Försvarshögskolan

BESLUT

Datum
2025-09-26

Diarienummer
Ö 515/2025

Sändlista
Försvarsdepartementet
fo.remissvar@regeringskansliet.se
fo.ech.remissvar@regeringskansliet.se (kopia)

Ert tjänsteställe, handläggare	Ert datum	Er beteckning
Felix Nolte	2025-07-01	Fö2025/01133

Vårt tjänsteställe, handläggare
IFS, Ulrik Franke

Remissvar – Samlade förmågor för ökad cybersäkerhet (SOU 2025:79)

Försvarshögskolans yttrande

Försvarshögskolan ser positivt på den pågående förstärkningen av Nationellt cybersäkerhetscentrum (NCSC), där den nu aktuella utredningen utgör det senaste steget. Informations- och cybersäkerhet är centralt för samhällets funktion i fred, kris och krig och den nya modellen under FRA:s huvudmannaskap har goda förutsättningar att på sikt stärka Sveriges förmåga på området.

Försvarshögskolan tillstyrker i stort utredningens förslag, men för fram följande kommentarer.

Verksamhetsöverföring

Utredningens första uppdrag har varit att åstadkomma en samlad och samordnad styrning av samhällets informations- och cybersäkerhets-arbete genom att utreda förutsättningarna för och konsekvenserna av en överföring av arbetsuppgifter från Myndigheten för samhällsskydd och beredskap (MSB) till Försvarets radioanstalt (FRA).

Det har upprepade gånger påpekats att rollfördelningen mellan myndigheter på cybersäkerhetsområdet i Sverige har varit oklar. Försvarshögskolan delar den bilden och instämmer i utredningens bedömning att samlingen av funktioner inom FRA kan leda till ökad tydlighet och, på sikt, förmågehöjning.

Försvarshögskolan delar dock också utredningens bedömning att verksamhetsövergången i sig troligen kommer att leda till merkostnader, framförallt på kort sikt. Det finns också en stor kulturell skillnad mellan FRA och MSB, som blir en viktig uppgift för NCSC:s chef att överbrygga.

Informationshantering

Utredningens andra uppdrag har varit att analysera om det finns behov av ändringar i offentlighets- och sekretesslagstiftningen och regelverket som gäller för personuppgiftsbehandling.

Vad gäller den föreslagna nya lagen om uppgiftsskyldighet (utredningens avsnitt 4.2) och den föreslagna nya lagen om personuppgiftsbehandling inom NCSC:s verksamhet (utredningens avsnitt 4.5) delar Försvarshögskolan utredningens bedömningar och har inga ytterligare synpunkter.

Vad gäller den föreslagna nya bestämmelsen om sekretess för uppgifter om enskildas personliga eller ekonomiska förhållanden (utredningens avsnitt 4.3) konstaterar Försvarshögskolan att utredningen fokuserar på behovet av sekretess för uppgifter från privat sektor. Tanken är att öka informationsflödet in och säkerställa att information inte kommer angripare till del. Försvarshögskolan instämmer i att detta är ett viktigt perspektiv: *Ibland kan fler framtida cyberincidenter motverkas genom sekretess.*

Försvarshögskolan menar emellertid att utredningen saknar ett annat viktigt – komplementärt –perspektiv: *Ibland kan fler framtida cyberincidenter motverkas genom offentliggörande*. Detta kan ske i många former:

- Det är en mycket väletablerad praxis inom s.k. etisk hackning att de sårbarheter som hittas i mjukvara offentliggörs genom s.k. *responsible disclosure*. Enligt denna princip ska den som hittar en sårbarhet i en mjukvara först höra av sig till den som förestår mjukvaran så att vederbörande hinner åtgärda sårbarheten inom rimlig tid, men därefter offentliggöra den. Hotet om offentliggörande anses allmänt vara nödvändigt för att de som förestår mjukvarorna ska ta sitt ansvar och åtgärda sårbarheterna.[1]
- Även om databaser över offentliggjorda sårbarheter som den amerikanska statliga *National Vulnerability Database* (NVD)[2] oftast bara innehåller teknisk information om själva sårbarheten så finns det även motsvarande databaser med uppgifter om huruvida

[1] För beskrivningar av denna praxis, se exempelvis Strout, Benjamin. 2023. *The vulnerability researcher's handbook: The comprehensive guide for discovering, reporting, and publishing security vulnerabilities*. Birmingham: Packt Publishing. eller Hickey, Matthew & Jennifer Arcuri. 2020. *Hands on Hacking.*
John Wiley & Sons. Praxisen finns även kodifierad i en internationell standard: ISO/IEC. 2018. *Information technology – Security techniques – Vulnerability disclosure* (ISO/IEC 29147:2018).
[2] https://nvd.nist.gov/

sårbarheten faktiskt nyttjas av angripare, exempelvis katalogen *Known Exploited Vulnerabilities (KEV*).[3] Detta innebär ett visst, om än litet, mått av offentliggörande inte bara av själva sårbarheten utan även av de cyberincidenter den orsakar.

- I Sverige publicerar MSB publika årsöversikter över cyberincidenter. NCSC kan antas fortsätta med detta inom ramen för uppgiften i NCSC-förordningen att till privata och offentliga aktörer ta fram samlade lägesbilder av antagonistiska cyberhot och andra it-incidenter. Sådana översikter och lägesbilder anses allmänt stärka säkerhetsmedvetandet och sprida kunskap för förbättrat cybersäkerhetsarbete.
- I USA kräver finansinspektionen *Securities and Exchange Commission* sedan några år att börsnoterade företag offentliggör information om cyberincidenter så att marknaden ska fungera bättre.[4] När företag som drabbas av cyberincidenter straffas av marknaden skapas ett incitament för företag att sköta sin cybersäkerhet bättre. Effekterna av SEC:s senaste regler på antalet incidenter har såvitt känt ännu inte utvärderats empiriskt. Studier av lagkrav på att rapportera personuppgiftsincidenter till de berörda personerna tyder dock på att sådana lagar minskar antalet incidenter.[5] Den uppenbara farhågan att den som offentliggör detaljer om hur man försvarar sig och hanterar incidenter gör det enklare för angriparna tycks inte stämma – en systematisk litteraturgenomgång finner bara studier med negativ korrelation mellan å ena sidan detaljeringsgraden i det som offentliggörs och å andra sidan sannolikheten för framtida angrepp.[6]
- Det finns ett väletablerat nationalekonomiskt argument för att dålig cybersäkerhet delvis beror på s.k. *asymmetrisk information*: eftersom köparna har mycket svårt att skilja mellan mer säkra och

---

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[4] Se Securities and Exchange Commission. *"SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies."* 26 juli 2023. https://www.sec.gov/newsroom/press-releases/2023-139.

[5] Se Romanosky, Sasha, Rahul Telang & Alessandro Acquisti. 2011. "Do data breach disclosure laws reduce identity theft?" *Journal of Policy Analysis and Management* 30 (2): 256–286. https://doi.org/10.1002/pam.20567 samt Kesari, Aniket. 2022. "Do data breach notification laws reduce medical identity theft? Evidence from consumer complaints data." *Journal of Empirical Legal Studies* 19 (4): 1222–1252. https://doi.org/10.1111/jels.12331.

[6] Se Amani, Farzaneh, Michel Magnan & Rucsandra Moldovan. 2025. "Cybersecurity Risks and Incidents Disclosure: A Literature Review." *Accounting Perspectives* 24(3): 605–667. https://doi.org/10.1111/1911-3838.12411 Resultatet om detaljeringsgrad sammanfattas på s. 655: "We believe this set of results is particularly important in this stream of research as it suggests that disclosing the specific protections the firm puts in place against cyberattacks does not translate into adversaries being able to break through these protections, which is one of the main arguments managers put forward against disclosing cyber-related details."

mindre säkra digitala tjänster eller programvaror varken kan eller vill de betala extra för mer säkerhet. När efterfrågan inte finns försvinner även utbudet.[7] Offentliggörande av cyberincidenter motverkar detta problem genom att ge köparna mer beslutsunderlag och kan därför i längden antas stärka utbudet av säkrare tjänster.

Försvarshögskolan vill understryka att exemplen ovan inte alls betyder att all information om alla cyberincidenter alltid bör offentliggöras. Tvärtom finns det ibland goda skäl för sekretess. Poängen är just att säkerheten *ibland* gagnas mest av sekretess, *ibland* gagnas mest av offentliggörande.[8] Det sistnämnda kan exempelvis kan vara fallet med *responsible disclosure* av sårbarheter, (fördröjt, aggregerat, maskat) offentliggörande av incidenter, anonymiserade dataset för forskning etc. Enligt Försvarshögskolans mening kan sådant offentliggörande mycket väl vara påkallat även om det innebär negativa ekonomiska konsekvenser för enskilda företag – om dessa vägs upp av större positiva konsekvenser för det övriga samhällets cybersäkerhet.

Sammanfattningsvis menar Försvarshögskolan att den lagstiftning som reglerar offentlighet och sekretess inom NSCS:s verksamhet bör fylla två funktioner: dels möjliggöra sekretess när detta gagnar säkerheten mest, dels möjliggöra offentliggörande när detta gagnar säkerheten mest.

Beslut

Beslut i detta ärende har fattats av rektor Robert Egnell efter föredragning av docent Ulrik Franke.

---

[7] Se Anderson, Ross & Tyler Moore. 2006. ”The economics of information security.” *Science* 314 (5799): 610–613. https://doi.org/10.1126/science.1130992 samt Moore, Tyler. 2010. ”The economics of cybersecurity: Principles and policy options.”*International Journal of Critical Infrastructure Protection* 3 (3-4): 103–117. https://doi.org/10.1016/j.ijcip.2010.10.002.

[8] För ett teoretiskt argument för att det är svårt att *a priori* veta om offentliggjord information hjälper angripare eller försvarare mest, se Anderson, Ross. 2007. ”Open and Closed Systems Are Equivalent (That Is, in an Ideal World).” I *Perspectives on Free and Open Source Software*, Joseph Feller, Brian Fitzgerald, Scott A. Hissam, & Karim R. Huff (red.), 127–142. MIT Press. https://ieeexplore.ieee.org/abstract/document/6277068.

Robert Egnell

Rektor

Ulrik Franke

Docent

Beslutet undertecknas elektroniskt.

Sändlista externt
Försvarsdepartementet

Sändlista internt
Rektor
Prorektor
Vicerektor
Högskoledirektören
Institutionen för försvarssystem
Institutionen för krigsvetenskap
Institutionen för militärhistoria
Institutionen för ledarskap och ledning
Institutionen för operativ juridik och folkrätt
Statsvetenskapliga institutionen
Centrum för totalförsvar och samhällets säkerhet
Programledning Högre officersprogrammet
Programledning Officersprogrammet
Högskoleförvaltningen
Försvarshögskolans studentkårer

Elektroniska underskrifter

Det här dokumentet har skrivits under elektroniskt av en eller flera personer

Alla elektroniska underskrifter listas i signaturpanelen. De tio första underskrifterna listas även på den här sidan.

Detta dokument med sina elektroniska underskrifter gäller som självständig handling och uppfyller krav på avancerade elektroniska underskrifter enligt eIDAS.

Varje underskrift kan valideras med en PDF-läsare med stöd för signaturvalidering eller med SignPorts valideringstjänst. Andra valideringstjänster kan användas förutsatt att dessa uppfyller de tekniska kraven enligt internationella standarder.

Om dokumentet skrivs ut på papper, eller om dokumentet 'skrivs ut' till ett nytt PDF-dokument, följer de elektroniska underskrifterna inte med. Endast det elektroniskt underskrivna originaldokumentet går att validera.

** Värden markerade med en asterisk har validerats mot beviset från den legitimeringstjänst som användes för underskriften.*

Underskrift 1

Namn: ULRIK FRANKE
Identifieringsmetod: Mobilt BankID
Datum och tid: 2025-09-26 14:33:27 GMT+02:00
Transaktions-ID: eaa46e0603b149e1876485e5760a26f2

Underskrift 2

Namn: ROBERT EGNELL
Identifieringsmetod: Mobilt BankID
Datum och tid: 2025-09-26 14:58:32 GMT+02:00
Transaktions-ID: a8a0c5878e4244478eecc5119c40f123