POSTER: How to best inform website owners about vulnerabilities on their websites

ANNE HENNIG, Karlsruhe Institute of Technology, Germany
FABIAN NEUSSER, University of Bamberg, Germany
ALEXSANDRA ALICJA PAWELEK, Karlsruhe Institute of Technology, Germany
DOMINIK HERRMANN, University of Bamberg, Germany
PETER MAYER, Karlsruhe Institute of Technology, Germany

Additional Key Words and Phrases: web security, CMS vulnerabilities, vulnerability notification

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.

REFERENCES

[1] Jan M. Ahrend, Marina Jirotka, and Kevin Jones. 2016. On the Collaborative Practices of Cyber Threat Intelligence Analysts to Develop and Utilize Tacit Threat and Defence Knowledge on Existing Practices, Shortcomings, System Circumventions and Implications for Design. *2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)* (2016), 1–10. https://doi.org/10.1109/cybersa.2016.7503279

[2] John L. Campbell, Charles Quincy, Jordan Osserman, and Ove K. Pedersen. 2013. Coding In-depth Semistructured Interviews: Problems of Unitization and Intercoder Reliability and Agreement. *Sociological Methods & Research* 42, 3 (2013), 294–320. https://doi.org/10.1177/0049124113500475

[3] Cosmin A. Conţu, Eduard C. Popovici, Octavian Fratu, and Mădălina G. Berceanu. 2016. Security issues in most popular content management systems. In *2016 International Conference on Communications (COMM)*. 277–280. https://doi.org/10.1109/iccomm.2016.7528327

[4] Zakir Durumeric, Frank Li, James Kasten, Johanna Amann, Jethro Beekman, Mathias Payer, Nicolas Weaver, David Adrian, Vern Paxson, Michael Bailey, and J Alex Halderman. 2014. The Matter of Heartbleed. In *Proceedings of the 2014 Conference on Internet Measurement Conference, IMC '14 (IMC '14)*. Association for Computing Machinery, Vancouver, BC, Canada, 475–488. https://doi.org/10.1145/2663716.2663755

[5] Ranjita Pai Kasturi, Jonathan Fuller, Yiting Sun, Omar Chabklo, Andres Rodriguez, Jeman Park, and Brendan Saltaformaggio. 2022. Mistrust Plugins You Must: A Large-Scale Study Of Malicious Plugins In WordPress Marketplaces. In *Proceedings of the 31st USENIX Security Symposium*.

[6] Marc Kührer, Thomas Hupperich, Christian Rossow, and Thorsten Holz. 2014. Exit from Hell? Reducing the Impact of Amplification DDoS Attacks. In *23rd USENIX Security Symposium (USENIX Security 14)*.

[7] Frank Li, Zakir Durumeric, Jakub Czyz, Mohammad Karami, Michael Bailey, Damon McCoy, Stefan Savage, and Vern Paxson. 2016. You've Got Vulnerability: Exploring Effective Vulnerability Notifications. In *25th USENIX Security Symposium (USENIX Security 16)*.

[8] Frank Li, Grant Ho, Eric Kuan, Yuan Niu, Lucas Ballard, Kurt Thomas, Elie Bursztein, and Vern Paxson. 2016. Remedying Web Hijacking: Notification Effectiveness and Webmaster Comprehension. In *Proceedings of the 25th International Conference on World Wide Web (WWW '16)*. International World Wide Web Conferences Steering Committee, Montreal, Quebec, Canada, 1009–1019. https://doi.org/10.1145/2872427.2883039

[9] Max Maass, Alina Stöver, Henning Pridöhl, Sebastian Bretthauer, Dominik Herrmann, Matthias Hollick, and Indra Spiecker. 2021. Effective notification campaigns on the web: A matter of Trust, Framing, and Support. In *30th USENIX Security Symposium (USENIX Security 21)*.

[10] Max Maaß, Henning Pridöhl, Dominik Herrmann, and Matthias Hollick. 2021. Best Practices for Notification Studiesfor Security and Privacy Issues on the Internet. In *The 16th International Conference on Availability, Reliability and Security (The 16th International Conference on Availability, Reliability and Security)*. Association for Computing Machinery, Vienna, Austria, 1–10. https://doi.org/10.1145/3465481.3470081

[11] Malcare. 2021. What is WordPress Pharma Hack & How to clean it? https://www.malcare.com/blog/what-is-pharma-hack-how-to-clean-it/

[12] Art Martori. 2020. Spamdexing: What is SEO Spam and How to Remove It. https://blog.sucuri.net/2020/02/spamdexing-seo-spam.html

[13] Ben Stock, Giancarlo Pellegrino, Frank Li, Michael Backes, and Christian Rossow. 2018. Didn't You Hear Me? - Towards More Successful Web Vulnerability Notifications. In *Proceedings of the 25th Annual Symposium on Network and Distributed System Security (NDSS '18)*. 1 – 15. https://doi.org/10.14722/ndss.2018.23171

[14] Ben Stock, Giancarlo Pellegrino, Christian Rossow, Martin Johns, and Michael Backes. 2016. Hey, You Have a Problem: On the Feasibility of Large-Scale Web Vulnerability Notification. In *25th USENIX Security Symposium (USENIX Security 16)*.

[15] StopBadware and Commtouch. 2012. Compromised Websites: An Owner's Perspective. (2012), 1 – 15. https://www.stopbadware.org/files/compromised-websites-an-owners-perspective.pdf

[16] Marie Vasek and Tyler Moore. 2012. Do Malware Reports Expedite Cleanup? An Experimental Study. In *5th Workshop on Cyber Security Experimentation and Test, CSET '12, Bellevue, WA, USA, August 6, 2012*.

[17] Eric Zeng, Frank Li, Emily Stark, Adrienne Porter Felt, and Parisa Tabriz. 2019. Fixing HTTPS Misconfigurations at Scale: An Experiment with Security Notifications. In *The 2019 Workshop on the Economics of Information Security (2019)*. Boston, MA, 1 – 19. https://www.semanticscholar.org/paper/Fixing-HTTPS-Misconfigurations-at-Scale%3A-An-with-Zeng-Li/b22c522c6201f8545e1626deaf6ca43db52444d7

[18] F. O. Çetin, C. Hernandez Ganan, M. T. Korczynski, and M. J. G. van Eeten. 2017. Make notifications great again: learning how to notify in the age of large-scale vulnerability scanning *(16th Workshop on the Economics of Information Security (WEIS 2017))*. San Diego, 1–23. http://resolver.tudelft.nl/uuid:621f4a4f-e5d9-4f04-abc4-46252f9db3db

[19] Orçun Çetin, Lisette Altena, Carlos Gañán, and Michel van Eeten. 2018. Let Me Out! Evaluating the Effectiveness of Quarantining Compromised Users in Walled Gardens. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*.

[20] Orçun Çetin, Carlos Gañán, Lisette Altena, Samaneh Tajalizadehkhoob, and Michel van Eeten. 2019. Tell Me You Fixed It: Evaluating Vulnerability Notifications via Quarantine Network. *2019 IEEE European Symposium on Security and Privacy (EuroS&P)* 00 (2019), 326–339. https://doi.org/10.1109/eurosp.2019.00032

[21] Orçun Çetin, Mohammad Hanif Jhaveri, Carlos Gañán, Michel van Eeten, and Tyler Moore. 2016. Understanding the role of sender reputation in abuse reporting and cleanup. *Journal of Cybersecurity* 2, 1 (2016), 83–98. https://doi.org/10.1093/cybsec/tyw005