Web Security and Privacy for Novices – Part 2

Updates, Mail Servers, and E-Commerce

Artur Lupp*, Alexander G. Mirnig* and Manfred Tscheligi†
*Center for Human-Computer Interaction
University of Salzburg, Salzburg, Austria
Email: firstname.lastname@sbg.ac.at
†Center for Human-Computer Interaction &
Austrian Institute Of Technology, Salzburg & Vienna, Austria
Email: firstname.lastname@sbg.ac.at

***Abstract*—This paper is the second part of a series of three thematically connected papers and presents four patterns for nonprofessional web developers. The patterns in this part of the series address updates, setting up and maintaining mail servers and securing a web shop. Starting with a pattern that provides basic information necessary for any type of web presence, while the subsequent patterns provide more in-depth information specializing on specific topics.**

Keywords–Patterns; On-line; Security; Privacy; Novice Users.

I. INTRODUCTION

Never has it been that easy to construct and set up a website. The internet offers a vast amount of easy to use tools and websites that allow nonprofessionals to develop, design and shape a personal web presence. This web presence can then be put online with only a few mouse clicks. Without the proper knowledge about web security and web privacy however, these websites may be turned into a potential threat to the internet community. Poorly set-up and maintained websites can easily be hijacked by cyber criminals. The criminals usually compromise the site in a way, that they start to distribute malware or ransomware to infect the computers of inexperienced users visiting the website.

We created a set of patterns describing common security and privacy issues and how they can be addressed on a high level. This paper constitutes the second part of a series of three thematically connected papers, which describe patterns from the same pattern collection. Paper one contains two meta-patterns and a general description how the patterns were generated and structured. Paper three contains a set of four additional patterns addressing concrete issues (e.g., frequency of backups, data protection compliance, etc.).

In this paper, we will first outline relevant related work from the domains of web privacy and web security focusing on updates, mail servers and the security of web shops. Section II provides a short outline of relevant related work from the aforementioned focus areas. Section III introduces the four patterns with the titles: "When and how often should I install updates?", "Should I set up or operate a mail server myself?", "How should I set up / operate a mail server myself?" and "How do I secure a web shop and what should be taken into consideration?". Section IV concludes this paper.

II. RELATED WORK

Updates are intended to improve previously installed programs. The necessary changes may range from simple and invisible changes, such as bug fixes or improved security patches up to major changes in the user interface, as well as the addition of new functions or changes of already existing features that may affect user workflow. Non-expert users tend to skip updates due to previous negative experiences, e.g., unwanted and unexpected changes in the user interface or annoying "update now" pop-up messages [1]. Skipping updates leads to more compromised computers, even though they could have been protected as security updates were available but had not yet been applied [2]. A more recent Security Intelligence Report from Microsoft [3] shows that the amount of compromised computers is still rising mainly because cyber criminals prefer easy targets, such as novice users and non-experts. It is easier to compromise computers and servers that are not efficiently protected due to missing protection software, security updates or poorly configured environments. Even when a computer, server or website uses protection software and is up-to-date, the exploitation of access control mechanisms with weak passwords is one of the bigger problems. Pearman at al. [4] show that a lot of users reuse passwords when they have to manage a large number of them. Additionally, there is trend to use weak passwords, if the system is allowing the creation and use of them [5].

III. PATTERNS

A. When and how often should I install updates?

Intent: This pattern addresses the topic of updates for software applications and operating systems on the personal computers, as well as on servers. The main aim is to answer when, how often and why updates should be installed in general.

Problem Statement: Keeping software or systems up to date is very important. Systems which are not updated frequently are more vulnerable to attacks from the outside compared to systems that are continuously held up to date.

Scenario: In order to secure your own system and reduce the vulnerabilities attackers may use to get into your system, it is necessary to maintain your system with the newest updates.

Solution: Updates should be installed in **regular intervals**. However, this definition does **not precisely define the actual time period**.

Therefore, we recommend the usage of automatic updates if an application is offering this feature. Important security-related programs (e.g., anti-virus software or operating systems) should be checked for updates on a daily basis. While,

 ISBN: 978-1-61208-708-5

for all other installed programs its sufficient to check for updates on a weekly or monthly basis.

Before the installation of any kind of update, we recommend to create a system backup for safetys sake.

In unfavorable cases, updates may lead to problems or incompatibilities. Especially major updates or version jumps in programs may be irreversible. Therefore, it is advised to plan ahead and calculate some time to test the system thoroughly after after bigger version jumps, upgrades and updates. More about backups can be found in pattern: When and how should I create backups? [6].

- It is recommended to keep **systems and software up-to-date from the beginning**.
  - Up-to-date means, that all (primarily security-relevant) updates for a system or software currently available are installed.
- Systems, software or websites working with **sensitive data** have **higher priority**.
  - It is recommended to check for updates on a daily basis. This applies to systems and computers accessing the web server and the applications running on the server. This point is especially important, if the website is working with personal or sensitive data (account data, addresses, etc.).
  - Usually, the hosting provider takes care core application updates (e.g., operating system, mySQL, PHP, etc.).
- Establishing of an **update day** is recommended. For example, **once a month** for the whole system or **once a week or day** for systems or applications that **handle important or personal data**.
- Automated updates are recommended, but you should also look **manually** regularly **(once a week)**.
  - In certain cases, it is possible that an automatic update messes up the automatic update function. In this case, manual updates are the way to go.
- Set up an information network which informs you about update releases. A couple of software and hardware providers offer mailing lists and info websites for that purpose.

In case certain software is not being updated anymore, it is advisable to look for alternatives that are kept up to date.

Examples: Automated Updates - At certain time intervals (e.g., hourly, daily or weekly), the system automatically searches for updates.

Patch Day - On a patch day, all updates currently available will be applied at a previous determined fixed day (e.g., once a week or once a month). The updates are usually tested on a separate system before being applied onto the main system, in order to eliminate any problems and / or compatibility issues.

Software Update Strategies - Create your own update strategy. Set up a schedule for update checking and deployment. This allows you to have a complete overview to when and if an update was deployed, which program the update was for and whether a certain machine already received an update.

WordPress update - WordPress offers two ways of updating the core application. The first option is the automatic update function and the second is the manual update.

- To utilize the automatic update function of WordPress, go to the WordPress Admin Panel and select ”Updates” on the left sidebar. In case that the WordPress version was installed with the default settings, you can also access this update function directly using the following url:www.example.com/wp-admin/update-core.php (replace example.com with your own url). This page shows you the currently available updates for the WordPress core installation, plugins, translations and themes. If updates are available, they can be applied by clicking the update button for the corresponding application or component.
- In order to update WordPress manually, please refer to the instructions provided on this page: Manually Update WordPress [ger].

Important Mailing Lists - The article linked below, offers interesting facts regarding updates. Furthermore, it provides important mailing lists at the end of the article: Important Mailinglists [7].

Additional mailing lists and more information can be found here: Additional Links, Mailinglists and Newsgroups [8].

References

D. L. Parnas, Software aging, Proceedings of 16th International Conference on Software Engineering, Sorrento, 1994, pp. 279-287. [9]

Bellissimo, Anthony, John Burgess, and Kevin Fu. Secure Software Updates: Disappointments and New Challenges. HotSec. 2006. [10]

Understanding Patch and Update Management: Microsofts Software Update Strategy [11]

Apple security updates [12]

SCCM Software updates Strategy [13]

Why updating your Software is a Must Do [14]

WordPress Security Category Archive [15]

Keywords

Updates, Security, Software, Backups

B. Should I set up or operate a mail server myself?

Intent: This pattern aims to help users to make a decision whether they should run their own mail server or not.

Problem Statement: The administration and maintenance of a mail server complicated and unfortunately often underrated. There are a vast amount of guides on the internet, that aim to explain how to set up a mail server. However, setting up, running and maintaining a mail server requires a lot of specialist knowledge. Unfortunately, laymen do not or only insufficiently possess this kind of knowledge.

Scenario: Sufficient web space and a domain were acquired. The page is now online. For obvious reasons, it seems like a good idea to get mail addresses matching your domain by setting up a mail server by yourself. But is that a good idea?

 ISBN: 978-1-61208-708-5

Solution

Operating and maintaining Mail servers is a complex task. If you are unsure whether you have the skills or not, don not risk anything and leave it to professionals.

The following points should be considered before the decision, whether it makes sense to operate your own mail server:

- **The optimal setup of a mail server is complicated.**
  - It is deceptively easy to set up a mail server. Myriads of guides and a hand full of easy to use applications can be found online. Unfortunately the security aspect is neglected in many of these guides, as it is time consuming and complicated.
  - Setting up a mail server requires expertise and certain knowledge of UNIX systems.
  - The default settings are definitely neither the best, nor are they recommended! Running a mail server using the default setting should be avoided at all costs!
- **Set-up a spam filter.**
  - A spam filter reduces the number of spam emails that would otherwise end up in users' mailboxes.
  - Spam filters should always be adjusted very carefully. Additionally, the filter needs readjustments every now and then, as the content of the spam emails will change over time. Setting up a good and reliable spam filter is very time consuming.
- **Antivirus Software**
  - Emails, especially with attachments should always be checked by an antivirus software before redirecting them to the receiver.
  - Security mechanisms like this have to be installed and adjusted. Additionally, they need to be kept up-to-date in order to do their work.
- **Offering webmail access.**
  - Usually, users want to retrieve their emails not only through a software. A web platform might be mandatory.
  - This web platform (usually, a piece of software installed on a webserver, e.g., roundcube [16]) has to hosted and adjusted.
  - This software has to be kept up-to-date. Backups and the maintenance are mandatory.
- **Blacklisting.**
  - The main task of a mail server is to send emails to the addressed receivers. This might not be possible if your own mail server is on a blacklist. Blacklisted mail servers usually fail to deliver the messages, as they will be blocked by the mail server at the receivers end.
  - Once a mail server is on a blacklist, removing it from the list might take a while.
  - A mail server is blacklisted in case it is used to send out spam mails. This usually happens when the mail server is compromised due to incorrect or faulty configuration.
- **Time consuming maintenance.**
  - Backups are mandatory and data recovery must be guaranteed.
  - All updates must be tested in advance.
    - Even the smallest changes can render the mail server dysfunctional.
  - Finding a problem in case the server is malfunctioning, is difficult.
    - Assuming that emails can no longer be received by other users; where should you start to look for the problem?

These are just but a few of many issues, illustrating how **complex** the operation and maintenance of a mail server is. Please consider whether it is worth the risk and the time hosting a mail server by yourself. There are a lot of companies offering low-priced email services with included maintenance, antivirus checks and spam filters.

The easiest and safe way to a mail server is though a email service provider!

Examples

Comparison of Mail Servers: The following link provides a comparison of mail servers (e.g., mail transfer agents, mail delivery agents, and other related software proving e-mail services):

https://en.wikipedia.org/wiki/Comparison_of_mail_servers

References

Roundcube - Free and Open Source Web mail Software [16]

Why You May Not Want To Run Your Own Mail Server [17]

Keywords

Mail Server, Security, Blacklist

C. How should I set up / operate a mail server myself?

Intent: This pattern elucidates the available options to secure your own mail server.

Problem Statement: Secure communication and data integrity are very important and highly valued in digital communications. Imagine that your email end up in the recipient's spam folder, or even worse, it will be blocked by the recipients mail server before it even reaches the in box. Whether your mails will be blocked before they reach the destination or not, is usually decided by the security and configuration of your own mail server.

Scenario: An mail address using the domain name should has to be set up by you. How can you set it up a secure mail service on your own server?

Solution: **Before you start to setting up your own mail server, please read the pattern Should I set up or operate a mail server myself?" [18]. Setting up and running a mail server is time consuming and complex.**

Definition of Terms - **SMTP** is the acronym for Simple Mail Transfer Protocol. This protocol is used to send or receive emails from different mail servers. **IMAP** and **POP3** are transmission protocols used to retrieve emails from a mail server.

In case a mail software is already installed on the server, step 1 can be skipped.

1. Install an email software application on the server - Independent of the mail application which will be used, following points need to be clarified in advance:

 ISBN: 978-1-61208-708-5

- Check whether your server meets the requirements for the software you intend to use.
  - Only one SMTP application per server is recommended.
- Pay attention to possible incompatibilities.
  - Remove previous SMTP applications completely, before installing a new one.
- Use only SMTP applications that are general available.
  - Applications handling any kind of communication should always be kept up-to-date.

It is recommended to use the IMAP protocol when retrieving the emails from the mail server. IMAP synchronizes the client (mail program on the smartphone or computer) with the server, when the client connects to the server. This synchronization allows other devices and applications to catch up to the most recent status. Therefore, you will not see already read emails as unread.

2. Securing the mail server -

Following points should always be kept in mind:

- **NEVER** use the default settings when setting up or securing a mail server.
- Immediately change the default passwords.
- Change passwords in regular intervals (especially admin accounts).
  - More information regarding passwords can be found in the pattern "How do I secure a web shop and what should be taken into consideration?" [19] please refer to the sections "Solution" and "Examples".
- All settings, configurations and functions should be tested **before** applying them.
- The functionality and security of the mail server has to be tested regularly.

After installing the mail server - please check your configuration and adjust the options as listed below to increase the security:

- Activate Secure Sockets Layer (SSL) / Transport Layer Security (TLS) encryption.
- Deactivate SSLv2 and SSLv3.
- Activate SMTP-AUTH.
- Activate TSL encryption for incoming and outgoing emails.
- Reduce the number of possible connections to mitigate DDoS attacks.
- Decrease the number of failed login attempts.
- Use DNS-blacklists to intercept spam mails.
- Use reverse DNS LookUp to verify the sender.
- Activate SPF (Sender Policy Framework).
- Create local blacklists. In case it is necessary to block IP-addresses manually.

Examples: A good guide for setting up a mail server

- https://workaround.org/ispmail

rspam Anti Spam Tool

- https://www.openhub.net/p/10349

Install Postfix on RedHat

- https://tecadmin.net/install-and-configure-postfix-on-centos-redhat/

Install Postfix on Ubuntu

- https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-postfix-on-ubuntu-16-04

Secure Postfix with Lets Encrypt (SSL)

- https://www.upcloud.com/support/secure-postfix-using-lets-encrypt/

Additional guide for setting up a mail server with Postfix

- https://www.codeproject.com/Articles/847650/How-to-Install-Configure-Email-Server-with-Postfix

SMTP authentication for Postfix

- http://postfix.state-of-mind.de/patrick.koetter/smtpauth/smtp_auth_mailclients.html

DNS-Blacklist in Postfix

- https://docs.iredmail.org/enable.dnsbl.html

Further configuration examples and improvements for Postfix

- http://www.postfix.org/TUNING_README.html

SSL/TLS Encryption

- Pattern "How do I encrypt the communication with my website?" [20] explains how to acquire an SSL/TLS certificate. This certificate can also be used for the encryption of your email transfer. However, in order to use the same certificate make sure, that the mail server is using the same domain (e.g., example.com) as your website and not a sub domain (e.g., mail.example.com)
- Change DNS MX entry (record) of the mail application from @mail.example.com to @example.com in order to get it working.

SMTP diagnostic tool to test your own SMTP configuration - https://mxtoolbox.com/diagnostic.aspx

References

https://www.upcloud.com/support/secure-postfix-using-lets-encrypt/

https://webmasters.stackexchange.com/questions/83442/single-ssl-certificate-for-web-and-email

https://wiki.archlinux.org/index.php/Virtual_user_mail_system

https://workaround.org/ispmail/jessie

https://www.howtoforge.com/effective_mail_server_defense

https://www.syn-flut.de/mit-postfix-spam-blockieren

https://blog.returnpath.com/blacklist-basics-the-top-email-blacklists-you-need-to-know-v2/

https://www.alienvault.com/blogs/security-essentials/basic-best-practices-for-configuring-email-servers

https://www.linode.com/docs/email/postfix/postfix-smtp-debian7/

http://www.postfix.org/BASIC_CONFIGURATION_README.html

Keywords

eMail, Mail Server, Security, SMTP, POP3, IMAP

 ISBN: 978-1-61208-708-5

D. How do I secure a web shop and what should be taken into consideration?

Intent: This pattern explains which aspects you need to keep in mind if you want to designing a good web shop focusing on security.

Problem Statement: Online shopping is getting more and more important. With its growth, the number of users accounts on e-commerce platforms exploded. Nowadays web shops, e-commerce places and other web presences with a lot of users are popular target for cyber criminals.

Scenario: Creating and setting up an online shop is quite simple with the right guides. Keeping the website and customer data safe however, can be challenging. Storing customer data safe and secure should be the highest priority!

Solution

Maintaining and operating an online shop is a lot of work. The recently introduced EU GDPR has strengthened the rights of customers. Thus, if you want to avoid any problems especially legal ones - consider to consult a professional web developer for the creation and maintenance of a web shop.

Attention: This pattern is not a legal advice! We addressed the GDPR (https://www.dsb.gv.at/gesetze-in-osterreich [ger]) and applicable data protection regulations during our research for the patterns, however, we are no legal advisors, nor are we lawyers or privacy experts. We shall not have any liability whatsoever for the accuracy, completeness, timeliness, or correct sequencing of the provided information.

If you still want to run a web shop by yourself after this warning, please pay attention to the following points:

GDPR - As the owner and operator of a web shop, you have to design and set up the shop in a GDPR compliant way. Some of the changes are simple and require only the addition of business information and contact details on your site, other changes may be technically more challenging. Please consider visiting this side https://www.wko.at/service/wirtschaftsrecht-gewerberecht/AGB_im_Internet_-_im_Detail.html [ger] in order to get informed on what information you have to provide to your visitors to be GDPR compliant.

Encrypted Communication - It is absolutely necessary to encrypt the communication with your web shop. Especially if you offer direct payment options on your site. The encrypted communication is used to ensure data integrity.

Data and System Security - The GDPR requires you to keep your system up-to-date! The data security on the systems has to be guaranteed.

Shop certificates and quality seals - Shop certificates and seals of approval create trust in the web shop. These certificates suggest the customer, that the web shop meets certain quality standards (e.g., data security, etc.). Many trusted certificate or seal of approval providers check the website and the associated system, before they evaluate them. Depending on different factors, they decide whether the web shop is worthy of receiving a seal of approval or a trusted certificate.

Secure Passwords - Most of the time users are required to create an account, before they can order from a web shop. During the account creation process, they usually have to pick a password. It is recommended to aid the users during the password creation process, persuading them to use stronger passwords. Recent studies show a longer password (8 characters or more) is much more secure than a password with less characters (even when they are using special characters).

The following rules can be set as an requirement to persuade users to create a stronger password:

- The password should contain at least one uppercase and lowercase character.
- One special character is required.
  - , (,), =, !, etc.
- Avoid simple words, birthday dates, names or repeated letter sequences, such as:
  - asdfasdf, 123456, Heinz1, 12.10.2019, 121212, Superman
- Minimum length should be 8 characters.

Examples

Safety Aspects - How to set up an SSL/TLS encrypted communication on a website is explained in the pattern "How do I encrypt the communication with my website?" [20]. As a web shop works with personal data (e.g., names, addresses, banking information, etc.) the safety of this data has to be assured. The following patterns explain how to assure this: What contributes to the security of a website? [21], When and how should I create backups? [6], How do I store data securely? [22], Which data am I allowed to save? [23], and What information do I have to provide to visitors of my website? [24].

A List of Providers for Trust Certificates and Seals of Approval

- https://www.trustedshops.at
- https://www.tuev-sued.de/fokus-themen/it-security/safer-shopping/onlinehaendler
- https://www.datenschutz-cert.de/ips-internet-privacy-standards.html
- https://ehi-siegel.de

Data Informative - The GDPR gives individuals a right to be informed about the collection and use of their personal data. If a user requests his personal data, the operator of the site has to provide the request information within one month. More Information concerning this topic can be found here: https://www.dsb.gv.at/fragen-und-antworten#Wie_beantworte_ich_ein_Auskunftsersuchen_

Password meter for secure passwords - The following Figures 123 show a password meter indicating the strength / security of a password depending on length, characters used and complexity. Figure 1 uses a password with more than the required six characters, however it is considered weak due to lack of complexity or the use of repeated strings, such as "abcdabcd". The approach in Figure 2 is better compared to the password shown in Figure 1, thus, it can be considered as a medium strength password. Even though the password is shorter, it may contain numbers apart from standard characters, making dictionary attacks more difficult. Figure 3 displays how a password meter would indicate the use of a strong password. A strong password should be at least 8 characters long, containing uppercase and lowercase characters, as well as numbers and special characters if possible.

 ISBN: 978-1-61208-708-5

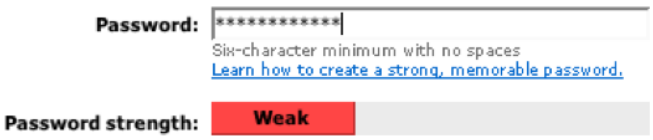

Figure 1. Password strength comparison - weak

weak

Figure 1 indicates that the password is longer than the required 6 characters, but a repeated string may have been selected (e.g., ”asdfasdf”), making the password less secure.

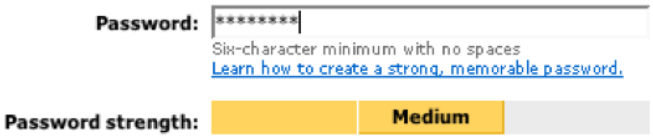

Figure 2. Password strength comparison - medium

medium

In Figure 2, the password is shorter compared to Figure 1. However, it meets the minimum of the required 6 characters. Since it meets the requirements and probably uses numbers apart from characters it is considered more secure but not overwhelmingly safe.

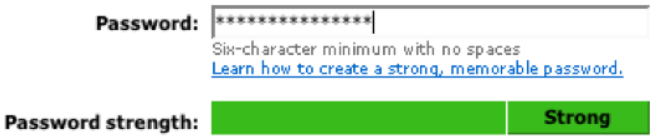

Figure 3. Password strength comparison - strong

strong

Figure 3 shows a much longer password using more characters as required and therefore, the most secure password out of the three shown examples.

References

86% of Passwords are Terrible (and Other Statistics) [25]

Wirtschaftsrecht/Gewerberecht Muster für den Bestellablauf - Info der WKO Datenschutzbehörde Österreich [26]

Keywords

GDPR, Data Privacy, Personal Data

IV. Conclusion

The patterns presented in this paper are interdependent and based on one another. The first pattern explains the necessity of updates for secure systems and offers recommendations for handling the update routine. This knowledge is the basis for the subsequent patterns in this work, addressing the set up / operation of a mail server, as well as security improvement of web shops, as they rely on safe, secure and up-to-date systems in order to keep the personal data of potential users safe and secure. While these patterns can address only a fraction of possible problems and questions that may occur during web development, they selected the most common ones, with the aim to provide applicable solutions and examples for them. Future work will focus on the extension of the problem list, while keeping the existing patterns updated to ensure the validity and usability.

Acknowledgment

The financial support by the Internet Privatstiftung Austria (IPA) under the program “netidee” with the title “SecPatt” under grant number 2390 is gratefully acknowledged.

References

[1] K. E. Vaniea, E. Rader, and R. Wash, “Betrayed by updates,” Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI ’14, 2014, doi: 10.1145/2556288.2557275.

[2] Microsoft, “Microsoft Security Intelligence Report, Volume 13, January through June 2012.” https://www.microsoft.com/en-us/download/details.aspx?id=34955, 2018 (retrieved April 10, 2019).

[3] Microsoft, “Microsoft Security Intelligence Report, Volume 23, March 2018.” https://info.microsoft.com/rs/157-GQE-382/images/EN-US_CNTNT-eBook-SIR-volume-23_March2018.pdf, 2018 (retrieved April 10, 2019).

[4] S. Pearman, J. Thomas, P. E. Naeini, H. Habib, L. Bauer, N. Christin, L. F. Cranor, S. Egelman, and A. Forget, “Let’s go in for a closer look: Observing passwords in their natural habitat,” in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, ser. CCS ’17. New York, NY, USA: ACM, 2017, pp. 295–310, doi: 10.1145/3133956.3133973.

[5] J. A. Cazier and B. D. Medlin, “Password security: An empirical investigation into e-commerce passwords and their crack times,” Information Systems Security, vol. 15, no. 6, 2006, pp. 45–55, doi: 10.1080/10658980601051318.

[6] SecPatt, “When and how should I create backups? [ger],” https://www.secpatt.at/patterns/pt_6/, 2018 (retrieved April 10, 2019).

[7] “Important Mailinglists [ger],” http://www.linux-magazin.de/ausgaben/2004/08/keine-wissensluecke/, 2004 (retrieved April 10, 2019).

[8] “Additional Links, Mailinglists and Newsgroups [ger],” http://www.netzmafia.de/skripten/sicherheit/sicher9.html, 2002 (retrieved April 10, 2019).

[9] D. L. Parnas, “Software aging,” in Proceedings of the 16th International Conference on Software Engineering, ser. ICSE ’94. Los Alamitos, CA, USA: IEEE Computer Society Press, 1994, pp. 279–287, http://dl.acm.org/citation.cfm?id=257734.257788 (retrieved April 10, 2019).

[10] A. Bellissimo, J. Burgess, and K. Fu, “Secure software updates: Disappointments and new challenges,” in Proceedings of the 1st USENIX Workshop on Hot Topics in Security, ser. HOTSEC’06. Berkeley, CA, USA: USENIX Association, 2006, pp. 7–7, http://dl.acm.org/citation.cfm?id=1268476.1268483 (retrieved April 10, 2019).

[11] Microsoft, “Understanding Patch and Update Management: Microsofts Software Update Strategy,” https://technet.microsoft.com/en-us/library/cc768045.aspx, 2003 (retrieved April 10, 2019).

[12] “Apple security updates,” https://support.apple.com/en-us/HT201222, 2019 (retrieved April 10, 2019).

[13] “SCCM Software updates Strategy,” http://www.sccm.ie/how-to/8-sccm-software-updates-strategy, (retrieved April 10, 2019).

[14] “Why updating your Software is a Must Do,” https://www.techlicious.com/tip/why-you-should-update-software-when-prompted/, 2012 (retrieved April 10, 2019).

[15] “WordPress Security Category Archive,” https://wordpress.org/news/category/security/, 2019 (retrieved April 10, 2019).

[16] “Roundcube - Free and Open Source Web mail Software,” https://roundcube.net, 2018 (retrieved April 10, 2019).

 ISBN: 978-1-61208-708-5

[17] "Why You May Not Want To Run Your Own Mail Server," https://www.digitalocean.com/community/tutorials/why-you-may-not-want-to-run-your-own-mail-server, 2014 (retrieved April 10, 2019).

[18] SecPatt, "Should I set up or operate a mail server myself? [ger]," https://www.secpatt.at/patterns/pt_14/, 2018 (retrieved April 10, 2019).

[19] SecPatt, "How do I secure a web shop and what should be taken into consideration? [ger]," https://www.secpatt.at/patterns/pt_10/, 2018 (retrieved April 10, 2019).

[20] SecPatt, "How do I encrypt the communication with my website? [ger]," https://www.secpatt.at/patterns/pt_4/, 2018 (retrieved April 10, 2019).

[21] SecPatt, "What contributes to the security of a website? [ger]," https://www.secpatt.at/patterns/pt_3/, 2018 (retrieved April 10, 2019).

[22] SecPatt, "How do I store data securely? [ger]," https://www.secpatt.at/patterns/pt_8/, 2018 (retrieved April 10, 2019).

[23] SecPatt, "Which data am I allowed to save? [ger]," https://www.secpatt.at/patterns/pt_9/, 2018 (retrieved April 10, 2019).

[24] SecPatt, "What information do I have to provide to visitors of my website? [ger]," https://www.secpatt.at/patterns/pt_12/, 2018 (retrieved April 10, 2019).

[25] "86% of Passwords are Terrible (and Other Statistics)," https://www.troyhunt.com/86-of-passwords-are-terrible-and-other-statistics/, 2018 (retrieved April 10, 2019).

[26] "Wirtschaftsrecht / Gewerberecht Muster für den Bestellablauf - Info der WKO Datenschutzbehörde Österreich," https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Webshop__In_7_Schritten_zur_Bestellung.html, 2019 (retrieved April 10, 2019).

 ISBN: 978-1-61208-708-5