Hochschule Niederrhein
University of Applied Sciences

Einfache Mechanismen für die Sicherheit von Webanwendungen in KMU unter Berücksichtigung der Personalstrukturen

Ausgangslage und Motivation:

Insbesondere in KMU ist das erforderliche Know-How, die eigene Internetpräsenz sicher zu gestalten, oft nicht vorhanden. Es werden Systeme wie Wordpress eingesetzt, die dann durch den Eigentümer inhaltlich gepflegt, aber nicht technisch administriert werden. Damit sind KMU einem erhöhten Risko ausgesetzt.

Ziel:

Ziel des Vorhabens ist, ein Konzept für die Erhöhung der Resilienz von bestehenden Webanwendungen bereitzustellen, ohne Eingriffe in die Webanwendung selbst vorzunehmen. Teilziele sind:

1. Entwicklung eines Konzeptes für ein Verfahren zur Resilienzerhöhung von Webanwendungen mit den folgenden Eigenschaften:
   a. Fokussierung auf die Schutzziele Integrität und Verfügbarkeit der Daten im Internet.
   b. Erkennung von Beschädigungen von Inhalten im Internet.
   c. Information des Eigentümers der Inhalte über Beschädigungen
   d. Automatisierte zeitnahe Regeneration von Inhalten.
2. Implementierung des Konzeptes an einem Modellsystem mit den Unterzielen:
   a. Auswahl eines Modellsystems
   b. Bereitstellung der erforderlichen Software.
   c. Erste Tests mit dem Modellsystem
3. Tests mit dem Modellsystem und Ableitung von weiteren Vorgehensweisen.

Forschungsfragen:

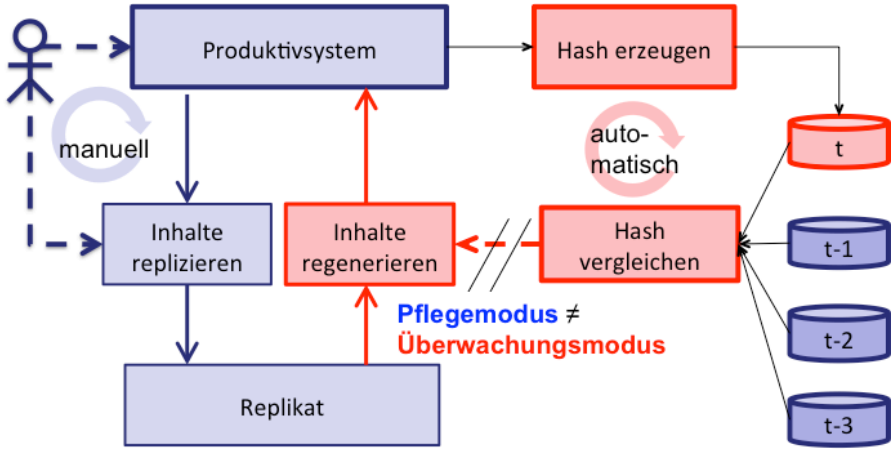
1. Wie kann grundsätzlich ein Verfahren zur Erhöhung der Resilienz von Webanwendungen konzipiert werden?
2. Lässt sich das Verfahren einfach und wenn dann wie in einem Modellsystem implementieren?
3. Für welche Webanwendungen kann die Implementierung beispielhaft sein und wo liegen die Grenzen des Konzeptes?

Vorgehen und Methodik:

Das Vorgehen folgt dem in Deutschland noch vorherrschendem deduktiv-konstruktiven Ansatz der Wirtschaftsinformatik. Um dem technischen Wettlauf gegen potenzielle Angreifer zu entgehen, wurde nicht versucht, ein generisches Verfahren zu finden, um die Schadenseintrittswahrscheinlichkeit zu senken. Vielmehr wird darauf gesetzt, einen Schaden zu erkennen und durch schnelle Wiederherstellung der Inhalte die Schadenshöhe zu senken. Das Konzept wurde aus bewährten Methoden der Business Intelligence abgeleitet.

Konzept

Das Konzept baut auf Regeneration statt Angriffsabwehr. Durch ein periodisch durchgeführtes Prüfverfahren wird festgestellt, ob eine Beschädigung der Inhalte stattgefunden hat. In diesem Fall werden die Produktivinhalte aus einem Replikat automatisch regeneriert. Für den Fall einer gewollten Inhaltsveränderung wird der Regenerationssmechanismus zeitlich begrenzt außer Kraft gesetzt und ein aktuelles Replikat der Inhalte erzeugt.



Implementierung des Konzeptes an einem Modellsystem.

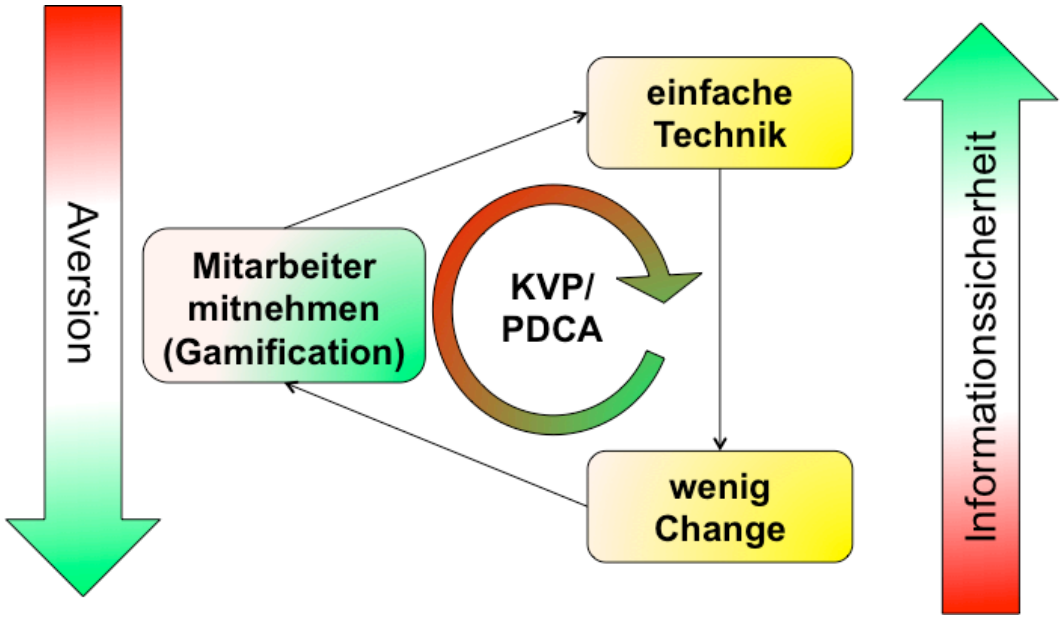
Zur Implementierung des Konzeptes wurde im ersten Schritt ein als CMS genutztes Dokuwiki-System im Internet verwendet und mit einigen PHP-Skripten sowie einem Raspberry Pi als Steuerungsrechner erweitert.

Ergebnis, Fazit und Ausblick:

Es liegt ein einfaches und leicht zu implementierendes Konzept vor, dass es ermöglicht, Webanwendungen mit den Schutzzielen Integrität und Verfügbarkeit sicherer zu machen. Am Modellsystem http://RPiTF.de wurden die Komponenten automatisierte Beschädigungserkennung und Eigentümerbenachrichtigung realisiert und mit Erfolg getestet. Das Modellsystem wies bereits einen Regenerationsmechanismus auf. Die Forschungsfragen konnten somit zufriedenstellend beantwortet werden. Die Implementierung des Konzeptes lässt sich leicht auf andere Gegebenheiten z.B. in KMU anpassen.

Die Grenzen des Konzeptes: Derzeit sind hochinteraktive Webanwendungen noch nicht untersucht, z.B. können Diskussionsforen vermutlich schlecht abgesichert werden. Es liegt weiterer Forschungs- und Entwicklungsbedarf vor. Ebenso wurde noch kein Modellsystem mit einem RDBMS untersucht.

Grundsätzlich kann die Informationssicherheit durch die Kombination von einfacher Technik, wenig Veränderungen für die Mitarbeiter in KMU und Mitnahme von Mitarbeitern in Digitalisierungsprozessen (ggf. Unterstützt durch Gamification) erhöht werden. Die Planung eines Kontinuierlichen Verbesserungsprozesses sollte einem Einführungsprojekt folgen.



Nächste Schritte: Übertragung des Konzeptes auf RDBMS-basierte Systeme (Wordpress u.a.)

Juni 2017

Clavis – Kompetenzzentrum für Informationssicherheit der Hochschule Niederrhein

Fachbereich Wirtschaftswissenschaften, Webschulstraße 41-43, 40165 Mönchengladbach

Bernhard Steffens, B.A., bernhard.steffens@stud.hn.de

Prof. Dr. rer. nat. Claus Brell, claus.brell@hsnr.de, http://claus-brell.de

Unterlagen im Internet:

webbri.cbrell.de