Well, Your CMS Just Got Hacked!

Bryan Soltis
Kentico Technical Evangelist

Take a deep breath…

How did this happen?

Environment

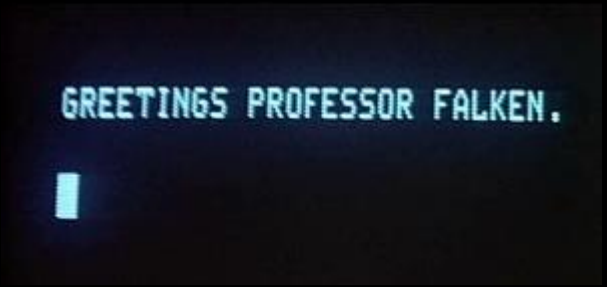
- Unsecure network
  - Firewalls
  - Intrusion Detection
- VPN
- Physical access
  - Data Center security
  - Restricted area violation
- Internal / External threat

CMS

- Has the CMS been updated / upgraded recently?
- Are there any known security vulnerabilities?
- Has the CMS been implemented according to best practices?
- Has a security audit been performed?
- Are there notification systems in place?
- Do you have access to the source code?

Code

- Are you following security best-practices?
- Are you doing code reviews?
- Is you whole team familiar with the code?
- Are your developers up to date on the latest threats?
- Is the code encrypted and signed?



```
GREETINGS PROFESSOR FALKEN.
```

Data

- Are you storing sensitive data?
- Are you encrypting data?
- Are you adhering to international guidelines / laws?
- Is your database accessible?
- Are you monitoring / controlling connections?

What to do now?

Lock Down the System

- Change logins / password
- Restrict access by IP / location
- Limit physical access
- Access data center / environment logs
- Access audit logging

Assess the Damage

- Is the system stable?
- Is there any threat to other areas of your business?
- How much data was accessed / lost?
- Do you need to restore from backups?
- How much data was at risk?

Go Exploring

- Investigate CMS Platform logs
- Investigate IIS logs
- Investigate Application / System Event logs
- Interview anyone with access

Communicate

- Inform at-risk users
- Minimize damage to personal information
- Define & communicate an action plan
- Understand and follow the appropriate laws
- Understanding government & geographical boundaries

Consider Alternatives

- Consider separate, isolated networks
- Eliminate/ Minimize sensitive data
- Tighten security / limit access
- Consider cloud hosting
- Consider “honeypot” environment

Prevention

Educate

- Train your people
  - IT / Development / Business
  - Frequent / Ongoing
  - Conferences / Workshops / Training
- Lock down your network
  - Establish security policies
  - Assign responsible parties
  - Review / Re-evaluate often
- Budgeting for Security
  - Add into to every project / budget
  - Designate resources

Update the CMS Platform

- Review product documentation / best practices
- Determine if others have reported the issue
- Check for any updates to your version of the platform
- Subscribe to Security Newsletters
- Contact support and discuss alternatives / next steps

Better Implementation

- Write secure code
  - Follow best practices
    - General standards
    - Platform-specific
  - Code Reviews
    - With every major build / deployment
- Store data properly
  - Avoid storing sensitive information, if possible
  - Encrypt sensitive data
- Review latest threats / standards

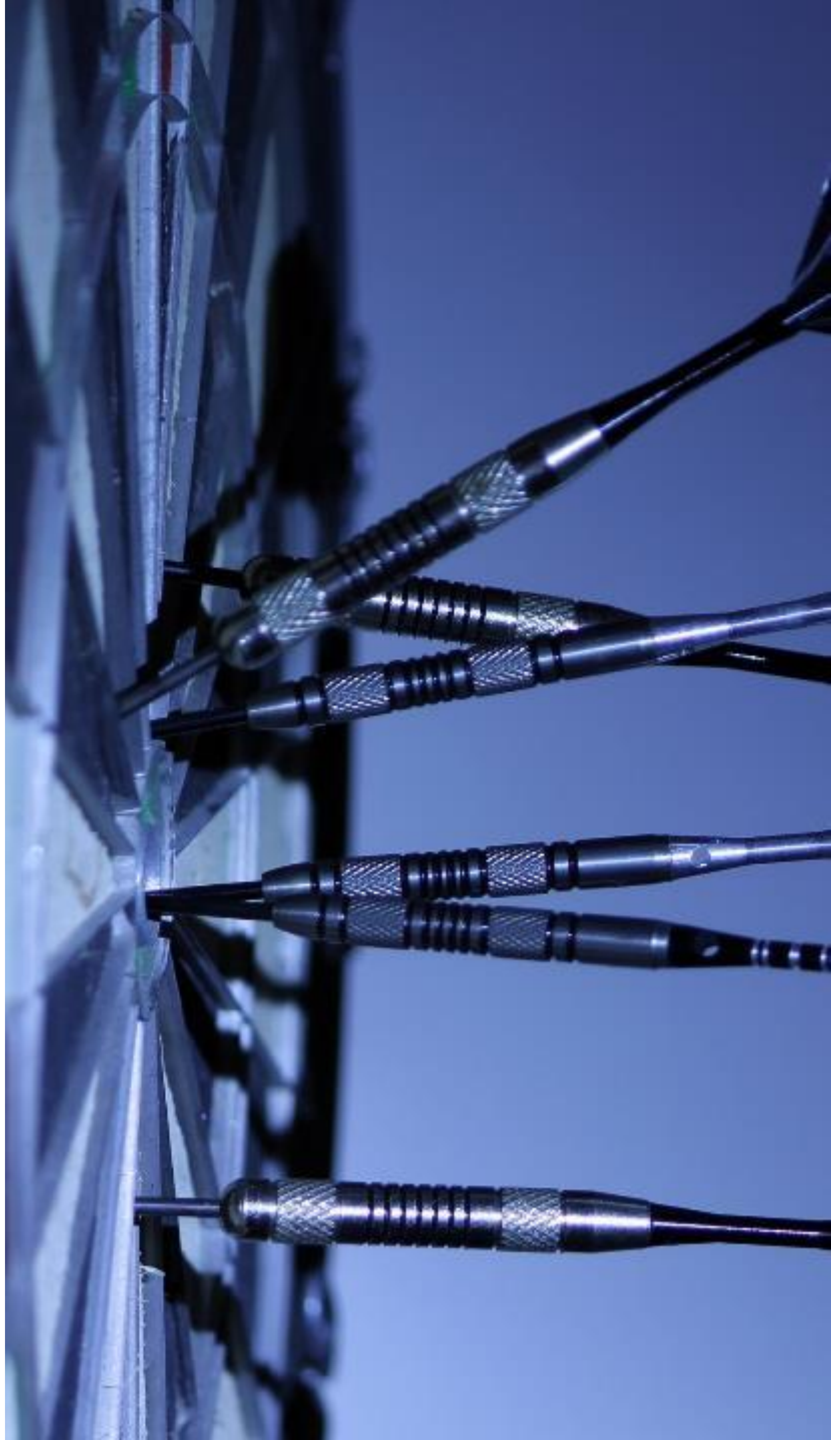
Test!

- Security testing
  - Identify all access points
  - Identify / harden “soft” areas of the application
  - Isolate sensitive areas and data
- Security Reviews
  - Use security experts to analyze the environment and implementation
  - Work with CMS vendor to ensure security
    - Consulting
    - Best practices
    - Security newsletters
- Think like a hacker!

Kentico

Review

- Stabilize the system
- Identify the cause
- Fix the vulnerability
- Test your systems
- Prevent future attacks



Questions?

Kentico

Bryan Soltis

E-mail:	bryans@kentico.com
Skype:	kentico_bryans
Twitter:	bryan_soltis

devnet.kentico.com
facebook.com/KenticoCMS
twitter.com/kentico
linkedin.com/company/kentico-software