netidee

PROJEKTE

Phishingtraining

Zwischenbericht | Call 15 | Projekt ID 5126

Inhalt

1 Einleitung

Dieses Dokument beschreibt die Arbeiten, die im Rahmen des Projekts bis einschließlich Mai 2021 durchgeführt wurden. Der Schwerpunkt der bisherigen Arbeiten lag auf der Entwicklung der Webplattform und der Engine für das Phishingtraining, der Erstellung des psychologischen Konzepts für die wissenschaftliche Studie an zwei Klassen, deren konkrete Konzeptionierung und Detailplanung sowie Betreuung der beteiligten Schulklassen.
Das Projekt befindet sich im Zeitplan und wir sind zuversichtlich, die geplanten Arbeiten bis zum Projektende fristgerecht abschließen zu können. Der Start der Pilotcases hat sich etwas verzögert, was zu kleinen Veränderungen in der Laufzeit der anderen Arbeitspakete führte.

2 Status der Arbeitspakete

2.1 Arbeitspaket 1 – *Detailplanung und Formales am Projektstart*

Arbeitspaket 1 wurde im Dezember 2020 mit der Abgabe und Abnahme des Detailprojektplans, dem ersten Blogeintrag und sowie dem ersten Förderratenabruf abgeschlossen.

2.2 Arbeitspaket 2 – *Entwicklung des psychologischen Konzepts*

Die Aufgabe dieses Arbeitspakets war die Entwicklung eines psychologischen Konzepts für ein effektives Training gegen Phishing. Nach einer ausführlichen Literaturrecherche zu bisherigen Studien und Statistiken zum Thema Phishing und Phishingtrainings wurde das Konzept erstellt. Das Konzept wurde bewusst so gestaltet, dass es für Laien verständlich ist und von LehrerInnen als Wissensgrundlage für die zukünftig geplante selbstständige Durchführung des Trainings genutzt werden kann. Es beschreibt die Relevanz des Themas, die bisherigen Lösungsversuche für das Problem von Phishingnachrichten und schließlich das entwickelte Training. Das Konzept wird am Ende der Förderperiode mit den Ergebnissen der aktuellen Studie ergänzt und öffentlich zugänglich gemacht.

2.3 Arbeitspaket 3 – *Implementierung der Webapplikation*

In diesem Arbeitspaket wird die Webplattform zum Erstellen und Verwalten von Phishing-Kampagnen geplant und implementiert. Die Ziele der Plattform und die erforderlichen Features wurden in Workshops mit dem gesamten Team festgelegt. Die wesentlichen Features umfassen:

- Phishing-Kampagnen anlegen und verwalten
- Benutzerverwaltung
- Metadateneingabe für personalisierte Nachrichten (z.B. Social Media Accounts, Telefonanbieter, Adresse)
- Verwaltung von Phishing-Templates

- Fragebogen nach Klick auf Phishing-Links

Als Technologiestack wurde .NET Core als etabliertes Framework für Webapplikationen mit einem breiten Ökosystem gewählt, in Kombination mit SQL als Datenbank. Da die Applikation im Kern mit externen Systemen kommuniziert (z.B. via E-Mails, SMS) sind sowohl die Entwicklungsumgebung als auch das Deployment eine Herausforderung. Um eine möglichst stabile Umgebung zu schaffen, wurde auf Docker Container gesetzt und die Plattform auf der IT-Infrastruktur der Universität Wien gehostet.
Um glaubhafte Phishingnachrichten zu erzeugen, mussten außerdem passende Domänen gekauft werden und der Mailserver entsprechend konfiguriert werden. Ebenso mussten mehrere SMS-API Provider getestet werden, um einen Anbieter zu finden, der selbstgewählte Absendernamen zulässt.

2.4 Arbeitspaket 4 – *Implementierung der Phishingengine*

Die Phishing-Plattform soll es ermöglichen, komplette Phishing-Kampagnen automatisiert mit TeilnehmerInnen durchzuspielen. Unser Konzept beinhaltet Phishing-Templates (Plain Text oder HTML), die Platzhalter für Metadaten vorsehen (z.B. Vorname, Geburtsdatum). In Templates kann man die Zieldomäne definieren (für Links), Absendernamen, ein Zeitfenster (z.B. zwischen 30.12 und 1.1 für Neujahrs-Phishingmails), ob es sich um Gruppenmails handelt, sowie Informationen zu Schwierigkeitsgrad und Auswirkungen. Es wird auch der Kanal gewählt, über den die Nachrichten gesendet werden – aktuell sind E-Mail und SMS implementiert.
Beim Klick auf einen Link in den Phishingnachrichten, wird die Teilnehmerin oder der Teilnehmer auf einen Feedback-Fragebogen weitergeleitet. Zusätzlich werden Bilder aus den HTML Templates dynamisch vom Server nachgeladen. Damit können wir den Zeitpunkt des Abrufens registrieren, als Information wann die Mail geöffnet wurde. Als Auswertungsexport können .csv-Files in Kampagnen erzeugt werden.
Das Gesamtkonzept und die Strategie Nachrichten für die einzelnen TeilnehmerInnen zu erzeugen war eine herausfordernde Aufgabe. Letztendlich haben wir die Templates erweitert, um mögliche Sendezeiträume zu definieren und erstellen nun für alle TeilnehmerInnen einer Kampagne individuelle Nachrichten im Kampagnen-Zeitraum und entsprechend der Template-Vorgaben. Schwierig war es auch, Templates so zu gestalten, dass diese nicht unmittelbar von E-Mail Providern wie Google und GMX als Spam klassifiziert werden.

2.5 Arbeitspaket 5 – *Betreuung der Schulklassen*

Dieses Arbeitspaket beinhaltet die Betreuung der Schulklassen. Direkt nach dem Abschluss der Detailplanung wurde mit mehreren Schulen Kontakt aufgenommen, um das von uns geplante Phishingtraining anzubieten. Entgegen unseren Erwartungen bekamen wir nur sehr begrenzt Rückmeldungen, trotz mehrmaliger Kontaktaufnahme. Wir führen dies auf die schwierige Situation in den Schulen zum damaligen Zeitpunkt, aufgrund von wechselnden Phasen von Präsenz-, Online- und Hybrid-Unterricht, zurück. Es gelang uns dennoch zwei Klassen an zwei Schulen von der Teilnahme zu überzeugen. Mit diesen wurde ein Online-Termin vereinbart, ein

Awarenesstraining durchgeführt und anschließend die Studie erklärt. Alle SchülerInnen, die an der Studie teilnehmen wollten, haben eine unterzeichnete Einverständniserklärung an uns geschickt und bekamen den Link zur Registrierung auf der Phishing-Plattform. Schließlich wurden mehrmals Erinnerungen zur Registrierung und der Angabe von Meta-Daten (für personalisierte Nachrichten) an die SchülerInnen geschickt, bevor das Training mit einer Trainingsphase begonnen hat. Die finale Anzahl der Teilnehmer an der Studie war leider deutlich geringer als geplant (n=14), weshalb nun eine rein deskriptive Auswertung der Daten geplant wird.

3 Umsetzung Förderauflagen

In der Fördervereinbarung wurden vier Förderauflagen festgelegt, von denen bereits drei berücksichtigt wurden und die letzte im Endbericht erfüllt wird.

Bereits erfüllt:
Auflage 1: Vor Förderabschluss Detaillierung Projektergebnis
Die Detailierung des konkreten Projektergebnisses wurde via E-Mail vor Projektstart durchgeführt.

Auflage 2: Vor Förderabschluss klären, ob Antragsteller Uni oder genannten Personen selbst sind
Das Projekt wurde als Universität Wien beantragt und ebendort durchgeführt.

Auflage 3: Konkrete Pilotcases mit Schulen durchführen & dokumentieren
Die Plattform wird mit Schülerinnen und Schülern von zwei niederösterreichischen Schulen im Rahmen von konkreten Pilotcases durchgeführt. Diese wurden bereits gestartet und laufen bis zum Sommer.

Noch zu erfüllen:
Auflage 4: Veröffentlichung psychologisches Konzept iSv open source
Das Konzept wird nach Einarbeitung der Ergebnisse der Pilotcases zusammen mit dem Endbericht des Projekts veröffentlicht.

4 Zusammenfassung Planaktualisierung

Beim Projektplan wurden keine grundlegenden Änderungen vorgenommen. Durch den leicht verspäteten Start der Pilotcases, kam es jedoch zu kostenneutralen Anpassungen der Laufzeit der anderen Arbeitspakete.
Das Arbeitspaket 3 wurde um zwei Monate verlängert, da bis zum Start der Pilotcases die Zeit genutzt wurde, die Plattform zu optimieren und gefundene Bugs zu beheben. Die Betreuung der Schulklassen (AP5) wurde verlängert, um den verspäteten Start der Pilotcases auszugleichen.

5 Öffentlichkeitsarbeit/ Vernetzung

Da die Anzahl der TeilnehmerInnen an den Pilotcases leider geringer ist als ursprünglich gehofft, planen wir im Herbst 2021 weitere Phishingtrainings an Schulen durchzuführen. Dazu wurden bereits Kontakte zu weiteren Schulen hergestellt.

6 Eigene Projektwebsite

Es wird keine eigene Webseite für das Projekt betrieben. Die Plattform wird auf Systemen der Universität Wien gehostet, diese ist jedoch während der Laufzeit der Pilotcases noch nicht öffentlich verfügbar.