Website Security in Vietnam

Survey Results and Best Practices

Prepared by:
Jim Fitzsimmons
MF8 International

a research project of TRG International and MF8 International
About Survey Respondents (17 Total)

**What Best Describes Your Company?**
- Non-governmental organisation or charity: 6.3%
- Privately owned company in Vietnam: 18.8%
- Privately owned company (outside of Vietnam): 12.5%
- Joint venture: 37.5%
- Publicly traded company (outside of Vietnam): 18.8%
- Publicly traded company (in Vietnam): 6.3%

**Number of Employees**
- 1-20 employees: 33.3%
- 21-200 employees: 46.7%
- 1000+ employees: 6.7%
- 201-500 employees: 6.7%

**What is the Website's Purpose?**
- Community news, information and comments/forum for a group of people: 18.8%
- Company description: information about the company and services, contact us...: 6.3%
- E-commerce: take orders and possibly payments for goods and/or services for...: 6.3%
- Company service: online banking, online bill pay, online acco...: 68.0%
Different Websites, Different Risks & Threats

- Company Information
- Customer Services
- Internet Services
- e-Commerce
- Social Network
- News
- Personal Content
- Community
- Online Service

- defacement
- denial of service
- data theft
- malicious software hosting

-the hacktivist
-the criminal
-the spy

copyright 2015 MF8 International
About Attacks on Respondent Sites

- Has your website ever been defaced?
  - No: 75%
  - Yes: 18.8%
  - Don’t know/not sure: 6.3%

- Has your site ever had a DOS attack?
  - No: 82.5%
  - Yes: 31.3%
  - Don’t know/not sure: 6.3%

- Has malicious software ever been installed on your site to attack your users?
  - No: 43.6%
  - Yes: 31.3%
  - Don’t know/not sure: 25%

- Has data ever been stolen from your site?
  - No: 50%
  - Yes: 43.6%
  - Don’t know/not sure: 6.3%
Operations & Security

your staff & service provider staff

your data center

Regulation, industry standards, best practices & policies for a security framework

the software development lifecycle

the cloud
About Survey Respondents’ Websites

What is the Website’s Purpose?

- Community news, information and comments [18.8%]
- Company description, information about the company and services, contact us [37.5%]
- E-commerce: take orders and possibly payments for goods and services [12.5%]
- Company service: online booking, online bill pay, online account [6.3%]
- Other [6.3%]

Can People Login to the Website?

- No, no one can login through the website [31.3%]
- Yes, employees only [18.8%]
- Yes, employees and/or clients, customers, partners [12.5%]
- Yes, clients and customers only [37.0%]

Who Maintains the Website?

- Service provider [50%]
- A combination of company employees and service provider [12.5%]
- Company employees [37.0%]

*note that only 1 respondent uses multi-factor authentication

Where is the Website Hosted?

- Hosted on a shared server with a service provider outside of... [29%]
- Hosted on a dedicated server with a service provider... [12.5%]
- In the company data center hosted elsewhere... [12.5%]
- In the company’s data center in the office [31.3%]
- Hosted on a shared server with a service... [31.3%]
- Provided to the company as a service... [6.3%]

Does the Website Have Information on Employees, Customers, Users, etc.?

- No [50%]
- Yes [50%]

8. Do you have a security policy for the secure implementation and operation?

- No [37.0%]
- Yes [62.5%]
Website Security Architecture

- Content delivery
- Intrusion detection
- Internet
- WAF firewall
- Web server
- DMZ firewall
- Authentication
- Cloud WAF/DDOS
- Log server
- App server
- DB server
Respondent Security Architecture

Is the site HTTPS only?
- No: 25%
- Yes: 75%

Do you use any tools or services to test impact of denial of service attacks?
- No: 62.5%
- Yes: 37.5%

Are your web servers in a firewall-isolated DMZ?
- No: 37.5%
- Yes: 62.5%

Is there a DMZ firewall between the web and other servers?
- No: 56.3%
- Yes: 43.7%

Do you use IDS/IPS?
- No: 43.8%
- Yes: 56.2%

Do you use a WAF?
- No: 60%
- Yes: 40%

Do you monitor for unauthorized changes to the site and code?
- No: 80%
- Yes: 20%

Do you scan the site for known vulnerabilities and misconfigurations?
- No: 75%
- Yes: 25%

Have your site had a pen test?
- No: 37.5%
- Yes: 62.5%

Did you test the website security for session IDs, authentication and access control?
- No: 75%
- Yes: 25%
According to FireEye, successful attacks are discovered on average after 205 days.
Cheer Up, It’s Easier Than You Think

- Inexpensive, orchestrated DEV environment
- Container ready
- Cloud-based security solutions
- Better physical security
- API-enabled architectures
- Automatable security testing tools and config standards
- As highly available as you want to pay for