Karlsruher Institut für Technologie

SECUSO
SECURITY · USABILITY · SOCIETY

How to best inform website owners about vulnerabilities on their websites

Anne Hennig[1], Fabian Neusser[2], Aleksandra Alicja Pawelek[1], Dominik Herrmann[2], Peter Mayer[1]

[1] Karlsruhe Institute of Technology, [2] University of Bamberg

Motivation and Methodology

Website builder are easy and convenient ways to built a website. But frameworks and plugins can be vulnerable to manipulations. Often, the malicious code is hidden within the website's database and cannot be easily found.

We conducted 25 interviews with German website owners to find out what aspects should be considered in future vulnerability notifications.

Findings

- Providing verification possibilities & creating a plausible notification process are most important
- A clear description of and information how to solve the problem, a plausible motivation, a personalized salutation, & contact information help the recipient to verify the notification
- Providing incentives for remediation helps the recipients to realize the severity of the problem.

Vulnerability Notification

An: <source.email>

Von: Absender

Betreff: Wichtige Informationen zu Ihrer Website <source.fqdn>

<title> <lastname> — personalized salutation

hiermit erhalten Sie eine dringende Mitteilung zu Ihrer Website <source.fqdn>.

Ihre Webseite wurde vermutlich von Dritten manipuliert. Bei einer Analyse der Suchmaschineneinträge sind Unterseiten Ihrer Website entdeckt worden, die allem Anschein nach auf betrügerische Online-Shops weiterleiten. Wahrscheinlich haben sich Dritte über eine Sicherheitslücke Zugriff zu Ihrer Website verschafft. } motivation

Dies können Sie selbst nachvollziehen, indem Sie auf Google im Suchfeld „site:<source.fqdn> <hacking_keyword>“ eingeben. Das Ergebnis zeigt Ihnen alle bei der Suchmaschine bekannten Einträge Ihrer Webseite auf. Für Ihre Seite sind hier Einträge gelistet, die inhaltlich nicht zu Ihrer Domain passen. Beim Anklicken werden Sie auf einen betrügerischen Online-Shop weitergeleitet. } verification possibility: problem

Bitte prüfen Sie welche Sicherheitslücke ausgenutzt wurde und schließen Sie diese. Bereinigen Sie anschließend die eingeschleusten Inhalte. Beachten Sie dabei bitte, dass sich Schadcode oder unerwünschte Weiterleitungen sowohl im Webspace selbst als auch in der Datenbank befinden können. Weitere Information finden Sie unter https://www.web-inspection.de/faq.

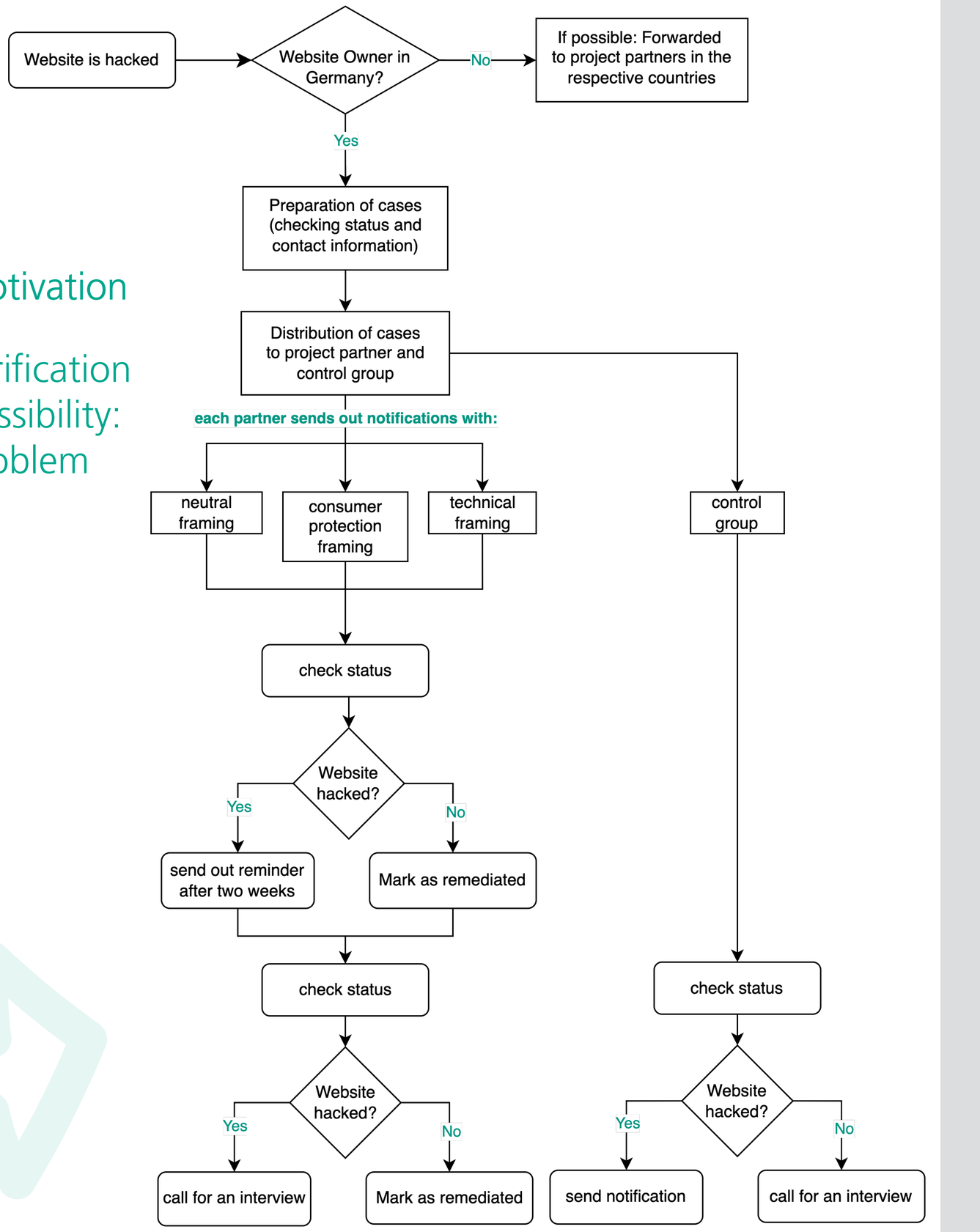
<framing> — incentive

Falls Sie noch Fragen haben, können Sie sich gerne an uns wenden.

Mit freundlichen Grüßen,
<sender>

<signature> — verification possibility: sender

Notification Experiment



Acknowledgements

Bundesministerium für Bildung und Forschung

Industry Partners

BDO

mindUp Web + Intelligence GmbH

aifb KASTEL KD²lab Decision&Design