Lernspiel in einen Gesamtkontext zu stellen. Aufgrund des Entdecker-Modus wird zuvor im emulierten Browser eine Detektivfigur (Abb. 6.1) eingeführt, welche die NuN in die Benutzung des emulierten Browser schult, damit [u. a.] das hier entwickelte Lernspiel gespielt werden kann. Die Einführung der Detektivfigur schuf die Möglichkeit, ebendiese weiterzuentwickeln und in eine Story einzubinden. Aus diesem Ansatz heraus wurde eine Story entwickelt, welches die Detektivfigur als Phishing-Detektiv in der fiktiven Stadt *Tech City* einführt und gegenüber den NuN als Mentor fungiert. Die NuN sind bereits selbst als „normale“ Detektive in *Tech City* „beschäftigt“ und sollen eine Weiterbildung zur Phishing-Detektivin oder zum Phishing-Detektiv⁶ absolvieren. Als Hinweis auf die „Ausbildung“ und die Inhalte zum Thema Phishing ergibt sich der Spieltitle: **Phishing Academy**.

Entwicklung
der Story



Abbildung 6.1.: Detektivfigur des emulierten Browsers [Rat18]

⁴ rein statische Interaktion versus dem Bewegen von (Text-)Elementen

⁵ vgl. Kapitel 4.1

⁶ ab hier nur noch angelehnt an die Abkürzung NuN die Kurzform Phishing-DuD.

Das Lernspiel unterteilt sich inhaltlich in vier Hauptkomponenten, denen jeweils unterschiedliche Aufgaben zu Teil werden und namentlich an den Spieltitel angeglichen wurden:

*Beschreibung
der Hauptkom-
ponenten des
Lernspiels*

1. Detektivdialoge

Durch die Detektivdialoge wird im Spiel der Kontext der Story getragen und weiterentwickelt. Die Detektivfigur führt die NuN durch das Lernspiel, erteilt die Arbeitsaufträge an die NuN und gibt Rückmeldung zum Spielfortschritt, sowie zur Leistung der NuN.

2. Einführung

Innerhalb der Einführung werden die NuN in die Story eingebunden. Das Lernspiel startet mit der Desktop-Ansicht eines fiktiven Betriebssystems. Daraufhin erscheint eine E-Mail in der die NuN implizit in ihre Rolle als Detektive eingeführt werden. Die E-Mail fordert die NuN auf, sich zum Phishing-Detektiv weiterzubilden. Als fiktiven Anhang enthält die E-Mail einen Zeitungsartikel des *Tech City Anzeigers*, der über immer mehr Phishing-Angriffe auf die Bewohner von *Tech City* berichtet. Daraufhin können die NuN fortfahren und sich zu Phishing-DuD ausbilden lassen.

3. Trainingscenter

Im Trainingscenter findet die eigentliche Vermittlung der Inhalte statt. Als Konzept wird hier der levelbasierte Spielfortschritt der App *NoPhish* übernommen. Als Grundlage sind sechs Level vorgesehen. Eine mögliche Erweiterung durch fortführende Level wird in der Implementierung berücksichtigt, damit auch nach Abschluss dieser Bachelorarbeit weitere Level hinzugefügt werden können. Nach der Absolvierung des Trainingscenters werden die NuN durch die Detektivfigur als Phishing-DuD bezeichnet. Im Anschluss werden die NuN dazu aufgefordert, sich mit den anderen NuN der Phishing Academy an verschiedenen *Kriminalfällen* (vgl 4.) zu messen.

4. Kriminalfälle

Da während der Vermittlung in Hinsicht auf das didaktische Konzept nur eine qualitative Bewertung der NuN vorgesehen ist, wird durch die *Kriminalfälle* eine spielerische sowie interaktive Komponente zur quantitativen Bewertung der NuN geschaffen. Dadurch kann eine Evaluation der Leistung durch die ausführende Person stattfinden. Geplant ist hierbei eine Adaption der Überprüfung des Spiels *Anti-Phishing Phil* hinein in den Entdecker-Modus. Durch die quantitative Bewertung wird erstmals im Spiel eine kompetitive Spielsituation durch die NuN gespielt. Die *Kriminalfälle* können durch die NuN erst aufgerufen werden, wenn das Trainingscenter erfolgreich durchlaufen worden ist.

Für die NuN ergibt sich ein in drei Phasen aufgeteilter Spielablauf:

*Beschreibung
der drei
Spielphasen*

Einführung → Trainingscenter → Kriminalfälle

Die Detektivdialoge sind diesem Ablauf übergeordnet und verbinden die einzelnen Phasen miteinander zu einem Gesamtkontext. Während sich die Detektivdialoge und die Einführung inhaltlich aus dem obigen Kontext ergeben, sind das *Trainingscenter* und die *Kriminalfälle* in ihrem spielerischen Konzept noch weiter auszuführen. Darüber hinaus sind erste grafische Konzepte zur spielerischen Verknüpfung der drei Phasen, sowie zur grafischen Gestaltung des Gesamtkontextes anzugeben.

6.3.1. Trainingscenter – Levelboard

*Vorstellung
zweier Level
des Trainings-
centers*

In der Spielkomponente *Trainingscenter* werden sechs Level umgesetzt, die aufeinander aufbauen und jeweils ein oder mehrere Teillernziele (siehe 6.1) adressieren. Die ersten zwei Level behandeln die Inhalte zur Erfüllung des ersten Lernziels zum Aufbau einer Website-URL, während die weiteren vier Level zum zweiten Lernziel hinführen. Ein Level kann aus den Bausteinen *Inhaltsanregung*, *Wissensvermittlung* und *Wissensüberprüfung* bestehen, wobei Mehrfach- oder Nichtnutzung von Bausteinen zugelassen sind. Das Lernspiel speichert den Fortschritt für jedes einzelne Level separat. Das erste und vierte Level können als exemplarisch für die weiteren vier Level angesehen werden.

Level 1

Titel: „Website-URL – Wie funktioniert die Adressierung einer Website?“

Teillernziele: 1.1 und 1.2

Levelaufbau:

1. Vermittlung:
Text durch Detektivfigur: „Um Phishing zu verstehen, müssen wir den Aufbau einer Website-URL kennen.“ Danach wird die Adresse *learntech.rwth-aachen.de/* in der Mitte angezeigt. Es können die vier Elemente Subdomain, Domain, Top-Level-Domain und das erste Slash der Website-URL mit Hilfe der Lupe untersucht werden. Sobald die Lupe auf ein Element trifft, erscheint eine Box, die das jeweilige Element erläutert. Besondere Bedeutung wird hier der Erkennung der Top-Level Domain zu Teil. Die NuN müssen dabei das Lesen der Boxen durch einen Button bestätigen. Wenn dies geschehen ist, schreitet das Level fort.
 2. Überprüfung:
Direkt im Anschluss findet eine Überprüfung statt. Dabei werden drei Leerfelder gegeben, die jeweils durch einen Punkt getrennt sind. Weiterhin sind die drei Drag & Drop Elemente Subdomain, Domain und Top-Level Domain gegeben. Die NuN müssen die Elemente korrekt einordnen, um fortzufahren. Ist die Zuordnung der NuN nicht korrekt, schreitet das Level nicht fort, sondern geht zurück zu Schritt 1. Bei korrekter Antwort folgt Schritt 3.
 3. Überprüfung:
Den NuN wird eine URL angezeigt und sie werden aufgefordert die Top-Level-Domain anzuklicken. Vorgesehen sind drei Durchläufe. Klicken die NuN zweimal die korrekte Top-Level Domain an, wird mit Schritt 4 fortgefahren. Falls nicht, geht das Spiel zurück zu Schritt 1. (Falls Schritt 2 davor bestanden wurde, wird nach erneutem Anzeigen von Schritt 1 direkt wieder Schritt 3 aufgerufen.)
 4. Vermittlung:
Es wird wieder die Adresse *learntech.rwth-aachen.de/* angezeigt. Über der Adresse wird weiterhin ein Pfeil von rechts nach links angezeigt. Über einen Dialog wird den NuN vermittelt, dass die Auflösung der URL von rechts nach links stattfindet.
 5. Überprüfung:
Mit Hilfe einer Multiple-Choice Frage wird getestet, ob die NuN sich mit der Vermittlung der Leserichtung auseinandergesetzt haben.
-

Das erste Level nutzt vier der fünf Möglichkeiten des didaktischen Konzepts zur Interaktion. Im vierten Level wird die fünfte Interaktionsmöglichkeit (im didaktischen Konzept 2.) genutzt.

Level 4

Titel: „Phishing – Angriff über ähnliche Namen?“

Teillernziele: 2.2 und 2.3

Levelaufbau:

1. Vermittlung:

Zuerst wird ein Fall betrachtet, der vor allem in der deutschen Sprache relevant ist. Umlaute werden anders aufgelöst, sodass beispielsweise `schueler-netzwerk.de` und `schüler-netzwerk.de` zu zwei verschiedenen Seiten führen. Diese beiden Seiten werden mit Hilfe des bereits implementierten Browsers in zwei Tabs angezeigt. Dazu erhalten die NuN den Hinweis, dass eine der beiden Website ein Phishing-Versuch ist. Die NuN werden daraufhin aufgefordert, die Phishing-Website zu markieren. Die korrekte Seite kann über das Logo identifiziert werden. Das Ergebnis der NuN ist im folgenden Kontext nicht von Bedeutung. Es soll nur deutlich gemacht werden, dass es schwer sein kann, die korrekte Adresse zu identifizieren.

2. Vermittlung:

Zwei Website-URLs werden angezeigt, wobei eine Adresse das lateinische a und die andere das kyrillische a enthält. Die NuN werden daraufhin dazu aufgefordert die Website-URLs mit der Lupe zu untersuchen, um einen Unterschied entdecken zu können. Das kyrillische a wird durch UTF-8 anders aufgelöst. Dabei wird unter der einen URL, sobald die NuN das Element mit der Lupe überfahren, die eigentliche Bedeutung angezeigt. Unter UTF-8 wird das kyrillische a in der URL zur Auswertung in `%d0%b0` umgewandelt, das lateinische a hingegen zu `%61`. In Folge der anschließenden Umwandlung durch *Punycode* sehen die NuN zwei unterschiedliche Zeichenketten für die Website-URLs. Daraufhin wird ein Tipp angezeigt, welcher den NuN nahelegt, die korrekte Adresse über eine Suchmaschine zu suchen, um diesen Angriffsvektor ausschließen zu können.

Die vier weiteren Level werden zur Vervollständigung kurz inhaltlich zusammengefasst. Eine umfassendere schriftliche Ausführung aller Level ist im Anhang C angegeben.

Level 2: „Website-URL – Pfade und Datenübermittlung“

Den NuN werden die Protokolle *https* und *http* anhand von Beispielen dargelegt. Insbesondere werden den NuN die Unterschiede zwischen den beiden Protokollen näher gebracht. Neben den Protokollen wird die Funktionsweise des Pfades eingeführt, sowie die Änderung der Leserichtung für den Pfad im Gegensatz zu dem Host-Anteil. Das Level adressiert die Teillernziele (1.3) und (1.4).

Level 3: „Phishing – Angriff über Subdomain“

Wie im vierten Level wird den NuN zu Beginn ein fiktiver Phishing-Versuch durch den emulierten Browser gezeigt. Im Anschluss wird die mögliche Phishing-Technik an Hand des fiktiven Phishing-Versuchs eingeführt und die NuN für den Angriff sensibilisiert. Eine Multiple-Choice Frage überprüft den Fortschritt der NuN. Das Level adressiert das Teillernziel (2.1).

Zusammenfassung der restlichen Level

Level 5: „Phishing – Angriff über IPs oder Pfadnutzung“

Den NuN wird erläutert, dass mit IP-Adressen eine weitere Möglichkeit zur Adressierung besteht. Dazu werden zu ausgewählten Domains die entsprechenden IP-Adressen angezeigt. Dazu erhalten die NuN den Tipp, dass Websites, die als Adresse im Browser eine IP-Adresse anzeigen, nicht seriös und sofort als Phishing klassifizierbar sind. Neben den IP-Adressen wird die mögliche Angabe eines Hosts im Pfad als Phishing klassifiziert. Das Level adressiert die Teillernziele (2.4) und (2.5).

Level 6: „Phishing – Vorbeugende Maßnahmen“

Das Level zeigt für gängige Programme und Applikationen (Apps) Möglichkeiten zur Anzeige der Website-URL hinter einem Link. Den Abschluss macht eine Zusammenfassung zu den Inhalten der vorherigen Level. Darüber hinaus wird ein Hinweis auf weitere Probleme wie Cross-Site-Scripting gegeben und Merkmale wie Zertifikate zur weiteren Überprüfung der Legitimität einer Website den NuN gegenüber benannt. Das Level adressiert das Teillernziel (2.6) und (2.7).

6.3.2. Kriminalfälle – Rahmenbedingungen

Wie im Lernspiel *Anti-Phishing Phil* sind zehn Website-URLs pro Spielrunde auf Phishing zu untersuchen. Die Website-URLs sind jedoch hinter zu suchenden Hotspots⁷ auf einem Hintergrundbild versteckt, die mit Hilfe einer digitalen Lupe gefunden werden müssen. Die Komponente stellt zwei verschiedene Modi bereit. Im ersten Modus werden die Hotspots einzeln und somit die Website-URLs nacheinander gefunden, sodass die Entscheidung (ob Phishing verdächtig oder nicht) durch die NuN direkt erfolgen muss. Im zweiten Modus können direkt alle zehn Hotspots gefunden werden und eine Entscheidung für eine Website-URL kann zurückgestellt werden. Die NuN haben in beiden Modi zwei Minuten Zeit. Nach Ablauf der Zeit wird die Runde automatisch beendet, sofern die NuN nicht vorher fertig sind. Im Anschluss wird eine Bewertung angezeigt und für jede einzelne Website-URL wird eine Erklärung inklusive Lösung angezeigt. Zudem wird durch die Detektivfigur in Abhängigkeit von der Bewertung ein Dialog angezeigt, um die NuN entweder zu ermutigen oder diese zu ihrer guten Leistung zu beglückwünschen. Es gibt einen Punkt pro korrekt eingeordneter Website-URL. Jede Spielrunde wird dabei inklusive der genutzten Fragen, der jeweiligen Antwort und der Gesamtbewertung gespeichert, um eine mögliche Evaluation der Ergebnisse auch digital durchführen zu können.

*Konzipierung
der Kriminal-
fälle*

⁷ Es handelt bei den Hotspots um eine kleine Grafik zum Markieren eines Punkts auf dem Bildschirm. Diese Hotspots werden bereits im emulierten Browser benutzt und werden erst nach dem Herüberfahren mit Hilfe der digitalen Lupe sichtbar. Im emulierten Browser kann nach dem Auffinden eines Hotspots, dieser angeklickt werden und das dahinter versteckte Lernspiel gestartet werden.

6.3.3. Grafische Konzepte zur Umsetzung

Um die Hauptkomponenten miteinander verbinden zu können, sind Überlegungen zum Design und zur Integration in das Lernspiel nötig. Nach dem Starten der Phishing Academy gelangen die NuN auf ein Startmenü, wo alte Spielstände geladen werden können oder auch zum emulierten Browser zurückgekehrt werden kann. Danach folgt die Einführung beziehungsweise der Aufhänger des Lernspiels. Nach Absolvierung „befinden“ sich die NuN in der Phishing-Academy und können im Spielermenü, die Hauptkomponenten *Trainingscenter* und die *Kriminalfälle* starten, falls bereits freigeschaltet worden sind. Die Detektivdialoge sind in allen Sequenzen in der unteren linken Ecke angeordnet, die wenn möglich immer frei bleibt, sodass Platz zur Anzeige vorhanden ist (Abb. 6.2).

*Grafischer
Spielfluss und
eigene Logos*

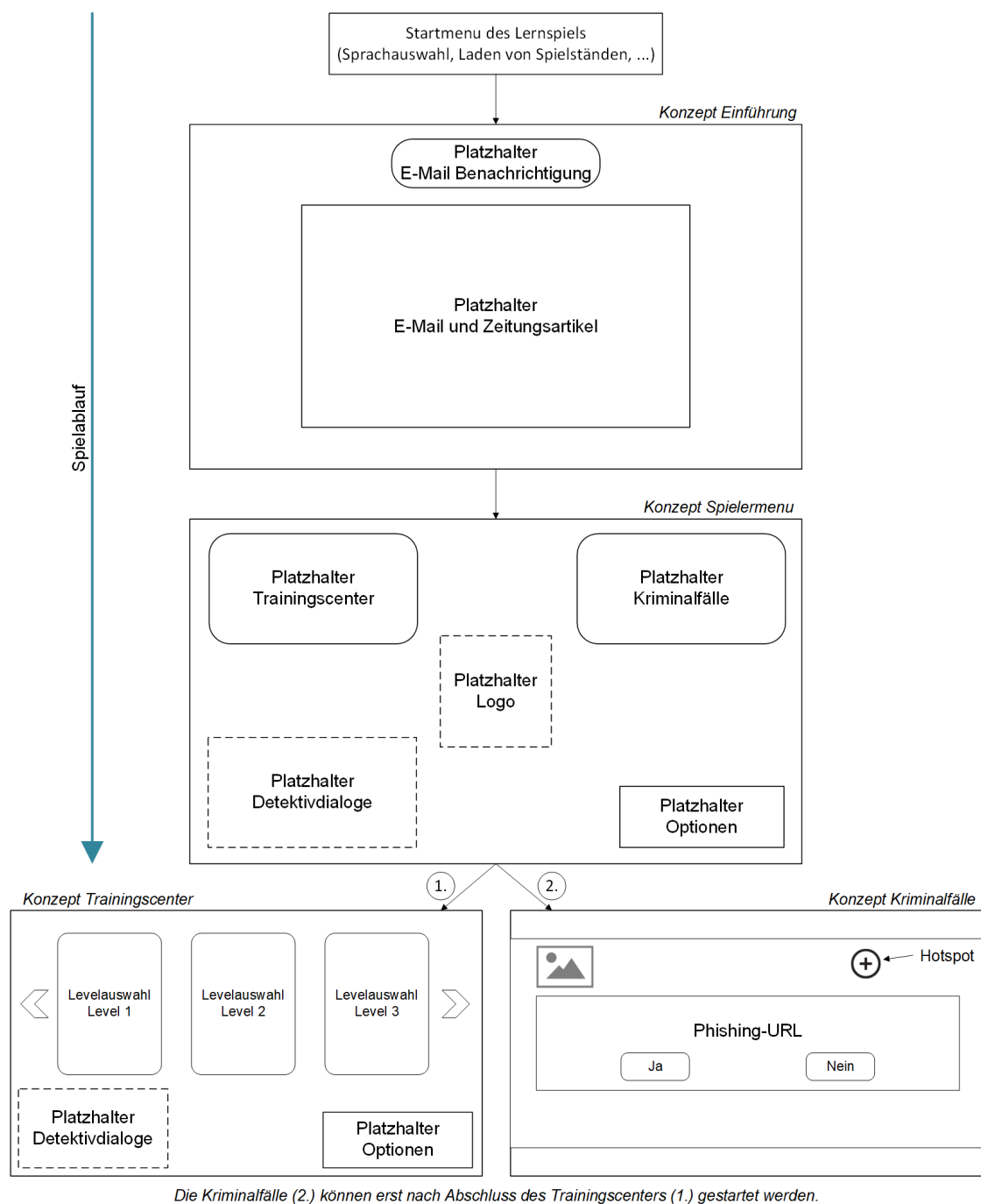


Abbildung 6.2.: Skizzierter konzeptioneller Spielablauf

Zur Förderung der persönlichen Einbindung und des Engagements der NuN wurden passende grafische Elemente erstellt, damit das Lernspiel auf die NuN realistisch und ansprechend wirkt. Durch entsprechende spielerisch, grafische Elemente ist es ebenfalls möglich der Definition Prenskys gerecht zu werden, das Lernspiel wie ein normales Computerspiel zu betrachten. In Anlehnung an die Detektivfigur werden daher erstellte Logos zur Phishing Academy und zur Polizei der fiktiven Stadt *Tech City* (Abb. 6.3) genutzt, die [u. a.] an den entsprechenden Platzhaltern im Spielablauf eingebunden werden (vgl. Abb. 6.2).



Abbildung 6.3.: Erstellte Logos zur Phishing Academy und zur Polizei *Tech Citys*

6.4. Analyse bezüglich (Design-)Merkmale von Computerspielen

Zur Analyse werden die (Design-)Merkmale von Computerspielen aus Kapitel 4 genutzt. Die ersten beiden Merkmale zur Abgrenzung von Computerspielen „a form of fun“ und „a form of play“ sind zum jetzigen Zeitpunkt nur schwer zu analysieren aufgrund der fehlenden Rückmeldungen von NuN. Die Nutzung der Detektivfigur, die Einbindung der NuN in die Story und die jeweiligen gestalteten Elemente wie die Logos tragen dazu bei, dass die NuN sich neben der Vermittlung des Inhalts involviert und unterhalten fühlen. Das Merkmal der Interaktivität kann als gegeben angenommen werden, da zu jeder Zeit im Lernspiel die NuN mit dem Spiel interagieren müssen, um Fortschritte zu erzielen. Hier wurde an den Vermittlungssituationen angesetzt, da diese in den bisherigen Lernspielen nicht interaktiv umgesetzt war. Ob das Lernspiel einen natürlichen „flow“ besitzt, kann noch nicht beantwortet werden, da keine Erfahrungen der NuN zu den Spielinhalten der Vermittlung vorliegen. In der Komponente *Kriminalfälle* ist es jedoch durchaus möglich bereits durch das Spielkonzept in einen Fluss zu geraten, da die Aufgabenstellung nicht variiert und durch die Zeitbeschränkung ein durchgängiges „spielen“ gefordert ist. Das Lernspiel hat in der Überprüfungsphase – wie durch die interaktiven Komponenten festgelegt (vgl. Kapitel 6.2) – durchaus Inhalte zum Problemlösen. Die eigene Kreativität der NuN

*Analyse des
konzipierten
Lernspiels*

ist hier jedoch nicht gefragt, da die Lösung strikt vorgegeben ist. Das Merkmal der „win states“ ist im Lernspiel durch das individuelle Lob der Detektivfigur, als auch durch das Abschließen des *Trainingscenters* oder der maximalen Punktzahl innerhalb der *Kriminalfälle* gegeben.

In Hinsicht auf die Design-Prinzipien sind bereits zwei Merkmale direkt durch das Konzept an sich erfüllt. Das Lernspiel speichert automatisch den Spielfortschritt und während des gesamten Lernspiels existieren keine direkten Strafen. Es ist lediglich eine Zurücksetzung innerhalb der Schritte eines Levels selbst geplant (vgl. Kapitel 6.1). Dadurch muss nicht ein ganzes Level von Beginn an gespielt werden, sondern nur der Teil, welcher den NuN Schwierigkeiten bereitet hat. Eine Belohnung erhalten die NuN auf sekundäre Weise durch das Lob des Detektivfigur, sobald ein Spielschritt absolviert worden ist. Durch das konzeptionell modulare Design der Vermittlungsinhalte können zudem jederzeit Erweiterungen (hier: weitere Level im *Trainingscenter*) hinzugefügt werden. Weiterhin ist die vollständige Phase der Vermittlung auf das Entdecken der Inhalte ausgelegt. Durch die konzeptionelle Modularität ist es möglich den Punkt „leicht zu lernen, schwer zu meistern“ anzugehen. Die Schwierigkeit innerhalb der Komponente *Kriminalfälle* könnte durch unterschiedliche Gruppen von Website-URLs angepasst werden. Dazu könnten weitere Level im *Trainingscenter* zu fortgeschrittenen Angriffsmöglichkeiten den Schwierigkeitsgrad erhöhen. Gegenüber den genannten Punkten kann zu diesem Zeitpunkt nicht eingeschätzt werden, ob das Lernspiel in Bezug auf die Zielgruppe hinreichend ausbalanciert ist und ob der Spannungsbogen bzw. die Story ein Engagement der NuN hervorruft. Damit keine zu schwierigen Situationen das Lernspiel zu Beginn aus der Balance bringen, wurde mit dem ersten Level ein möglichst leichter Einstieg geschaffen, da dieses nur die Erklärung der Basiselemente (Host) einer Website-URL enthält.

Auf Basis der hier genannten Punkte ist daher festzustellen, dass die (Design-)Merkmale soweit wie konzeptionell möglich umgesetzt sind. Eine finale Austarierung einzelner Punkte ist jedoch noch nicht möglich.

6.5. Anwendungsfälle des Lernspiels

Durch die Konzeption ergeben sich mehrere Möglichkeiten zur Nutzung des Lernspiels. Das zugrunde liegende Hauptspiel des emulierten Browsers könnte beispielhaft eine Unterrichtsreihe in der Schule darstellen, sobald weitere Lernspiele zu anderen Themenbereiche entwickelt worden sind. Das hier konzipierte Spiel könnte dann Inhalt einer 90-minütigen Unterrichtseinheit in einer Schulsituation sein. In den Regierungsbezirken Köln und Düsseldorf wurden zum Schuljahr 2018/2019 an achtzig Gymnasien Modellversuche gestartet, wodurch Informatik als Pflichtfach in der fünften und sechsten Klassenstufe in den jeweiligen Stundenplan eingefügt wird [Ges18]. Diese Klassenstufen sind die zu Beginn benannte Zielgruppe des Lernspiels. Aber auch für Differenzierungskurse bis hin zur achten Klasse kann das Lernspiel ein Konzept zur Vermittlung darstellen. Die Relevanz des Inhalts, ergibt sich bereits durch die Bildungsstandards der GI für die Sek. I (vgl. Kapitel 3.1). Weitere Anwendungsfälle sind abseits des Unterrichts Arbeitsgemeinschaften oder auch Kurse zur informationstechnischen Grundbildung. Durch die freie Lizenzierung des Lernspiels sind aber auch Nutzungsszenarien außerhalb von schulischen Situationen denkbar, wie beispielsweise Schülerlabore.

In der folgenden Umsetzung des Lernspiels es möglich, sich ein Bild über die hier angesprochenen Punkte und ebenjener der vorherigen Unterkapitel zu machen.

*Beschreibung
möglicher An-
wendungsfälle*

Kapitel 7 Umsetzung des Lernspiels

Das Kapitel beginnt mit der Beschreibung der genutzten Werkzeuge in 7.1 und den spezifischen Problemen der Werkzeuge für Cross-Platform-Development (7.1.2). Danach wird die umgesetzte Spielstruktur erläutert (7.2). Es folgt mit der Umsetzung der Detektivdialoge in Kapitel 7.3 die erste Komponente. Danach werden die Umsetzung der Einführung und des Spielmenüs in Kapitel 7.4 dargestellt. Auf die Interaktionsmöglichkeiten in 7.5 folgen die allgemeinen Umsetzungen des *Trainingscenters* in 7.6 und der *Kriminalfälle* in 7.7. Im Anschluss werden die umgesetzten Möglichkeiten zur Darbietung von Feedback 7.8 beleuchtet. Es folgt die Umsetzung der Speichermöglichkeit des Spielfortschritts in 7.9. Zum Abschluss werden zukünftige Erweiterungen und offene Umsetzungspunkte in 7.10 dargelegt. In allen Unterkapiteln zur Umsetzung werden zudem die Änderungen am Konzept zur Implementation selbst erläutert und kritisch hinterfragt.

7.1. Werkzeuge und technische Gegebenheiten

7.1.1. Multitouch-Learning-Game-Framework

Das Multitouch-Learning-Game-Framework (MTLG-Framework) ist ein JavaScript-Framework, das am Lehr- und Forschungsgebiet Informatik 9 (LuFg i9) der RWTH Aachen entwickelt worden ist und ebenda zur Entwicklung von browserbasierten digitalen Lernspielen genutzt wird. Das Framework bietet mit der Analyse des Nutzerverhaltens (im Englischen *Learning Analytics*), einer Ablaufsteuerung für Spiellevel und einer (zukünftigen) Nutzerverwaltung nützliche Funktionen zur Implementation eines digitalen Lernspiels.

Neben den bisher vorgestellten Framework-Funktionalitäten implementiert das MTLG-Framework zusätzlich die öffentlich zugängliche JavaScript Bibliothek CreateJS¹. Die Bibliothek stellt mehrere unterschiedliche Komponenten zur Verfügung, um mit Hilfe von HTML5² die Nutzung von Grafiken, Texten, Videos, Sounds und Bewegungen von Elementen im Webbrowser zu ermöglichen. Durch die direkte Implementation können daher alle vorgefertigten Funktionen der Bibliothek genutzt werden.

Da das entwickelte Lernspiel für den Einzelspieler-Modus vorgesehen ist, sind als Anwendungsgeräte Tablets und Laptops unumgänglich. In diesem Gerätebereich existiert momentan keine einheitlich genutzte Bildschirmauflösung mehr (wie z. B. Full HD), daher ist eine Skalierung des Lernspiels notwendig. Das Framework bietet eine automatische Möglichkeit zur Skalierung, sodass dieser Punkt nicht weiter betrachtet werden muss. Durch die Nutzung des Frameworks wird zudem sichergestellt, dass sowohl das Spielen mit einer Maus als auch das Spielen über einen Touchscreen reibungslos funktioniert.

¹ CreateJS ist verfügbar unter: <https://createjs.com/>

² HTML5 ist die 2014 veröffentlichte Version der Auszeichnungssprache HTML. Durch die Spezifikation von mehreren neuen Schnittstellen können auf einer Zeichenoberfläche per JavaScript visuelle Elemente realisiert werden.

7.1.2. Herausforderung von Cross-Platform-Development

Die Implementierung als JavaScript-basiertes Browsergame gewährleistet eine generelle Plattformunabhängigkeit in Bezug auf alle gängigen Systeme (Windows, Android, iOS, MacOS und Linux). Dadurch kann das Lernspiel bereits auf allen Geräten gespielt werden, die einen Webbrowser mit JavaScript-Engine mitbringen. Durch das MTLG-Framework ist die Nutzung von Geräten mit Touchscreens (Tablets, Laptops etc.) möglich und auch vorgesehen. Die verschiedenen Geräte sind jedoch auch für einige Hürden verantwortlich. Durch die unterschiedlichen Größen der Displays muss auf die Größe aller dargestellten Elemente geachtet werden. Die Schrift darf nicht zu klein sein, da sonst auf einem Tablet diese nicht mehr richtig zu lesen ist. Gleichzeitig darf der Text nicht zu groß sein, da er sonst auf einem Laptop oder stationärem Computer riesig wirkt. Ein weiteres Problem ist die unterschiedliche Ausführung der Browser auf Geräten mit mobilem oder vollwertigem Betriebssystem. Während Browser für Windows, MacOS und auch Linux einen Vollbildmodus integriert haben, besitzen die mobilen Varianten keinen Vollbildmodus. Dadurch geht ein erheblicher Teil des nutzbaren Bildschirms verloren. Auf Tablets wird daher die Installationen von freien Vollbildbrowsern empfohlen³. Diese lassen dem digitalen Lernspiel mehr Platz auf dem Bildschirm, sodass durch die Skalierung des Frameworks eine größere Bildfläche genutzt werden kann. Durch die Fokussierung auf Plattformunabhängigkeit kommt es zu solchen Einschränkungen gegenüber nativen Apps, jedoch kann mit den genannten Möglichkeiten ein gutes Darstellungsergebnis erzielt werden.

*Probleme und
Hürden bei der
Entwicklung
für
verschiedene
Systeme*

7.2. Umsetzung der konzeptionellen Spielstruktur

Das Lernspiel wurde zur Implementierung in zwei Bereiche aufgeteilt. Alle konzeptionellen Elemente die zur Darstellung des *Spielablaufs* beitragen, wurden als Level dem MTLG-Framework hinzugefügt und in einer jeweiligen Datei abgelegt. Dazu gehören die einzelnen inhaltlichen Level des Trainingscenters an sich, die Übersicht des Trainingscenters, das Start- und Spielermenü, die Einführung in das Thema und die Kriminalfälle. Alle weiteren Funktionen verteilen sich auf die drei Gruppen *Allgemeine Darstellungsobjekte*, *Spielinteraktionen* und *Logik/Speicher*. Die jeweiligen Funktionen der Gruppen sind ebenfalls in einzelnen Dateien implementiert worden (Abb. 7.1). So ist beispielsweise die vollständige Umsetzung zur Anzeige einer Website-URL und der dazugehörigen Logik zur Interaktion in der Datei *url.js* implementiert worden. Damit es möglichst wenig verstreute globale Variablen⁴ gibt, wurde in der Gruppe *Logik* beispielsweise der Namespace *phishingAcademy* hinzugefügt und alle globalen Variablen dort gebündelt. Der Namespace steht dabei zu Beginn durch die Umsetzung als *Immediately-invoked Function Expression* sofort zur Verfügung. Zur einfachen Speicherung der benötigten Websites-URLs wurde das JSON-Datenformat gewählt, in welchem nach einer vorgegebenen Syntax die Website-URLs hinterlegt sind. Die Website-URLs, die im ersten Level angezeigt werden, befinden sich beispielsweise in der Datei *urllevel1.json*.

In den folgenden Unterkapiteln wird nur vereinzelt die implementationstechnische Struktur weiter ausgeführt, hervorgehoben werden auf Grund der Fülle des Inhalts nur grundsätzliche Änderungen gegenüber dem Konzept oder Besonderheiten wie eingesetzte Software-Patterns.

*Beschreibung
der Grund-
struktur des
Codes*

³ Vollbildbrowser oder auch eine einfache Webview-Apps finden sich den jeweiligen App-Stores.

⁴ abgesehen von den einzelnen Hauptfunktionen

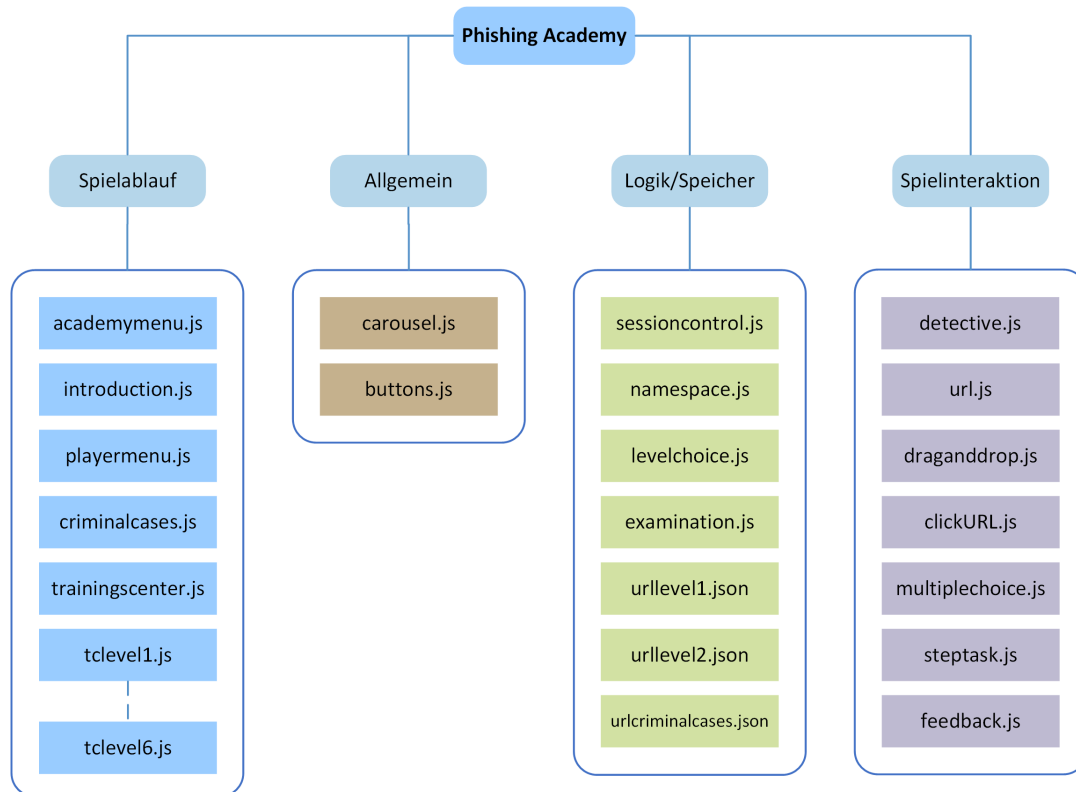


Abbildung 7.1.: Implementation des Lernspiels - Dateistruktur

7.3. Umsetzung der Detektivdialoge

Die Detektivfigur ist die verbindende Komponente der einzelnen Teilkomponenten und wurde in der Datei *detective.js* umgesetzt. Zur Darstellung der Dialoge erhielt die Detektivfigur eine Sprechblase in die beliebig Texte eingefügt werden können (Abb. 7.2). Als Name der Detektivfigur wurde im Lernspiel *Detektiv Dot* festgelegt. Die Detektivfigur erscheint immer im linken unteren Quadranten des Bildschirms und der letzte angezeigte Dialog kann über einen Button wiederholt abgespielt werden. Durch das Klicken auf die Figur wird der Dialog fortgesetzt. Eine Nichtbeachtung des Dialogs ist nicht möglich, da der Rest des Bildschirms währenddessen durch ein Overlay keine Eingaben außerhalb des Dialogs zulässt. Neben der Begleitung der NuN durch die Level des Trainingscenters, sind auch Dialoge zum Spielfortschritt implementiert worden. So gratuliert die Figur beispielsweise zum erfolgreichen Abschluss des Trainingscenters und begrüßt die NuN als baldige Kollegen in der „Bekämpfung“ von Phishing-Angriffen. Um der Detektivfigur eine gewisse Elastizität hinzuzufügen, „schwebt“ die Grafik mit einer kurzen Zick-Zack-Bewegung in das Spielgeschehen. Bei der Übergabe an die erzeugende Funktion muss jedoch der Text selber in Einzelstücke geteilt werden, da durch die unterschiedlichen Wortlängen und durch das Fehlen einer automatischen Silbentrennung der Text nicht durch das Framework automatisiert aufgeteilt werden kann. Während der Entwicklung wurde als grober Richtwert maximale 160 Zeichen (ohne Leerzeichen) genutzt. Die Funktion zur Erzeugung des Detektivs *detectiveSpeech()* erhält daher ein Array von Textbausteinen, ein Attribut, ob man den Dialog wegklicken kann und optional eine Callback-Methode, falls eine Aktion ausgelöst werden soll, wenn alle übergebenen Textbausteine angezeigt worden sind. Der Detektivdialog kommt in allen weiteren Komponenten immer wieder zur Anwendung.

*Funktion der
Detektivfigur*



Abbildung 7.2.: Detective Dot mit einem Textbaustein

7.4. Umsetzung von Einführung und Spielermenü

Die Einführung wurde wie im Konzept angegeben zweigeteilt. Zuerst wird den NuN die E-Mail angezeigt (Abb. 7.3). Durch diese wird das erste Engagement der NuN forciert. Durch einen Knopf können die NuN den in der E-Mail angesprochenen Zeitungsartikel öffnen und lesen (Abb. 7.4). Als Umgebung wird ein selbst erstelltes User Interface eines Computers der Polizei von *Tech City* simuliert. Das Logo verbirgt sich dabei hinter der E-Mail ist jedoch im Lernspiel selbst zu sehen, da die E-Mail sich öffnet, nachdem eine Benachrichtigung zur neuen E-Mail in das Blickfeld der NuN gerückt ist. Durch einen automatisch bewegten Cursor wird diese E-Mail zu Beginn geöffnet. Wenn die NuN den Zeitungsartikel gelesen haben, können diese die Phishing Academy über einen weiteren Knopf starten.

*Inhaltliche
Punkte der
Einführung*

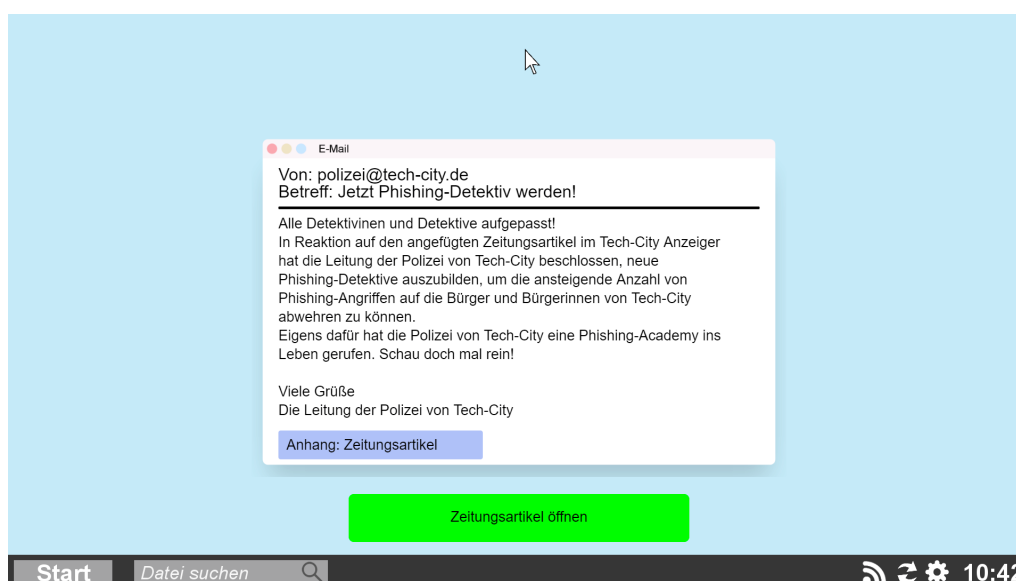


Abbildung 7.3.: Einführung – Aufhänger E-Mail



Abbildung 7.4.: Einführung – Aufhänger Zeitungsartikel

Sobald die NuN die Phishing Academy gestartet haben, finden die NuN als Menüstruktur die konzipierte Oberfläche wieder (Abb. 7.5). Aus diesem Menü führen die beiden Hauptkomponenten *Trainingscenter* und *Kriminalfälle* ab. Neben der weiteren Spieloptionen kann immer mit dem Knopf „Detektiv Dot sprechen“ der letzte Detektivdialog wiederholt werden. Haben die NuN das Trainingscenter noch nicht beendet, wird der Knopf ausgegraut und bei einem Klick erscheint ein Detektivdialog, warum diese Komponente noch nicht verfügbar ist. Zu Beginn stellt sich Detektiv Dot gegenüber den NuN vor und erläutert die Funktionsweise des Lernspiels. Der nächste Anlaufpunkt ist somit das *Trainingscenter* und die erste Vermittlung der fachlichen Inhalte.

*Beschreibung
des Spieler-
menüs*



Abbildung 7.5.: Spielermenü – Oberfläche zum Starten der weiteren Komponenten

7.5. Umsetzungen der Interaktionsmöglichkeiten

Im ersten Level des Trainingscenters werden bereits vier der fünf konzipierten Interaktionsmöglichkeiten verwendet. Zum Start des ersten Levels kann der Aufbau einer Website-URL mit Hilfe einer Lupe (vgl. Unterkapitel 6.2) entdeckt werden. Diese Interaktionsmöglichkeit ist in der Datei *url.js* umgesetzt worden. Sobald die Lupe über ein Bestandteil der Website-URL fährt, wird der entsprechende Informationstext angezeigt. Um zu verdeutlichen in welchem Kontext eine Website-URL genutzt wird, ist die Website-URL in eine fiktive Adresszeile eingearbeitet (Abb. 7.6).

*Das Entdecken
der Struktur
einer Website-
URL per Lupe*

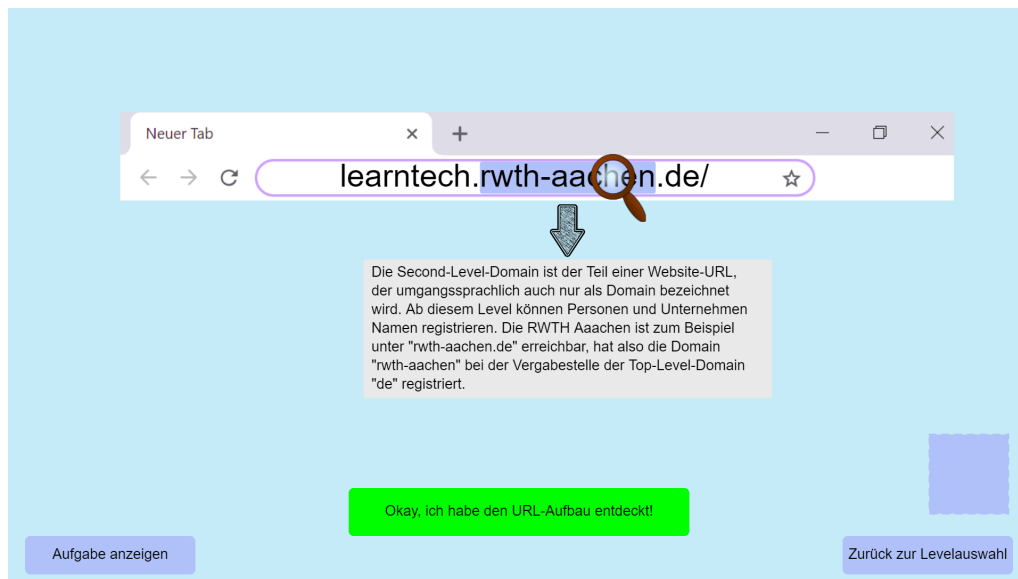


Abbildung 7.6.: Aufbau der Website-URL – Entdecken per Lupe

Eine Überprüfung des Inhalts kann durch die Interaktion per Drag & Drop umgesetzt werden. Die Implementation ist unter *draganddrop.js* erfolgt. Wichtig war hierbei vor allem aus implementationstechnischer Sicht, dass sich die Lösung nicht durch die Größe der Drag & Drop Felder zu erkennen gibt. Daher wurden die Felder so implementiert, dass nach jedem Loslassen eines Textelements durch die NuN eine Aktualisierung der Boxgrößen vorgenommen wird. Wird ein Textelement in den Bereich eines Feldes gezogen, passt sich das Feld automatisch an die Größe des Textelements an. Wird das Textelement wieder herausgezogen, wird die Größe des Feldes wieder auf den Standardwert zurückgesetzt (Abb. 7.7).

*Drag & Drop
von Elementen*

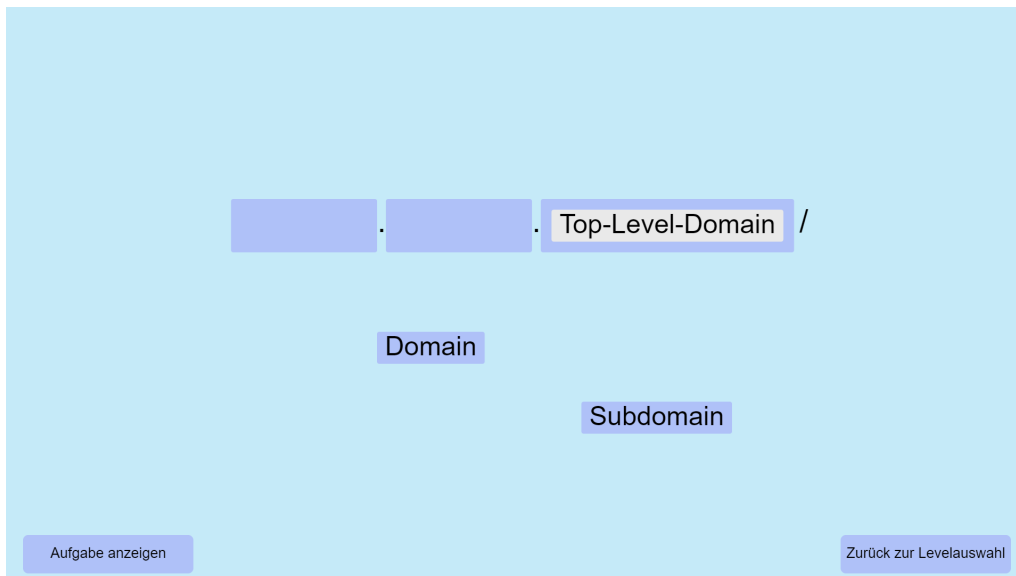


Abbildung 7.7.: Überprüfung – Drag & Drop von Textelementen

Als dritte Interaktionsmöglichkeit begegnet den NuN das Anklicken von Textelementen, welches in der Datei *clickURL.js* umgesetzt wurde. In den Spielsituationen ist das Anklicken hinsichtlich vorher festgelegter Bestandteile einer Website-URL relevant, um kontrollieren zu können, ob die NuN gezielt die Bestandteile einer Website-URL bestimmen können. Sind sich die NuN nach der Erklärung der Aufgabe durch Detektiv Dot nicht mehr sicher, welcher Bestandteil angeklickt werden soll, können die NuN sich die Aufgabenstellung erneut ansehen (Abb. 7.8).

*Anklicken von
Elementen
einer URL*

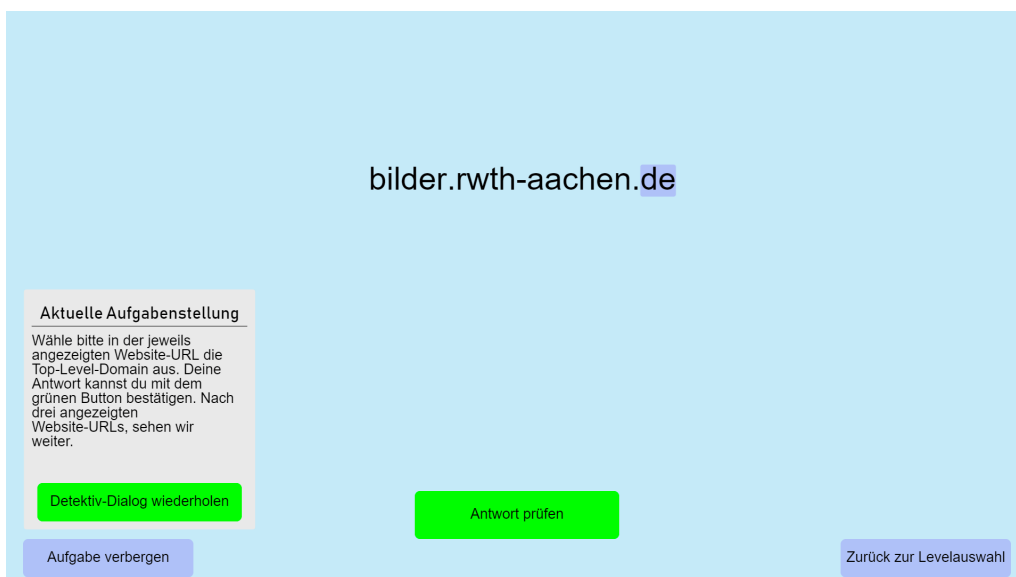


Abbildung 7.8.: Überprüfung – Anklicken von URL-Bestandteilen

Die Multiple-Choice Frage und somit die letzte Interaktionsmöglichkeit im ersten Level dient ebenfalls zur Überprüfung der NuN. Es können bis zu vier mögliche Antworten neben der Frage an die implementierte Funktion in der Datei *multiplechoice.js* übergeben werden. Die angezeigte Box passt sich dabei automatisch an die Länge der Frage an.

*Details zu
Multiple-
Choice
Fragen*

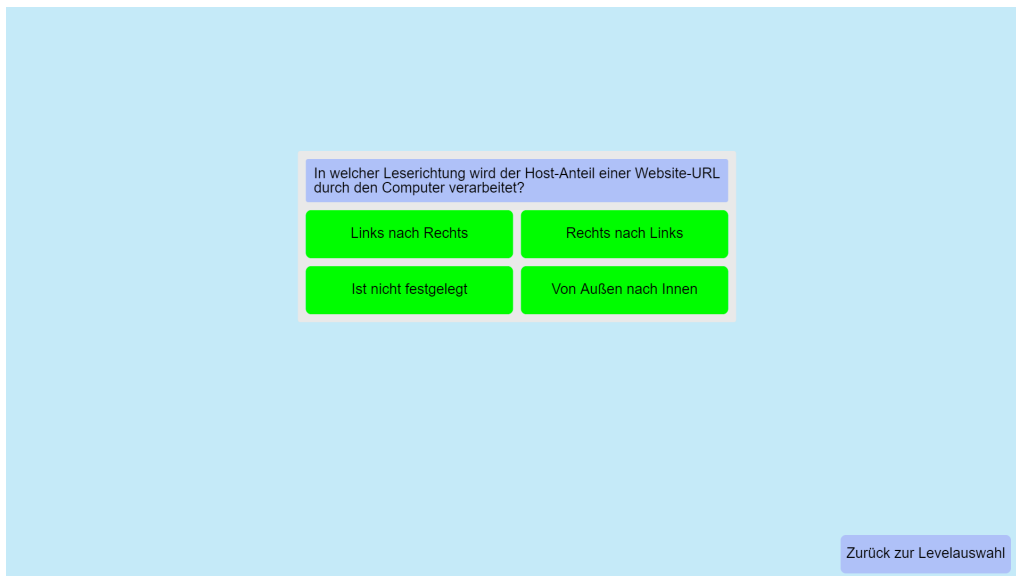


Abbildung 7.9.: Überprüfung – Multiple-Choice Frage

Neben der Möglichkeit neues Wissen per Entdecken durch die Lupe umzusetzen, wird ab dem dritten Level die fünfte konzeptionierte Interaktionsmöglichkeit eingeführt. Dabei wird unter anderem bereits das Interface des emulierten Browsers aus dem Hauptspiel zum „Surfen auf Websites“ erneut eingebunden. Mehrere Websites werden dabei ebenso wie im Alltag durch mehrere Tabs realisiert. Geladen werden jedoch keine realen Websites⁵ oder HTML-Dokumente, sondern Screenshots Grafiken vorher eigens gestalteter Websites eingebunden. Wie im Konzept dargestellt, ist im vierten Level durch die NuN herauszufinden, in welchem angezeigten Tab sich die reale Anmeldeseite des fiktiven Netzwerks *schueler-netzwerk.de* befindet. Die Abgabe der vermuteten Lösung erfolgt über einen Button (Abb. 7.10).

*Neues
Entdecken
durch den
emulierten
Browser*



Abbildung 7.10.: Vermittlung – Anzeige von Websites

⁵ Viele Websites blockieren die im Hauptspiel implementierte Anzeige im *iframe*. Daher musste hier ein anderer Weg gefunden werden.

7.6. Umsetzung der Level des Trainingscenters

*Änderungen
der Level
gegenüber dem
Konzept*

Die einzelnen konzipierten Level aus 6.3.1 und Anhang C konnten inhaltlich vollständig umgesetzt werden. Es sind jedoch zur Implementationsphase noch Änderungen an den einzelnen Levelstrukturen vorgenommen worden. Die Änderungen geschahen vor allem in Hinblick auf die Aufrechterhaltung des Spielflusses und auf Grund vorhandener Limitierungen innerhalb der Implementation. In den Konzepten war in Hinsicht auf das dritte und vierte Level vor der Implementierung keine Überprüfung vorgesehen, dadurch hätte jedoch genau wie im Spiel *Anti-Phishing Phil* der Spielfluss durch einfaches Durchklicken durch die Level an Bedeutung verloren. Daher sind im dritten und vierten Level jeweils eine Multiple-Choice Frage hinzugefügt worden. Das fünfte Level hat formal betrachtet keine Überprüfung. Die Multiple-Choice Frage wurde entfernt und durch ein *Anklicken von Textelementen* ersetzt, um die Breite der Interaktionsmöglichkeiten besser auszunutzen. Das falsche Anklicken des gewünschten URL-Elements führt dann ebenfalls direkt zur Erklärung, da vorher keine Vermittlung zu dem abgefragten Inhalt (Host im Pfad) stattgefunden hat, sondern die NuN bereits durch das *Anklicken* angeregt werden, sich selbst eine Lösung zu erschließen. Die NuN werden an dieser Stelle mit in den Denkprozess eingeschlossen, sodass auf eine Überprüfung verzichtet wurde.

Die Level des Trainingscenters wurden in einzelne *steps* unterteilt, um später den Spielfortschritt speichern zu können (vgl. 7.9). Aus Sicht der Implementierung mussten daher die einzelnen Schritte der Konzepte aufgeteilt werden, da die vielen einzelnen Elemente in einem Schritt zu intransparentem und nicht modularem Code geführt hätten. Schlussendlich wurde in der Implementation für jede Überprüfungs- und Vermittlungssituation ein einzelner *step* erstellt. Die Umsetzung der Level ist in den Dateien *tlevel1.js* bis *tlevel6.js* zu finden.

7.7. Umsetzung der Kriminalfälle

*Durchführung
einer Runde in
den Kriminal-
fällen*

Die zweite spielerische Hauptkomponente ist in den Dateien *criminalcases.js* und *examination.js* umgesetzt. Die Funktionen der ersten Datei übernehmen dabei die visuelle Abwicklung der Kriminalfälle, während in der zweiten angeführten Datei alle logischen Elemente, wie das Zusammenstellen des Test-Objekts implementiert sind. Das Test-Objekt und die Fragen werden über eigene Konstruktoren erzeugt. Dabei werden im Test-Objekt die Fragen der jeweiligen Runde, die Nutzerantworten sowie die Bewertung der NuN gespeichert. Bei jedem Aufruf wird ein neues Test-Objekt erzeugt und „zufällig“ zehn Website-URLs aus dem bestehenden Set mit zwanzig Website-URLs ausgewählt. In diesem Set befinden sich jeweils zehn Phishing-URLs und zehn reale Website-URLs. Nach dem Ende eines Tests wird das Test-Objekt für eine spätere Evaluation gespeichert⁶.

Zur Durchführung eines Tests konnte die konzipierte Struktur umgesetzt werden. Die Hotspots zu einer Website-URL können auf einem Hintergrundbild mit Hilfe der Lupe gefunden werden (Abb. 7.11). Während der Konzeption war geplant auch hier die bereits implementierten Funktionen des Hauptspiels zu nutzen. Da dort die Lupe jedoch auf einer eigenen *Stage* implementiert war, musste die Lupe nochmals in einer angepassten Version implementiert werden. Für die Hotspots konnte die Funktion des Hauptspiels genutzt werden. Die Fortschrittsanzeige sowie der Counter werden in der oberen linken und rechten Ecke angezeigt. Wird eine Hotspot durch die NuN angeklickt, wird eine Box mit der zugehörigen Website-URL und der Frage, ob die Website-URL verdächtig wird, einen Phishing-Angriff darzustellen (Abb. 7.12).

⁶ Eine weitere Erläuterung zur Speicherung erfolgt im Kapitel 7.9

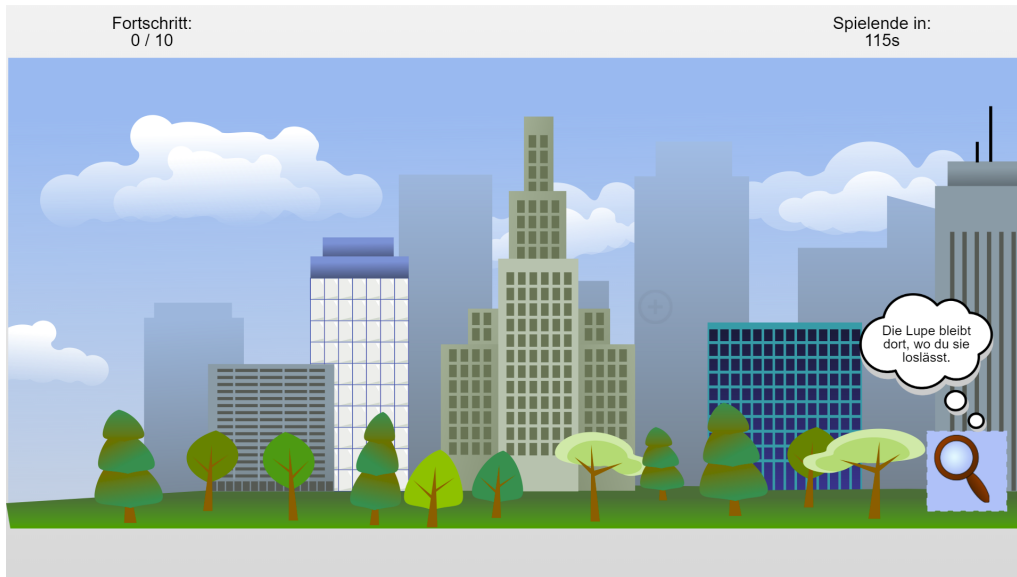


Abbildung 7.11.: Kriminalfälle – Suchen mit Hilfe der Lupe (Hotspot rechts neben der Bildmitte)

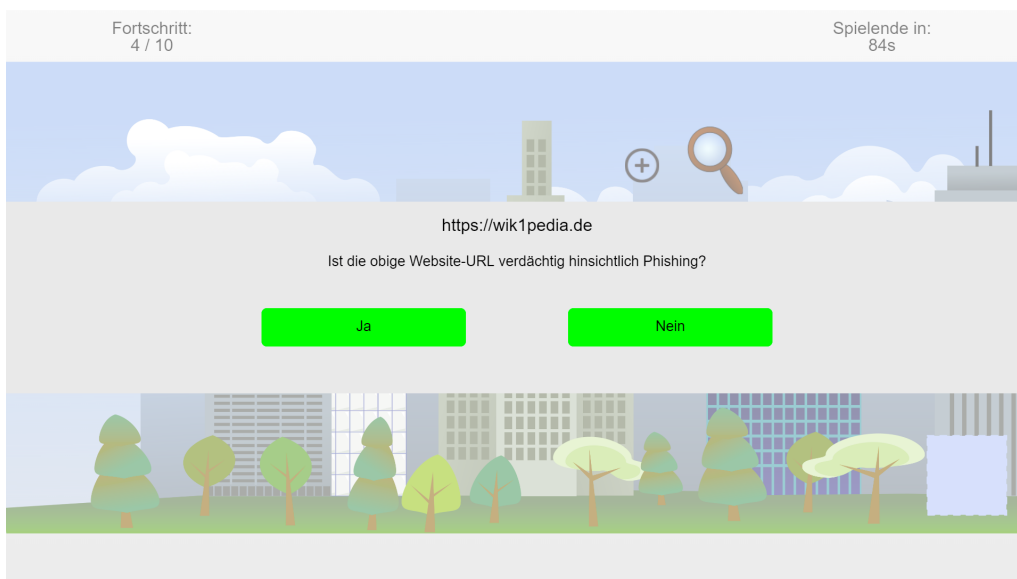


Abbildung 7.12.: Kriminalfälle – Frage Phishing-URL

7.8. Umsetzung von informativem Feedback

Damit die NuN ihre eigene Leistung reflektieren können, wurde die Möglichkeit zur Gabe von individuellem Feedback nach den Überprüfungssituationen implementiert. Für die drei überprüfenden Interaktionsmöglichkeiten sind zwei Feedback-Funktionen in der Datei *feedback.js* hinterlegt. Die Funktion *addFeedbackForStep()* kann beliebigen Text als Feedback nach einem *step* der Level im Trainingscenter darstellen. Weiterhin können zwei Callback-Funktionen übergeben werden, um passend auf die Leistung der NuN reagieren zu können. Diese Feedback-Funktion wird vor allem durch die Multiple-Choice Fragen und die Drag & Drop Elemente genutzt. Für das Anklicken der Elemente von

*Beschreibung
der unter-
schiedlichen
Funktionen zur
Gabe von
Feedback*

7.8. Umsetzung von informativem Feedback

Website-URLs steht mit `addFeedBackClickableURL()` eine eigene Feedback-Funktion zur Verfügung. Die Besonderheit ist, dass den NuN sowohl auf textuelle als auch visuelle Weise die korrekte Lösung und Korrektur angezeigt wird. Dadurch ist es möglich unterschiedliche Lerntypen anzusprechen, da die Feedback-Information sowohl textuell als auch grafisch angezeigt wird. Falsch angeklickte Elemente werden dabei rot und korrekte Elemente grün unterlegt (Abb. 7.13).

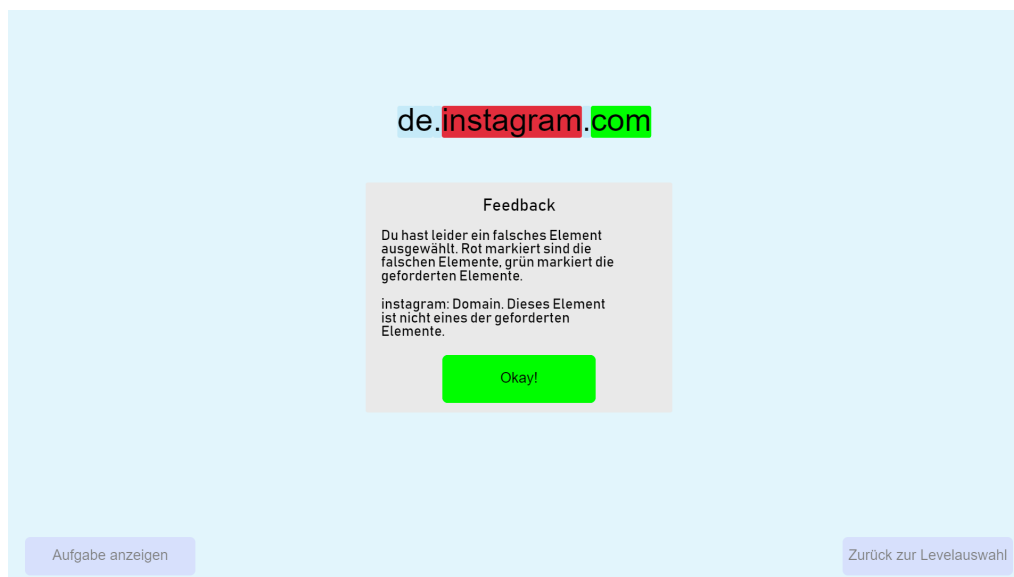


Abbildung 7.13.: Anklicken Website-URL – Feedback

Neben den Feedback-Möglichkeiten für die Überprüfungen im Trainingscenter, ist auch für die Kriminalfälle eine Feedback-Funktion implementiert worden, die sich wie die Kriminalfälle selbst in der Datei `criminalcases.js` befindet. Nach einer Runde beziehungsweise einem Test wird per `drawQuestionFeedback()` neben der Gesamtbewertung für jede einzelne Website-URL der Runde die korrekte Lösung und eine entsprechende Begründung angezeigt. Die NuN können daher nach einer Runde für jede Website-URL die eigene Leistung reflektieren (Abb. 7.14).

*Feedback
innerhalb der
Kriminalfälle*



Abbildung 7.14.: Kriminalfälle – Feedback

Außerdem wird über die Detektivfigur weiteres Feedback übermittelt. Je nach Abschneiden in den Kriminalfällen wird durch die Detektivfigur den NuN geraten, bei Problemen die entsprechenden Level im Trainingscenter zu wiederholen. In den Leveln des Trainingscenter selbst ist hingegen eher generalisiertes Feedback hinterlegt, je nachdem, ob eine Überprüfung erfolgreich verläuft oder nicht. Durch das direkte Ansprechen der NuN über die Detektivfigur besteht die Möglichkeit, dass die NuN sich persönlich involviert fühlen, da das Spiel durch die Detektivfigur auf die Leistung reagiert.

*Detektivfigur
für Feedback
nutzen*

7.9. Speichermöglichkeit des Spielfortschritts

Das Speichern des Spielfortschritts ist eines der zentralen Punkte des konzipierten Lernspiels. Als Implementation wurde ein Controller mit Hilfe des *Revealing Module Pattern* in der Datei *sessioncontrol.js* umgesetzt. Die Funktionen des Moduls stehen über die nach außen verfügbare Funktion *sessionControl* sofort zu Verfügung, da diese neben dem Namespace auch als IIFE implementiert wurde. Hinter der Funktion *sessionControl* sind die weiteren Funktionen zum Interagieren mit dem Speicherobjekt implementiert. Dazu gehören unter anderem das Setzen von Werten für existierende Variablen oder auch das Zurücksetzen von Spielfortschritten. Zu Beginn des Lernspiels wird automatisch ein neues Speicherobjekt über die veröffentlichte Funktion *newSession()* erzeugt. Auf das Speicherobjekt an sich haben die NuN über das Modul keinen Zugriff, da dieses nicht nach außen hin verfügbar gemacht wird. Lediglich ein Austausch ist möglich für das Laden alter Speicherobjekte. Durch diese Gegebenheit wird der Vorteil des genutzten Patterns deutlich. Über die veröffentlichten Funktionen des Moduls kann das Speicherobjekt aktualisiert werden, das Objekt wird jedoch durch das Modul nach außen vor ungewollten Änderungen abseits der Funktionen geschützt. In der jetzigen Implementation wird das Speicherobjekt noch im *Local Storage* des genutzten Browsers als JSON-String gespeichert. Dadurch ist es momentan noch möglich, das Speicherobjekt zu verändern und im Anschluss das Lernspiel auf Basis des veränderten Objekts zu starten.

*Umsetzung des
Controllers per
IIFE und des
Speicherobjekts
als JSON-
String*

Das Speicherobjekt an sich ist in der Implementation ein JSON-String, der zu Beginn des Lernspiels zu einem Objekt geparkt wird. Jedes neue Speicherobjekt erhält eine generierte ID zwischen 1 und 999, um den NuN das Laden über eine kurze einprägsame Nummer zu ermöglichen. Neben mehreren Variablen zum generellen Spielfortschritt (z. B. zur Absolvierung der Einführungssequenz) werden auch die Test-Objekte der Kriminalfälle in einem eigenen Array im Speicherobjekt hinterlegt. Den größten Anteil stellen die Level des Trainingscenters dar. Für jedes Level existiert ein einzelner Schlüssel unter dem die Absolvierung der einzelnen *steps* und des gesamten Levels gespeichert wird. Die *steps* werden dabei unter dem Schlüssel in dem Array *savePoints* gespeichert, das heißt die Absolvierung von *step1* wird in *savePoint1* hinterlegt. In den Leveln selbst ist für jeden *step* eine Funktion zum Aufruf des *steps* hinterlegt. Da innerhalb der Konzeption nur eine übersichtliche Zahl an *steps* für jedes Level vorgesehen war, wurden die *steps* hartcodiert. Während der weiteren Implementierung hat sich dieses Verfahren aus mehreren Perspektiven als nicht optimal herausgestellt. Zum einen nahm die Anzahl an *steps* durch das Auftrennen von Vermittlungs- und Überprüfungssituation zu, sodass es bei größeren Leveln mühsam ist, alle *steps* einzeln einzupflegen. Zwar ist das Einfügen neuer Level in das Lernspiel und in das Speicherobjekt durch eine manuelle Hartcodierung ohne Probleme möglich, jedoch ist dies für ein Level mit vielen möglichen *steps* zukünftig nicht praktikabel. Ebenso lassen sich nur mit Mühe einzelne *steps* aus den einzelnen Leveln entfernen. Aufgrund der Hartcodierung müssten die nachfolgenden *steps* ebenfalls im Namen geändert werden.

Aufgrund der hier angesprochenen nicht optimalen Lösung ist die Reimplementierung des Controllers zur Speicherung des Spielfortschritts auch ein zukünftiger Umsetzungspunkt.

7.10. Offene Umsetzungspunkte und zukünftige Erweiterungen

Damit die Level des Trainingscenters modular geändert werden können hinsichtlich der einzelnen Schritte und eine automatische Verwaltung die Hartcodierung überflüssig macht, ist es notwendig den Controller zur Speicherung des Spielfortschritts zu verändern. Anstatt der Hartcodierung wäre es zukünftig denkbar ein Level-Objekt zu erstellen, dass zu Beginn durch den Controller abgefragt wird, um das Speicherobjekt aus den erhaltenen Informationen der Level zu konstruieren. Dadurch wäre es möglich dynamisch weitere Level und *steps* zu ändern, ohne das Speicherobjekt selbst verändern zu müssen. Einzig die Registrierung eines neuen Level gegenüber der Ablaufsteuerung des MTLG-Frameworks wäre noch nötig. Durch die mögliche Änderung des Spielablaufs müsste aber auch sichergestellt werden, dass alte gespeicherte Fortschritte im Falle einer neuen Spielversion nicht mehr geladen werden können. Darüber hinaus wird momentan der Spielfortschritt noch im *Local Storage* gespeichert. Es wäre wünschenswert das Lernspiel an ein automatisiertes Evaluationssystem anzubinden, um die Ergebnisse der NuN bezüglich der Kriminalfälle und somit des Lernerfolgs untersuchen zu können.

*Neukonzeption
Controller zur
Speicherung*

Neben dem veränderten Speicherkonzept ist als weitere zukünftige Umsetzung die Erweiterung der gespeicherten Website-URLs für die Kriminalfälle notwendig. Die bisherigen zwanzig Website-URLs stellen nur eine extrem kleine Testbasis dar. Gleichzeitig wäre es möglich die Website-URLs je nach verwendeter Phishing-Technik in verschiedene Schwierigkeitsgrade einzuteilen. Es ist jedoch zu beachten, dass eine Einordnung nach objektiven Kriterien erfolgen muss, da sonst eine zu hohe Variation des Schwierigkeitslevel entstehen könnte.

*Erweiterung
der Kriminal-
fälle*

Momentan besteht die Story nur aus dem Auftreten von Detektiv Dot. Denkbar wäre das Einfügen weiterer Charaktere wie beispielsweise der Polizeichef von *Tech City*, der sich ein Bild von der Phishing Academy machen will. Mit weiteren Storyelementen wäre es auch möglich weitere plastische Storyelemente darzustellen, um den Anspruch als Computerspiel ganz im Sinne der Definition Prenskys voranzutreiben.

*Erweiterung
der Story*

Neben den eher spielerischen Elementen wäre auch die Implementierung eines lokalen und nachher globalen Belohnungssystem denkbar. Für die Absolvierung des Trainingscenters oder für besonders gute Leistungen in den Kriminalfällen, erhalten die NuN *Badges*⁷, die über alle weiteren im Hauptspiel eingebundenen Lernspiele zentral gesammelt werden können. Dadurch könnte man einen zusätzlichen visuellen Reiz für die NuN schaffen und den Eigenschaften eines Computerspiels in Bezug auf *win states* - *ego gratification* noch mehr entsprechen.

*Einführung
eines Beloh-
nungssystems*

Ein weiterer denkbaren Umsetzungspunkt ist der die momentan verwendete Sprache. Damit sich keine Person egal welchen Geschlechts ausgeschlossen fühlt, sind Anpassungen zum Einsatz geschlechtergerechter Sprache notwendig. Schon das Wort

*Anpassung der
genutzten
Sprache*

⁷ Eine Form von Abzeichen im Videospielkontext, die durch die NuN gesammelt werden können, um das eigene Prestige oder Können gegenüber anderen zu präsentieren.

„Detektiv“ ist schwer in einen geschlechtergerechten Kontext zu rücken, da keine entsprechende Form für das Wort existiert. Andere Formulierungen wie „die Opfer von Phishing-Angriffen“ sind bereits durch die verwendeten Wörter neutral. Wichtig bei den Anpassung ist jedoch, den Spielfluss nicht durch zu umständliche Wortwahl zu stören. Eine Möglichkeit eine generelle Ansprache zu umgehen, ist die Abfrage des Namens der NuN. Für die Abfrage ist jedoch eine Filterung des Inputs notwendig.

Mit der hier erfolgten abschließenden Darstellung zukünftiger Erweiterungen und Umsetzungspunkte kann nun ein Fazit gezogen werden.

Teil IV

FAZIT UND AUSBLICK

Kapitel 8 Fazit

Im Rahmen dieser Bachelorarbeit konnte mit der **Phishing Academy** ein digitales Lernspiel bezüglich der Struktur von Website-URLs und verschiedener Phishing-Techniken konzeptioniert, entwickelt und implementiert werden. Das Lernspiel kann ohne Einschränkung auf Laptops, Desktop-Computern und Tablets mit einem Vollbildbrowser gespielt werden. Als Spielsprachen stehen sowohl Deutsch als auch Englisch zur Verfügung. Die zeitliche Projektplanung, konnte bis auf eine Verschiebung von einer Woche eingehalten werden. Als Grund für die Verschiebung kann eine längere Dauer der Phase zur Konzeption genannt werden, in welcher bereits auf Basis der entwickelten Lernziele der vollständige Inhalt des Lernspiels geplant wurde.

Mit dem Ergebnis der Arbeit bin ich persönlich sehr zufrieden. Ich konnte meine eigenen Ansprüche vor allem in Hinblick auf eine grafisch ansprechende Umsetzung des Lernspiels erfüllen. Eine Schwierigkeit zu Beginn war vor allem die Entwicklung passender interaktiver Elemente zur Vermittlung, wodurch sich der Start der Implementation des Lernspiels um eine Woche verschoben hat. Die schlussendlich konzipierten Interaktionsmöglichkeiten sowohl zur Vermittlung der fachlichen Inhalte als auch zur Überprüfung des Lernfortschritts konnten jedoch vollständig umgesetzt werden. Positiv für mich selbst kann ich hervorheben, dass ich durch die sorgfältige Analyse zu Beginn den Fokus während der Umsetzung nicht verloren habe. Jedoch habe ich gelernt, dass auch während der Umsetzung die eigene Arbeit aus anderen Perspektiven betrachtet werden muss, da sonst eigene konzeptionelle Fehlentscheidungen nicht erkannt werden können. Als Beispiel ist hier die Umsetzung des hartcodierten Controllers zur Speicherung des Spielfortschritts zu nennen. Diese Lösung funktioniert zwar wie konzipiert, jedoch ist zur Änderung der eigentlich dynamischen Inhalte mehr manuelle Arbeit nötig als eigentlich notwendig.

Der tatsächliche Nutzen des umgesetzten Lernspiels steht und fällt mit den noch zu entwickelnden Lernspielen zu anderen inhaltlichen Themen im Bereich der sicheren Nutzung von Webanwendungen. Das entwickelte Lernspiel ist jedoch in sich abgeschlossen und könnte daher auch ohne weitere Lernspiele außerhalb größerer Projektumgebungen genutzt werden. Wichtig für die Weiterentwicklung des Lernspiels sind vor allem die ersten Erfahrungen der NuN, um das Lernspiel gegebenenfalls sowohl inhaltlich als auch strukturell anpassen zu können.

Kapitel 9 Ausblick

Da in der vorliegenden Bachelorarbeit keine Evaluation vorgesehen war, ist diese als nächster Schritt unumgänglich. Durch erste Rückmeldungen von zwei Testpersonen, die in der angepeilten Altersgruppe liegen, kann der zeitlich angedachte Rahmen als machbar angenommen werden. Beide Testpersonen hoben die Gestaltung des Lernspiels positiv hervor, kritisierten jedoch die inhaltliche Dichte der letzten beiden Level des Trainingscenters. Eine Evaluation könnte nicht nur weitere Erkenntnisse zu diesen zwei Punkten liefern, sondern auch aufzeigen, ob ein erfolgreicher Lernprozess stattgefunden hat. Eine Möglichkeit zur Prüfung des Lernprozesses steht mit der Spielkomponente *Kriminalfälle* schon bereit. Zur Evaluation mit Hilfe der *Kriminalfälle* müssen aber noch weitere Rahmenbedingungen geklärt werden. So ist die momentan verwendete Stichprobe von zehn Website-URLs zu klein, um konkrete Aussagen über den Lernprozess machen zu können. Hier wäre eine Erhöhung der abgefragten Website-URLs oder eine mehrfache Wiederholung des Tests innerhalb der *Kriminalfälle* denkbar. Um mit den Testergebnissen arbeiten zu können, ist zudem die Implementation einer automatischen Verarbeitung notwendig. Das verwendete Verfahren zur Leistungsmessung innerhalb der *Kriminalfälle* wurde (wie in Kapitel 5.1 thematisiert) bereits evaluiert und in seiner Wirksamkeit (für Erwachsene) bestätigt.

Neben der Evaluation des Lernprozesses ist aber auch eine allgemeine Evaluation des entwickelten Lernspiels an sich notwendig. Dies betrifft vor allem die umgesetzte Story und die interaktiven Elemente der Vermittlungssituationen. Es ist zu evaluieren, ob die entwickelte Story in der Altersklasse eine akzeptierte Lösung darstellt, bevor ebendiese Story noch erweitert wird. Darüber hinaus könnte in diesem Kontext auch evaluiert werden, ob aus der Sicht der NuN der Anteil an reinen Spielelementen ausbalanciert ist gegenüber den fachlichen Inhalten. Dies ist vor allem in Hinblick auf die angepeilte Entwicklung des Lernspiels im Sinne des DGBL von Relevanz. Zur allgemeinen Evaluation könnte daher ein digitaler Fragebogen auf Basis einer quantitativen Bewertung durch die NuN genutzt und dieser im Anschluss statistisch ausgewertet werden. Neben der quantitativen Bewertung wären zusätzlich Freitextkommentare hilfreich, um den NuN in der Fülle der unterschiedlichen Situationen gezieltes Feedback zu einzelnen Situationen ermöglichen zu können.

Auf Basis der Evaluation könnten auch die vorgestellten zukünftigen Erweiterungen aus Kapitel 7.10 bewertet werden. Damit das Lernspiel nicht an Aktualität verliert, ist auch zu prüfen, ob sich möglicherweise neue Phishing-Angriffe entwickelt haben oder bisherige Phishing-Angriffe nicht mehr relevant sind. Zusammen mit der Evaluation könnten im Anschluss die nächsten Meilensteine in der Entwicklung des Lernspiels festgelegt werden.

Anhang A Literaturverzeichnis

- [Ant18] Anti-Phishing Working Group. *Phishing Activity Trends Report 3rd Quarter 2018*. 2018. URL: http://docs.apwg.org/reports/apwg_trends_report_q3_2018.pdf (besucht am 16.01.2019).
- [ATL15] Nalin A. G. Arachchilage, Ali Tarhini und Steve Love. *Designing a mobile game to thwarts malicious IT threats: A phishing threat avoidance perspective*. 2015.
- [BE76] Benjamin Bloom und Max Engelhart. *Taxonomie von Lernzielen im kognitiven Bereich*. Weinheim, Basel: Beltz, 1976.
- [BM10] Andreas Böhn und Kurt Möser. *Techniknostalgie und Retrotechnologie*. Karlsruhe: KIT Scientific Publishing, 2010.
- [BMF05] Tim Berners-Lee, Larry Masinter und Roy T. Fielding. *RFC 3986: Uniform Resource Identifier (URI): Generic Syntax*. 2005. URL: <https://tools.ietf.org/html/rfc3986> (besucht am 27.10.2018).
- [Bre10] Johannes Breuer. „Spielend Lernen? Eine Bestandsaufnahme zum (Digital) Game-Based Learning“. In: (2010), S. 68.
- [Brü+17] Niels Brügger u. a. *Jugendmedienschutzindex: Der Umgang mit onlinebezogenen Risiken - Ergebnisse der Befragung von ELtern und Heranwachsenden*. 2017. URL: https://www.fsm.de/sites/default/files/FSM_Jugendmedienschutzindex.pdf (besucht am 03.02.2019).
- [Bun] Bundesamt für Sicherheit in der Informationstechnik. *BSIFB - Phishing*. URL: https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/Phishing/phishing_node.html (besucht am 02.10.2018).
- [Cos03] Adam M. Costello. *RFC 3492: Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)*. 2003. URL: <https://tools.ietf.org/html/rfc3492> (besucht am 04.02.2019).
- [Deu] Deutsche Kinder- und Jugendstiftung. *Ziele nach SMART-Kriterien*. URL: http://www.sachsen.ganztaegig-lernen.de/sites/default/files/Ideenb%C3%B6rse_Bildungsvereinbarung_SMART_Ziele.pdf (besucht am 04.02.2019).
- [Ent16] Harry Enten. *How Much Did WikiLeaks Hurt Hillary Clinton?* FiveThirtyEight. 23. Dez. 2016. URL: <https://fivethirtyeight.com/features/wikileaks-hillary-clinton/> (besucht am 16.01.2019).

-
- [GAP18] B. B. Gupta, Nalin A. G. Arachchilage und Kostas E. Psannis. „Defending against phishing attacks: taxonomy of methods, current issues and future directions“. In: *Telecommunication Systems* 67.2 (Feb. 2018), S. 247–267. URL: <http://link.springer.com/10.1007/s11235-017-0334-z> (besucht am 16.01.2019).
- [Ges08] Gesellschaft für Informatik. *Bildungsstandards Informatik Sek I*. 2008.
- [Ges16] Gesellschaft für Informatik. *Dagstuhl Erklärung: Bildung in der digitalen vernetzten Welt*. 2016. URL: https://gi.de/fileadmin/GI/Hauptseite/Themen/Dagstuhl-Erklärung_2016-03-23.pdf.
- [Ges18] Gesellschaft für Informatik. *Einführung des Faches Informatik in die Stundentafeln an weiterführenden Schulen*. 2018. URL: https://gi.de/fileadmin/GI/Hauptseite/Themen/Stellungnahme_IBN_zur_Stundentafel_APO_SI_2.pdf (besucht am 13.01.2019).
- [Hol18] Martin Holland. *Missing Link: Wie Russen einmal erfolgreich Cyberwar führten*. heise online. 2018. URL: <https://heise.de/-4198408> (besucht am 03.02.2019).
- [Kin18] Kinder-Medien-Studie. *Kinder-Medien-Studie 2018*. 2018. URL: https://kinder-medien-studie.de/wp-content/uploads/2018/08/KMS2018_Berichtsband_v2.pdf (besucht am 16.01.2019).
- [MAB17] Gaurav Misra, Nalin Asanka Gamagedara Arachchilage und Shlomo Berkovsky. „Phish Phinder: A Game Design Approach to Enhance User Confidence in Mitigating Phishing Attacks“. In: *arXiv:1710.06064 [cs]* (16. Okt. 2017). arXiv: 1710.06064. URL: <http://arxiv.org/abs/1710.06064> (besucht am 28.08.2018).
- [Moc87] P. Mockapetris. *STD 13: Domain names - concepts and facilities*. 1987. URL: <https://www.rfc-editor.org/std/std13.txt> (besucht am 27.10.2018).
- [Möh18] Cornelia Möhring. *Phishing-Mails erkennen und richtig handeln*. Tipps & Tricks - Ein Angebot von heise online. 2018. URL: <https://www.heise.de/-3974927> (besucht am 03.02.2019).
- [Pre07] Marc Prensky. *Digital Game-based Learning*. St. Paul: Paragon House, 2007. 472 S.
- [Rat18] Oleksandr Ratner. *Browse’n’Play: Spielerisch sicher Surfen im World Wide Web*. 2018. URL: <https://publications.rwth-aachen.de/record/745917> (besucht am 31.01.2019).
- [She+07] Steve Sheng u. a. *Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish*. Jan. 2007.
- [Ver18] Verbraucherzentrale. *Merkmale einer Phishing-Mail*. Verbraucherzentrale.de. 2018. URL: <https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/merkmale-einer-phishingmail-6073> (besucht am 03.02.2019).
- [W3T19] W3Techs. *Usage Statistics of UTF-8 for Websites, February 2019*. 2019. URL: <https://w3techs.com/technologies/details/en-utf8/all/all> (besucht am 04.02.2019).

-
- [WRN10] Colin Whittaker, Brian Ryner und Marria Nazif. „Large-Scale Automatic Classification of Phishing Pages“. In: *Proceedings of the Network and Distributed System Security Symposium, NDSS 2010, San Diego, California, USA, 28th February - 3rd March 2010*. Jan. 2010.

Anhang B Abbildungsverzeichnis

2.1. Komponenten einer einzelnen URL	7
2.2. Beispielhafte Zusammensetzung einer alltäglichen Domain	8
3.1. Dagstuhl-Dreieck [Ges16]	14
4.1. Abgrenzung der Begriffe zur Einordnung von Lernspielen (vgl. [Bre10]) .	16
5.1. User Interface einer Runde im Spiel Anti-Phishing Phil	19
5.2. Feedback Seite im Spiel Anti-Phishing Phil	20
5.3. Beispielhafter Inhalt einer Lerneinheit zum URL-Aufbau im Spiel Anti- Phishing Phil	21
5.4. Level: Vermittlung, Vertrauensfrage und Anklicken des Hosts im Spiel No- Phish	22
5.5. Feedback und Bewertung im Spiel NoPhish	23
6.1. Detektivfigur des emulierten Browsers [Rat18]	31
6.2. Skizzierter konzeptioneller Spielablauf	36
6.3. Erstellte Logos zur Phishing Academy und zur Polizei <i>Tech Citys</i>	37
7.1. Implementation des Lernspiels - Dateistruktur	41
7.2. Detective Dot mit einem Textbaustein	42
7.3. Einführung – Aufhänger E-Mail	42
7.4. Einführung – Aufhänger Zeitungsartikel	43
7.5. Spielermenü – Oberfläche zum Starten der weiteren Komponenten	43
7.6. Aufbau der Website-URL – Entdecken per Lupe	44
7.7. Überprüfung – Drag & Drop von Textelementen	45
7.8. Überprüfung – Anklicken von URL-Bestandteilen	45
7.9. Überprüfung – Multiple-Choice Frage	46
7.10. Vermittlung – Anzeige von Websites	46
7.11. Kriminalfälle – Suchen mit Hilfe der Lupe (Hotspot rechts neben der Bild- mitte)	48
7.12. Kriminalfälle – Frage Phishing-URL	48
7.13. Anklicken Website-URL – Feedback	49
7.14. Kriminalfälle – Feedback	49

Anhang C Konzipierte Level

Alle Level des Trainingscenters kurz zusammengefasst.

Level 1

Titel: „Website-URL – Wie funktioniert die Adressierung einer Website?“

Teillernziele: 1.1 und 1.2

Levelaufbau:

1. Vermittlung:
Text durch Detektivfigur: „Um Phishing zu verstehen, müssen wir den Aufbau einer Website-URL kennen.“ Danach wird die Adresse *learntech.rwth-aachen.de/* in der Mitte angezeigt. Es können die vier Elemente Subdomain, Domain, Top-Level-Domain und das erste Slash der Website-URL mit Hilfe der Lupe untersucht werden. Sobald die Lupe auf ein Element trifft, erscheint eine Box, die das jeweilige Element erläutert. Besondere Bedeutung wird hier der Erkennung der Top-Level-Domain zu Teil. Die NuN müssen dabei das Lesen der Boxen durch einen Button bestätigen. Wenn dies geschehen ist, schreitet das Level fort.
 2. Überprüfung:
Direkt im Anschluss findet eine Überprüfung statt. Dabei werden drei Leerfelder gegeben, die jeweils durch einen Punkt getrennt sind. Weiterhin sind die drei Drag & Drop Elemente Subdomain, Domain und Top-Level Domain gegeben. Die NuN müssen die Elemente korrekt einordnen, um fortzufahren. Ist die Zuordnung der NuN nicht korrekt, schreitet das Level nicht fort, sondern geht zurück zu Schritt 1. Bei korrekter Antwort folgt Schritt 3.
 3. Überprüfung:
Den NuN wird eine URL angezeigt und sie werden aufgefordert die Top-Level-Domain anzuklicken. Vorgesehen sind drei Durchläufe. Klicken die NuN zweimal die korrekte Top-Level Domain an, wird mit Schritt 4 fortgefahren. Falls nicht, geht das Spiel zurück zu Schritt 1. (Falls Schritt 2 davor bestanden wurde, wird nach erneutem Anzeigen von Schritt 1 direkt wieder Schritt 3 aufgerufen.)
 4. Vermittlung:
Es wird wieder die Adresse *learntech.rwth-aachen.de/* angezeigt. Über der Adresse wird weiterhin ein Pfeil von rechts nach links angezeigt. Über einen Dialog wird den NuN vermittelt, dass die Auflösung der URL von rechts nach links stattfindet.
 5. Überprüfung:
Mit Hilfe einer Multiple-Choice Frage wird getestet, ob die NuN sich mit der Vermittlung der Leserichtung auseinandergesetzt haben.
-

Level 2

Titel: „Website-URL – Pfade und Datenübermittlung“

Teillernziele: 1.3 und 1.4

Levelaufbau:

1. Benutzeranregung und Vermittlung:
Einblendung einer Website URL mit angegebenen Transportprotokoll `https://`. Die NuN sollen nun wiederum versuchen die Top-Level Domain anzuklicken. Die NuN sind also gefordert selbst zu überlegen. Das Ergebnis ist dabei irrelevant. In beiden Fällen wird nach dem Anklicken durch die NuN eine Erklärung bereitgestellt, welche nochmals auf die Regel *Top-Level-Domain vor dem ersten einzelnen Slash* hinweist. Weiterhin wird ein Hinweis auf ein weiteres Lernspiel gegeben, welches die Transportprotokolle `http://` und `https://` behandelt. Danach schreitet das Level zu Schritt 2 fort.
 2. Wissensvermittlung:
Anzeige einer kompletten Website-URL bestehend aus Top-Level Domain, Domain, Subdomain, Transportprotokoll und einem Pfad. Bekannte Elemente sind als bereits bekannt markiert. Durch die NuN soll wiederum die Lupe benutzt werden, um Informationen zum Pfad zu erhalten. Daraufhin erscheint wieder eine Infobox und zwei Pfeile über der Domain, um die beiden Leserichtungen besser zu verdeutlichen. Es folgt die Überprüfung in Schritt 3.
 3. Überprüfung:
Es wird eine URL angezeigt und die NuN werden dazu angehalten, das Element anzuklicken, mit dem der Pfad beginnt. Dabei werden drei URLs nacheinander angezeigt und die NuN kriegen nach jeder URL ein einzelnes Feedback. Nach der dritten URL wird ein Gesamtfeedback angezeigt und es wird entschieden, ob die NuN sich die Wissensvermittlung wiederholt anschauen müssen (im Fall: 2 von 3 falsch). Falls nicht, ist das Level abgeschlossen.
-

Level 3

Titel: „Phishing – Angriff über Subdomain“

Teillernziele: 2.1

Levelaufbau:

1. Text Detektivfigur:

„Nachdem wir uns mit dem Aufbau einer Website-URL auseinandergesetzt haben, können wir nun verschiedene Phishing Angriffe anschauen.“ (evtl. auch schon nachdem die ersten beiden Level zum URL-Aufbau erledigt sind und nicht hier im ersten Level zu Phishing)

2. Vermittlung:

Nutzung des integrierten Browsers: Dabei wird in jeweils einem Tab die Seite *rwth-aachen.de.boese-website.com* angezeigt und im zweiten Tab die Seite *rwth-aachen.de*. Die NuN werden daraufhin aufgefordert, die richtige Seite auszuwählen mit der Frage: „Mit welcher Seite gelangst du auf die offizielle Seite der RWTH Aachen?“. Egal wie die Antwort der NuN ausfällt, erhalten diese danach eine Erklärung der korrekten Lösung inklusive einer expliziten Erklärung des konkreten Phishing-Angriffs. Weiterhin wird bei einer falschen Antwort jedoch die Wiederholung des ersten Levels empfohlen.

Level 4

Titel: „Phishing – Angriff über ähnliche Namen?“

Teillernziele: 2.2 und 2.3

Levelaufbau:

1. Vermittlung:

Zuerst wird ein Fall betrachtet, der vor allem in der deutschen Sprache relevant ist. Umlaute werden anders aufgelöst, sodass beispielsweise `schueler-netzwerk.de` und `schüler-netzwerk.de` zu zwei verschiedenen Seiten führen. Diese beiden Seiten werden mit Hilfe des bereits implementierten Browsers in zwei Tabs angezeigt. Dazu erhalten die NuN den Hinweis, dass eine der beiden Website ein Phishing-Versuch ist. Die NuN werden daraufhin aufgefordert, die Phishing-Website zu markieren. Die korrekte Seite kann über das Logo identifiziert werden. Das Ergebnis der NuN ist im folgenden Kontext nicht von Bedeutung. Es soll nur deutlich gemacht werden, dass es schwer sein kann, die korrekte Adresse zu identifizieren.

2. Vermittlung:

Zwei Website-URLs werden angezeigt, wobei eine Adresse das lateinische a und die andere das kyrillische a enthält. Die NuN werden daraufhin dazu aufgefordert die Website-URLs mit der Lupe zu untersuchen, um einen Unterschied entdecken zu können. Das kyrillische a wird durch UTF-8 anders aufgelöst. Dabei wird unter der einen URL, sobald die NuN das Element mit der Lupe überfahren, die eigentliche Bedeutung angezeigt. Unter UTF-8 wird das kyrillische a in der URL zur Auswertung in `%d0%b0` umgewandelt, das lateinische a hingegen zu `%61`. In Folge der anschließenden Umwandlung durch *Punycode* sehen die NuN zwei unterschiedliche Zeichenketten für die Website-URLs. Daraufhin wird ein Tipp angezeigt, welcher den NuN nahelegt, die korrekte Adresse über eine Suchmaschine zu suchen, um diesen Angriffsvektor ausschließen zu können.

Level 5

Titel: „Phishing – Angriff über IPs oder Pfadnutzung“

Teillernziele: 2.4 und 2.5

Levelaufbau:

1. Vermittlung:
Mehrere Website-URLs und eine Erklärung werden dargestellt. Fahren die NuN mit der Lupe über Website-URLs wird die zugehörige IP-Adresse angezeigt. In der Erklärung wird den NuN erläutert, dass seriöse Websites nie über die IP-Adresse operieren und solche Adressen gemieden werden sollten.
 2. Vermittlung:
In der zweiten Phase wird den NuN die URL *phishing1.de/www.phishing2.de* angezeigt. Daraufhin wird wiederum eine Multiple-Choice Frage gestellt, welche Website die NuN sehen, denn bei einem Aufruf sehen. Unabhängig von der Antwort der NuN wird dann eine Erklärung gegeben, welche Website aufgerufen wird. Bei einer falschen Antwort wird den NuN zudem empfohlen, sich nochmal das zweite Level anzuschauen.
-

Level 6

Titel: „Phishing – Vorbeugende Maßnahmen“

Teillernziele: 2.6 und 2.7

Levelaufbau:

1. Vermittlung:
Zu Beginn werden Bilder von verschiedenen Anwendungen und System gezeigt, wie die URL ohne Anklicken eines Links angesehen werden kann. Danach werden die NuN über die Detektivfigur aufgefordert, später zu erforschen wie die Anzeige von Links in den von ihnen genutzten Apps oder Programmen funktioniert.
 2. Vermittlung:
Als inhaltlicher Abschluss des Trainingscenters wird den NuN eine Zusammenfassung angezeigt mit dem zusätzlichen Hinweis auf die weiteren Merkmale zur Überprüfung der Legitimität wie beispielsweise Zertifikate. Es wird zudem ein Ausblick auf das Thema Cross-Site-Scripting bereitgestellt.
 3. Dialog:
Die Detektivfigur gratuliert den
-

Eidesstattliche Versicherung

Schöbel, Sven

Name, Vorname

Matrikelnummer (freiwillige Angabe)

Ich versichere hiermit an Eides Statt, dass ich die vorliegende ~~Arbeit~~/Bachelorarbeit/
Masterarbeit* mit dem Titel

Phishing Academy: Entwicklung und Umsetzung
eines digitalen Lernspiels zu Website-URLs und Phishing

selbstständig und ohne unzulässige Hilfe erbracht habe. Ich habe keine anderen als
die angegebenen Quellen und Hilfsmittel benutzt. Für den Fall, dass die Arbeit zusätz-
lich auf einem Datenträger eingereicht wird, erkläre ich, dass die schriftliche und die
elektronische Form vollständig übereinstimmen. Die Arbeit hat in gleicher oder ähnli-
cher Form noch keiner Prüfungsbehörde vorgelegen.

Aachen , 05.02.2019

Ort, Datum

Unterschrift

*Nichtzutreffendes bitte streichen

Belehrung:

§ 156 StGB: Falsche Versicherung an Eides Statt

Wer vor einer zur Abnahme einer Versicherung an Eides Statt zuständigen Behörde eine solche
Versicherung falsch abgibt oder unter Berufung auf eine solche Versicherung falsch aussagt, wird
mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

§ 161 StGB: Fahrlässiger Falscheid; fahrlässige falsche Versicherung an Eides Statt

(1) Wenn eine der in den §§ 154 bis 156 bezeichneten Handlungen aus Fahrlässigkeit begangen
worden ist, so tritt Freiheitsstrafe bis zu einem Jahr oder Geldstrafe ein.

(2) Strafflosigkeit tritt ein, wenn der Täter die falsche Angabe rechtzeitig berichtigt. Die Vorschrif-
ten des § 158 Abs. 2 und 3 gelten entsprechend.

Die vorstehende Belehrung habe ich zur Kenntnis genommen:

Aachen , 05.02.2019

Ort, Datum

Unterschrift