SecPatt

Endbericht | Call 12 | Projekt ID 2390

Inhalt

1 Einleitung

SecPatt ist ein Projekt zur Erstellung und Bereitstellung von Lösungen für häufig auftretenden Probleme hinsichtlich Privatsphäre und Sicherheit im Internet. Das Ziel von SecPatt ist es, Informationen zur Erstellung von Sicheren Webseiten auf eine leicht zugängliche Weise öffentlich bereitzustellen. Dies geschieht in Form sogenannter *Patterns*, welche praxisorientierte Problemlösungen inklusiver exemplarischer Beispiele anbieten, gleichzeitig den Anwender Schritt für Schritt an die Lösung heranführen. Die einzelnen Probleme und deren Lösungen werden zunächst von und mit Sicherheitsexperten erarbeitet, so dass diese dann in Patternform leicht zugänglich aufbereitet werden können. Es geht also darum, Experten wissen für Nichtexperten aufzubereiten und für diese anzubieten.

Da Sicherheit im Netz jeden betrifft, soll SecPatt eine öffentlich zugängliche und stetig wachsende Ressource darstellen, die sowohl mehr Aufmerksamkeit und Grundwissen schafft (etwa: Ab wann das Thema „Sicherheit“ im Erstellungsprozess beginnt oder welche Faktoren eigentlich zur Sicherheit einer Webseite beitragen) und gleichzeitig konkrete Umsetzungslösungen anbietet. Der Fokus liegt jedoch eindeutig auf Letzterem: SecPatt soll vor Allem schnell anwendbare Lösungen bieten, damit eine sichere Webpräsenz keine finanziellen oder zeitlichen Ressourcen erfordern muss, die vielen schlicht und einfach nicht zur Verfügung stehen.

2 Projektbeschreibung

SecPatts sind Designpatterns, die Webentwickler/Innen sowie Webdesigner/Innen dabei unterstützen sollen ihre Webpages von Beginn an sicher zu gestalten. SecPatts zielen auf einfachen Zugang und ein niedriges Einstiegsniveau ab. Wie implementiert man eine SSL Verschlüsselung? Wie helfe ich dem User, ein sicheres Passwort zu erstellen? Auf all diese Fragen gibt es Antworten, die jedoch auf eine Vielzahl an Quellen verteilt sind und oft ein beachtliches Ausmaß an Vorwissen erfordern - sprich: man muss bereits Wissen über Websicherheit verfügen, um sich solches aneignen zu können. Das Projekt wird direkt umsetzbare Lösungen in einem leicht zugänglichen Format bereitstellen. SecPatt bedient sich hierzu der bewährten Patterns-Methodik. Patterns sind dabei erprobte Lösungen zu wiederkehrenden Problemen. Diese Designlösungen werden kategorisch nach Problemen geordnet über eine Webpage öffentlich bereitgestellt.

SecPatt soll Webentwickler/innen als die zentrale Anlaufstelle bei Fragen und Problemen zu Security und Privacy einer Webpage dienen. Die Lösungen werden kostenlos bereitgestellt. SecPatt soll vor allem unerfahrenen Nutzern (u.A. Einzel-/Kleinunternehmer, Schüler, Hobbyisten) helfen, sich für den Internetauftritt notwendige Kenntnisse anzueignen. Die Einstiegsschwelle wird dadurch auf nationalem Niveau gesenkt und gleichzeitig wird zur Erhöhung der Sicherheit im Netz beitragen.

2.1 Zielgruppe

Entwickler von Webseiten, die über kein Expertenwissen verfügen. Es gibt hierbei keine Beschränkung Altersbeschränkung – sowohl Schüler als auch Hobbyisten höheren Alters werden also potentielle Nutzer solcher Patterns gesehen. Als Einschränkungen setzen die Patterns Basis-Computerkenntnisse sowie Lesekenntnis in Deutsch voraus.

2.2 Projektziele

Das Ziel des Projektes ist es, Patterns zu 16 der relevantesten Sicherheits- und Privacy-Probleme zu erstellen und diese via der eigenen Projektwebseite öffentlich und kostenfrei zur Verfügung zu stellen.

2.3 Projektergebnis

Nach mehreren Expertengesprächen, umfassender Recherchearbeit, mehreren internen Iterationen und zwei Iterationsworkshops mit externen Teilnehmern wurden schließlich 16 wichtige Problembereiche identifiziert und als Patterns aufgearbeitet. Die Patternstruktur wurde für dieses Vorhaben adaptiert und basiert auf Ergebnissen vergangener Arbeiten zur Patternthematik. Sie ist wie folgt aufgebaut:

a) **Name**

b) **Intention**

Eine Kurzbeschreibung des Patterns in 1-2 Sätzen. Dieser Abschnitt sowie der Patternname dienen der Orientierung innerhalb der Kollektion, so dass der Anwender schnell entscheiden kann, ob ein bestimmtes Pattern für ein vorliegendes Problem relevant ist oder nicht.

c) **Problemstellung**

Eine Beschreibung der Problemstellung. Eine Erweiterung der Intention um es dem Anwender zu ermöglichen, alle Komponenten eines oft simpel anmutenden Problemes zu erkennen.

d) **Szenario**

Ein Beispielszenario, welches die Problembeschreibung im Kontext klarer macht und gleichzeitig dem Anwender weiter Orientierung hinsichtlich Anwendbarkeit des Patterns gibt.

e) **Lösung**

Eine Schritt-für-Schritt-Anleitung der Lösungsimplementierung. Zusammen mit den nachfolgenden Beispielen sozusagen das Kernstück eines jeden Patterns.

f) **Beispiele**

Jedes Pattern erfordert mindestens ein Beispiel einer erfolgreichen Implementierung. Dies dient als kontextbezogene Orientierungshilfe und zeichnet den Patternansatz gegenüber theoriorientierter Literatur aus.

g) **Referenzen**

Alle im Pattern referenzierten Informationen werden hier aufgelistet. Dies umfasst Links zu anderen Seiten und Literaturangaben aber auch Referenzen auf andere Patterns oder sonstige Quellen.

h) **Keywords**

Schlüsselwörter, die primär der Sortierung sowie Navigation innerhalb der Patternkollektion bilden.

Die einzelnen Unterkategorien eines jeden Patterns sind intentional gemäß Lesepriorität gereiht: a-d stellen die Präambel dar, welche primär dazu dient, die Anwendbarkeit des Patterns festzustellen und den Kontext zu erkennen. D und e enthalten die Lösungsanleitung inklusive Beispielanwendungen, während g auf weiterführende Informationen verweist und h primär der internen Strukturierung dient. Der Vorteil dieser Strukturierung ist, dass man nicht das gesamte Pattern gelesen haben muss, um dessen Relevanz entscheiden zu können (oft genügt ein Blick auf Name und Intention) und gezielt nach bestimmten Informationen innerhalb des Patterns gesucht werden kann.

Die in den Interviews und Gesprächen identifizierten und schlussendlich bezüglich Priorität bewerteten Probleme resultierten in 16 Patterns. Diese wurden nach Schwierigkeit der Implementierung eingeteilt; das Ergebnis ist folgende Patternkollektion:

1. **Basis**
   - 1.1. Was trägt alles zur Sicherheit einer Website bei?
   - 1.2. Wie überprüfe ich die Sicherheit meiner Website?
2. **Einsteiger**
   - 2.1. Wann und wie oft sollte man Updates installieren?
   - 2.2. Wie stelle ich einen Hackerangriff fest?
   - 2.3. Wie verschlüssele ich die Kommunikation mit meiner Website?
   - 2.4. Wann und wie sollte man Backups erstellen?
   - 2.5. Was ist ein sicherer Hoster und wie wähle ich diesen aus?
3. **Fortgeschritten**
   - 3.1. Was kann man gegen DDoS Attacken tun?

3.2. Wie speichere ich Daten von Websitebesuchern sicher?

3.3. Welche Daten darf ich auf meiner Website speichern?

3.4. Welche Informationen muss ich den Besuchern auf meiner Website bereitstellen?

3.5. Was ist während oder nach einem Hackerangriff zu tun?

3.6. Sollte ich einen Mailserver selbst einrichten oder betreiben?

4. **Fortgeschritten+**

4.1. Wie sieht ein guter und sicherer Webshop aus?

4.2. Wie richte ich einen sicheren Mailserver ein?

4.3. Benötige ich eine Internetversicherung?

Die Kategorie *Basis* wurde zusätzlich zu den Schwierigkeitsgraden hinzugefügt, da die darin enthaltenen Patterns Grundwissen zur Webseitensicherheit und Überprüfung enthalten, somit sozusagen Anfangs- und Endpunkt der Patternkollektion darstellen. *Fortgeschritten+* wurde zusätzlich hinzugefügt, um jene Patterns zu denotieren, die nicht nur schwieriger zum implementieren sind sondern mitunter auch mehr Vorwissen als die Patterns der Kategorie *Fortgeschritten* erfordern. Die Schwierigkeitsgrade waren ursprünglich nicht geplant, wurden jedoch nach Feedback der externen Beteiligten in das Projekt aufgenommen und schlussendlich umgesetzt, um den Anwendern eine zusätzliche Orientierungshilfe zu bieten.

3 Verlauf der Arbeitspakete

3.1 Arbeitspaket 1 - *Projektmanagement*

In AP1 finden alle organisatorsichen Tätigkeiten (Organisation, Meetings, QA, Conrolling, etc.) statt.

3.2 Arbeitspaket 2 - *Problem Mining*

In diesem AP geht es darum, die 16 relevantesten Problemstellungen zu identifizieren und aufzubereiten, welche dann als Grundlage für die 16 zu erstellenden Patterns dienen.

Hierbei wird ein Interview-basierter Ansatz verfolgt, da die Probleme auch tatsächlich - sowohl hinsichtlich Häufigkeit des Auftretens als auch möglicher Folgen – von entsprechender Relevanz sein sollen. Die aus den Interviews identifizierten Probleme werden anschließend aufbereitet (Konsolidierung, Clustering, hierarchische Anordnung) und hinsichtlich ihrer tatsächlichen Relevanz nochmals quantitativ bewertet.

In der ersten Phase wurden erfolgreich 4 Interviews geführt: Eines mit einem Universitätsprofessor der Computerwissenschaften der Universität Salzburg, eines mit einem Experten des CERT Austria, zwei mit professionellen Webentwicklern einer

Softwarefirma in München. Die Patternstruktur wurde an das Projektziel angepasst (AP2_Ergebnis 1), so dass die identifizierten Probleme als Patternname integriert werden können. Ein Rating der Problemstatements wurde im Rahmen des NetIdee Spring Talk 2018 mit den Teilnehmer vorgenommen und die finale Anzahl an 16 statements für die weitere Arbeit in AP4 erreicht (AP2_Ergebnis 3).

Besonders hervorzuheben ist hierbei die Unterstützung durch nic.at Salzburg, welche den Kontakt zum CERT Wien herstellten.

3.3 Arbeitspaket 3 - *Pattern-Website*

Die Pattern-Website wurde via Wordpress erstellt und über eine eigene Domain unter www.secpatt.at bereitgestellt. Erste Formatierungen und Anpassungen wurden vorgenommen sowie die Basisstruktur für die späteren Patterns (AP3_Ergebnis 1). Hierzu wurde zunächst ein Probepattern integriert, um Präsentation und Inhalt zu testen. Öffentlich freigeschalten wurde zu diesem Zeitpunkt nur die Landing Page, welche generelle Information zum Projekt bietet. Anleitung zur Benutzung, Teamübersicht sowie die Patterns selbst werden zu Projektende nach und nach öffentlich gestellt.

Eine Schwierigkeit stellte sowohl die Navigation innerhalb der Website als auch die Begriffserklärung dar, da für beides passende Widgets gesucht und angepasst werden mussten. Dies wurde mittlerweile gelöst: Fachbegriffe werden nun via Popups inkl. Links direkt im Text erläutert. Die Patterns werden in einer leichter verständlichen Baumstruktur als Sideframe dargestellt. Die Landing Page bietet somit auf einen Blick die Projektübersicht und Anwendungserklärung sowie direkten Zugang zu den Patterns via Sideframe, was dem Anwender den Einstieg erheblich erleichtert.

3.4 Arbeitspaket 4 – *Pattern Writing & Iteration*

In diesem AP finden alle Arbeiten zur Patternerstellung und weiteren Verfeinerung nach der Identifizierung und Aufbereitung der Probleme in AP2. Dies besteht in Recherche (on- und offline) und Schreibarbeit zu den initialen Pattern Drafts (AP4_Ergebnis 1). Diese Drafts werden in Workshops mit externen Teilnehmern einzeln bewertet und diskutiert. In Folge eines solchen Workshops werden die Patterns dann einzeln anhand des Feedbacks iteriert und gegebenenfalls auch erweitert.

Zunächst wurde ein Workshop mit Web Development Experten aus Salzburg durchgeführt. Zwei der Teilnehmer wurden extern rekrutiert, zwei sind Mitarbeiter des Center für HCI, die ansonsten nicht in das Projekt SecPatt involviert sind. Die Patterns haben eine erste Iterationsrunde durchlaufen, wobei die Änderungen teils sehr umfangreich ausfielen, so dass die Durchführung eines zweiten Workshops beschlossen wurde. Dieser wurde direkt bei der Softwareentwicklungsfirma in München durchgeführt, bei welchen das Projektvorhaben im Rahmen der Interviews in AP2 besonderen Zuspruch gefunden hatte.

Nach dem finalen Workshop wurden die Patterns ein letztes Mal iteriert und finalisiert, so dass sie dann in AP3 öffentlich bereitgestellt werden konnten. Also besondere

Schwierigkeit stellten sich die Referenzierung zwischen den Patterns sowie der oft unterschiedliche Komplexitätsgrad der Lösungsanwendung heraus. Daher wurde, zusätzlich zu den ursprünglich geplanten Aktivitäten ein System an Schwierigkeitsgraden eingeführt und jedes Pattern nochmal hinsichtlich diesem evaluiert und gegebenenfalls überarbeitet.

Durch die in AP5 erfolgte Gelegenheit zur Dissemination auf internationaler Ebene (siehe 3.5) ergab sich die Notwendigkeit der Übersetzung der Patterns in englische Sprache. Da die Patterns in deutscher Sprache – gemäß Planung – erst Ende November finalisiert werden konnten, ergab sich hierdurch eine Verzögerung in das Frühjahr 2019 hinein. Dies betrifft jedoch nur die publikationsbezogene Erweiterung – die Patterns (AP4) sowie die Patternwebseite (AP3) standen Ende 2018 planungsgemäß in deutscher Sprache final online.

3.5 Arbeitspaket 5 – *PR & Dissemination*

In diesem AP finden alle Tätigkeiten zu PR (Aussendungen über Verteiler, soziale Medien, etc.) sowie wissenschaftliche Publikationen statt.

Die Projektwebsite (secpatt.at) wurde in AP3 mit einer landing page mit Basisinformationen versehen, so dass Benutzer auch vor Fertigstellung nicht auf einer leeren Seite landen. Blogposts auf der NetIdee-Website wurden regelmäßig zum jeweiligen Monatsende vorgenommen.

Für die ComputationWorld PATTERNS 2019 sind mind. 2 full paper Einreichungen geplant. Die Deadline hierfür wurde in das Frühjar 2019 verlegt, weshalb die Publikationen zum Berichtzeitpunkt noch nicht abgeschlossen sind.

Ein besonderer Erfolg ist hierbei die Einrichtung eines Special Tracks bei auf der Konferenz aus dem Projekt heraus: (https://www.iaria.org/conferences2019/filesPATTERNS19/SECPAT.pdf)

4 Liste Projektendergebnisse

Kurzbeschreibung der erreichten Projektendergebnisse jeweils mit Open Source Lizenz und Webadresse (netidee Vorgaben beachten!)

1	*Ergebnis 1* *SecPatt Webseite entwickelt und online*	*Lizenz* *CC BY-SA 3.0 AT*	*www.secpatt.at*

2	*Ergebnis 2* *16 Patterns entwickelt und online bereitgestellt*	*Lizenz* *CC BY-SA 3.0 AT*	*www.secpatt.at* *www.secpatt.at*
3	*Ergebnis 3* *Website-Aufrufe: 1790* *Besucher: 472 (Stand: 04-02.2019)*	*CC BY-SA 3.0 AT*	*www.secpatt.at*
4	*Ergebnis 4* *Thematischer Special Track auf int. Fachkonferenz (IARIA ComputationWorld PATTERNS 2019)*	*CC BY-SA 3.0 AT*	*www.secpatt.at* *https://www.iaria.org/conferences2019/filesPATTERNS19/SECPAT.pdf*
5	*Ergebnis 5* *Wissenschaftlicher Beitrag auf PATTERNS 2019 Konferenz*	*Open access*	*https://www.thinkmind.org/index.php?view=article&articleid=patterns_2019_2_10_78006*
6	*Ergebnis 6* *Wissenschaftlicher Beitrag auf PATTERNS 2019 Konferenz*	*Open access*	*https://www.thinkmind.org/index.php?view=article&articleid=patterns_2019_2_20_78004*
7	*Ergebnis 7* *Wissenschaftlicher Beitrag auf PATTERNS 2019 Konferenz*	*Open access*	*https://www.thinkmind.org/index.php?view=article&articleid=patterns_2019_2_30_78005*
8	*Wissenschaftlicher Beitrag auf CHI 2019 Konferenz*	*ACM rights retained*	*https://dl.acm.org/citation.cfm?id=3312789*

5 Verwertung der Projektergebnisse in der Praxis

Die Patterns stehen öffentlich zur Verwendung zur Verfügung, wobei seitens der an den Interviews und Workshops beteiligte Softwarefirma bereits explizites Interesse an deren betriebsinterner Verwendung ausgesprochen wurde. Die Patterns sind außerdem Grundlage eines Bachelorvorhabens an der Universität Salzburg.

6 Öffentlichkeitsarbeit/ Vernetzung

Das Projekt wurde über die eigene Website, die Website des Centers für HCI sowie Aussendungen über den Verteiler der Universität Salzburg beworben. Weiters wird Dissemination auf internationaler Ebene im Rahmen der ComputationWorld PATTERNS 2019 erfolgen. Zum Projektabschluss ist noch ein Zeitungsbeitrag in den Salzburger Nachrichten geplant.

7 Geplante Aktivitäten nach netidee-Projektende

Die bestehenden Patterns sind Basis mindestens eines Bachelorvorhabens an der Universität Salzburg. Die Patterns sowie die Webseite stellen den Grundstein für eine geplante umfassendere Ressource dar. Inhaltlicher Umfang sowie Nutzbarkeit sollen in Nachfolgeprojekten erweitert werden. Weiters streben wir stärkere Synergien mit nationalen Entitäten (CERT, Chaos Computer Clubs, Hochschulen) an, um die Patterns als offen verfügbare Ressource stärker zu integrieren und gleichzeitig eine Community rund um das Thema aufzubauen.

8 Anregungen für Weiterentwicklungen durch Dritte

Die entwickelten Patterns lassen sich in jegliche Webentwicklungsaktivitäten, in welchen einfacher Zugang zu praxisrelevanten Informationen notwendig ist, integrieren. Dies umfasst professionelle Anwendung (wie wir durch Rückmeldung über unsere Industriekontakte erfuhren, ist niederschwellig aufbereitetes Wissen selbst für Experten sehr wertvoll und in Unternehmen oft stark gefragt) aber auch in Tutorin- oder Unterrichtssettings.

Bei der weiteren Nutzung der Patterns ist stets darauf zu achten, ob zu den darin enthaltenen Empfehlungen eventuelle Neulösungen bestehen. Bei den Patterns handelt es sich stets um „Best Practices“, d.h. Bestandsaufnahmen guter Lösungsansätze zum Zeitpunkt der Pattern Erstellung. Was hier als gute Lösung gilt, unterliegt natürlich ebenso wie das World Wide Web konstanter Änderung und ist dementsprechend zu prüfen und gegebenenfalls zu aktualisieren.