Tingenes tilstand:
Programvaresikkerhet i offentlig sektor

Martin Gilje Jaatun
Seniorforsker
SINTEF IKT

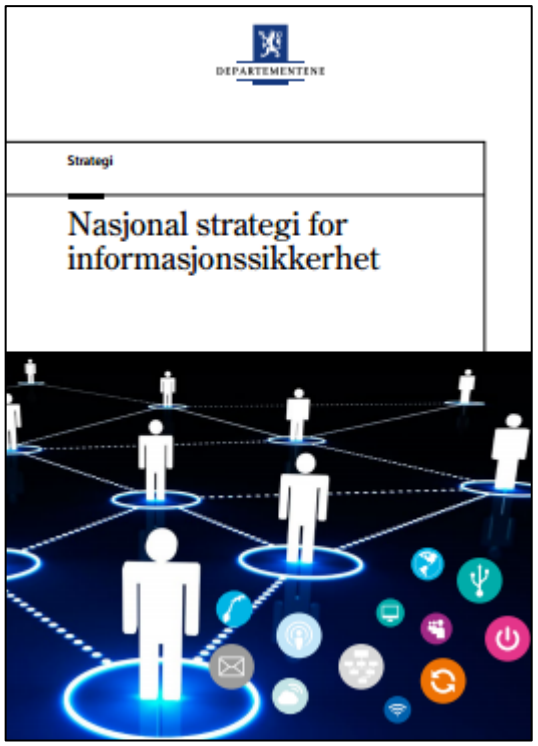
Lillian Røstad
Seksjonssjef
Difi

Daniela Soares Cruzes, SINTEF
Inger Anne Tøndel, SINTEF
Karin Bernsmed, SINTEF
Håkon Styri, Difi

SINTEF

difi Direktoratet for forvaltning og IKT

Difi: Seksjon for informasjonssikkerhet



Jobbe for en styrket og mer helhetlig tilnærming til informasjonssikkerhet i statsforvaltningen.

Forenkle – Fornye - Forbedre.

Bakgrunn for studien

2015: Handlingsplan for informasjonssikkerhet i staten

SINTEF

difi Direktoratet for forvaltning og IKT

Utvalget

- 32 offentlige virksomheter invitert til å delta
- Har større digitaliseringsprosjekter
- (Antar) har interne utviklingsmiljøer

- 20 svarte (62,5%)

Hva har vi gjort?

- En spørreundersøkelse knyttet til i hvilken grad aktiviteter for å sikre programvaresikkerhet er tatt i bruk som en del av programvareutviklingsprosessene i 20 offentlige virksomheter.
- Undersøkelsen er basert på rammeverket til *Building Security In Maturity Model* (BSIMM).

https://www.bsimm.com/

Agenda

- Hva er BSIMM?
- Metode for datainnsamling og rangering av resultater
- Virksomhetenes modenhetsnivå
- Oppsummering og videre arbeid

BSIMM

- En **studie** av en rekke virksomheter (67) og deres programvaresikkerhetsaktiviteter
- Et **Rammeverk**
  - som **beskriver** aktiviteter som gjennomføres hos en større andel av de virksomhetene som er med i BSIMM-studien.
- Måler hvilke aktiviteter som inngår i en virksomhets samlede **livssyklus** for sikker utvikling av programvare (*Secure Software Development Lifecycle* – SSDL).
- Konseptet "**programvaresikkerhetsgruppe**" (*Software Security Group* – SSG) er sentralt
  - de som har ansvaret for å følge opp programvaresikkerheten i en virksomhet.

BSIMM programvaresikkerhetsrammeverk

Programvaresikkerhetsrammeverk (*Software Security Framework*)			
Ledelse og styring (*Governance*)	**Etterretning (*Intelligence*)**	**SSDL Trykkpunkter (*SSDL Touchpoints*)**	**Utrulling (*Deployment*)**
Strategi og måling (*Strategy and Metrics*)	Angrepsmodeller (*Attack Models*)	Arkitekturanalyse (*Architecture Analysis*)	Penetreringstesting (*Penetration Testing*)
Etterlevelse av lover, regler og retningslinjer (*Compliance and Policy*)	Sikkerhetsfunksjonalitet og design (*Security Features and Design*)	Kodegjennomgang (*Code Review*)	Programvaremiljø (*Software Environment*)
Opplæring og øvelser (*Training*)	Standarder og krav (*Standards and Requirements*)	Sikkerhetstesting (*Security Testing*)	Konfigurasjonsstyring og sårbarhetsstyring (*Configuration Management and Vulnerability Management*)

SINTEF

difi Direktoratet for forvaltning og IKT

Agenda

- Hva er BSIMM?
- **Metode for datainnsamling og rangering av resultater**
- Virksomhetenes modenhetsnivå
- Oppsummering og videre arbeid

Deltakerne

- 20 norske offentlige virksomheter
- For enkelte virksomheter har flere personer vært involvert i besvarelsen
- Følgende roller har vært involvert:
  - IT-direktør
  - Avdelingsdirektør utvikling
  - IT-sjef drift
  - Seksjonssjef IT
  - Seksjonsleder utvikling
  - Gruppeleder
  - IT-leder
  - Utviklingsleder
  - Løsningsarkitekt
  - Sjefsarkitekt
  - Systemutvikler
  - IKT-rådgiver
  - Sikkerhetsleder
  - Informasjonssikkerhetsleder
  - Sikkerhetssjef
  - Sikkerhetsarkitekt
  - Informasjonssikkerhetskonsulent
  - Sikkerhetsanalytiker
  - Sikkerhetsrådgiver
  - Senioringeniør
  - Seniorrådgiver

Spørreundersøkelse og Oppfølgingsintervjuer

- **Selve spørreundersøkelsen**
  - Generell bakgrunnsinformasjon knyttet til:
    - Stilling, antall utviklere i virksomheten, andel av innleide utviklere og hvorvidt virksomheten kontraherte utvikling av nøkkelferdige løsninger fra eksterne firma.
  - Konkrete spørsmål om hvilke av de 112 BSIMM-aktivitetene virksomhetene utfører i sin daglige drift.
    - Yes / No / Don't Know
- **Oppfølgingsintervjuer**
  - Avtalte på telefon eller videokonferanseløsningen GoToMeeting.
  - Sistnevnte løsning ga mulighet til å dele visning av spørreskjemaet med respondenten under intervjuet.

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.	

Dataanalyse og måling av modenhetsnivå

- **Konservativ modenhet** (*Conservative Maturity*; Skala 0-3)
  - en virksomhet får kun godkjent et modenhetsnivå dersom alle aktivitetene i nivået er oppfylt ("Yes"), pluss at alle aktiviteter på lavere nivå også er oppfylt

- **Vektet modenhet** (*Weighted Maturity*; Skala 0-6)

$$\frac{\textit{aktiviteter på nivå 1}}{\textit{tot antall aktiviteter på nivå 1}} \times 1 + \frac{\textit{aktiviteter på nivå 2}}{\textit{tot antall aktiviteter på nivå 2}} \times 2 + \frac{\textit{aktiviteter på nivå 3}}{\textit{tot antall aktiviteter på nivå 3}} \times 3$$

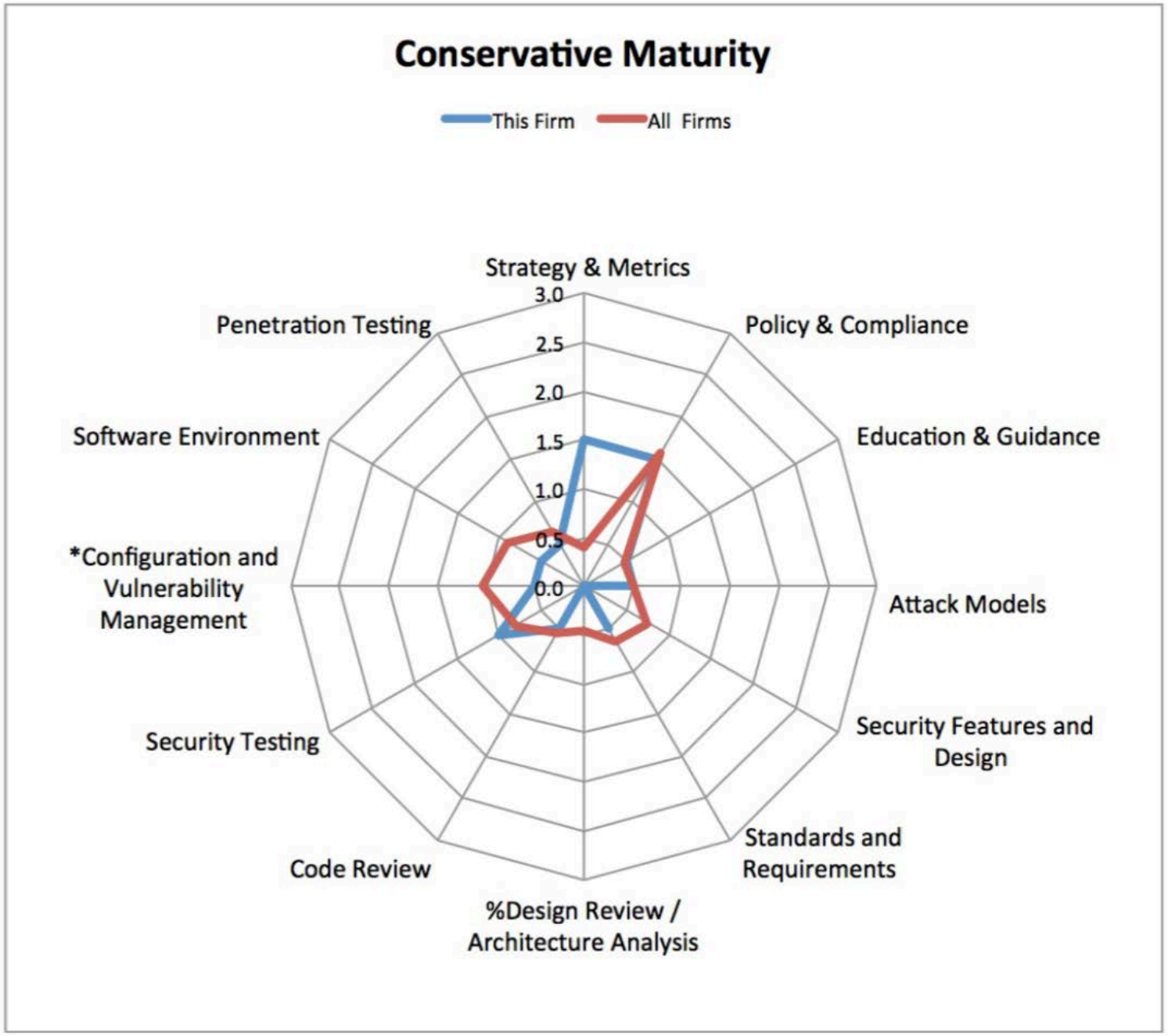
- **Høyvannsmodenhet** (High Watermark Maturity; Skala 0-3)
  - Samme måte som i BSIMM;
  - Hvis virksomheten har minst en aktivitet på nivå 3 får den modenhetsnivå 3.
  - Høyvannsmodenheten sier derfor kun noe om hvilket nivå den høyest rangerte aktiviteten de utfører er på.

Eksempel – for en tenkt virksomhet

Assessment Worksheet

Business Functions	Security Practices	BSIMM	Activities	Answer	Levels	Weighted Score (0-6)	Conservative Maturity (0-3)	High Watermark (0-3)
Governance	Strategy & Metrics	SM 1.1	We publish our	Yes	Level 1 ●	2,0	1+	2
		SM 1.2	We have a secure ...	Yes	Level 2 ◑			
		SM 1.3	We educate our ...	Yes	Level 3 ○			
		SM 1.4	We have *identified* ...	Yes				
		SM 2.2	We *enforce* the ...	Yes				
		SM 1.6	We have a process ...	Yes	**Percentage of Practices 63 %**			
		SM 2.1	The software	No				
		SM 2.3	In addition to the	Yes				
		SM 2.5	We have identified....	No				
		SM 3.1	The SSG has ...	No				
		SM 3.2	The SSG advertises ...	No				
	Policy & Compliance	CP 1.1	The SSG has an ...	Yes	Level 1 ●	2,6	1+	2
		CP 1.3	We have a ...	Yes	Level 2 ◑			
		CP 1.2	The SSG is ...	Yes	Level 3 ○			
		CP 2.1	We have identified	Yes				
		CP 2.2	All identified risks	No				
		CP 2.3	We can demo....	Yes	**Percentage of Practices 63 %**			
		CP 2.4	We make sure	Yes				
		CP 2.5	We promote	Yes				
		CP 3.1	We have all the ...	No				
		CP 3.2	When managing ...	No				
		CP 3.3	Information from ...	No				
	Education & Guidance	T 1.1	We have a security ...	No	Level 1 ○	0,6	0+	3
		T 1.5	We offer role	No	Level 2 ○			
		T 1.6	The security ...	No	Level 3 ◑			
		T 1.7	We deliver	No				
		T 2.5	We encourage ...	No				
		T 2.6	We provide...	No	**Percentage of Practices 8 %**			
		T 2.7	We use the ...	No				
		T 3.1	We have a reward ...	No				
		T 3.2	We provide...	No				
		T 3.3	We host external ...	No				
		T 3.4	We require an ...	No				
		T 3.5	The SSG has ...	Yes				

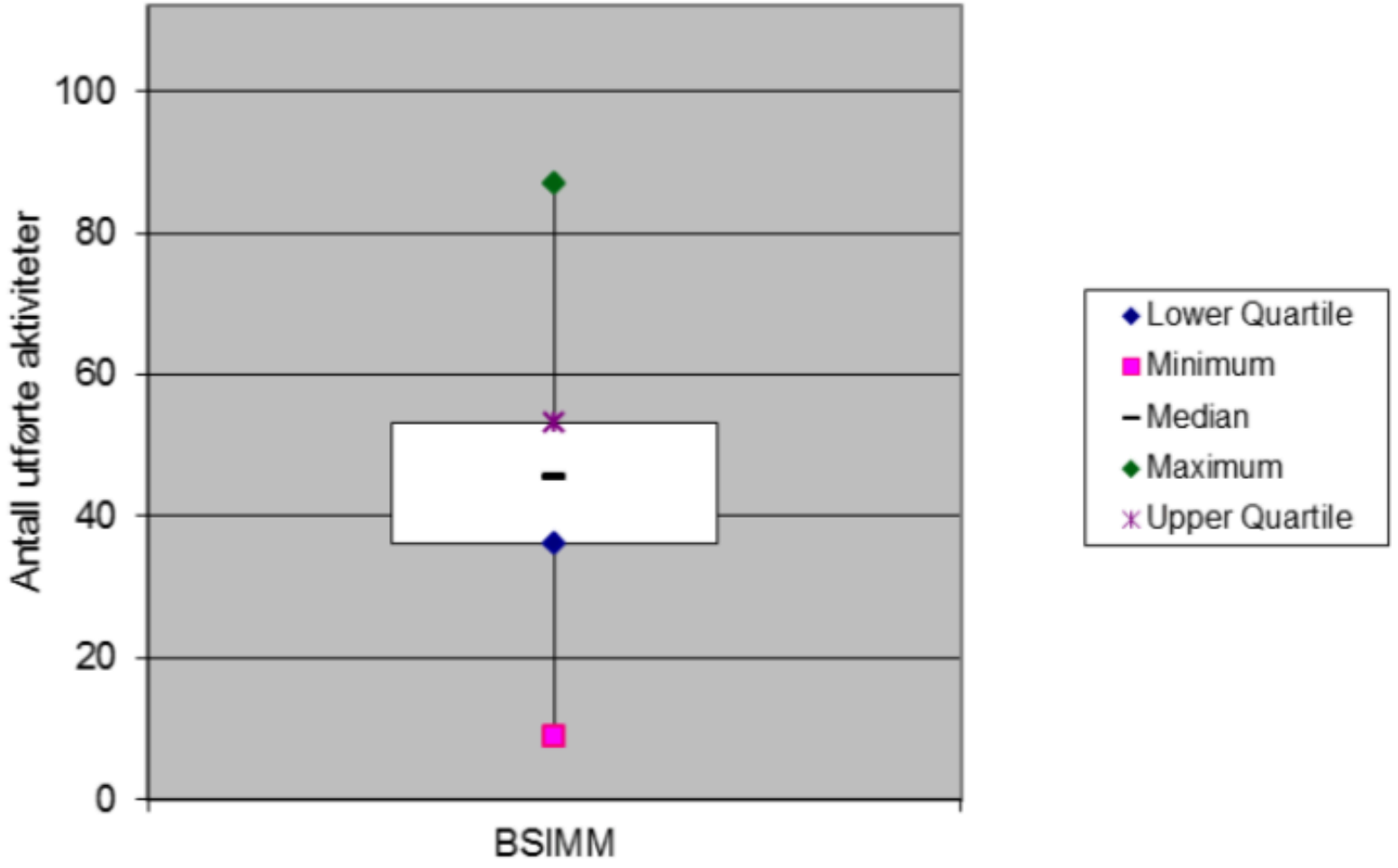
Eksempel, forts.



Agenda

- Hva er BSIMM?
- Metode for datainnsamling og rangering av resultater
- **Virksomhetenes modenhetsnivå**
- Oppsummering og videre arbeid

Fordeling av totalt antall aktiviteter

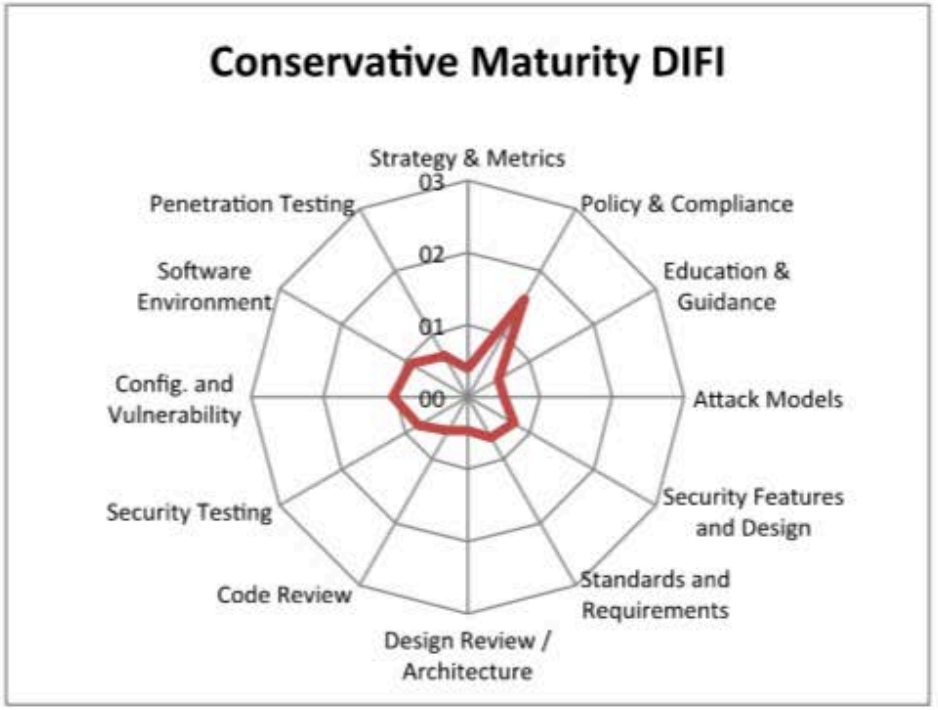


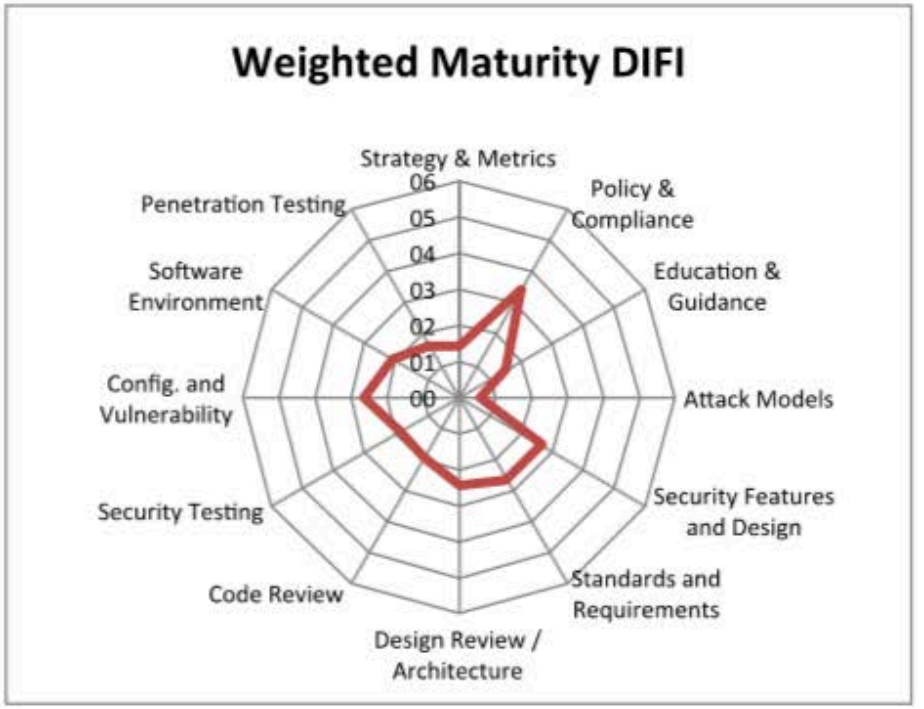
De hyppigst utførte aktivitetene blant alle norske virksomheter

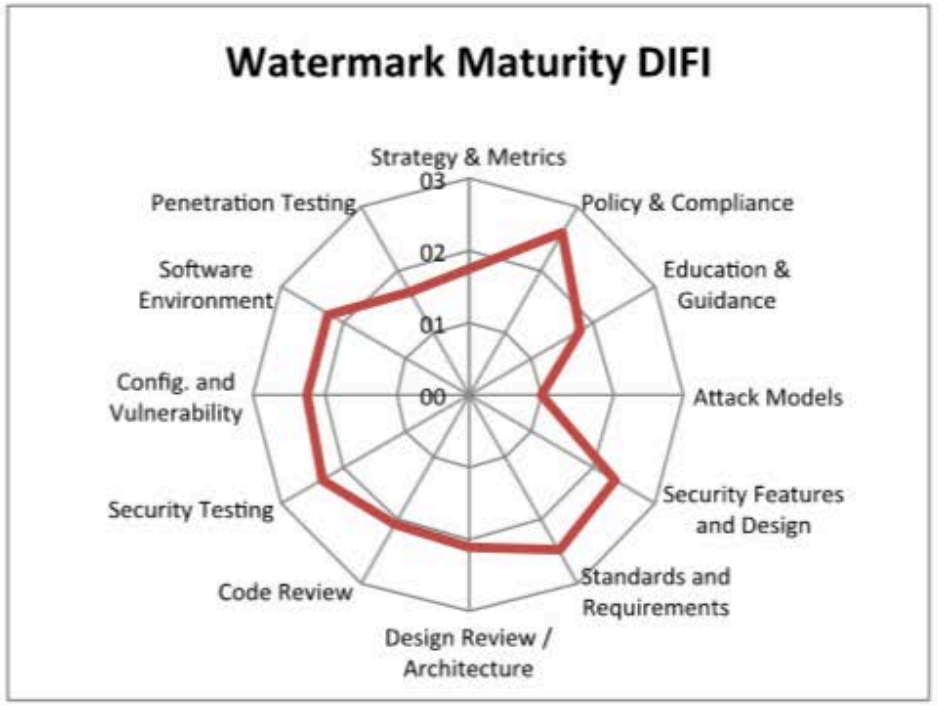
ID	Aktivitetstekst	%
SE 1.2	We use accepted good practice mechanisms for host/network security.	90%
CMVM 2.1	We are able to make quick changes in the software when under attack.	85%
CMVM 2.2	We track software defects found during operations until they are closed.	85%
CP 1.1	The software security group 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%

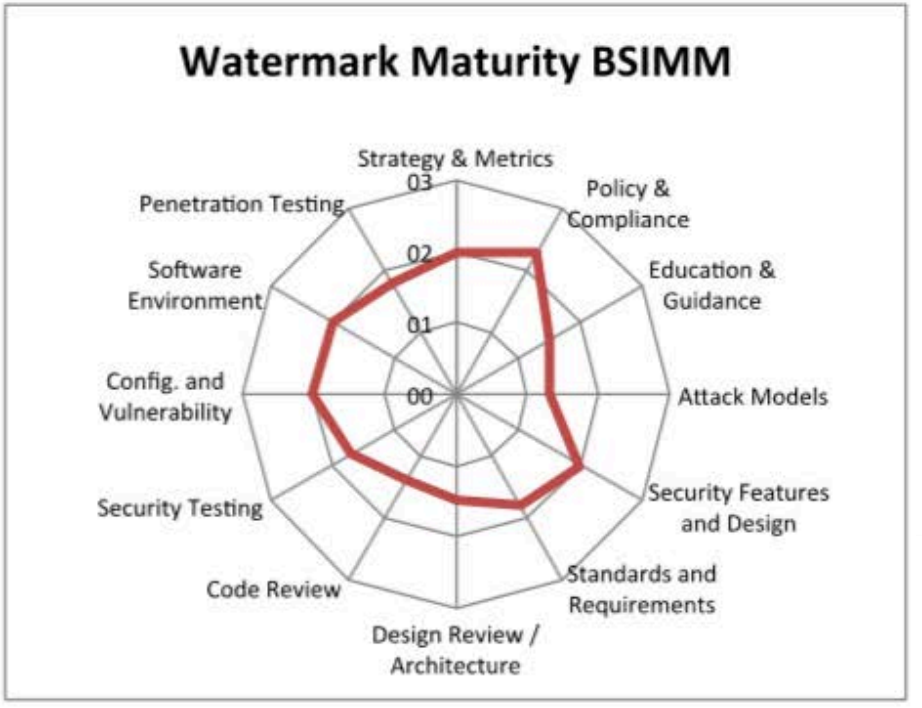
https://www.flickr.com/photos/125207874@N04/14450220780/

Overordnede resultater

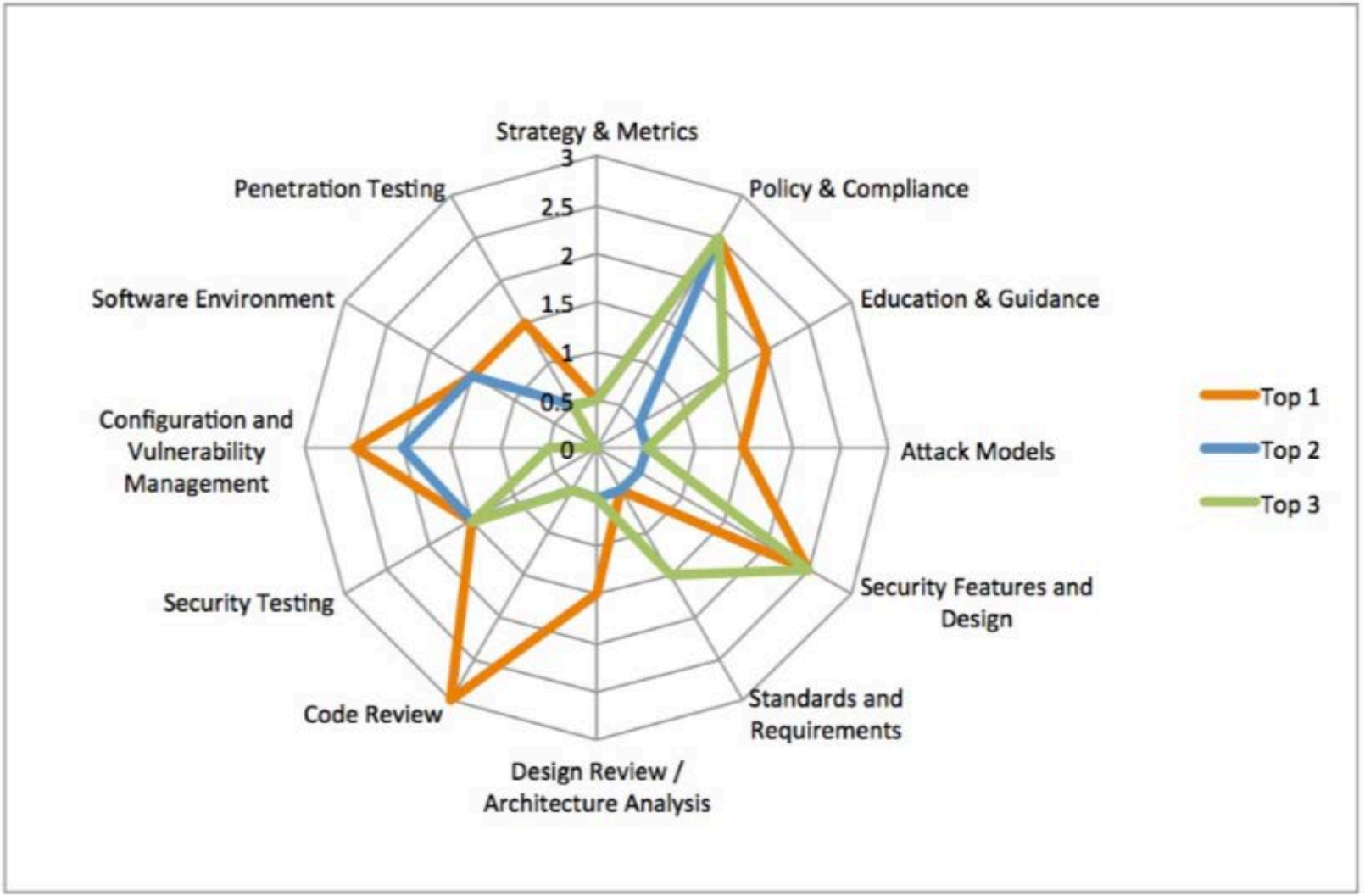








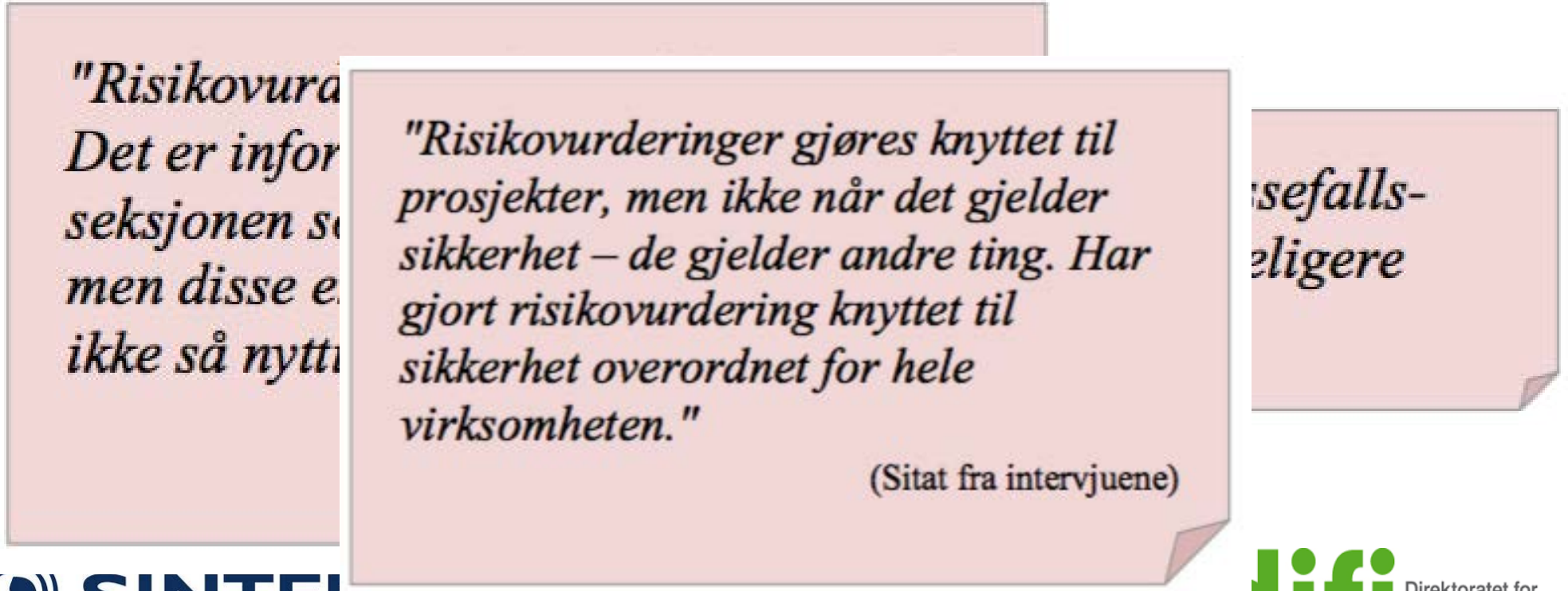
Konservativt modenhetsnivå for de tre mest modne virksomhetene



Strategi og måling

- Hovedmål:
  - Transparens av forventninger og ansvarlighet for resultater.
  - Forankring i toppledelsen

Et av områdene med dårligst modenhet.



Etterlevelse av lover, regler og retningslinjer

- Hovedmål:
  - Sikre etterlevelse av relevante lover og regler.
  - Generere artefakter for revisjon.

Best modenhetsverdi på alle skalaene; stor prosentandel av svarene er positive.

"Vi har mange jurister som jobber hos oss, og vi som organisasjon har mye instrukser og policyer som gjør at vi dekker dette med compliance. Men er usikker på i hvor stor grad dette har konsekvenser for kodingen".

(Sitat fra intervjuene)

Opplæring og øvelser

- Hovedmål:
  - Lage en kunnskapsrik arbeidsstokk og rette opp feil i prosesser.

Det er overraskende lave tall for opplæring

"Vil ikke kalle det et program. Har ikke kjempegod struktur, men er mer ert."

(Sitat fra intervjuene)

"Alle som begynner hos oss må gjennom obligatorisk innføring i sikkerhet, samt underskrive sikkerhetsinstruks. Men er ikke noe om programvaresikkerhet her. Siden utviklerne er innleide er det ingen av de som må gjennom dette opplegget."

(Sitat fra intervjuene)

Angrepsmodeller

- Hovedmål:
  - Kunnskap om angrep som er relevant for virksomheten.

<u>Angrepsmodeller er generelt en praksis med lav modenhet.</u>

"Har et forum for å d
IKT-drift, men er usi
kommer videre derfr
forvaltning."

"Vet ikke hva utviklere følger med på, men mange følger med på software-komponenter de bruker. Får noen ganger krav fra utviklere om å få patchet komponenter de bruker."

(Sitat fra intervjuene)

SINTEF

Sikkerhetsfunksjonalitet og design

- Hovedmål:
  - Etablering av tilpasset kunnskap om sikkerhetsfunksjonalitet, rammeverk og mønster.

Bare 15% av virksomhetene sier at de gjør SFD1.1 (*Our software security group builds and publishes a library of security features*),

Mens 80% påstår at de oppfyller SFD 1.2 (*Security is a regular part of our organization's software architecture discussion*).

"I flere prosjekter er det sikkerhetskrav med fra starten. Der har vi blitt bedre. IT-sikkerhetsleder kan da være med og stille krav. Det varierer fra prosjekt til prosjekt om sikkerhet tas med. Det er mer vanlig at sikkerhet er med om det er nyutvikling enn om det er videreutvikling."

(Sitat fra interviuene)

Standarder og krav

- Hovedmål:
  - Lage retningslinjer.
  - Også for eksterne aktører.

Rundt halvparten av virksomhetene viser tegn til generelt høy grad av modenhet innenfor denne praksisen.

"Vi har standardisert på Microsoft platform og .net."

(Sitat fra intervjuene)

Arkitekturanalyse

- Hovedmål:
  - Kvalitetskontroll.

Generelt virker det som om det er lav modenhet innen designgjennomgang og arkitekturanalyse.

"Arkitektur involverer ofte sikkerhetsarkitekter når de lager arkitekturen, men de kan i virksomheten bli flinkere til å sjekke at sikkerhetsarkitekter er involvert. Nå er det prosjektet som bestiller ressurser, f.eks. en sikkerhetsarkitekt. Det er vanlig at sikkerhetsarkitekter er med når det er åpenbart sikkerhets-ting, men dette kan falle gjennom om fokus er på funksjonaliteten."

(Sitat fra intervjuene)

Kodegjennomgang

- Hovedmål:
  - Kvalitetskontroll.

Kodegjennomgang var også en praksis med gjennomgående lav modenhet.

Det er mange som nevner i intervjuene at utviklerne sjekker hverandres kode.

"Det dukker av og til opp feil, og da blir dette tatt opp med utviklerne, men vet ikke hva utviklerne gjør med det."

(Sitat fra intervjuene)

Sikkerhetstesting

- Hovedmål:
  - Kvalitetskontroll

Også for sikkerhetstesting observerer vi et generelt lavt modenhetsnivå.

Flere respondenter indikerte at testing og QA er noe som utviklerne selv gjør, men at fokuset er på funksjonell testing, ikke sikkerhetstesting.

"Vi har ikke egne, spesifikke tester for sikkerhet. [...] Kvalitetssikringstestere utfører ikke sikkerhetstester."

(Sitat fra intervjuene)

Konfigurasjonsstyring og sårbarhetsstyring

- Hovedmål:
  - Endringsledelse.

Mer enn halvparten av virksomhetene gjør aktivitetene på nivå 1

"Om en feil skulle oppdages trekker vi inn de som kjenner produksjons-systemet. Siden de har bygget det selv vet de hvor komponenten er i bruk. Dette er kunnskap som ligger i hodene til folk."

(Sitat fra intervjuene)

Programvaremiljø

- Hovedmål:
  - Endringsledelse.

Virksomhetene har god tiltro til eget sikkerhetsnivå når det gjelder nettverk og datamaskiner.

Det er viktig å huske på at nettverkssikkerhet generelt er mye modnere enn programvaresikkerhet.

Penetreringstesting

- Hovedmål:
  - Kvalitetskontroll
  - Oppdage sikkerhetsdefekter

Minst halvparten av virksomhetene gjør de to første aktivitetene på nivå 1

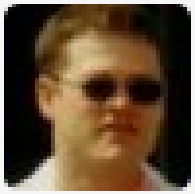
"Initiativer til å gjøre penetrasjons-testing kommer ikke fra utviklersiden men fra nettverkssiden. Da gjøres det ikke testing spesielt av egenutviklet kode, eller på prosjekter, men bredere."

(Sitat fra intervjuene)

Oppsummering

- Hva gjør leverandører av aktiviteter knyttet til informasjonssikkerhet?
- Kan være lang veg fra intern kompetanse knyttet til lover og regler, til utvikler/konsulent
- Ulike kulturer mellom infrastruktur og programvareutvikling
- Bra at utviklerne sjekker hverandres kode
  - Men er det kunnskap om programvaresikkerhet hos utviklerne?
- Det er typisk de sikkerhetsansvarlige som sendes på sikkerhetsrelaterte kurs, ikke utviklerne
- Risikovurderinger på virksomhetsnivå oppleves ikke som relevante for programvareutviklingen
- Det testes for lite med henblikk på sikkerhet

Kunne det gjøres bedre?



Martin Gilje Jaatun @SeniorFrosk 15 Apr

@cigitalgem Our software security maturity survey is online difi.no/sites/difino/f... - might be of interest to your Norwegian friends...

Gary McGraw

@cigitalgem

Follow

Yes. Of course the #bsimm itself does not rely on self-reporting or e-surveys. @SeniorFrosk

1:32 PM - 15 Apr 2015

Veien videre: hva skal vi bruke dette til?

- Benchmark - nullpunktsmåling
- Fokusere innsatsen på tiltaksområde 2 og 4:
  - Sikkerhet i digitale tjenester
  - Felleskomponenter
- Gjøre opp status
  - Fungerer tiltakene?
  - Blir vi bedre?

http://infosikkerhet.difi.no

infosikkerhet@difi.no

Spørsmål?

twitter.com/
SINTEF_Infosec

Infosec
Blogg

http://infosec.sintef.no/?s=bsimm

http://infosec.sintef.no

Martin.G.Jaatun@sintef.no