YAN&co

# WORDCAMP 2015 DENMARK

We have a responsibility for the customers
of our customers

YAN&co

# AGENDA

Troduction

We have a responsibility

Definition

The Challenge

Solutions

Questions

# YAN KNUDTSKOV

**Twitter**
@yanknudtskov

**LinkedIn**
http://linkedin.com/in/yanknudtskov

http://yanco.dk
yan@yanco.dk

## PERSONALLY

31 år

## PROFESSIONAL

(2004) IT Engineer
(2005) Ementor Danmark
(2005) Danish Ministry of Foreign Affairs
(2006) Danmarks Radio (DR)
(2007) Personal Trainer
WordPress since 2008
(2008) International Practical Wing Chun Instructor
(2012) Self Employed, Yan&Co
(2015) National Trainer, DGI

## PASSIONER

WordPress
Martial Arts
Personal Leadership

YAN&co

# WE HAVE A RESPONSIBILITY

*“How much does it cost you if your website is down?”*

*“What are the implications for your business if one of your clients websites are hacked?”*

*“Do you have a plan, if you website is hacked?”*

*“Have you written it down?”*

*“Have you tested it?”*

YAN&co

# WHAT IS SECURITY?

YAN&co

# WHAT IS SECURITY

## Definition

### Protection

*Are you leaving the keys in the door?*

*WordPress Administration*
*File-server (FTP)*
*Database*
*Hosting providers controlpanel*

### Monitoring

*Look for suspicious activity*

*Turn on the alarms*
*E-mail notifications*
*Audit logs*
*File Changes*
*Malware Scans*

### Response

*Because, sometimes shit happens*

*Backup*
*Damage Control*
*Audit logs*
*Notification of affected users*

# THE CHALLENGE

YAN&co

# THE CHALLENGE

## Levels of competency

Unconsciously competent

Consciously competent

Consciously incompetent

Unconsciously incompetent

YAN&co

# THE CHALLENGE

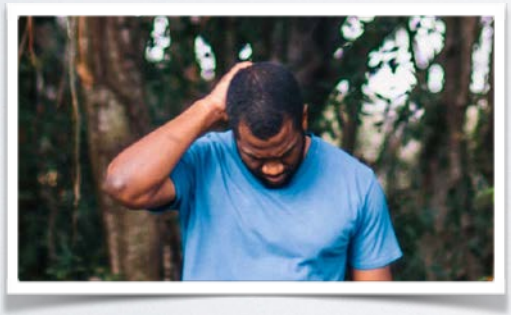
## Do you recognize any of these?

***"I know I should do something..***
***But I don't know where to start - and what if I break something?"***

This is about not knowing where to start and being afraid of doing more harm than good!

***"NOBODY wants to break in on my site !***
***- I have nothing they want!"***

Often this is about, now knowing where to start. And then its easier for the person to tell themself a story about it not being important, to avoid worry!



***"But.. what do the hackers want from me,***
***I'm just a small business with out any important information!"***

This is often about lack of congruency between the PERCEIVED value and the ACTUAL value, as well as the PERCEIVED effort it would require to solve the problem.

# THE CHALLENGE

## Are you in the hackers target group?

If you could recognize the previous statements - either from you or your clients, then you / they are exactly the target group for hackers and automated hacking.

The most recent statistics from 2015 show that small and medium sized businesses are often target to hackers, because the businesses don't prioritize security.

YAN&co

# THE CHALLENGE

## What do the hackers want?

Even if your website doesn't have banking information or or high value information, it will have the following:

- User emails and passwords
- Sensitive personal information (Names, adresses, phonenumbers, etc.)
- Server resources

**Which potentially grants access to**


**Because the users are using the same email and passwords on most websites**

YAN&co

# THE CHALLENGE

## How does the hackers get access

### COMMON METHODS

- Administrator users with an insufficiently strong password
- Plugins and/or themes with unsafe code
- Lack of system updates
- Malware on the local machine
- “Free” Premium Plugins

YAN&co

# SOLUTIONS

YAN&co

# SOLUTIONS

## Protection

## Administrator users with an insufficiently strong password

**All users with editor priviledges and higher**

- Force strong passwords
- Use two-factor authentication
- Avoid the username ‘admin’
- Auto-ban anyone who attemps to login with username ‘admin’
- Block repeatedly failed login

**If possible (medium advanced)**

- White-list IP adresses who can access /wp-admin/
- Setup .htpasswd on /wp-admin/ and /wp-login.php

### Block repeatedly failed login, Strong Passwords, Avoid the username ‘admin’

**Sucuri Security (Free + Paid)**
https://wordpress.org/plugins/sucuri-scanner/

**iThemes Security (Free + Paid)**
https://wordpress.org/plugins/better-wp-security/

**WordFence (Free + Paid)**
https://wordpress.org/plugins/wordfence/

### Two-Factor Authentication

**Rublon Account Security (Free + Paid)**
https://wordpress.org/plugins/rublon/

**Clef Two-Factor Authentication (Free)**
https://getclef.com/
https://wordpress.org/plugins/wpclef/

### HTPASSWD

http://www.htaccesstools.com/htpasswd-generator/

YAN&co

# SOLUTIONS

## Protection

### Plugins and/or themes with unsafe code

- Block ‘weird’ HTTP requests
- Blacklist with HackRepair.com blacklist
- Remove direct access and execution of .php files /wp-content/ and subdirectories
- Remove direct access and execution of .php files /wp-includes/ and subdirectories
- Update plugins and themes

### Remove direct .php access, Blacklisting

**Sucuri Security (Free + Paid)**
https://wordpress.org/plugins/sucuri-scanner/

**iThemes Security (Free + Paid)**
https://wordpress.org/plugins/better-wp-security/

**WordFence (Free + Paid)**
https://wordpress.org/plugins/wordfence/

### Block ‘weird’ HTTP requests

**BBQ: Block Bad Queries (Free + Paid)**
https://wordpress.org/plugins/block-bad-queries/

YAN&co

# SOLUTIONS

## Protection

### Lack of system updates

- Auto update WordPress Core
- Auto update (most) plugins
- (Perform regular backups)

**“Yes, you’d rather have an updated site with a technical malfunction than a website with malware that has been hacked.**

**…**

**Wouldn’t you prefer an unfunctional washing machine over a break in, in your home?”**

### Auto Updates

**Advanced Automatic Updates (Free)**
https://wordpress.org/plugins/automatic-updater/

**Automatic Plugin Updates (Free)**
https://wordpress.org/plugins/automatic-plugin-updates/

# SOLUTIONS

## Monitoring

## Monitoring

- Notify about created admin users
- Notify about admin logins
- Scan for malware
- Scan for file changes
- Keep an updated list of installed plugins vs. reported security issues
- Keep an audit log

### Malware Scans and File Changes

**Sucuri Security (Free + Paid)**
https://wordpress.org/plugins/sucuri-scanner/

**iThemes Security (Free + Paid)**
https://wordpress.org/plugins/better-wp-security/

**WordFence (Free + Paid)**
https://wordpress.org/plugins/wordfence/

### Notify of logins and created admins

**Sucuri Security (Free + Paid)**
https://wordpress.org/plugins/sucuri-scanner/

### Audit Logs

**WP Security Audit Log (Free)**
https://wordpress.org/plugins/rublon/

### Plugin Vulnerabilities

**Plugin Vulnerabilities (Free)**
https://wordpress.org/plugins/plugin-vulnerabilities/

# SOLUTIONS

## Response

## Response

- Remote storage
- Notify if a backup fails
- Ideally more than one remote backup location
- Test your worst-case scenario

### Backup

**BackupBuddy (Paid)**
https://ithemes.com/purchase/backupbuddy/

**VaultPress (Paid)**
https://vaultpress.com/

**BackWPUp (Free + Paid)**
https://wordpress.org/plugins/backwpup/

**UpdraftPlus (Free)**
https://wordpress.org/plugins/updraftplus/

### Remote Storage

**Dropbox (Free + Paidt)**
**Amazon S3 (Free + Paid)**
**FTP(S) (Paid)**
**Google Drive (Free + Paid)**

### Notify Users

**Email Users (Free)**
https://wordpress.org/plugins/email-users/

YAN&co

# SUMMARY

## WE HAVE A REPONSIBILITY

How does it affect your business if yours or a client of yours is hacked?

## WHAT IS SECURITY

Protection, monitoring, response

## THE CHALLENGES

Confusing, lack of competencies,
resistance due to a lack of understanding

## SOLUTIONS

Setup atleast a minimum of security for you and your clients

YAN&co

# QUESTIONS

# THANK YOU FOR YOUR TIME!


**Slides are available**
**http://yanco.dk/wordcamp-english**