Direktoratet for forvaltning og IKT

Software Security in eGovernment

Håkon Styri

Senior adviser

Agency for Public Management and eGovernment (Difi)

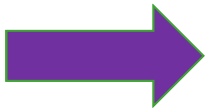
2015-06-03

Background

- 2012 - «Cyber Security Strategy for Norway»
  - «Our networks and systems must be secure and stable at all times. Industry, government and the general public must all feel confident that the digital services our society relies on work.»
  - The immediate follow-up to the strategy was an Action Plan with 42 actions.
- 2013 – The Agency for Public Management and eGovernment (Difi) established an Information Security Section (action 0.5)

Our approach…

The problem (as seen by some)

Attacks  Incidents
Disasters

The problem (the SW viewpoint)

The 2015 study - overview

- Topic: Security in software development in the public sector
- Main goal: Establish a baseline to measure improvement over time
- Short term goal: Identify security practices that may be improved within a two year time frame.

The 2015 study - team

- The study was requested by Difi and performed by SINTEF IKT
  - Martin Gilje Jaatun

    Daniela Soares Cruzes
    Inger Anne Tøndel
    Karin Bernsmed
- Difi contacts
  - Lillian Røstad

    Håkon Styri

The 2015 study - method

- Method based on the Building Security In Maturity Model (BSIMM) framework
- Data collected by assisted self evaluation
  - Participants returning a questionnaire, followed up by video conference or phone interview to sort out misunderstandings and other issues related to filling out the questionnaire.
- Questionnaire distributed to 32 public sector organizations. 20 organizations responded (62.5%)

Disclaimer

- The 2015 study was based on the BSIMM framework, but isn’t a proper BSIMM study.

Building Security In Maturity Model (BSIMM)

https://www.bsimm.com/

BSIMM – a very short intro

- The BSIMM is a study of real-world software security initiatives organized so that you can determine where you stand with your software security initiative and how to evolve your efforts over time.
- BSIMM-V describes the software security initiatives at 67 well-known companies.
- BSIMM-V describes 112 activities organized in 12 practices according to the Software Security Framework.

BSIMM Software Security Framework

(12 practices organized into 4 domains of governance)			
Governance	**Intelligence**	**SSDL Touchpoints**	**Deployment**
Strategy and Metrics	Attack Models	Architecture Analysis	Penetration Testing
Compliance and Policy	Security Features and Design	Code Review	Software Environment
Training	Standards and Requirements	Security Testing	Configuration Management and Vulnerability Management

Assessment Worksheet			
Business Functions	**Security Practices**	**Activities**	**Answer (Yes, No, Don't Know)**
Governance	Strategy & Metrics	We publish our process for addressing software security; containing goals, roles, responsibilities and activities.	
		We have a secure software evangelist role to promote software security internally.	
		We educate our executives about the consequences of inadequate software security.	
		We have *identified* gate locations in our secure software development process where we make go/no go decisions with respect to software security.	
		We *enforce* the identified gate locations in our secure software development process where we make go/no go decisions with respect to software security, and track exceptions.	
		We have a process of accepting security risk and documenting accountability. In this process we assign a responsible manager for signing off on the state of all software prior to release.	
		The software security group publishes data internally on the state of software security within the organization.	
		In addition to the software security group, we have also identified members of the development teams that have a special interest in software security, and have a process for involving them in the software security work.	
		We have identified metrics that measure software security initiative progress and success.	
		The software security group has a centralized tracking application to chart the progress of all software.	
		The software security group advertises the software security initiative outside the organization (for example by writing articles, holding talks in conferences, etc).	
	Policy & Compliance	The software security group has an overview of the regulations that our software has to comply with.	
		We have a software security policy to meet regulatory needs and customer demands.	
		The software security group is responsible for identifying all legislation related to personally identifiable information (for example personopplysningsloven).	
		We have identified all the personally identifiable information stored by each of our systems and data repositories.	
		All identified risks have to be mitigated or accepted by a responsible manager.	
		We can demonstrate compliance with regulations that we have to comply with.	
		We make sure that all vendor contracts are compatible with our software security policy.	
		We promote executive awareness of compliance and privacy obligations.	
		We have all the documentation necessary for demonstrating the organization's compliance with regulations we have to comply with (for ex. written policy, lists of controls, artifacts from software development).	
		When managing our third party vendors, we impose our software security policies on them.	
		Information from the secure software development process is routinely fed back into the policy creation process.	
	Education & Guidance	We have a security awareness training program.	
		We offer role-specific security courses (for example on specific tools, technology stacks, bug parade).	
		The security awareness training content/material is tailored to our history of security incidents.	
		We deliver on-demand individual security training.	
		We encourage security learning outside of the software security group by offering specific training and events.	
		We provide security training for new employees to enhance the security culture.	
		We use the security training to identify individuals that have a particular interest in security.	
		We have a reward system for encouraging learning about security.	
		We provide security training for vendors and/or outsourced workers.	
		We host external software security events.	
		We require an annual software security refresher course.	
		The software security group has defined office hours for helping the rest of the organization.	

Most common security activities identified in the 2015 study

ID	Aktivitetstekst	%
SE 1.2	We use accepted good practice mechanisms for host/network security.	90%
CMVM 2.1	We are able to make quick changes in the software when under attack.	85%
CMVM 2.2	We track software defects found during operations until they are closed.	85%
CP 1.1	The software security group has an overview of the regulations that our software has to comply with.	85%
CP 2.1	We have identified all the personally identifiable information stored by each of our systems and data repositories.	85%
CP 1.2	The software security group is responsible for identifying all legislation related to personally identifiable information (for example personopplysningsloven).	80%
AM 1.5	The software security group keeps up to date by learning about new types of attacks / vulnerabilities.	80%
SFD 1.2	Security is a regular part of our organization's software architecture discussion.	80%
SR 2.3	We use a limited number of standard technology stacks.	80%

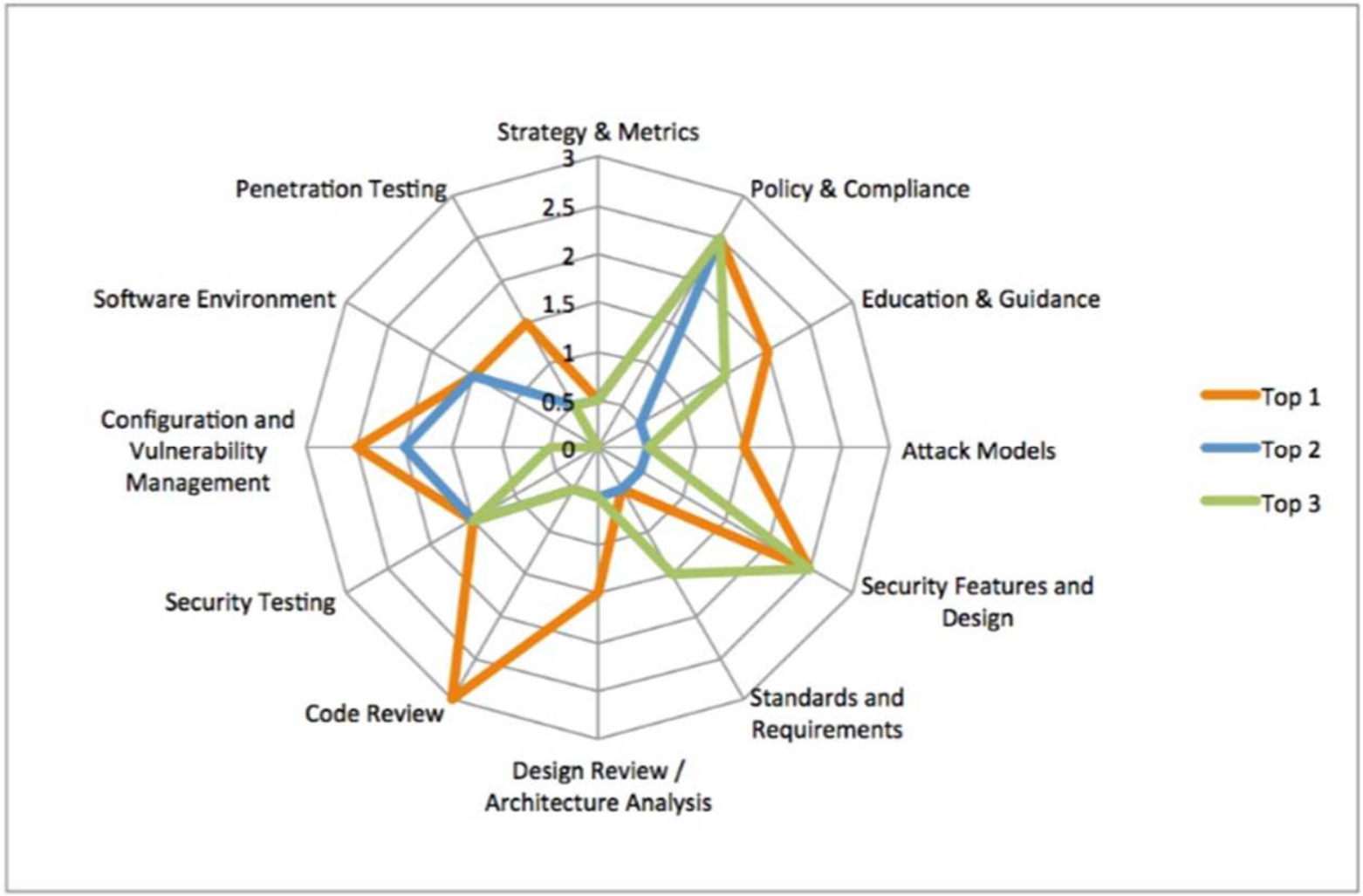
Conservative Maturity DIFI

Weighted Maturity DIFI

Watermark Maturity DIFI

Watermark Maturity BSIMM

Conservative maturity of the three most mature organizations



The full report (in Norwegian)

«Modenhetskartlegging av programvaresikkerhet i offentlige virksomheter»

A26860

SINTEF IKT

2015-03-27

http://www.difi.no/rapport/2015/04/modenhetskartlegging-av-programvaresikkerhet-i-offentlige-virksomheter


difi
Direktoratet for
forvaltning og IKT