Background. Content management systems (CMS) provide default features that make it easy even for laypersons to create and maintain sophisticated websites [3]. But a CMS also poses a security risk. Not only can the CMS’s framework itself contain vulnerabilities. Also, there is a vast number of plugins and templates that may introduce vulnerabilities [3, 5]. We are looking for websites that are vulnerable to search engine Spam (SEO Spam) or Pharma Hacks, where an attacker deploys code on a website to redirect to fake web shops [11, 12]. The manipulation is not visible on the genuine website, but the sites appear in the search engine results as shops selling illegal or banned drugs / 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 [11].

Aim. Since the problem is not easy to detect and only visible in a website’s search results, most website owners have to rely on vulnerability notifications by the security community to be informed about the manipulation. In trying to create suitable vulnerability notifications, with which we could inform the website owners about the security issues, we conducted 25 semi-structured interviews with affected website owners and discussed the perception of vulnerability notifications with them. To our knowledge, none of the experimental studies on vulnerability notifications [1, 4, 6–9, 13–21] have conducted qualitative interviews with affected website owners, to identify common themes and trust-promoting factors for a vulnerability notification.

The motivation of our work was to answer the following research questions: (1) How did website owners perceive previous web vulnerability notifications? (2) What are suitable senders and communication channels that the website owners deem trustworthy? (3) What aspects should we consider in future notifications to be deemed trustworthy? Finally, by answering these questions, we aimed at designing a vulnerability notification that is suitable to inform website owners about the security issue on their website.

Method. We used web crawling results to identify German website owners that were affected by a Pharma Hack or a related SEO spam in the past. Between July and September 2021, we contacted 65 German website owners via email, and asked, if we could call them for an interview. We used the contact information given on their websites. In our request, we introduced ourselves and announced that we would call them in the upcoming days. We also provided our email address and phone number so the recipients could opt out or verify the legitimacy of our request. We called the website owners at least three times afterwards. In total, 25 persons agreed to an interview (response rate: 39 %).

All interviews were transcribed using verbatim transcription. Any personal data, like names of persons, companies, places, and domain names were anonymized. We used the software MaxQDA to transcribe and code the interviews. To analyze the interviews, we used open coding as described in [2].
Results. As researched by [9], formal and content-related aspects of a notification increase its perceived trustworthiness. We looked at these factors in more detail and could show that especially a clear description of the problem, a clear motivation for the notification, and, if applicable, information to solve the problem should be included in a notification. These factors enable the recipients to verify the problem. Providing contact information (a phone number or email address, a signature, a letterhead, or an imprint) and using a well-known domain in the sender's email address helps recipients to verify the sender. Future notifications should also consider a personalized salutation, correct orthography and a meaningful subject. These factors help recipients to establish a connection to the sender, which, again, helps them to verify the notification.

Two of our interviewees said that although they deemed the initial notification trustworthy, they did not see the severity of the problem and therefore did nothing to remediate the hacking. We, therefore, endorse the suggestions of [9, 10, 16, 18] and highly recommend providing incentives for remediation or name potential negative consequences from inaction since some interviewees underestimated the severity of the problem.

We confirm the findings of [9], that no single factor consistently increases trust. And we can also show that even if a sender itself (like the police) or a notification channel (like email) is deemed suitable, the notification is not automatically deemed trustworthy. Previous research could not clearly identify an effective sender and/or notification channel. We, therefore, conclude that the whole process, composed of sender and notification channel and content of the message must be reasonable and verifiable to establish trust in a notification.

Conclusions. Previous quantitative research found, that the sender of a vulnerability notification and its reputation seems to play an important role (i.a. [9, 13, 17, 21]). But still, the impact of sender, sender reputation or other factors is not entirely clear, since none of these factors was able to increase remediation rates significantly.

In 25 qualitative interviews with affected website owners, we were able to identify common themes concerning vulnerability notifications. With our work, we could verify existing research and, by using semi-structured interviews instead of quantitative surveys, summarize key factors for creating trustworthy vulnerability notifications, and identify less important factors. Key factors for vulnerability notifications are: Providing verification possibilities like a clear motivation and contact information (a phone number or email address, a signature, a letterhead, or an imprint); providing some incentives for remediation; and making the whole notification process plausible to the recipient.

Based on our findings we designed a vulnerability notification that includes a personalized salutation, a clear motivation for the notification, possibilities to verify the problem, further information on the hacking and first information how to remediate it as well as incentives and contact information to verify the sender of the notification. We then recruited three different types of senders, each who can be tied to a different framing: Two hosting provider that can be tied to a technical framing with technical incentives; the German Federal Office for Information Security that can be tied to a reputational framing with reputational incentives; and a university group that can be tied to a neutral framing with no incentives. Each sender is currently sending out vulnerability notifications via e-mail based on our template.

ACKNOWLEDGMENTS

This research is supported by the Federal Ministry of Education and Research, Germany, as part of the BMBF INSPECTION project (Zuwendungsnummer 16KIS1113), and it is supported by funding from the topic Engineering Secure Systems, topic 46.23.01 Methods for Engineering Secure Systems, of the Helmholtz Association (HGF) and by KASTEL Security Research Labs.
POSTER: How to best inform website owners about vulnerabilities on their websites

REFERENCES


