Mjukvarors säkerhet beror på utvecklarnas motivationer och hinder

En enkätundersökning

Henrik Karlzén, Jerry Falkcrona,
Daniel Eidenskog och Martin Karresand

FOI-R--5691--SE

December 2024

FOI

Henrik Karlzén, Jerry Falkcrona, Daniel Eidenskog och Martin Karresand

Mjukvarors säkerhet beror på utvecklarnas motivationer och hinder

En enkätundersökning

Titel	Mjukvarors säkerhet beror på utvecklarnas motivationer och hinder – En enkätundersökning
Title	Software security depends on the developers' motivations and deterrents – A survey study
Rapportnr/Report no	FOI-R--5691--SE
Månad/Month	December
Utgivningsår/Year	2024
Antal sidor/Pages	43
ISSN	1650-1942
Uppdragsgivare/Client	Försvarsmakten
Forskningsområde	Informationssäkerhet
FoT-område	Operationer i cyberdomänen
Projektnr/Project no	E38529
Godkänd av/Approved by	Emil Hjalmarson
Ansvarig avdelning	Cyberförsvar och ledningsteknik

Bild/Cover: Tony Johannot, Faust and Mephisto in Fausts's study (gravyr ca. 1845–1847).

Sammanfattning

Att säkerhetsnivån i mjukvara inte alltid håller måttet visas bland annat av de incidenter som inträffat i säkerhetskritiska it-system, med potentiellt allvarliga konsekvenser till följd. Det finns många samverkande orsaker till att mjukvara inte har tillräckligt säkerhet, däribland mjukvaruutvecklarnas motivation och hinder i säkerhetsfrågor. Att förstå motivationen och hindren är ett viktigt steg i att höja säkerhetsnivån i mjukvaror.

Denna rapport presenterar resultaten från en enkät om mjukvaruutvecklares motivationsfaktorer och hinder när det gäller säkerhet i mjukvara. Enkäten baseras på en tidigare nordamerikansk enkät och har här besvarats av mjukvaruutvecklare som utvecklar säkerhetskritiska system för svenska myndigheter och företag.

Resultaten visar att de starkaste motivationsfaktorerna är interna och därmed kommer inifrån utvecklaren. De interna motivationsfaktorerna inkluderar sådant som ansvarstagande och medvetenhet. Externa motivationsfaktorer motiveras utifrån och är svagare, men omfattar bland annat obligatorisk säkerhetspraxis och företagskultur. Hinder bedöms överlag ha mindre påverkan än motivationsfaktorerna. De högst rankade hindren inkluderar bristande konkurrens som gör att säkerhet upplevs som oviktigt samt att utvecklaren inte får skulden för en uppkommen sårbarhet. Andra relativt betydande hinder är låg prioritering av mjukvarusäkerhet samt att ekonomiska resurser saknas.

Nyckelord: mjukvara, säkerhet, motivation, hinder, enkät

Summary

The security level of Swedish software does not measure up, as shown by several incidents in societally critical IT systems, resulting in potentially severe consequences. There are many interacting reasons for software not being secure enough, including the security-related motivators and deterrents of software developers. Understanding these motivators and deterrents is an important step to increasing the security level of software.

This report presents the results from a survey on software developers' motivators and deterrents related to software security. The survey is based on a previous North American survey. The survey was filled out by software developers working with societally critical IT systems in Swedish authorities and companies.

The results show that the strongest motivators are internal to the developer and relate to developer responsibility and awareness. The external motivators, originating from others, are weaker but include, among others, mandatory security practices and organisational culture. Deterrents are generally assessed as having a smaller impact than the motivators. The highest ranked deterrents include that limited competition makes security feel less important, and that the developer is not blamed for vulnerabilities that occur. Other relatively important deterrents include low priority and lack of financial resources concerning software security.

Keywords: software, security, motivator, deterrent, survey

Innehållsförteckning

1 Inledning

Säkerhetsnivån i mjukvara håller inte alltid måttet. Mängder av sårbarheter publiceras varje år och det finns exempel på incidenter som inträffat i samhällskritiska it-system i vårt närområde, med potentiellt allvarliga konsekvenser.[1] Varför mjukvaror inte är tillräckligt säkra har många orsaker. Rapporten fokuserar på varför mjukvarornas utvecklare oavsiktligt inför sårbarheter i mjukvarorna. Ett sätt att undersöka detta beteende hos utvecklarna är via motivationen till beteendet och via vilka hinder som finns för att utföra beteendet.

Rapporten svarar därför på två forskningsfrågor:

- Vad motiverar mjukvaruutvecklare till att bry sig om mjukvarusäkerhet?
- Vad hindrar mjukvaruutvecklare från att bry sig om mjukvarusäkerhet?

Frågorna besvaras med hjälp av en enkätundersökning där svenska utvecklare får ge sin syn på vad som motiverar eller hindrar dem. Framförallt rör det sig om utvecklare verksamma vid organisationer som utvecklar system med höga säkerhetskrav. Rapporten riktar sig till därför till den som vill veta mer om varför mjukvarusäkerheten ser ut som den gör i sådana system i Sverige. Detta passar väl in i det projekt som rapporten ingår i och som syftar till att ta fram relevant IT-säkerhetskunskap åt Försvarsmakten.[2]

Rapporten presenterar forskningen på ett lättfattligt och diskuterande sätt, snarare än att ha fokus på forskningsmässiga detaljer och komplicerad statistik. Den kan därför läsas av personer med roller från utvecklare till verksamhetschefer eller forskare. Nästa kapitel har dock fokus på metodmässiga detaljer. En mer akademisk forskningsartikel är också planerad.

[1] Se nvd.org samt SektorCERT (2023).

[2] Projektet heter Analys av koncept och teknik för cyberförsvar och informationssäkerhet och ingår i Försvarsmaktens samlingsbeställning inom forskning och teknikutveckling (FoT).

1.1 Vad är mjukvarusäkerhet?

Det finns olika sätt att definiera mjukvarusäkerhet. Enkätundersökningen i den här rapporten utgår från en tidigare studie av Assal och Chiasson (2019). Där definieras mjukvarusäkerhet som:

> idén att skapa en applikation som är motståndskraftig mot: antagonistiska angrepp, att den används av obehöriga eller att den orsakar skada genom felaktig och möjligen oavsiktlig användning. Mjukvarusäkerhet syftar till att minimera mjukvarusårbarheter som skulle kunna utnyttjas av en angripare (t.ex. genom att avlägsna buffertöverskridningssårbarheter).[3]

Definitionens första mening är lik den definition som ges i en väldigt högt citerad forskningsartikel om mjukvarusäkerhet (McGraw, 2004). Där ingår dock inte oavsiktlig användning. I rapportens enkät framgick inte någon definition och respondenterna fick själva tolka begreppet mjukvarusäkerhet.

1.2 Varför är mjukvaror inte helt säkra?

Ett kort, men inte så hjälpsamt, svar är att mjukvaror innehåller sårbarheter som utnyttjas av angripare. En följdfråga blir förstås varför sårbarheterna finns där och den frågan har ett lite mer komplicerat svar. Nedan ges några exempel på relevant FOI-forskning. Dessutom finns det förstås mycket forskning som publicerats utanför FOI. Bara under 2024 har det publicerats flera tusen forskningsartiklar om mjukvarusäkerhet enligt sökning i Google Scholar.

En tidigare rapport i projektet genomförde en litteraturstudie av forskningsartiklar och kom fram till orsaker såsom kostnadsbesparingar, att hålla leveranstider, osäkra programmeringsspråk, svåranvända verktyg och kodbibliotek, ovetenskapliga utvecklingsmetoder, bristande säkerhetskompetens och ansvarstagande, försök att klistra på säkerheten i efterhand samt komplexiteten som följer av mjukvarans många funktioner (Karlzén m.fl., 2023).

FOI har också gett ut många andra rapporter som på någon nivå undersöker varför mjukvaror inte är helt säkra. En rapport som publicerades nyligen undersökte specifikt fältnära system som utvecklas åt Försvarsmakten. Den rapporten intervjuade intressenter och drog slutsatsen att ”processerna kan följas men ändå leda till it-system med sårbarheter som lätt hade kunnat undvikas” (Vestlund m.fl., 2024, s. 67). Den rapporten föreslår att anledningarna är avsaknad av vägledningar, bristande säkerhetskultur och brist på personal med rätt kompetens.

[3] Vår översättning av enkätfrågebilagan till Assal och Chiasson, (2019).

Utgångspunkten i den här rapporten är att mjukvaruutvecklare är centrala för mjukvarusäkerheten. Utvecklarna kan ju införa bra funktioner i mjukvarorna men också (oavsiktligt) införa sårbarheter. Ett sätt att studera vad utvecklarna kommer göra är att undersöka vad som ger upphov till utvecklarnas beteenden. Ett sätt att undersöka beteenden är just via motivationen till beteendet och via vilka hinder som finns för att utföra beteendet. Rapporten studerar dessa motivationer och hinder.

1.3 Vad är det intressanta med den här rapporten?

Den här rapporten undersöker utvecklares roll i mjukvarusäkerheten. Det är vanligt att skylla just på de som infört sårbarheterna, men å andra sidan är säkerhet inte huvudsysslan för en utvecklare. Det är därför relevant att undersöka vad som trots allt gör att utvecklare känner sig motiverade (eller hindrade) att bry sig om mjukvarusäkerheten. I projektets tidigare rapport (Karlzén m.fl., 2023) identifierades just behov av mer forskning om bland annat hur svenska utvecklares drivkrafter och attityder ser ut kring säkerhet. Den nya rapporten möter detta behov genom en enkätundersökning bland svenska mjukvaruutvecklare, som i huvudsak utvecklar för säkerhetskritisk verksamhet.

En liknande enkätundersökning genomfördes av Assal och Chiasson (2019)[4] med utvecklare i Nordamerika. De fann att utvecklarna var motiverade till att skapa säker mjukvara men också att de upplevde olika hinder för motivationen, såsom brist på resurser, kunskap, medvetenhet, verktyg eller tid.[5] Den här rapporten upprepar delar av enkätundersökningen, fast i en svensk kontext. Upprepningar kan vara svårgenomförda på grund av bristande metodbeskrivningar. Projektet kontaktade Assal som gav sitt stöd till vår enkätundersökning. Rapportens resultat jämförs även med den tidigare enkätundersökningen. Att upprepa tidigare forskning gör också att forskningen kvalitetssäkras (Ryan m.fl., 2023).

[4] Den tidigare enkätundersökningen refereras även till som ”den tidigare studien” i den här rapporten.

[5] De engelska orden för motivation och hinder är *motivation* och *deterrence* (eller *amotivation*), i enlighet med Assal (2018), som också beskriver den liknande enkätundersökningen (tidigare studien).

2 Forskningen utförs med en enkätundersökning

Detta kapitel beskriver hur enkätfrågorna togs fram utifrån en tidigare enkätstudie, hur den tidigare enkätens frågor översattes från engelska till svenska, hur datainsamlingen gick till samt hur insamlade data analyserades. De fullständiga enkätfrågorna finns i Bilaga A.

2.1 Enkätfrågorna togs fram i en annan studie

Enkätens centrala frågor (om framförallt motivation och hinder) är baserade på en tidigare enkät inom mjukvarusäkerhet från studien av Assal och Chiasson (2019). Den studiens frågor om motivation och hinder togs fram i deras intervjustudie med utvecklare, vilken beskrivs av Assal (2018). Det beskrivs att intervjusvaren analyserades genom att hitta teman i svaren med hjälp av grundad-teori-analys. Därtill konstaterades att intervjuanalysresultat visade på likheter med den etablerade självbestämmandeteorin om motivation för att utföra aktiviteter. I den teorin ses motivation som ett spektrum där motivationen varierar från externt reglerad till internt. För de mest interna motivations-faktorerna behövs ingen övertalning eller utvärdering, utan faktorerna rör glädje och njutning. För mer externa motivationsfaktorer sker mer eller mindre utvärdering av aktivitetens gynnsamhet. I extremfallet sker bara aktiviteten om de externa kraven är tillräckligt höga. Vi gjorde inte dessa intervjuer och analyser utan utgick från de frågor som användes i enkätundersökningen av Assal och Chiasson (2019). Valet av att återanvända deras enkätfrågor baserades dock delvis på tidigare intervjuer utförda i vårt projekt vid arbetet inför litteraturstudien av Karlzén m.fl. (2023).

2.2 Enkätfrågorna översattes till svenska

Översättningarna utgick från enkätfrågorna om motivation och hinder i den tidigare studien av Assal och Chiasson (2019). Dessa frågor översattes från engelska till svenska. Varje rapportförfattare genomförde en individuell översättning, varpå resultaten jämfördes i grupp. De individuellt framtagna översättningarna skiljde i de flesta fall inte markant. Det fanns dock oftast inte en specifik översättning som var uppenbart bättre än de andra och i flera fall tog gruppen fram en anpassad översättning eller i vissa fall en helt ny översättning.

Översättningarna testades sedan i tre steg:[6]

1. Två forskare från samma organisation som rapportförfattarna granskade översättningen genom att jämföra den mot originalfrågorna i den tidigare studien av Assal och Chiasson (2019). De ansåg att vissa av översättningarna hade onaturliga meningsbyggnader och bedömde att det var till flöjd av ordagrann översättning. Översättningen uppdaterades baserat på återkopplingen. Det förekom även synpunkter kopplat till ordningen på frågorna och att det fanns frågor med liknande innehåll, men dessa synpunkter lämnades utan åtgärd eftersom enkäten var avsedd att se ut så.
2. Fyra intervjuer à 1 timma genomfördes där utvecklare inom författarnas organisation fick svara på frågor om de översatta frågorna. Intervjuerna resulterade i anmärkningar som mestadels inte hade med språk att göra. Översättningen uppdaterades och förbättrades sedan baserat på resultatet från intervjuerna.
3. En pilotenkät genomfördes och skickades ut till 38 utvecklare inom samma organisation som författarna, varav 14 fullständiga svar inkom. Pilotenkäten skickades inte ut till de personer som varit delaktiga i tidigare granskningssteg. Pilotenkäten innehöll, utöver de frågor som ingick i den slutgiltiga enkäten, en fråga där respondenterna ombads att utvärdera enkäten utifrån hur väl ett antal påståenden stämde. Dessa påståenden var av typen ”frågorna var lätta att förstå”. Svaren på frågan visade att det inte fanns några svårigheter att tolka frågorna. Därtill var svaren på enkätens andra frågor rimliga och speciellt utifrån en jämförelse med den tidigare studien av Assal och Chiasson (2019). Därför gjordes bedömningen att enkäten var redo att skickas ut till målgruppen.

I den färdiga enkäten formulerades frågorna om motivation respektive hinder enligt exemplen i Figur 1 och Figur 2.

[6] Översättningsarbetet vägleddes av en etablerad metod för översättning av enkätfrågor: TRAPD-metoden (Survey Research Center, 2016) samt av en forskningsartikel om erfarenheter av översättningsarbete: Forsyth m.fl. (2006).

Hur väl stämmer följande påståenden?

Jag bryr mig om säkerhet eftersom...

	Stämmer mycket bra	Stämmer ganska bra	Stämmer varken bra eller dåligt	Stämmer ganska dåligt	Stämmer mycket dåligt	Ej tillämp-ligt
...företaget där jag arbetar gransk-as av en extern part med avse-ende på mjukvarusäkerhet.	○	○	○	○	○	○

Figur 1 En av enkätfrågorna om motivation.

Hur väl stämmer följande påståenden?

	Stämmer mycket bra	Stämmer ganska bra	Stämmer varken bra eller dåligt	Stämmer ganska dåligt	Stämmer mycket dåligt
Mjukvarusäkerhet är inte mitt an-svar eftersom det inte ingår i min arbetsbeskrivning	○	○	○	○	○

Figur 2 En av enkätfrågorna om hinder.

2.3 Enkäten skickades ut till svenska organisationer

Respondenter rekryterades genom att kontakta statliga myndigheter och företag som vi förmodade utvecklade mjukvara åt organisationer med höga cybersäkerhetsbehov. Sådana behov förekommer exempelvis i system som hanterar sekretessbelagd information, utför samhällsviktiga funktioner eller utsätts för en omfattande hotbild. Rapportförfattarna använde sin erfarenhet från FOI och utvecklingsföretag för att bedöma vilka svenska myndigheter och större företag som kunde ha sådana behov. Kontaktade organisationer fick även själva göra motsvarande bedömning. Till sist valde sju organisationer att delta, av tjugo kontaktade.

Deltagande organisationer fick under oktober–november 2024 en unik länk till en FOI-server med enkätmjukvaran Limesurvey. Länkarna distribuerades med hjälp av en kontaktperson i varje organisation. Organisationerna valde potentiella

respondenter i sina organisationer. De potentiella respondenterna fick själva välja om de ville samtycka till att svara på enkäten. Utifrån kontakten med kontaktpersonerna verkar de allra flesta av de potentiella respondenterna ha samtyckt. Vi har dock inte fullständig information om hur många personer som valde att inte samtycka eller alls klicka på enkätlänken. Respondenterna fick välja mellan att få enkätfrågorna på svenska (förvalt) eller på engelska. Alla valde svenska.

2.4 Enkäten besvarades av organisationernas utvecklare

De potentiella respondenterna i respektive organisation hade fyra veckor på sig att svara på enkäten och en påminnelse skickades ut efter två veckor. Alla utom fem respondenter svarade innan påminnelsen. Totalt inkom 66 fullständiga svar på enkäten. Tabell 1 visar antalet respondenter från varje organisation och vilken typ av organisation det rörde sig om. Över två tredjedelar av svaren kom från respondenter vid organisationer med 1 000 eller fler anställda.[7]

Tabell 1 Organisationstillhörigheter för de utvecklare som svarade på enkäten.

Organisation	**Antal**	**Procent**
Myndighet X	29	44 %
Myndighet Y	13	20 %
Företag 1	7	11 %
Företag 2	5	8 %
Företag 3	5	8 %
Företag 4	4	6 %
Myndighet Z	3	5 %
–	*66*	*100 %*

[7] Respondenterna från samma organisation höll inte alltid med varandra om organisationens storlek. Kanske har vissa svarat utifrån verksamhetsställen eller liknande.

Enligt enkätmjukvaran tog varje respondent 3–70 minuter (median 9 min.) för att svara på enkäten och svaren inkom 0–26 dagar (median 3 dagar) efter att länken skickades ut. Förutom frågor om motivationsfaktorer och hinder fick de frågor om sin erfarenhet av mjukvaruutveckling. I sitt nuvarande team hade respondenterna arbetat 0–12 år (median 3 år), i sin organisation 0–25 år (median 5 år) och som yrkesverksam utvecklare i 1–40 år (median 11 år). Medianerna är samma som i den tidigare studien av Assal och Chiasson (2019), utom för yrkesverksamhet där vår median är fyra år lägre.

2.5 Enkätsvaren analyserades

I möjligaste mån analyserades enkätsvaren på samma sätt som i studien av Assal och Chiasson (2019). Motivationsfaktorerna jämfördes med varandra utifrån respondenternas svar. För varje motivationsfaktor togs det också fram ett medelvärde av alla respondenters svar. De olika motivationsfaktorernas medelvärden jämfördes sedan med varandra. I jämförelserna ingick det att undersöka den statistiska signifikansen, dvs. om eventuella skillnader var statistiskt säkerställda och därmed troligen inte bara kan förklaras av slumpen. Eftersom många motivationsfaktorer jämförs med varandra ökar sannolikheten att få resultat som ser ut som statistiskt säkerställda. En justering med så kallad Bonferroni-korrektion gjordes då som kompensation för det stora antalet jämförelser.[8]

Svaren på enkätfrågorna om motivation jämfördes också med motsvarande svar i den tidigare studien av Assal och Chiasson (2019), när sådana data fanns. Detta inkluderade att gruppera motivationsfaktorerna enligt den studiens statistiska faktoranalys för att sedan jämföra grupperna mot varandra på liknande sätt som de enskilda motivationsfaktorerna. Hindren analyserades på motsvarande sätt som motivationsfaktorerna. Därtill undersöktes det om det fanns skillnader i svar mellan olika respondenter och om det i så fall berodde på olika organisationstillhörighet, olika erfarenhet, eller något annat.

En del detaljer om statistiken ges i fotnoter i resten av rapporten. De statistiska analyserna gjordes med kalkylprogrammet Excel och statistikprogrammet Jamovi.

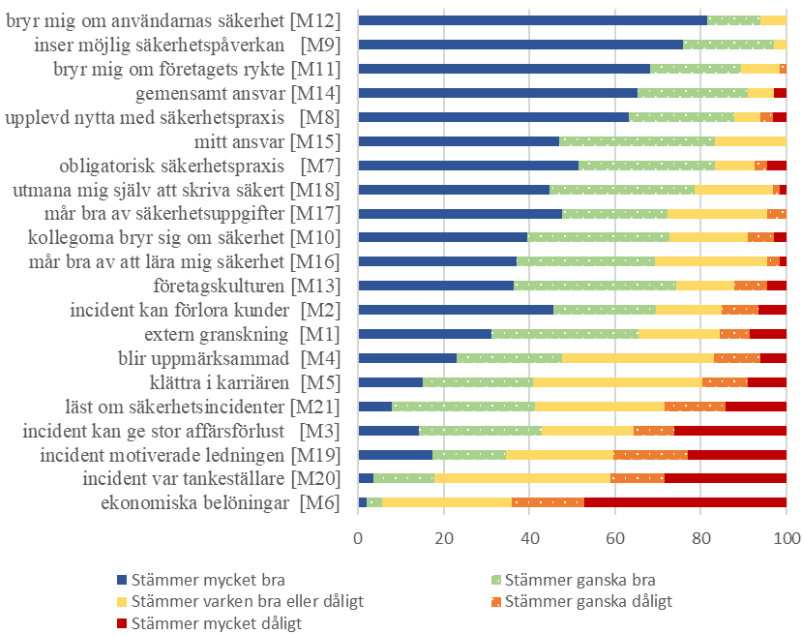
[8] Bonferroni-korrektion är väldigt konservativ (överdrivet noggrann) och multiplicerar varje p-värde med antalet jämförelser.

3 Utvecklare motiveras av mycket angående mjukvarusäkerhet

I detta kapitel beskrivs respondenternas svar på frågorna om motivation. Först ges en överblick över motivationsfaktorerna. Därefter följer beskrivningar av de största motivationsfaktorerna, de minsta motivationsfaktorerna samt en gruppering av motivationsfaktorerna.

3.1 Många viktiga motivationsfaktorer

När alla respondenters svar sammanvägs framkommer det att alla utom tre motivationsfaktorer har en medelbedömning som är minst *Stämmer varken bra eller dåligt*. För de största motivationsfaktorerna svarade de allra flesta respondenter med *Stämmer mycket bra*. En rankning av motivationsfaktorerna finns i Figur 3. Överst i figuren ligger den största motivationsfaktorn, vilken rankats högst. Det är alltså den motivationsfaktor där respondenterna i störst utsträckning instämt med att de motiveras av den. Ju längre ner i figuren man kommer desto mindre blir motivationsfaktorerna.



Figur 3 Vad som motiverar utvecklare till att bry sig om säkerhet. Motivationsfaktorerna har rankats där instämmande i skalsteg översatts till 1–5 och sedan adderats för varje respondent, följt av division med antalet bedömningar.

3.2 Intern motivation är viktigast

De största motivationsfaktorerna, längst upp i figuren, är *bryr mig om användarnas säkerhet (M12)*, *inser kodens möjliga säkerhetspåverkan (M9)*, *bryr mig om organisationens rykte (M11)*, *säkerhet är mitt ansvar* (M14), *säkerhet är ett gemensamt ansvar (M15)* samt *upplever nytta med obligatorisk säkerhetspraxis (M8)*.[9] Dessa faktorer har i viss mån gemensamt att de fokuserar på utvecklarnas ansvarstagande, men också deras medvetenhet. De största motivationsfaktorerna rör alltså intern motivation. Några lite mindre motivationsfaktorer rör ännu mer tydligt inre motivation, nämligen *gillar att utmana mig själv att skriva säkert (M18)* samt *mår bra av säkerhetsuppgifter (M17)* eller *mår bra av att lära mig om säkerhet (M16)*.

Det finns dock också motivationsfaktorer som rörde extern motivation. Där hittas *obligatorisk säkerhetspraxis som måste följas (M7)*, *kollegorna bryr sig om säkerhet (M10)*, *säkerhet är en del av organisationskulturen (M13)* samt *extern säkerhetsgranskning sker (M1)*. Dessa motivationsfaktorer är inte särskilt stora och ligger ungefär i mitten av figuren.

3.3 Extern motivation är mindre viktigt

Bland de minsta motivationsfaktorerna, längst ner i figuren, hittas *karriärfaktorer (M4, M5)*, *säkerhetsansträngningar belönas (M6)*, *potentiella affärsförluster (M3)* samt *incidenter som tankeställare för utvecklare eller som motiverar ledningen (M19, M20)*. Dessa är alla förknippad med extern motivation. Det är möjligt att utvecklare inte säger sig drivas av sådana belöningar för att deras organisation inte erbjuder belöningar.

På en del frågor använde många respondenter svarsalternativet *Ej tillämpligt*. Dessa frågor var *M3*, *M2*, *M19*, *M6*, *M20* och rör aspekter som inte nödvändigtvis är relevanta för alla organisationer och deras anställda.[10] Exempelvis anser vi det rimligt att myndighetsanställda tolkar frågor om konkurs eller att förlora kunder som mindre relevanta, än vad företagsanställda gör. Detta bekräftas också av några fritextsvar.

---

[9] Att dessa motivationsfaktorer är störst enligt figuren medför inte att det är statistiskt säkerställt att de verkligen är störst. För att jämföra de olika faktorerna används one-way ANOVA utan att anta lika varians, dvs. Welchs-Games-Howell. Som exempel är M12 signifikant större ($p < 0{,}001$, utan korrektion) än elva andra motivationsfaktorer. De tolv är de minsta motivationsfaktorerna i figuren, utom M2. Övriga stora motivationsfaktorer är större än ett urval av dessa samma motivationsfaktorer (men också i förekommande fall mindre än de som nämnts tidigare). Med Bonferroni-korrektion blir $p < 0{,}001 = 0{,}21$ vid 210 jämförelser (21 motiveringar som alla jämförs med varandra: 21*(21-1) = 210). På så vis skulle 0,001 inte ses som signifikant men korrektionen är överdrivet noggrant. Därtill skulle icke-korrigerade p-värden kunna vara mindre, eftersom detta är det minsta som visas av statistikprogrammet.

[10] Antalet respondenter som svarade *Ej tillämpligt* på respektive fråga var: M3 (24 ej tillämpligt), M2 (20), M19 (14), M6 (13), M20 (10).

3.4 Motivationsfaktorerna kan grupperas

I den tidigare studien av Assal och Chiasson (2019) grupperades motivationsfaktorerna i fem grupper: 1) *arbetsmiljö, 2) identifiering med att säkerhet är viktigt, 3) belöningar, 4) uppfattade negativa konsekvenser* samt *5) övrigt.* Den sista *övrigt*-gruppen innehöll motivationsfaktorer som inte passade i de andra grupperna och den gruppen undersöktes inte. Tabell 2 visar vilka säkerhetsrelaterade motivationsfaktorer som finns i vilken grupp. Med samma gruppering ger våra respondenters svar att gruppen med störst motivationsfaktorer (förklaringskraft) är *identifiering med att säkerhet är viktigt.*[11] Näst störst är *arbetsmiljö* och därefter *uppfattade negativa konsekvenser.* Gruppen med lägst bedömda motivationsfaktorer är *belöningar.*[12] Dessa resultat stämmer väl med den tidigare studien. Det kan också noteras att gruppen *belöningar* är den grupp som mest präglas av extern motivation.

Tabell 2 Gruppering av motivationsfaktorerna.

Id	**Arbetsmiljö**
M7	obligatorisk säkerhetspraxis
M8	upplevd nytta med obligatorisk säkerhetspraxis
M10	kollegornas bryr sig om säkerhet
M13	företagskulturen
Id	**Identifiering med att säkerhet är viktigt**
M9	inser möjlig säkerhetspåverkan
M11	bryr mig om företagets rykte
M12	bryr mig om användarnas säkerhet
M14	gemensamt ansvar
M15	mitt ansvar
M16	mår bra av att lära mig säkerhet
Id	**Belöningar**
M4	blir uppmärksammad
M5	klättra i karriären
M6	ekonomiska belöningar

[11] Reliabiliteten per grupp är för de tre första grupperna > 0,75 (mätt med Cronbachs alpha). Gruppen *Uppfattade negativa konsekvenser* har kraftigt undermålig reliabilitet: 0,03.

[12] Varje grupp jämfördes med varje annan grupp med hjälp av Wilcoxons icke-parametriska motsvarighet av t-test. Grupp 1 var större än varje annan grupp, p <= 0,001. Grupp 2 var därefter större än övriga grupper (utom grupp 1). Grupp 3 var större än grupp 4 med p = 0,046. Även det senare kan ses som statistiskt signifikant. Det är dock inte längre det efter att Bonferroni-korrektion appliceras (för sex jämförelser).

Id	**Uppfattade negativa konsekvenser**
M1	extern granskning
M21	läst om säkerhetsincidenter
Id	**Övrigt**
M2	incident kan förlora kunder
M3	incident kan ge stor affärsförlust
M17	mår bra av säkerhetsuppgifter
M18	utmana mig själv att skriva säkert
M19	incident motiverade ledningen
M20	incident var tankeställare

4 Utvecklare hindras delvis att bry sig om mjukvarusäkerhet

I detta kapitel beskrivs respondenternas svar på frågorna om potentiella hinder. Först ges en överblick över hindren. Därefter följer beskrivningar av de största hindren, de minsta hindren samt en gruppering av hindren. Som *hinder* (av motivationen) menas de faktorer som bidrar till att motivationen för någon aktivitet (såsom säkerhetsarbete) minskar eller helt uteblir. Dessa hinder kan uppstå för att utvecklaren upplever att aktiviteten: inte behöver göras; behöver göras av någon men inte just av utvecklaren ifråga; behöver göras av utvecklaren men med lägre prioritet än annat; eller behöver göras men är svårgenomfört eftersom nödvändiga verktyg saknas.

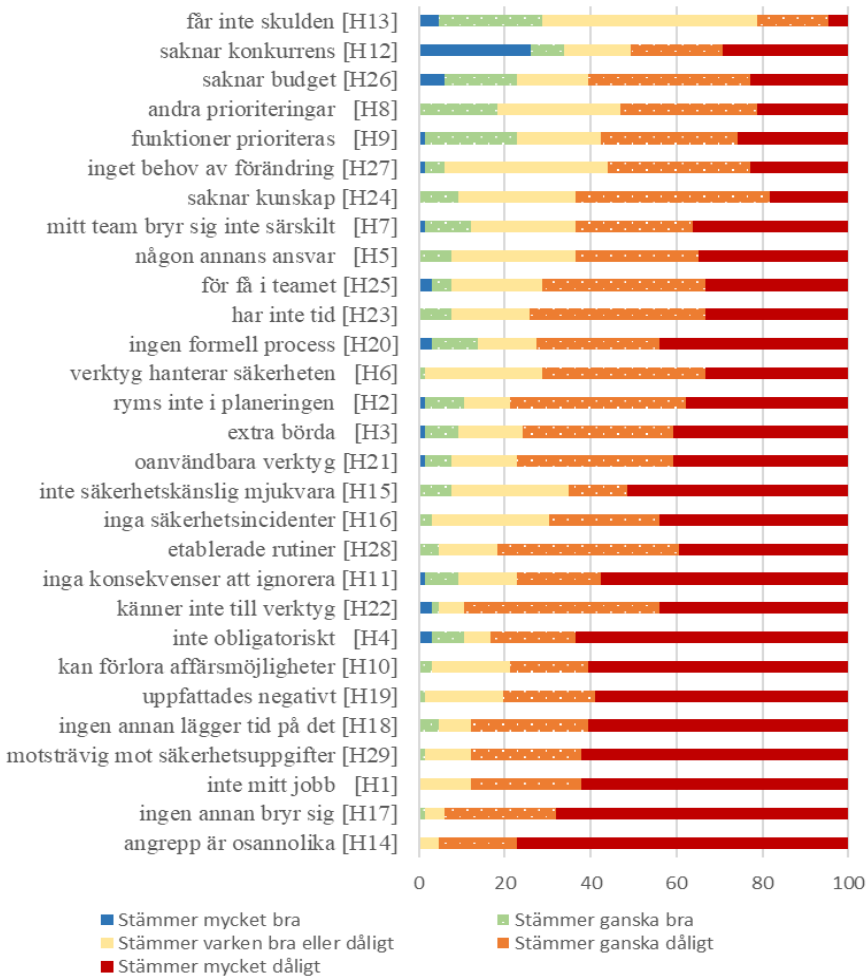
4.1 Hindren är små men många

När alla respondenters svar sammanvägs ger det en rankning av de potentiella hindren, vilket visas av Figur 4. Överst i figuren ligger det största hindret, som rankats högst. Det är alltså det hinder där respondenterna i störst utsträckning instämt med att de hindras av det. Ju längre ner i figuren man kommer desto mindre blir hindren. Vissa av hindren är blockerande eller avskräckande. Andra av hindren är mer renodlat motivationsmotverkande, som en anti-motivation.

Hindren har överlag lägre instämmanden än motivationsfaktorerna, med en medelbedömning för ett hinder som motsvarar *Stämmer ganska dåligt*.[13] En möjlig tolkning är att säkerhet prioriteras högt. Å andra sidan är hindren (29) fler än motivationsfaktorerna (21). Om några av hindren klumpades ihop skulle de kanske bli lika stora som motivationsfaktorerna överlag. Det är dock inte helt enkelt att hitta en bra gruppering av hindren. Generellt sett är skillnaderna i resultat mot den tidigare studien av Assal och Chiasson (2019) större för hindren än den var för motivationsfaktorerna.[14]

[13] Det finns också betydligt färre *Stämmer mycket bra* här (2 %), medan motivationsfaktorerna hade betydligt färre *Stämmer mycket dåligt* (8 %).

[14] För motivationsfaktorerna korrelerar vår ordning med den i Assal och Chiasson (2019), med rankningskorrelationerna Spearmans rho: 0,478 (p = 0,030) och Kendalls tau-b: (0,343 p = 0,031). För hindren finns ingen sådan statistiskt signifikant korrelation.



Figur 4 Vad som hindrar utvecklare från att bry sig mjukvarusäkerhet. Det högst rankade (största) hindret är överst. Hindren har rankats där instämmande i skalsteg översatts till 1–5 och sedan adderats för varje respondent, följt av division med antalet bedömningar.

4.2 Frånvaro av klander och konkurrens är de största hindren

De högst bedömda hindren, längst upp i figuren, är *får inte skulden om säkerhetsproblem hittas i min kod (H13)* och *saknar konkurrens så riskerar inte att förlora kunder (H12)*. Det förstnämnda hindret är klart störst[15] och det enda hindret där svarsalternativet *Stämmer* används av fler respondenter än *Stämmer inte*. Hindret *saknar konkurrens (H12)* är det hinder där flest respondenter använt svarsalternativet *Stämmer mycket bra*. Jämfört med den tidigare studien är båda dessa hinder (*saknar konkurrens, H12 och får inte skulden, H13*) klart större i vår studie, jämfört med övriga hinder.

Att hindret *saknar konkurrens (H12)* är ett relativt stort hinder, ganska högt upp i figuren, är inte så konstigt med tanke på att det är flera organisationer som inte är direkt konkurrensutsatta. Det finns också tydlig skillnad i svaren beroende på typen av organisation. Mer konkurrensutsatta organisationer bedömer hindret som lägre. Hur detta hinder ska hanteras för de övriga organisationerna, t.ex. vad gäller att öka konkurrensen, ligger utanför ramen för denna rapport.

Hindret *får inte skulden (H13)* kan innebära att utvecklarna vill ha mer ansvarsutkrävande. Å andra sidan kan det gå till överdrift där den som gjort något fel inte vågar erkänna det av risk för att råka ut för repressalier. Det går också att använda en mer positiv tolkning om att utvecklare accepterar att få skulden för säkerhetsproblem för att de ser sig som författare, vilket också kan vara en prestigefull roll. För detta hinder finns inte någon tydlig koppling till organisationstyp.

Ett relativt stort hinder är *funktioner levereras i tid prioriteras framför säkerhet (H9)* och det både i den här rapportens studie och i studien av Assal och Chiasson (2019). I vår studie är även det snarlika hindret *skjuter upp säkerheten på grund av andra prioriteringar (H8)* relativt stort, vilket också gäller *saknar budget för mjukvarusäkerhet (H26)*. Dessa hinder rör klassiska problem på säkerhetsområdet. Säkerheten ses ofta enbart som en kostnad, medan de positiva effekterna av att undvika säkerhetsincidenter inte lyfts fram på ett övertygande sätt.[16]

[15] Welchs-Games-Howell ger att H13 är statistiskt signifikant större ($p < 0{,}001$ utan korrektion) än alla hinder (utom H8, H9, H12, H26). H12 är på liknande sätt större än H1, H10, H14, H17, H18, H19, H29.

[16] Mer om ekonomi och informationssäkerhet går att läsa i FOI-rapporten av Hermelin m.fl. (2014).

4.3 Säkerhetsfokus verkar göra många hinder små

Bland de minsta hindren, längst ner i figuren, skiljer det inte så mycket i respondenternas bedömningar. Detta gällde också den tidigare studien av Assal och Chiasson (2019). Generellt sett är hindren mindre än i den tidigare studien, vilket ses i skillnaden i medel på cirka ett halvt skalsteg och framförallt genom fler *Stämmer inte alls* här. Detta kan bero på att vår studie främst innehåller respondenter från organisationer där säkerhet är viktigare än i de flesta organisationer. Den andra studien hade en mer allmän samling utvecklare som respondenter.

De specifika hinder som är mindre än i den tidigare studien (och bland de minsta här) är framförallt *osannolikt att vi angrips (H14)* och *säkerhet är inte mitt jobb (H1)*.[17] Mindre än den tidigare studien (men i mitten) är även *känner inte till säkerhetsverktyg (H22)* samt till viss del *mer fokus på säkerhet kan ge förlorade affärsmöjligheter (H10)*, *osannolikt att mjukvaran drabbas av angrepp (H15)* och *ingen formell process för säkerhet (H20)*. Anledningarna till att dessa hinder är mindre kan även bero på att våra respondenter har mer säkerhetsfokus. I båda studierna är *jag är motsträvig mot säkerhetsuppgifter (H29)* ett litet hinder. Det visar på att det finns en allmän syn på att säkerhet är viktigt.

4.4 Hindren är svårgrupperade

I studien av Assal och Chiasson (2019) grupperades hindren i flera grupper men bara en grupps resultat skiljde sig från övriga gruppers. Detta gäller också i vår studie när samma gruppering sker.[18] Gruppen benämns *desillusionerad* och omfattar hindren *ingen annan bryr sig om säkerhet (H17)*, *ingen annan lägger tid på säkerhet (H18)* och jag *uppfattades negativt när jag brydde mig om säkerhet (H19)*. Desillusionerad innebär en arbetsmiljö där säkerhetsansträngningar motarbetas snarare än uppmuntras. Att grupperingen fungerar bra tyder på att dessa hinder är relativt lika varandra och att övriga hinder inte har samma likhet sinsemellan. Att de desillusionerade hindren dessutom avviker från övriga hinder kan bero på det faktum att de också är bland de minsta hindren i båda studierna. Det kan i sin tur bero på att den allmänna säkerhetskulturen är stark och att säkerhetsarbete utförs och uppskattas.

[17] Dessa skillnader har bedömts utifrån en figur i den tidigare studien.

[18] $p < 0{,}001$ med Wilcoxons test, jämfört med var och en av de andra tre grupperna.

5 Organisationer kan i viss mån utföra förbättringsinsatser

I de följande diskussionsavsnitten beskrivs förslag på hur organisationer kan arbeta med att förbättra sig när det gäller säkerhetsmässiga motivationsfaktorer och hinder. Därtill beskrivs hur olika organisationer och utvecklare kan behöva olika förbättringsinsatser. Läsaren bör ha i åtanke att enkätsvaren är utvecklarnas egna bedömningar och upplevelser. Förmodligen skulle observationer av utvecklarnas faktiska beteende visa en delvis annan bild (Assal och Chiasson, 2019). Detta är normalt för enkätstudier.

5.1 Hur kan motivationen ökas?

Det finns störst utrymme att öka motivationsfaktorer som är små. Då kan det vara nödvändigt att genomföra förändringar som påverkar i önskad riktning för ökad säkerhet. De minsta motivationsfaktorerna rör extern motivation som karriärklättring, belöningar, affärsförluster samt incidenter som drabbat organisationen eller liknande mjukvaror hos andra. Om respondenterna varit med om incidenter är det intressant att de inte motiveras av incidenterna, vilket kan innebära att inga lärdomar dras. Det är också möjligt att respondenterna inte varit med om incidenter. Att de minsta motivationsfaktorerna rör extern motivation kan utgöra en särskild utmaning för de verksamhetsledare som tvärtom styr sin verksamhet utifrån ekonomiska faktorer och hierarkisk organisering.[19] Å andra sidan är det förstås bekvämt att inte behöva skjuta till särskilda medel eller befordringar för att driva säkerhetsarbetet. Även här behöver resultaten dock tolkas med försiktighet. Det är möjligt att säkerheten skulle kunna bli bättre om det fanns större möjligheter att få uppskattning för sitt säkerhetsarbete.

Det finns också motivationsfaktorer som rör extern motivation och som ligger i mitten bland alla faktorer. En sådan motivationsfaktor rör extern granskning. Utifrån organisationsspecifika svar är det rimligt att anta att vissa organisationer har mer extern granskning än andra.[20] Om sådan granskning inte finns på plats är det knappast heller möjligt att motiveras av den. Å andra sidan är extern granskning ofta lagstadgad eller på annat sätt ett resultat av reglering, vilket innebär att det är svårt att påverka dess förekomst. Om frånvaron av reglering är ett resultat av lägre bedömda risker behöver detta inte vara ett problem. Några andra motivationsfaktorer som ligger i mitten är organisationens säkerhetskultur och kollegornas säkerhetsattityder. Här krävs förmodligen allmänna

[19] En studie om ledarskapsstilar för olika chefsnivåer beskrivs i en forskningsartikel av Oshagbemi och Gill (2003).

[20] Det finns dock inga tydliga mönster mellan organisationer för antal svar med *Ej tillämpligt* för frågan.

organisatoriska förbättringar. Sådana förbättringar har studerats av FOI i ett tidigare projekt, där chefshandledning kombinerats med medarbetarutbildning. Särskilt chefernas ageranden förbättrades ur ett informationssäkerhetsperspektiv (Pousette m.fl., 2023, s. 22-25).

Även om hög motivation uppnås betyder inte det att det automatiskt blir lagom hög säkerhet. Det kan finnas andra faktorer som hindrar omsättandet av motivation i bra säkerhetsarbete. Exempelvis är kanske säkerhetsverktyg alltför dåliga eller mjukvaror alltför komplexa för att undvika större mängder sårbarheter. Hög motivation behöver inte heller innebära hög medvetenhet om hoten och lösningarna. Att öka säkerhetsmedvetenheten har visat sig någorlunda påverkansbart genom utbildningar och liknande insatser (Cram m.fl., 2019; samt Sommestad och Karlzén, 2019). Exempelvis kan insatser fokusera på att höja medvetenheten för vilka negativa konsekvenser säkerhetsincidenter kan ha för användarna och för företagets rykte. Ett snarlikt sätt att arbeta för öka säkerhet är att öka samarbetsytorna mellan utvecklare och säkerhetsexperter, genom exempelvis säkerhetsförkämpar som visar vägen med personligt engagemang (Haney m.fl., 2018). Å andra sidan kan förkämpar också leda till att andra utvecklare tror sig slippa ta säkerhetsmässigt ansvar (Thomas m.fl., 2018).

5.2 Hur kan hindren undanröjas?

Överlag är hindren bedömda som små. Å andra sidan är hindren nästan femtio procent fler än motivationsfaktorerna. Om några av hindren klumpades ihop skulle de kanske var och en bli ungefär lika stora som var och en av motivationsfaktorerna. Ett av de relativt största hindren rör avsaknad av konkurrens, och då bland de organisationer som inte är konkurrensutsatta. Det ligger dock utanför ramen för denna rapport att analysera eventuellt behov av ökad konkurrens. Det andra relativt stora hindret rör att utvecklare inte upplever att de kommer få skulden vid säkerhetsproblem. Här finns det utrymme för mer ansvarstagande och den potentiella yrkesstolthet som kommer med det, men med beaktande av att det kan leda till en repressiv kultur där säkerhetsincidenter inte rapporteras.

Det finns också någorlunda stora hinder som rör prioriteringar och budgetering. Sådana hinder är förmodligen svåra för utvecklarna själva att påverka. Troligen krävs snarare att organisationsledningarna inser vikten av förebyggande säkerhetsarbete. Att höja statusen hos säkerhetsarbete kan vara en möjlighet. Exempelvis har Microsoft nyligen gjort säkerhet till högsta prioritet för varje medarbetare (Nadella, 2024). Denna ändring verkar ha skett till följd av yttre påverkan från tillsynsmyndigheter. Sådant kan ha betydelse även i Sverige.

Bland de minsta hindren finns aspekter som att vara motsträvig mot säkerhetsuppgifter, inte se säkerhet som ens jobb och att det till och med upplevs negativt med kollegor som bryr sig om säkerhet. Att dessa hinder är små kan bero på att den allmänna säkerhetskulturen är stark samt att säkerhetsarbete redan nu utförs och uppskattas.

Jämfört med den tidigare studien av Assal och Chiasson (2019) är skillnaderna generellt sett större för hindren än för motivationsfaktorerna. Detta tyder på att olika organisationer behöver komma till rätta med olika hinder, eller åtminstone prioritera olika. Jämfört med den tidigare studien ser våra respondenter många hinder som mindre, kanske för att deras organisationer har mer säkerhetsfokus.

5.3 Är alla utvecklare likadana?

Utvecklare kan på flera sätt skilja sig från varandra. Det kan handla om skillnader i sådant som personlighet och erfarenhet. Det kan också handla mer om att de är verksamma i olika organisationer och att organisationerna skiljer sig åt. Dessa möjliga skillnader diskuteras närmare nedan.

Det är möjligt att bra säkerhetsbeteende samvarierar med ett ansvarstagande som i sin tur samvarierar med vedertagna psykologiska personfaktorer som exempelvis samvetsgrannhet. Då skulle bra säkerhetsbeteende, i åtminstone viss mån, kunna bero på utvecklarens inneboende personlighet. Exempelvis verkar utvecklare med ett öppet sinne utveckla säkrare kod (Mokhberi och Beznosov, 2021). Med andra ord skulle organisatoriska förbättringsinsatser handla mindre om att utbilda och mer om att anställa personer med rätt personlighet. Alternativt skulle förbättringsinsatserna behöva anpassas till de olika personernas styrkor och svagheter. I den här rapportens resultat finns det dock begränsat stöd för personberoende. Exempelvis verkar erfarenhet inte ha någon koppling till motivationsfaktorer och hinder.[21] Det finns det både par av utvecklare som svarat väldigt likt varandra och par vars svar inte alls har statistiskt signifikant korrelation med varandra. Detta är normalt för enkäter och det är svårt att analysera detta vidare utifrån enkätsvaren.

[21] Det fanns en Bonferroni-korrigerad korrelation $p < 0,10$ mellan erfarenhet och någon av variablerna: Kendall's tau-b 0,290 ($p = 0,084$) för yrkeserfarenhet och motivation rörande organisationens rykte. Det vore i och för sig rimligt om den som är mer etablerad i branschen också bryr sig mer om branschens företag, men detta är knappast specifikt för mjukvarusäkerhet.

Utvecklare arbetar i olika organisationer och dessa organisationer kan skilja sig från varandra genom till exempel olika krav på extern granskning eller olika konkurrens. Då kan även utvecklarnas arbete skilja sig och på så vis göra att deras svar inte är helt jämförbara. Det är också känt att allmänna bedömningar av säkerhetsbeteende inte är lika tillförlitliga som bedömningar av mer konkret beteende. Allmän beteendeforskning har också visat att skillnader kan uppstå redan av små subtila skillnader i specificerat beteende.[22] Med detta i åtanke kan intentionen att utveckla säkert vara högre innan arbetsdagens andra arbetsuppgifter och tillhörande stress tillkommit.

I våra resultat skiljer sig inte svaren så mycket åt från utvecklare verksamma i olika organisationer. Organisationsmedel för hinderfrågorna uppvisar samband mellan myndigheter samt samband mellan företag, men inte mellan myndigheter och företag.[23] Våra resultat skiljer sig delvis från den tidigare studien av Assal och Chiasson (2019) som utfördes med utvecklare från Nordamerika. Det är möjligt att nationell kultur kan förklara en del av skillnaderna i svar. Jämfört med den tidigare studien ser vi störst skillnad vad gäller vilka hinder som är stora. Kanske beror detta på att hinder är mer beroende på populationen. Det kan dock också bero på att hinder är svårare att mäta eftersom de är relaterade till alla andra beteenden (som kanske prioriteras högre), medan motivationsfaktorer är ett mer avgränsat säkerhetsbeteende. Samtidigt bör läsaren ha i åtanke att respondenterna i enkätundersökningen delvis valdes ut baserat på forskarnas kännedom om relevanta organisationer. Därtill bestämde organisationerna själva vilka utvecklare som skulle erbjudas att vara respondenter. Andra utvecklare skulle förmodligen ha delvis andra svar.

Något som talar emot att organisationer har olika säkerhetsproblem är mjukvarors täta sammanvävning i komplexa leveranskedjor. Som en respondent uttryckte det i enkätens avslutande fritextfält: *”kod kan ligga orörd och samla på sig säkerhetshål i tredjepartbibliotek i flera år innan de åtgärdas då hantering av teknisk skuld och förvaltning inte prioriteras”.* Mer om säkerhetsrisker i leveranskedjor kan läsas om i en annan FOI-rapport av Eidenskog m.fl. (2019).

[22] Som Ajzen (2015) påpekar kan hypotetiska situationer i exempelvis enkäter skilja sig från verkliga situationer: intentionen att träna efter jobbet kan vara högre på morgonen (vid enkätbedömningen), men mindre efter jobbet (när det väl är dags att träna).

[23] Myndigheterna är betydligt större varför försiktighet bör iakttas vid tolkningen av detta resultat. Därtill saknades sambandet för motivationsfaktorerna. För hinder- och motivationsfrågor tillsammans var korrelationen ($p < 0{,}001$) allt från 0,35 mellan två par organisationer till 0,80.

6 Svaren på forskningsfrågorna

Resultaten från enkätundersökningen med svenska utvecklare gör att de två forskningsfrågorna kan besvaras enligt nedan.

Vad motiverar mjukvaruutvecklare till att bry sig om mjukvarusäkerhet?

Utvecklarna motiveras mest av interna motivationsfaktorer såsom ansvarstagande och medvetenhet. De tvärtom minst motiverande faktorerna är externa och rör sådant såsom karriärklättring, belöningar, affärsförluster och inträffade incidenter. Organisationer som drivs utifrån dessa mindre viktiga faktorer kan därför hamna snett. Å andra sidan bör man inte falla i den klassiska fällan där säkerhetsarbete upplevs som otacksamt och inte belönas eller uppmuntras.

Vad hindrar mjukvaruutvecklare från att bry sig om mjukvarusäkerhet?

Hindren är små men många. Två hinder är klart störst där det ena rör avsaknad av konkurrens, specifikt bland de organisationer som inte är konkurrensutsatta. Det andra stora hindret rör att utvecklare inte upplever att de kommer få skulden vid säkerhetsproblem. Här finns det utrymme för mer ansvarstagande, men utan att det leder till en repressiv kultur där säkerhetsincidenter inte rapporteras. Bland hindren syns också prioritering och budgetering. Här kan tillsynsmyndigheter spela en roll som extern motivation genom olika regleringar. Det bör noteras att de största hindren skiljer sig från den nordamerikanska studien av Assal och Chiasson (2019). Kanske är alla utvecklare motiverade på samma sätt, men hindrade på olika sätt.

7 Referenser

Acar, Y., Fahl, S., & Mazurek, M. L. (2016). You are not your developer, either: A research agenda for usable security and privacy research beyond end users. *2016 IEEE Cybersecurity Development (SecDev)*, 3-8. https://doi.org/10.1109/SecDev.2016.013

Ajzen, I. (2015). The theory of planned behaviour is alive and well, and not ready to retire: a commentary on Sniehotta, Presseau, and Araújo-Soares. *Health psychology review*, 9(2), 131-137. https://doi.org/10.1080/17437199.2014.883474

Assal, H. (2018). *The human dimension of software security and factors affecting security processes* (Doktorsavhandling, Carleton University). https://doi.org/10.22215/etd/2018-13347

Assal, H., & Chiasson, S. (2019). 'Think secure from the beginning' A Survey with Software Developers. *Proceedings of the 2019 CHI conference on human factors in computing systems* (pp. 1-13). https://doi.org/10.1145/3290605.3300519

Cram, W. A., D'arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. *MIS quarterly*, 43(2), 525-554. https://doi.org/10.25300/misq/2019/15117

Eidenskog D., Bildsten C., & Endres B. (2019). *Säkra leveranskedjor för IT-system*. FOI-R--4851--SE. Totalförsvarets forskningsinstitut.

Forsyth, B. H., Kudela, M. S., Lawrence, D., Levin, K., & Willis, G. B. (2006). Methods for translating survey questionnaires. *American Association for Public Opinion Research*, 4114-4119.

Haney, J. M., Theofanos, M., Acar, Y., & Prettyman, S. S. (2018). "We make it a big deal in the company": Security Mindsets in Organizations that Develop Cryptographic Products. *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)* (s. 357-373).

Hermelin J., Karlzén H., & Nilsson P. (2014). *Informationssäkerhet och ekonomi – Ett skannande projekt av aktuell forskning*. FOI-R--3927--SE. Totalförsvarets forskningsinstitut.

Karlzén H., Eidenskog D., Falkcrona J., & Valassi C. (2023). *Varför har mjukvaror sårbarheter?* FOI-R--5550--SE. Totalförsvarets forskningsinstitut.

McGraw, G. (2004). Software security. *IEEE Security & Privacy*, 2(2), 80-83. https://doi.org/10.1109/MSECP.2004.1281254

Mokhberi, A., & Beznosov, K. (2021). SoK: human, organizational, and technological dimensions of developers' challenges in engineering secure software. *Proceedings of the 2021 European Symposium on Usable Security* (s. 59-75). https://doi.org/10.1145/3481357.3481522

Nadella S. (2024). *Prioritizing security above all else.* Microsoft. https://blogs.microsoft.com/blog/2024/05/03/prioritizing-security-above-all-else/

Oshagbemi, T., & Gill, R. (2004). Differences in leadership styles and behaviour across hierarchical levels in UK organisations. *Leadership & Organization Development Journal*, 25(1), 93-106.

Pousette m.fl. (2023). *Informationssäkerhetskultur i praktiken – Populärvetenskaplig sammanfattning*. MSB2283. Myndigheten för samhällsskydd och beredskap.

Ryan, I., Roedig, U., & Stol, K. J. (2023). Unhelpful assumptions in software security research. *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (s. 3460-3474). https://doi.org/10.1145/3576915.3623122

Sektor CERT. (2023). The attack against Danish, critical infrastructure. https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf

Sommestad, T., & Karlzén, H. (2019). A meta-analysis of field experiments on phishing susceptibility. *2019 APWG symposium on electronic crime research (eCrime)*, 1-14. https://doi.org/10.1109/eCrime47957.2019.9037502

Survey Research Center. (2016). *Guidelines for Best Practice in Cross-Cultural Surveys*. ISBN 978-0-9828418-2-2 (pdf). University of Michigan.

Thomas, T. W., Tabassum, M., Chu, B., & Lipford, H. (2018). Security during application development: An application security expert perspective. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (s. 1-12). https://doi.org/10.1145/3173574.3173836

Vestlund C., Nilsson S., Karlzén H., & Eidenskog D. (2024). *IT-säkerhet fram till frontlinjen - Utvecklingsprocesser för IT-system i Försvarsmakten*. FOI-R--5598--SE. Totalförsvarets forskningsinstitut.

Bilaga A: Enkätfrågor

Nedan återges enkäten. Motivationsfaktorerna står under ”Påståenden: Del 1/2" medan hindren står under ”Påståenden: Del 2/2”. Versionen av enkäten nedan skiljer sig något åt från hur respondenterna såg den i det mer interaktiva enkätverktyget. Exempelvis finns det variationer i texten om hur varje svar skulle fyllas i.

Utvecklares syn på mjukvarusäkerhet

Det finns 6 frågor i denna enkät.

Utvecklares syn på mjukvarusäkerhet

Information om enkäten

Enkäten riktar sig till dig som utvecklar mjukvara åt organisationer med höga cybersäkerhetsbehov, exempelvis i system som hanterar sekretessbelagd information, utför samhällsviktiga funktioner eller utsätts för en omfattande hotbild.

I enkäten frågar vi om ditt företag. Med det avses den organisation du arbetar för, dvs. ett företag, en myndighet eller en annan typ av organisation.

Vi som tagit fram enkäten är forskare inom cybersäkerhet vid Totalförsvarets forskningsinstitut, FOI. I denna studie undersöker vi hur utvecklare ser på sårbarheter i mjukvara. Studien finansieras av Försvarsmakten.

Dina svar är värdefulla för oss och vi hoppas att du svarar på enkäten!

Att svara på enkäten

Vi bedömer att det tar **ca 15 minuter** att svara på enkäten. Sista svarsdag är **8 november**.

Du kan välja att besvara enkäten på svenska eller engelska.

Frågor om enkäten

Om du har frågor om enkäten får du gärna höra av dig till oss.
(kontaktuppgifter)

Hantering av dina data

Om du väljer att svara på enkäten kommer vi att spara dina svar och sammanställa dem tillsammans med andra respondenters svar. De sammanställda resultaten från studien kan komma att publiceras i vetenskapliga artiklar och publikt tillgängliga rapporter. Svaren lagras enligt arkivlagens bestämmelser i minst tio år.

För att besvara enkäten behöver du ge ditt informerade samtycke till behandlingen av dina svar. Behandlingen av dina personuppgifter sker i enlighet med dataskyddsförordningen (GDPR). Du kan när som helst dra tillbaka ditt samtycke och i sådana fall tar vi bort dina svar eller anonymiserar dem helt. Om du väljer att inte svara på enkäten eller vill avbryta ditt deltagande behöver du inte uppge varför. Om du vill ta del av dina registrerade uppgifter ska du kontakta

forskaren som leder studien (se ovan) eller FOI:s dataskyddsombud (dataskyddsombud@foi.se, 08-555 030 00). Om du är missnöjd med hur dina personuppgifter behandlas kan du rätt att klaga hos Integritetsskyddsmyndigheten (IMY), som är tillsynsmyndighet.

Informerat samtycke – deltagande i denna studie

Du behöver bekräfta ditt informerade samtycke för att delta i denna studie och fortsätta till enkätfrågorna.

Du måste bocka i alla tre rutorna för att fortsätta.
Välj **alla** som stämmer:

- ☐ Jag har läst informationen som ges under rubriken "Hantering av dina data" ovan.
- ☐ Jag samtycker till att delta i denna studie.
- ☐ Jag samtycker till att mina data behandlas i den här studien.

Bakgrund

Hur länge har du arbetat... *

Endast tal får anges i dessa fält.
Skriv ditt/dina svar här:

...i ditt nuvarande företag?

...i ditt nuvarande team?

...som yrkesverksam utvecklare?

Företaget där du arbetar

Hur många anställda har företaget du arbetar på? *

Välj ett av följande svar
Välj **bara en** av följande:

- ◯ 1 till 9
- ◯ 10 till 249
- ◯ 250 till 499
- ◯ 500 till 999
- ◯ 1 000 eller fler

Påståenden: Del 1/2

Hur väl stämmer följande påståenden?

Jag bryr mig om säkerhet eftersom... *

Välj det korrekta svaret för varje punkt:

	Stämmer mycket bra	Stämmer ganska bra	Stämmer varken bra eller dåligt	Stämmer ganska dåligt	Stämmer mycket dåligt	Ej tillämpligt
...företaget där jag arbetar granskas av en extern part med avseende på mjukvarusäkerhet.	◯	◯	◯	◯	◯	◯
...företaget där jag arbetar skulle förlora kunder om mjukvarusäkerheten brast.	◯	◯	◯	◯	◯	◯
...företaget där jag arbetar skulle kunna gå i konkurs (eller upphöra med verksamheten) om mjukvarusäkerheten brast.	◯	◯	◯	◯	◯	◯
...mina ansträngningar för mjukvarusäkerhet uppmärksammas.	◯	◯	◯	◯	◯	◯
...mina ansträngningar för mjukvarusäkerhet hjälper mig att växa inom företaget.	◯	◯	◯	◯	◯	◯

	Stämmer mycket bra	Stämmer ganska bra	Stämmer varken bra eller dåligt	Stämmer ganska dåligt	Stämmer mycket dåligt	Ej tillämpligt
...mina ansträngningar för mjukvarusäkerhet belönas ekonomiskt (genom bonusar eller löneförhöjning).	◯	◯	◯	◯	◯	◯
...företaget jag arbetar för har en obligatorisk säkerhetspraxis och jag måste följa den.	◯	◯	◯	◯	◯	◯
...jag ser nyttan med den säkerhetspraxis som krävs av det företag jag arbetar för.	◯	◯	◯	◯	◯	◯
...jag inser att min kod kan ha säkerhetspåverkan.	◯	◯	◯	◯	◯	◯
...mina kollegor bryr sig om mjukvarusäkerhet.	◯	◯	◯	◯	◯	◯
...jag bryr mig om ryktet för företaget där jag arbetar.	◯	◯	◯	◯	◯	◯
...jag bryr mig om mina användares säkerhet och personliga integritet.	◯	◯	◯	◯	◯	◯
...mjukvarusäkerhet är en del av kulturen på	◯	◯	◯	◯	◯	◯

	Stämmer mycket bra	Stämmer ganska bra	Stämmer varken bra eller dåligt	Stämmer ganska dåligt	Stämmer mycket dåligt	Ej tillämpligt
företaget där jag arbetar.						
...mjukvarusäkerhet är ett gemensamt ansvar för alla inblandade i utvecklingslivscykeln.	◯	◯	◯	◯	◯	◯
...jag ser mjukvarusäkerhet som mitt ansvar.	◯	◯	◯	◯	◯	◯
...jag mår bra när jag lär mig mer om mjukvarusäkerhet.	◯	◯	◯	◯	◯	◯
...jag mår bra när jag hanterar potentiella säkerhetsproblem i min kod.	◯	◯	◯	◯	◯	◯
...jag gillar att utmana mig själv att skriva säker kod.	◯	◯	◯	◯	◯	◯
...en mjukvara liknande den som jag arbetar med drabbades av en säkerhetsincident och ledningen bryr sig nu om att säkra våra applikationer.	◯	◯	◯	◯	◯	◯

	Stämmer mycket bra	Stämmer ganska bra	Stämmer varken bra eller dåligt	Stämmer ganska dåligt	Stämmer mycket dåligt	Ej tillämpligt
...en mjukvara liknande den som jag arbetar med drabbades av en säkerhetsincident, vilket blev en ögonöppnare för mig.	◯	◯	◯	◯	◯	◯
...jag insåg att det är viktigt att säkra min kod efter att ha läst om säkerhetsincidenter i nyheterna.	◯	◯	◯	◯	◯	◯

Påståenden: Del 2/2

Hur väl stämmer följande påståenden? *

Välj det korrekta svaret för varje punkt:

	Stämmer mycket bra	Stämmer ganska bra	Stämmer varken bra eller dåligt	Stämmer ganska dåligt	Stämmer mycket dåligt
Mjukvarusäkerhet är inte mitt ansvar eftersom det inte ingår i min arbetsbeskrivning	◯	◯	◯	◯	◯
Mjukvarusäkerhet ryms inte i min planering.	◯	◯	◯	◯	◯
Mjukvarusäkerhet är en börda utöver mina huvudsakliga ansvarsområden.	◯	◯	◯	◯	◯
Mjukvarusäkerhet är inte något som min arbetsgivare kräver.	◯	◯	◯	◯	◯
Mjukvarusäkerhet hanteras av någon annan under produktens livscykel.	◯	◯	◯	◯	◯
Vi behöver inte oroa oss så mycket för säkerhet eftersom de ramverk (inklusive API:er) och interna programmeringsverktyg vi använder hanterar	◯	◯	◯	◯	◯

	Stämmer mycket bra	Stämmer ganska bra	Stämmer varken bra eller dåligt	Stämmer ganska dåligt	Stämmer mycket dåligt
mjukvarusäkerhet åt oss.					
Mitt team anstränger sig inte specifikt för mjukvarusäkerhet.	◯	◯	◯	◯	◯
Vi skjuter upp mjukvarusäkerhet på grund av andra prioriteringar.	◯	◯	◯	◯	◯
I mitt team är det viktigare att leverera funktioner i tid än att hantera mjukvarusäkerhet.	◯	◯	◯	◯	◯
Om företaget jag arbetar på fokuserar mer på mjukvarusäkerhet kan vi förlora affärsmöjligheter.	◯	◯	◯	◯	◯
Att ignorera mjukvarusäkerhet får inga konsekvenser.	◯	◯	◯	◯	◯
Företaget jag arbetar på saknar konkurrens, så vi riskerar inte att förlora kunder på grund av mjukvarusäkerhetsproblem.	◯	◯	◯	◯	◯

	Stämmer mycket bra	Stämmer ganska bra	Stämmer varken bra eller dåligt	Stämmer ganska dåligt	Stämmer mycket dåligt
Jag kommer inte att få skulden om ett säkerhetsproblem hittas i min kod.	◯	◯	◯	◯	◯
Det är osannolikt att en antagonist skulle attackera oss.	◯	◯	◯	◯	◯
Det är osannolikt att mjukvaran som jag utvecklar drabbas av angrepp.	◯	◯	◯	◯	◯
Det är bra som det är, företaget jag arbetar på har inte upplevt några säkerhetsincidenter.	◯	◯	◯	◯	◯
Ingen annan bryr sig om mjukvarusäkerhet, jag gör det inte heller.	◯	◯	◯	◯	◯
Jag förstår vikten av att beakta säkerhet, men jag kommer inte slösa tid på det när ingen annan gör det.	◯	◯	◯	◯	◯

	Stämmer mycket bra	Stämmer ganska bra	Stämmer varken bra eller dåligt	Stämmer ganska dåligt	Stämmer mycket dåligt
Jag brukade driva på inom mjukvarusäkerhet, vilket uppfattades negativt av mina kollegor.	◯	◯	◯	◯	◯
Företaget jag arbetar på har inte någon formell process för mjukvarusäkerhet.	◯	◯	◯	◯	◯
Tillgängliga säkerhetsrelaterade kodanalysverktyg är inte användbara.	◯	◯	◯	◯	◯
Jag känner inte till verktyg som möjliggör säkerhetsanalys av min kod.	◯	◯	◯	◯	◯
Jag har inte tid att hantera mjukvarusäkerhet.	◯	◯	◯	◯	◯
Jag har inte tillräcklig kunskap för att hantera mjukvarusäkerhet.	◯	◯	◯	◯	◯
Vi är för få i mitt team för att hantera mjukvarusäkerhet.	◯	◯	◯	◯	◯

	Stämmer mycket bra	Stämmer ganska bra	Stämmer varken bra eller dåligt	Stämmer ganska dåligt	Stämmer mycket dåligt
Mitt team saknar budget för att hantera mjukvarusäkerhet.	◯	◯	◯	◯	◯
Vi klarar oss bra, jag tycker inte att vi ska förändra oss när det gäller mjukvarusäkerhet.	◯	◯	◯	◯	◯
Företaget jag arbetar på har följt samma rutiner i åratal och jag vill inte ändra dem.	◯	◯	◯	◯	◯
Jag tenderar att vara motsträvig när jag tilldelas en säkerhetsrelaterad uppgift.	◯	◯	◯	◯	◯

Tillägg

Övriga kommentarer *

Skriv ditt svar här:

Fritextsvar.

Tack för att du svarade på vår enkät!

Totalförsvarets forskningsinstitut

2024-11-30 – 01:00
Skicka in din enkät.
Tack för att du svarat på denna enkät.

ISSN 1650-1942

www.foi.se