Titel: "Your website has been hacked" – Finding out how website owners were informed about security vulnerabilities on their websites

Abschlussarbeitstyp: Bachelor

Betreuung: Anne Hennig (https://aifb.kit.edu/web/Anne_Hennig)

Forschungsgruppe: Security – Usability – Society (https://secuso.aifb.kit.edu/)

Abschlussarbeitsstatus: offen

Beginn: so bald wie möglich

Weitere Informationen

Background

Nowadays, running a business without having a website is nearly impossible because information about goods and services are mainly retrieved from online resources. Content management systems (CMS) provide default features that make it easy even for laypersons to create and maintain sophisticated websites. But CMSs also pose a security risk. Not only can the CMS's frameworks themselves contain vulnerabilities. Also, there is a vast number of plugins and templates that may introduce vulnerabilities. Those vulnerabilities can be used to induce several attacks.

A specific attack aims at the search results of the original website. In case of search engine Spam (SEO Spam) or Pharma Hacks, an attacker deploys code on a website to redirect to fake web shops. The manipulation is not visible on the genuine website, but in the search engine results. These sites appear as shops selling illegal or banned drugs and medicines, luxurious brand-name clothing, or expensive appliances for cheap. Often, the malicious code is hidden within the CSS files of a website and cannot be easily found - even by skilled developers.

Objectives

We used web crawling results to identify German website owners that were affected by a Pharma Hack or a related SEO spam. With the help of our project partners, we already informed some website owners about the manipulation. But during the course of the project, we also identified several website owners who closed the vulnerability on their own.

The aim of this thesis will be to find out, how those website owners got aware of the manipulation. If they were notified by a third party, we would also like to know how and by whom they were notified and what their feelings were with respect to the notification. To answer these questions, a survey needs to be designed. The survey will then be sent to a

list of website owners who closed the vulnerability on their own. The study should be run as an online survey using for example SosciSurvey.

Important information

Please visit https://secuso.aifb.kit.edu/121.php for our thesis guide and more information on our procedure.