SME Free Web Security Health Check Pilot Scheme (2016)

Final Report

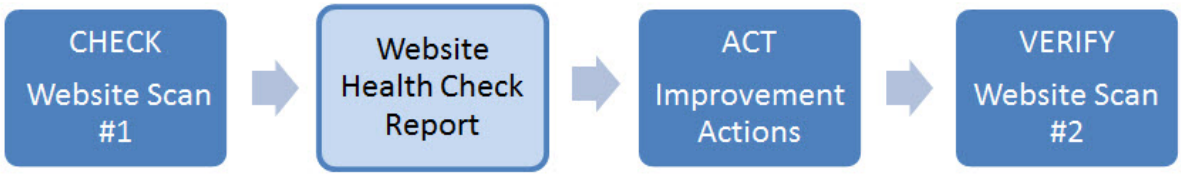
HKCERT

November 2016

1. Background and Objective

Website is an important tool for businesses to promote service, handle customer relationship management and provide online transaction services. However, some enterprises, especially Small Medium Enterprises (SMEs) do not possess resources to secure the websites.

To promote the best practice of "Check-Act-Verify" approach for website security health check to the SMEs of Hong Kong, the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), operated by Hong Kong Productivity Council (HKPC) organizes the "**SME Free Web Security Health Check Pilot Scheme**" project to promote good practice in web security.



1.1 Scheme Details

- The scheme called for participants from Jan 2016, through trade associations, SME One and HKCERT website (https://www.hkcert.org/smewebscan).
- The applicants must own a website, and they need to commit to allocating resources on scanning activities and follow-up.
- The "health check" is based on the result of "vulnerability scanning", i.e. discovering the security weakness of the websites (but no intrusive penetration testing), using vulnerability testing solution Rapid7 Nexpose. The result is organized and analyzed according to "OWASP Top 10" web application vulnerabilities.
- 2 rounds of scanning are arranged for participants. Report with advice is delivered after 1st round completed, so that the participant can arrange vulnerability fixing and any other security improvement actions. Then 2nd round of scanning is conducted and a comparison report is delivered to comparing any improvement on the website security.
- The report contains the following information:
    - Website vulnerability severity levels
    - Classify vulnerabilities into 6 types
    - Business impacts
    - Titles of vulnerabilities found
    - Remediation advice for technical staff to fix problems

1.2 Timeline

Jan	Scheme announced Application started (1st phase) 1st round of scanning started
Mar	Due for application (1st phase)
Apr	Application started (2nd phase)
May	Due for application (2nd phase) 1st round of scanning completed
Jun - Jul	Reports on 1st round delivered to participants
Aug	Seminar to announce 1st round result
Sep	2nd round of scanning started
Oct	2nd round of scanning completed
Nov	Reports on 2nd round delivered to participants Report and seminar to announce overall result

2. Acknowledgement

We would like to express our sincere thanks to the following organizations on co-organizing the scheme and promoting to their members:

- The Chinese Manufacturers' Association of Hong Kong
- Federation of Hong Kong Industries
- Hong Kong General Chamber of Commerce
- Hong Kong Small and Medium Enterprises Association
- SME One, HKPC

We would also like to express our sincere thanks to our technology partners on providing the tools for vulnerability scanning and report generation:

- Rapid7
- Wise Key

3. Result and Observation

Out of 35 applicants, 30 of them have gone through in the scanning, and 26 of them have responded to the survey. The following result and observation are based on their response.

3.1 Participant Profile

Here is the industry distribution of the participants:

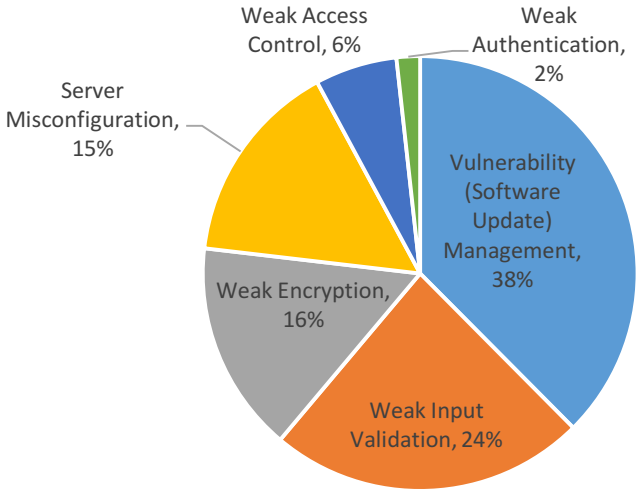
Industry	Count	% of total 26
Manufacturing	5	19%
Wholesale / Retail	5	19%
Import / Export Trades	3	12%
Information Technology	3	12%
Legal / Accounting / Marketing / Business Service / Consultancy	2	8%
Others	2	8%
Personal Beauty / Fitness	2	8%
Banking / Finance / Insurance / Securities	1	4%
Community & Social Services	1	4%
Construction / Architecture / Decoration	1	4%
Media / Publication	1	4%

3.2 Business values of your website

Business value of website (can select more than 1)	Count	% of total 26
Showcase goods/services/work	21	81%
Customer can use service via website	13	50%
Provide online purchase	**9**	**35%**
Save time and cost	9	35%
Retain customer loyalty	7	27%
Global customers access 24/7	7	27%

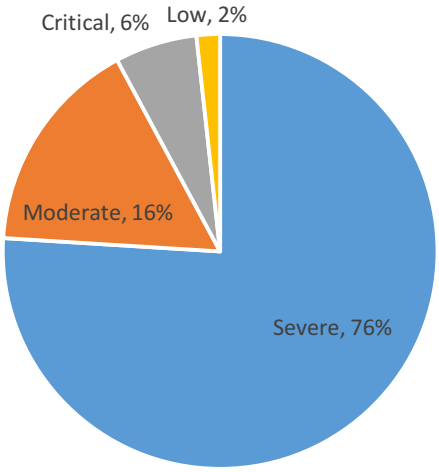
Remarks: We can see that though there is 35% of participants providing online purchase through their websites, many of others mainly make use of website for promotion. When observing the most common types of vulnerabilities found in their websites (refer to 3.3), we worry that many companies have the misconception that “websites for promotion purpose need no patch and maintenance”.

3.3 Distribution of vulnerability classification



Remarks: It can be seen that "vulnerability management (i.e. no patching on systems and applications) vulnerability was mostly found in all websites. Patching is most critical to website security, since cybercriminals usually target websites which are not kept updated of patches. With latest security patch applied, the time and cost to break into your websites will be much higher.

3.4 Distribution of vulnerability severity levels



Remarks: The severity levels follow the levels of Common Vulnerability Scoring System (CVSS) scores, which aim to classify the severity level of software vulnerabilities. It showed that most websites contain 'critical' and 'severe' vulnerabilities which require immediate handling. The severity level can also indicate the priority of handling, i.e. patch 'critical' and 'severe' vulnerabilities first and then others.

3.5 Participant industry vs number of vulnerabilities found

Industry	Count	# companies	Average
Wholesale / Retail	59	5	**11.8**
Manufacturing	35	5	7.0
Import / Export Trades	16	3	5.3
Legal / Accounting / Marketing / Business Service / Consultancy	15	2	7.5
Information Technology	13	3	4.3
Community & Social Services	10	1	**10.0**
Construction / Architecture / Decoration	10	1	**10.0**
Others	8	2	4.0
Personal Beauty / Fitness	7	2	3.5
Banking / Finance / Insurance / Securities	3	1	3.0
Media / Publication	1	1	1.0

Remarks: When counting the average number of vulnerabilities for each industry, the top 3 are wholesale/retail, community & social services and construction/architecture/decoration.

3.6 Online transactions vs number of vulnerabilities

Classification of vulnerabilities	Provide online transaction (9)		No online transaction (17)	
	Total	Average	Total	Average
Vulnerability (Software Update) Management	75	**8.3**	11	0.6
Weak Input Validation	40	**4.4**	14	0.8
Server Misconfiguration	18	**2.0**	17	1.0
Weak Encryption	14	**1.6**	22	1.3
Weak Access Control	12	**1.3**	2	0.1
Weak Authentication	2	**0.2**	2	0.1

Remarks: Websites providing online transactions (9 out of 26) may need more features enabled in the web server and web applications, their average number of overall vulnerabilities is higher.

3.7 Comparison with the round of 1st scanning

Comparison with the 1st round	Count	% of total 26
Not participated in 2nd scan	**2**	**8%**
No vulnerabilities fixed	**13**	**50%**
Fixed some of vulnerabilities	7	27%
Fixed all vulnerabilities	4	15%

Remarks: There are more than 50% of participants who could not allocate resources on 2nd scanning or fixing any vulnerabilities. This is what we worry: we hope participants could consider to spend resources on securing their websites through our scheme.

4. Conclusion and preventive measures

There is a misconception that website with no sensitive data is not worth breaching. From the statistics of the incidents handled by HKCERT, we can surely tell that most of websites breached are not for stealing data but for the websites themselves. Websites themselves are valuable resources for cybercriminals, who can make use of your website to reach more potential victims (e.g. infect your visitors with malware), or use the websites to launch DDoS attack to others.

Even though your website has no data for stealing, when your websites are involved in the attacks, they could be blacklisted, which in turn affect your business operations and communications (e.g. your email under your website domain blacklisted). If your visitors were infected by visiting your websites, you may even face lawsuit for the liability of damages caused. So website security is not only essential to your data security and business reputation, but also critical to your operation and even financial aspect.

Here are the preventive measures suggested for securing your websites:

1. Assessment:
    a. Perform website scanning regularly.
    b. Ensure that the assessment is based on credited standard, e.g. OWASP Top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project), PCI DSS (https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_eCommerce_Guidelines.pdf).
    c. After scanning your websites, please do follow up with 'remediation advice' in the scanning result to fix the vulnerabilities.
    d. Please understand the limitations of web hosting company on follow-up (e.g. shared hosting). If there is something out of your control, you should ask for their assistance.
2. Infrastructure:
    a. Ensure that hosting company can guarantee to provide secure features, e.g. regular patch, secure WordPress/Joomla hosting, secure shopping cart, encryption etc.
    b. Implement web application firewall (but not to confuse with network firewall).
    c. Consider migrating to cloud services if the web hosting company cannot provide enough security protection, as cloud services may allow you to implement more suitable and customized security protections for your website.
3. Detection:
    a. Google Webmasters tools provide useful features for your to monitor your websites and recovery (https://developers.google.com/webmasters/hacked/).
    b. Make use of online reputation checking tool (e.g. http://mxtoolbox.com/blacklists.aspx).
4. User:
    a. Maintain basic security of user workstations and devices, e.g. regular security updates of OS and software, install security protection application.
    b. If users can manage website at home, their private devices should also get basic security protection.
5. Website:
    a. Regular patch, update and vulnerability scanning of web server.
    b. For web applications such as content management system (CMS) and eCommerce, they may need specific tool for security checking. Consult the vendor of these applications for any suitable tools.
    c. Regular offline backup.
6. Prepare for emergency:
    a. Evaluate how critical is your website to your business. If your business cannot operate with the website, you should have a business contingency plan on any website problem.
    b. Drill for website down/breached.
    c. Provide reachable contact on website/WHOIS so that organizations like HKCERT can contact you if your site was found breached.
7. If your website does not function any more, remove it completely (note: you may need to keep the domain).