SAMMANFATTNING TILL LEDARE OCH BESLUTSFATTARE

# Sakernas internet i en osäker tid

**Rapporten belyser risker kopplade till Internet of Things (IoT) för individuella användare och samhälle.**

RISE RAPPORT 2023:MARS

Centrum för Cybersäkerhet
ri.se/sv/centrum-for-cybersakerhet

Kontakta oss:
cybersakerhetscentrum@ri.se

# Sammanfattning

Sakernas internet (IoT, Internet of Things) är en ledande komponent i digitaliseringen av samhället, industrin och ekonomin. Det finns i dagsläget fler uppkopplade enheter än människor och snart är det enklare att räkna upp vilka enheter som inte är uppkopplade än de som är eller kan bli det.

Teknikexperter och analytiker förväntar sig en fortsatt utbredning av IoT. Detta beror bland annat på att fler användningsområden ideligen uppkommer, samt att IoT-tekniken fortlöpande blir både bättre och billigare. Den snabba utvecklingen innebär dock en hel del risker för såväl individuella användare som samhället i stort. En central förutsättning för att IoT ska skapa värde är tillgången till detaljerad information och data om användare och/eller miljön den verkar i. Detta riskerar dels att skapa integritetsproblem, dels att känslig information tillgängliggörs. En bakomliggande orsak till detta är att många IoT-enheter är begränsade i datorkraft, vilket gör att säkerhetsfunktioner tenderar att vara undermåliga.

Arenan där detta utspelar sig är en osäker tid präglad av ett försämrat säkerhetsläge, i vilket uppkopplade enheter kan utgöra såväl potentiella angreppsytor som medel för att genomföra angrepp. Alla parter kan bidra till att bedriva ett aktivt arbete för att minska riskerna med IoT; från enkla åtgärder hos individuella användare till multilaterala överenskommelser om IoT-standarder- och certifiering.

Denna rapport syftar till att skapa intresse för IoT och att belysa risker kopplade till tekniken och dess utbredning. Rapporten riktar sig till chefer och beslutsfattare i den offentliga och privata sektorn.

## Om centrum för cybersäkerhet

Centrum för cybersäkerhet på RISE stärker den tillämpade forskningen och kompetensutvecklingen inom cybersäkerhet i Sverige.

RISE är ett oberoende, statligt ägt forskningsinstitut. Centret skapar en neutral nationell plattform som stöttar näringsliv och offentlig sektor genom expertstöd, forskningspartnerskap, innovationsledning samt test-och demonstrationsmöjligheter.

Ett samarbete med RISE innebär tillgång till ett stort nätverk av tvärvetenskapliga team som innehar både en bred domänkompetens såväl som en djup cybersäkerhetsexpertis.

Vi kan erbjuda stöd inom olika tillämpningsnivåer av cybersäkerhet – från forskning och utveckling, certifiering, utbildning/träning till systemtest i kontrollerade virtuella miljöer.

**Läs mer på vår hemsida:**
www.ri.se/sv/centrum-for-cybersakerhet

# 1. Inledning

Sakernas internet (IoT, Internet of Things) är centralt i den globala digitaliseringen av samhället, industrin och ekonomin.

Uppkopplade enheter kan vara allt från smarta armbandsur till strömbrytare och finns i allt från smarta elnät, intelligenta transport- och vattensystem till kroppsburna medicintekniska enheter. 2019 fanns det 26.66 miljarder uppkopplade enheter och antalet bedöms växa till 74.44 miljarder år 2025[1]. Flera marknadsanalytiker förutspår att privatpersoner kommer äga en majoritet av dessa IoT-enheter[2]. En viktig anledning till utbredningen och den växande populariteten av IoT är att det kan skapa omfattande ekonomiska möjligheter och förbättringar inom industrier, affärsverksamheter och sjukvård.

Med dessa tekniska innovationer kommer betydande utmaningar inom säkerhet och sekretess. Detta beror främst på att många IoT-enheter är begränsade i processorkraft och minne och operativsystemen är förenklade, vilket försvagar säkerhetsfunktionerna. EU:s cybersäkerhetsbyrå ENISA publicerade i november 2022 en lista över de tio allvarligaste cybersäkerhetshoten 2030[3]. Bland dessa finns bland annat risken för digital övervakning/integritetsförlust och riktade attacker förstärkta av data från uppkopplade enheter. Vikten av allvaret återspeglas inte minst i EU:s arbete för att skapa rutiner och förordningar genom bland annat Cyber Security Act och Cyber Resilience Act medan NIS2-direktivet bland annat kommer att föreskriva hur IoT tas in i kritiska miljöer. IoT har även implikationer på fysiska världen. Dels i bemärkelsen att konsumentorienterade enheter kan innebära risker för kroppslig skada, dels att det finns risker för betydande konsekvenser alltmedan fabriker, energianläggningar, transportsystem och andra system i högre grad integreras i IoT. Detta exemplifieras senare i rapporten.

Den ökande utbredningen av IoT innebär en ökning av potentiellt sårbara angreppsytor och detta sker parallellt med en försämring av säkerhetsläget i Europa, som bedöms vara det allvarligaste sedan 1980-talets början[4]. Till skillnad mot situationen då har den tekniska utvecklingen möjliggjort att användandet av nya tillvägagångssätt för antagonistiskt agerande blivit vanligare[5]. På det sättet kan påverkan på produkter, processer och tjänster som samhället är beroende av användas för att sätta press på det och dess invånare.

Rapporten riktar sig till chefer och beslutsfattare i den offentliga och privata sektorn.

**”Syftet med rapporten är att erbjuda en översikt av vad IoT är och att belysa risker kopplade till tekniken och dess utbredning.”**

# 2. Vad är IoT?

Det finns i dagsläget ingen allmänt vedertagen definition av IoT, snarare förefaller olika aktörer definiera begreppet utifrån deras egen verksamhet och intressen. I huvudsak kan en sak bli en IoT-enhet genom att den tilldelas prefixet ”smart”, i bemärkelsen att den är **beskaffad med en eller flera sensorer och kan programmeras** att genom analys, utbyte och bearbetning av data från sina miljöer utföra en situationsanpassad funktion i stort sett utan mänsklig interaktion. Ett exempel är belysningsarmaturer som tänds och släcks beroende på om någon är i närheten. **Interoperabilitet - förmågan hos olika system att fungera tillsammans och kommunicera med varandra - är en av nyckelaspekterna av IoT** och som bidrar till dess växande popularitet. Detta kan exemplifieras av en brandvarnare som genom IoT är sammankopplad med dörrar som kan stängas för att förhindra spridning av brand.

Konceptuellt innebär IoT alltså att fysiska objekt, eller noder, kan använda internet eller andra kommunikationsnätverk för att snabbt kommunicera data om tillstånd, position och andra attribut för ”smart” agerande. Informationen skapar värde när den används för att modifiera och förbättra framtida åtgärder. Detta ger i sin tur upphov till ny information, vilket gör att inlärningsprocessen kontinuerligt förbättras[6]. Ett exempel på detta är när Tesla införde en autopilot på sina bilar. Bilarna rapporterade fortlöpande in till Teslas centrala system om bland annat trafik, navigering och andra faktorer och efter en tid uppgav bilförare att autopiloten blivit påtagligt bättre – **systemet lär sig kontinuerligt** från situationer bilarna var med om och varje enskild bil lär sig av alla bilars samlade erfarenhet[7].

En av de centrala drivande faktorerna för IoT är data, som samlas in, förädlas och förvaras i molnservrar för vidare bearbetning. Tillväxten av IoT speglas i den ökande mängden data som genereras - International Data Corporation bedömer att **mängden data genererad av IoT-enheter årligen växer med 28,8 procent under perioden 2018 – 2025**[8]. Enligt The Economist passerade data oljan i att vara världens mest värdefulla resurs redan 2017[9]. Den stora volymen data som IoT genererar utgör i sig en utmaning, men än viktigare är styrningen av datan och dess lagring[10].

## 2.1 Användningsområden

Som nämnts används IoT i en mängd olika områden, varav några kommer att belysas i detta avsnitt. Ett sätt att åskådliggöra områdena som redogörs för här är att dela upp dem i två generella områden: **företags- och industrisegmentet och konsumentsegmentet**. Konsumentsegmentet är oftast förankrat i kundupplevelsen och en mer offentlig molnmiljö. Företags- och industrisegmentet av IoT tenderar att drivas av tillverkningsindustri och produktutveckling inom en relativt avskild molnmiljö och innefattar stora och relativt komplexa datamängder men betydligt färre enheter jämfört med konsumentsegmentet[11].

Ett område inom konsumentsegmentet som fortfarande är relativt outforskat är **hemmet**. Utöver uppkopplade tv-apparater, belysningsarmaturer, larmsystem- och kameror, lås, vitvaror och robotdammsugare är många hem generellt inte särskilt datoriserade[12]. Detta innebär kommersiella möjligheter för producenter men det finns även ekonomiska incitament på konsumentsidan eftersom uppvärmning och nedkylning utgör en stor utgift i många hem. Hemautomatiseringsenheter kan spara pengar genom att gå in i energisparläge när ingen är hemma och återställa ett bekvämt inomhusklimat lagom tills de boende återvänt[13].

Ett växande område inom IoT är människan och **kroppsburna uppkopplade enheter.** En vanlig accessoar som många använder för att övervaka sin hälsa är aktivitetsarmband som läser av omgivningen och bärarens tillstånd och som genom en smart mobiltelefon är uppkopplad till internet, där molntjänster tar vid och bearbetar insamlade data[14] . IoT har även djupgående effekter på traditionell sjukvård. Genom att förse patienter med **uppkopplade medicintekniska enheter** såsom hjärt- och andningsmonitorer och aktivitetsarmband kan vårdgivare utvärdera kliniska data och utrustning på distans. I framtiden kommer diabetiker kanske kunna övervaka sig själva mer finkalibrerat genom att bära kontaktlinser försedda med ett trådlöst chip och en liten sensor som mäter glukosnivå i tårvätska[15].

IoT används också brett inom marknadsföring och **handel**, bland annat för att förbättra distributionskedjor och individanpassa köpupplevelser. De senaste åren har möjligheten att använda ansiktsigenkänning i butiker diskuterats i Sverige. I dataskyddsförordningen finns särskilda bestämmelser om biometriska data som måste beaktas vid användandet av ansiktsigenkänningsteknik. Biometrisk data tillhör en kategori av personuppgifter som anses vara särskilt skyddsvärda och behandling av sådana känsliga personuppgifter är som utgångspunkt förbjuden, även om det finns undantag[16]. Ett förslag som lanserades 2019 var en form av anonymiserad ansiktsigenkänning att användas i butiker, som inte behandlar biometrisk data eller sparar personuppgifter[17].

Ett annat område inom IoT som ofta nämns är **transportnäringen**, som står inför omfattande förändringar – exempelvis självkörande fordon kommer sannolikt att bli ett vanligt inslag på vägarna inom en inte alltför avlägsen framtid. IoT innebär även stor potential för smarta städer, som kan använda digitala lösningar för att öka energieffektivitet, underlätta hållbar vattenhantering samt mäta och minska koldioxidutsläpp[18]. I en smart stad kan kollektivtrafiken anpassa sig till antalet trafikanter och deras destinationer, sopkärl meddela när de behöver tömmas och gatubelysning dämpas när inga människor är i området.

IoT kan användas för att förbättra **jordbruk**. Lantbrukare kan exempelvis använda anslutna sensorer, kameror och drönare för att förbättra översikten över sin gård och justera driften för att förbättra sin skörd[19]. Artificiell intelligens och big data kan spåra solljus, temperatur, luftfuktighet och andra miljöfaktorer för att optimera tid och metod för sådd, skörd och andra jordbrukselement[20].

IoT har använts länge i **industrin**, som även den påverkas av den snabba utvecklingen, i synnerhet av de ökande möjligheterna till automatisering. Många industrier använder IoT för att löpande förbättra maskiner och system och effektivisera verksamheter. Inom industrin är en övergripande fördel med IoT kopplad till underhåll – i stället för att lägga tid och resurser på att regelbundet inspektera en sak i onödan möjliggör IoT konstant övervakning av den, vilket skapar möjligheter att reparera saken innan den går sönder[21]. IoT finns även i s**amhällskritisk infrastruktur**, såsom vattenverk och vattenkraftstationer. Genom att mäta och lagra uppgifter såsom nederbörd, grundvattennivåer och vattennivåer kan berörda aktörer få tidiga varningar om översvämningar och vidta åtgärder[22].

## 2.2 Tillväxt

Teknikexperter och analytiker förväntar sig ännu större användning av IoT-enheter och appar framöver. Ett antal faktorer driver tillväxten av IoT - i korthet kan det sammanfattas med att IoT-tekniken blivit bättre och billigare. Sensorteknik, som är inbäddad i IoT-enheter, fortsätter att bli billigare, mer avancerad, har mindre felmarginaler och är mer tillgänglig[23]. Kostnaderna för att överföra, lagra och analysera data har sjunkit betydligt under de senaste två decennierna[24]. Även kommunikationsteknikerna - nätverken som används för att koppla upp IoT-enheterna – blir allt snabbare och kapaciteten att skicka större mängder data ökar[25]. 5G-nätet är den första nätgenerationen som är utvecklad för IoT från början och är en viktig komponent till utbredningen och förbättringen av IoT. Detta beror på att 5G möjliggör högre datahastigheter, ännu fler uppkopplade enheter och lägre latens (tidsfördröjning)[26]. Tillväxten och efterfrågan av IoT drivs bland annat av sektorspecifika strömningar. Exempelvis tillverkningsindustrin går igenom en bred digital transformation i samband med utvecklandet av Industri 4.0 som ligger till grund för utbyggnaden av avancerade IoT-analysfunktioner[27].

**”Teknikexperter och analytiker förväntar sig ännu större användning av IoT-enheter och appar framöver.”**

# 3. Risker och sårbarheter

IoT har stora fördelar och möjligheter, men med dessa följer även en omfattande mängd **säkerhets- och sekretessutmaningar.** Utvecklingen av framgångsrika tekniska innovationer som IoT går ofta i en hög hastighet som accelererar ju fler användningsområden som uppkommer. Detta i kombination med den parallella utvecklingen av minskande kostnader och prestandaförbättring har bidragit till att IoT vuxit oerhört, i synnerhet under det senaste decenniet.

Utvecklingen av produkter och användningsområden går ibland snabbare än utvecklingen av säkerhet, så även med en del IoT-teknik. Incitamentet att sälja stora volymer IoT-enheter med relativt kort livslängd och begränsad energi- och beräkningskapacitet till ganska låga anskaffningskostnader begränsar möjligheterna- såväl som drivkraften till att skapa god säkerhet. Detta blir ytterligare problematiskt eftersom IoT inte bara ger tillgång till den virtuella världen men även till den fysiska världen i form av uppkopplade sensorer, ställdon, kontrollsystem och vardagliga objekt vilket möjliggör fler och nya typer av angrepp[28].

Parallellt med denna utveckling sker en försämring av **säkerhetsläget** i världen, inte minst i Europa. Betydelsen av detta konkretiseras i ljuset av möjligheterna som cyberdomänen erbjuder aktörer att påverka säkerhetsläget, och ytterligare försämra det, genom olika typer av angrepp mot eller genom IoT. Säkerhetspolisen skriver i sin senaste årsbok att man ser en utveckling där stater använder privatpersoners uppkopplade enheter i syfte att genomföra cyberangrepp. Anledningen till detta förklaras med att dessa sällan uppdateras och därmed har fler sårbarheter[29]. Ytterligare en viktig anledning är att det stora antalet uppkopplade enheter erbjuder ett stort antal potentiella angreppsytor.

Oaktat dess komplexitet är en IoT-enhet per definition en nätverksansluten, och därmed i varierande grad exponerad, dator. En sådan kan manipuleras av angripare och i värsta fall orsaka en mängd konsekvenser utanför sitt tilltänkta användningsområde, trots att enheten kan uppfattas som liten eller begränsad i sin funktion. När angripare tagit kontroll över en IoT-enhet har de i princip möjlighet att utföra cyberangrepp på samma sätt som från en dator. Det kan dock nämnas att det kan vara svårare att utföra attacker som kräver mer beräkningar och att överbelastningsattacker kan bli begränsade av mindre kraftfulla enheter. Angrepp som komprometterar IoT-infrastrukturen har möjlighet att åstadkomma skada inte enbart i form av intrång och påverkan på funktionalitet, utan även fysiska skador på anläggningar eller på människor som bär IoT-enheter och/eller är beroende av dem [30].

Varför har många IoT-enheter undermålig säkerhet? IoT-enheter är ofta batteridrivna och använder billiga och strömsnåla, men svaga, processorer. Detta kan trots tillverkarens goda avsikter begränsa säkerhetsåtgärder, framför allt de som krypterar kommunikationen och som kräver mycket bandbredd och datorkraft (och som snabbt kan tömma ett batteri)[31]. Dessutom kommunicerar IoT-enheter ofta via långsammare och mindre säker trådlös media då säkerhetsprotokollen som används i mobilt internet i princip inte går att använda i de resursbegränsade IoT-enheterna[32]. Flertalet IoT-enheter har en relativt kort livslängd, vilket skulle kunna bidra till att säkerhetsåtgärder inte prioriteras. Därtill är IoT-marknaden hårt konkurrensutsatt, vilket innebär höga krav på att pressa kostnaderna för utformningen av enheter.

Många IoT-enheter tillverkas av mindre, ganska unga företag. Dessa har inte alltid samma resurser och kompetens som större företag att lägga på kvalitetssäkring (exempelvis att felsöka mjukvara innan produkten lanseras - det är dessutom inte alltid möjligt att uppdatera och korrigera eventuella säkerhetshål i efterhand)[33]. Dessutom saknas det än så länge tydliga och enhetliga c**ybersäkerhetsstandarder** för området jämfört med hos större, äldre organisationer i etablerade affärsområden[34]. Användare av IoT-enheter bär också ett personligt ansvar för säkerheten. Här syftas framför allt på vikten av att inte använda samma inloggningsuppgifter och lösenord för flera ändamål, att ändra fabriksinställda lösenord när en enhet installeras och att uppdatera enheten när det är möjligt. Just fabriksinställda lösenord tenderar att vara kända eller enkla att knäcka[35]. Osäkra inloggningsuppgifter och lösenord kan kanske framstå som ganska anspråkslösa sårbarheter men försumlighet kan leda till allvarliga konsekvenser.

Att en IoT-enhets säkerhet och/eller funktioner kan påverkas negativt kan bero på många anledningar, inklusive mänskligt felhandlande eller andra slumpmässiga händelser, men även avsiktliga angrepp. Hur vanligt förekommande cyberangrepp är på uppkopplade enheter är svårt att ge ett exakt svar på, dels för att det sannolikt inte alltid rapporteras och sammanställs, dels för att det kan ske utan att användare upptäcker det.

Ett flertal undersökningar har gjorts på uppkopplade enheter, exempelvis i hemmiljöer. En sådan undersökning fann att den vanligaste angreppsmetoden utgjordes av försök till att logga in i uppkopplade enheter genom **svaga standardinloggningsuppgifter** och lösenord såsom ordet ”admin”. De flesta enheterna i undersökningen motstod angreppsförsöken, men en trådlös kamera hackades vilket möjliggjorde för angriparen att kunna övervaka hemmet. Kameran togs sedan bort från försäljarens sortiment[36].

I en annan studie genomfördes penetrationstester på 22 enheter i uppkopplade hem, däribland smarta dörrlås, kameror, garage och biladaptrar[37]. Sammanlagt **17 olika sårbarheter identifierades**. Studien kom fram till att de upptäckta sårbarheterna potentiellt kunde leda till allvarliga konsekvenser för boende, såsom möjligheter för en angripare att tillskansa sig fysiskt tillträde till ett hem genom att manipulera det uppkopplade dörrlåset[38].

Distinktionen kan göras om IoT är målet för ett angrepp, eller används som medel för att genomföra eller förstärka ett angrepp. Ett exempel på när IoT-enheter kan utgöra mål för angrepp är när forskare i december 2022 upptäckte att det genom en musikströmningsapp som kommunicerar med en bil gick att låsa upp den, starta den, tuta och blinka med strålkastarna utan att befinna sig i närheten av fordonet. Den enda informationen de behövde var bilens chassinummer[39]. Sårbarheten åtgärdades genom att tjänsten uppdaterades. Tester har även visat att det går att bryta sig in i och köra i väg med en viss typ av bil till följd av sårbarheter i trådlösa nyckelbrickor som ägaren använder för att låsa upp den. De enda verktygen som behövdes var en Raspberry Pi-dator med en extern hårddisk samt radiosändare och radiomottagare, till en kostnad av ungefär 600 dollar[40].

Ytterligare ett exempel på när IoT-enheter skulle kunna utgöra mål för angrepp uppdagades när amerikanska läkemedelsmyndigheten (Food and Drug Administration, FDA) 2017 återkallade 465,000 pacemakers. Beslutet föranleddes av att MedSec, ett cybersäkerhetsbolag specialiserat på att undersöka sårbarheter i medicinsk utrustning, lyckades exploatera säkerhetshål som skulle kunna få pacemakerns batteri att ta slut i förtid och omprogrammera enheten för att påverka bärarens hjärtslag. Enligt undersökningen skulle sårbarheten kunna exploateras med hjälp av kommersiellt tillgänglig utrustning. Det bör understrykas att det framgick att en potentiell angripare dels skulle behöva vara mycket skicklig, dels skulle behöva befinna sig tillräckligt nära pacemakern för att möjliggöra radiokommunikation[41].

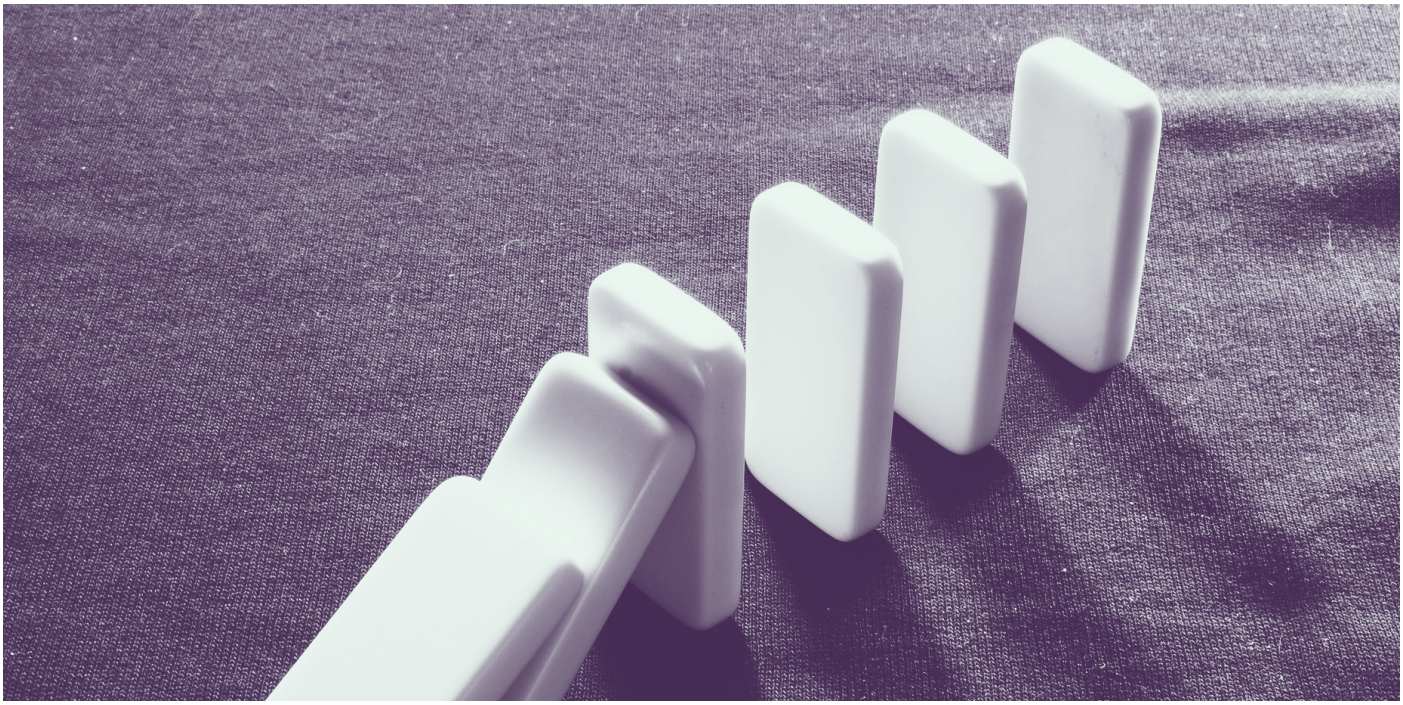
Trots att IoT-enheter ofta är begränsade i datorkraft kan de infekteras av skadlig programvara, och användas för att förstärka angrepp. Ett exempel på detta är när angripare tillskansar sig stora mängder datorkraft genom att bygga upp ett **botnät**. Ett botnät omfattar en samling internetanslutna enheter såsom persondatorer, servrar, mobila enheter och IoT-enheter, som infekterats och styrs med hjälp av skadlig programvara[42]. Dessa används sedan för att utföra överbelastningsangrepp på system genom att de infekterade enheterna kontaktar en specifik server, webbplats eller webbtjänst samtidigt[43]. Den skadliga programvaran sprider sig genom att skanna internet efter sårbara och oskyddade enheter i syfte att infektera dem. Den tenderar att leta efter äldre versioner av operativsystem som inte blivit eller har kunnat bli säkerhetsuppdaterade, men även IoT utsätts i högre utsträckning eftersom enheter kan ha fabriksinställda lösenord, är svåra eller omöjliga att uppdatera, ständigt är påslagna och finns i stora (och växande) antal[44].

Ett omskrivet botnät är Mirai, som till stora delar bestod av IoT-enheter inom konsumentsegmentet såsom IP-kameror och routers, och var inriktat på att ansluta IoT-enheter genom att logga in på dem med deras fabriksinställda användarnamn och lösenord[45]. Mirai användes bland annat vid överbelastningsangreppen mot namnserverleverantören Dyn i oktober 2016, vilket ledde till att flera stora webbplatser i Europa och Nordamerika blev otillgängliga i perioder[46].

System i samhällsviktiga sektorer har ofta anslutning till internet och bygger åtminstone delvis på IoT-enheter, vilket gör att de riskerar att utsättas för cyberangrepp[47]. IoT-enheter kan vara kopplade till ställdon[48] och fysisk skada kan orsakas av de inte fungerar som de ska (till följd av exempelvis manipulation), som exemplet med brandvarnare som genom IoT är sammankopplade med dörrar för att förhindra spridning av brand. Applicerat i ett samhälleligt perspektiv kan angrepp på IoT-enheter kopplade till ställdon få omfattande konsekvenser om en angripen enhet utgör en kritisk komponent i ett system som ska tillhandahålla en samhällsviktig funktion. Ett exempel skulle kunna vara ett uppkopplat ställdon till en pump i ett vattenverk[49].

Ett **intrång i en IoT-enhet kan ge tillgång till andra enheter** kopplade till det nätverk som enheten är uppkopplad mot. Angriparen kan sedan få möjlighet **tillskansa sig ytterligare uppgifter, manipulera data** och **införa skadlig kod**. 2018 lyckades ett IT-säkerhetsbolag tillskansa sig omfattande datamängder från en databas tillhörande ett casino genom att ta sig in på nätverket via ett uppkopplat akvarium i casinots lobby, i vilket vattnets temperatur och salthalt kontinuerligt kontrollerades och kunde **fjärrstyras**[50]. Ett intrång i exempelvis en uppkopplad högtalare i ett vattenreningsverk eller hos en livsmedelsdistributör skulle med samma tillvägagångssätt kunna ge access till andra delar av verksamheten, vilket i sin tur skulle möjliggöra omfattande störningar.

Ytterligare en risk kopplad till IoT-enheter som är relevant att belysa rör **integritet och sekretess**. En förutsättning för att uppkopplade enheter ska kunna utföra sina funktioner och förbättras är att de har tillgång till detaljerad information, bland annat om användarens förehavanden och geografiska plats. Många uppkopplade enheter är även röststyrda och registrerar vad bäraren och andra i omgivningen säger, och/eller innehåller kameror. Premissen är att IoT-enheter används med åtminstone bärarens medgivande, men **emellanåt samlar uppkopplade IoT-enheter in data och kommunicerar och interagerar med varandra utan bärarens tillstånd och/eller utan att bäraren är medveten om det**. Kombinationen av mängden tillgänglig information, som ofta inte är väl skyddad, och IoT-enheters beräkningskapacitet skapar stora möjligheter att identifiera, övervaka, avlyssna och spåra individer samt att kartlägga deras beteendemönster[51]. På så sätt kan exempelvis personer med viktiga befattningar i samhället utsättas för riktade angrepp som använder IoT-enheter[52] .



Utöver de etiska aspekterna av integritetsproblemen finns det ytterligare risker med att en viss typ av information når obehöriga - det kan även röra sig om information som ger tillgång till tekniska system eller företagshemligheter. En IoT-enhet kan dessutom användas som språngbräda in i traditionella IT-system för att **stjäla information**[53]. Det vill säga, det system eller den enhet som exploateras behöver inte vara det primära målet, utan kan utgöra en portal som används för att ta sig vidare i IT-miljön[54]. Detta är särskilt relevant i ljuset av att underrättelseinhämtning inom vetenskap och teknik blivit ett alltmer prioriterat område[55].

Sett till vilken typ av aktörer som skulle kunna ha kapacitet och intresse av att genomföra angrepp mot IoT-enheter- och infrastruktur skiljer det sig troligen inte mycket från andra typer av cyberangrepp.

Angrepp kan vara statsunderstödda, finansiellt- och ideologiskt motiverade och kanske även konkurrensmotiverade.

Risker med IoT-enheter rör sig alltså i ett brett spektrum—från stöld och manipulation av data till övervakning, avlyssning och integrering i botnät, för att nämna några exempel.

Vissa experter tror även att **utpressningsangrepp** kommer att kunna drabba IoT-enheter i framtiden. Konsekvenserna kan vara allt från mindre olägenheter för användare till avbrott i affärskritiska system till livsfara.

Syftet med exemplen i avsnittet är att belysa **olika scenarion som är möjliga** idag. Ansatsen att det är möjligt att skapa omfattande störningar på individ- såväl som samhällsnivå till följd av kompromitterade IoT-enheter- och infrastruktur kan kanske te sig alarmistisk, men det finns ett värde i att förhålla sig till det. Värdet består framför allt i möjligheten att **förbereda sig, att kunna avvärja angrepp och att kunna begränsa potentiell skada om de sker.** Idag kan exempelvis ett synkroniserat angrepp som gör att ett stort antal räddningstjänstfordon inte kan genomföra sina uppdrag förefalla avlägsen men kanske är det en realitet i framtiden.

**”Risker med IoT-enheter rör sig alltså i ett brett spektrum — från stöld och manipulation av data till övervakning, avlyssning och integrering i botnät, för att nämna några exempel. ”**

# 4. Förslag på åtgärder

Alla parter i IoT-enheters livscykel bör bedriva ett **aktivt säkerhetsarbete,** från systemutvecklare och tillverkare till importörer, distributörer och användare. Säkerhetsarbete bör vara en **kontinuerlig och dynamisk process**, inte en eftertanke. Utvecklingen av nya IoT-enheter och användningsområden går ständigt framåt, samtidig som angripare ideligen letar efter nya sårbarheter och säkerhetshål att exploatera.

Som nämndes i rapportens inledning bedömer ENISA risken för digital övervakning/integritetsförlust och riktade attacker förstärkta av data från smarta enheter som ett av de **allvarligaste cybersäkerhetshoten 2030**[56]. Vad som förefaller vara ganska enkla IoT-enheter kan medföra komplexa risker. Det allvarliga säkerhetsläget har visat att det är angeläget att vara förberedd för scenarion som tidigare föreföll ganska osannolika, och snarare än att fokusera på hur hög sannolikheten är för att ett säkerhetshot realiseras, bör utgångspunkten vara att bedöma hur allvarlig konsekvensen av en viss skada kan bli.

På individnivå bör användare av IoT-enheter **läsa på om produkten** innan inköp, bland annat för att kontrollera om leverantören tillhandahåller **säkerhetsuppdateringar** – cybersäkerhet bör utgöra ett viktigt kriterium vid inköpstillfället. Efter inköp **bör förinställda inloggningsuppgifter och lösenord ändras**. Dessa bör även **bytas med jämna mellanrum**, exempelvis i samband med att enheten uppdateras. Om möjligt, bör **flerfaktorsautentisering** tillämpas. Dessutom är det viktigt att veta vilka enheter i ens hem som är avsiktligt uppkopplade och som kan kommunicera med varandra - vissa enheter kan ha blivit föråldrade och ha sämre säkerhetsfunktioner. En försummad säkerhetskonfiguration i en enhet kan påverka hela hushållsnätverket - exempelvis kan ett uppkopplat spel med säkerhetsproblem ge åtkomst till ens värmepump. Användare av uppkopplade enheter bör även vara uppmärksamma på om enheten börjar bete sig avvikande och då ta kontakt med leverantören. Slutligen kan det vara klokt att **reflektera över behovet av att en enhet är uppkopplad** kontra riskerna det innebär.

Företag bör bedriva sin verksamhet enligt devisen att alla företag (om än i varierande utsträckning) är IT-företag. Företag bör utvärdera sin IoT-säkerhet genom att **lära sig om de mest troliga hoten, välja utvärderingsstrategier, förstå riskerna och få råd från experter**[57]. Som ett led i arbetet att bättre förstå hur en angripare kan kompromettera ett helt system kan företag hotmodellera genom exempelvis digitala tvillingar[58], så att man kan implementera nödvändiga åtgärder för att förhindra eller begränsa angrepp. Red team-övningar, där säkerhetsexperter aktivt försöker gå förbi nödvändiga säkerhetsåtgärder i systemen, är också ett bra verktyg för att höja säkerheten. **Kunskap om cybersäkerhet bör inte begränsas till IT-säkerhetsavdelningen** – målgruppsanpassade utbildningar med stöd i den senaste forskningen är ett värdefullt sätt för ledningsgrupper och beslutsfattare att bidra till att kunskap och kompetens inom området genomsyrar hela verksamheten. Säkra och insynsskyddade forum och nätverk där medlemmar kan dela information och erfarenheter, och främja samverkan, inte minst privat-offentlig sådan, är också bra verktyg. Företag kan även som en del av sitt säkerhetsarbete ta fram **riktlinjer för vilken typ av IoT-enheter som är tillåtna** på en arbetsplats, särskilt om den är ett skyddsobjekt.

System- och produktutvecklare och tillverkare borde utgå från att säkerheten i IoT-enheter inte är avhängig av hur användare använder den. Av den anledningen bör s**äkerheten i möjligaste mån vara automatiserad** - exempelvis kan tillverkare av IoT-enheter leverera dem med ett unikt och säkert lösenord som kan ändras om användaren vill det. Det skulle även kunna vara aktuellt att ställa krav på att tillverkare av IoT-enheter har en sektion i bruksanvisningen avsedd för att underlätta för användare att höja enhetens säkerhet. Detta då metoderna som krävs kan uppfattas som komplicerade för vanliga användare, såsom att lägga sina enheter i ett separat virtuellt nätverk och säkerställa att de inte är nåbara från det publika internet. IoT-enheter skulle även kunna innehålla en funktion som gör att den stängs av automatiskt vid misstanke om att den kompromettерats. För att minska angreppsytan bör funktionaliteten hos IoT-enheter begränsas så att de bara kan utföra det de är avsedda för, utan onödiga kringfunktioner[59]. Merparten av alla IoT-enheter som importeras och säljs i Sverige kommer från tillverkare i andra länder, och importörer och distributörer bör kunna ställa krav på att produkterna håller en godtagbar säkerhetsnivå[60]. En enhet kan, i bästa fall, ha god säkerhet i början av sin livsbana men den kan ganska snabbt bli föråldrad varför tillverkare bör erbjuda säkerhetsuppdateringar under hela produktens livslängd. Att IoT-enheter kan innehålla stora mängder personliga, operativa och företagsrelaterade data gör detta än viktigare. Även om det inte alltid går att balansera säkerhetsmekanismer mot enheters primära syfte, behöver inte säkerhetsarbete förhindra innovation. Innovations- och säkerhetsarbete kan ske parallellt om säkerhetsåtgärder byggs in tidigt i designfasen av IoT-enheter, enligt principen security by design.

EU har ett antal instrument för att skydda elektroniska kommunikationsnätverk- och produkter, däribland **Cybersecurity Act och Cyber Resilience Act**. Cybersecurity Act syftar till att uppnå en enhetlig säkerhetsnivå och standard i EU och reglerar certifieringar genom att bland annat fastställa en ram för frivilliga europeiska system för cybersäkerhetscertifiering av produkter, tjänster och processer inom informations- och kommunikationstekniken[61]. Certifieringen kommer att underlätta för företag att erbjuda affärer över landsgränser och göra det enklare för kunder att kunna bedöma hur säker en produkt, tjänst eller process som de avser köpa är[62]. Cyber Resilience Act är ett förslag från 2022 och siktar på en gemensam cybersäkerhetsstandard för tillverkare och leverantörer av uppkopplade saker och tjänster[63]. Lagstiftningen är den första i sitt slag med tvingande krav på digitala produkter, genom hela deras livslängd, och föreslås gälla alla produkter som direkt eller indirekt ansluts till en annan enhet eller till ett nätverk [64].

Att ta fram standarder för IoT-enheter innebär en del utmaningar. En förutsättning för att de ska kunna appliceras brett är att de är inriktade på grundläggande och allmängiltiga säkerhetskrav. De behöver även vara anpassningsbara; dels för att utvecklingen av produkter och användningsområden växer snabbt, dels för att det sannolikt finns - och kommer att uppstå nya - angreppsytor som ännu inte är kända, men som så småningom kommer att behöva förhållas till. En metod för att kunna bemöta och parera förändrade säkerhetsproblem skulle kunna vara återcertifiering av produkter när allvarliga sårbarheter upptäcks, ett ansvar som kunde åligga certifieringsorgan. För att minska risken för att små och medelstora företag utesluts från marknaden är det är viktigt att processen för att åstadkomma en acceptabel lägstanivå vad gäller säkerhet är så enkel och tydlig som möjligt och att stöd finns att få. Detta kan understödjas genom samarbeten mellan teknikexperter specialiserade på IoT-säkerhet, andra aktörer i IoT-leveranskedjan, policymakare och regeringar.

Standarder kan även bidra till att **förtydliga ansvarsfördelningen** eftersom det inte alltid är tydligt vem som bär ansvaret för säkerhetsåtgärder när exempelvis ett företag står för utformningen av en produkt, ett annat står för delar av mjukvaran, ett tredje hanterar det nätverk som enheten ska kopplas in i och ett fjärde företag driftsätter produkten. Ansvarsaspekten är för närvarande ytterligare problematisk då kostnaden för bristande säkerhet sällan bärs av de som har bäst förutsättningar att höja den[65].

Vikten av att öka medvetenhet och intresse i samhället kring cybersäkerhet anförs med jämna mellanrum och detta är centralt för att hela spektret av användare av IoT-produkter ska kunna förstå hur de kan bidra till att uppnå och upprätthålla en tillräcklig säkerhetsnivå. Insatser på området kan innefatta bland annat riktade **utbildnings- och informationsinsatser** från myndigheter, stöd till forskning inom säkerhet och IoT samt **samverkan** mellan myndigheter och näringslivet. Ansträngningar bör riktas både till det offentliga, näringslivet och till privatpersoner för att få brett genomslag. Det är även angeläget att inse att samhällets viktiga digitala tillgångar inte är begränsade till kritisk infrastruktur som energi-, kommunikation-, transport- eller banksektorn utan även mindre företag utgör en viktig del av de komplexa och bitvis sårbara leveranskedjor som samhället är beroende av.

Ovannämnda insatser spelar en viktig roll för att stärka samhällets och näringslivets robusthet och resiliens för att bättre kunna förhindra och motstå störningar orsakade av bristande IoT-säkerhet. En dimension av robusthet och resiliens är tillit, i bemärkelsen att befolkningen är trygg i förvissningen att grundläggande samhällstjänster och funktioner fungerar och finns tillgängliga för dem (och att så är fallet). Detta kan uppfattas som ett mått på befolkningens förtroende för styrande maktens förmåga att utföra sitt uppdrag gentemot dem.

Militära underrättelse- och säkerhetstjänsten (Must) skriver i sin årsöversikt 2022 att hotnivån för subversion, exempelvis i form av påverkansoperationer, har höjts i och med det försämrade säkerhetsläget[66]. Aktörer som vill tillfoga samhället skada kan exempelvis använda sig av olika narrativ för att försöka skapa splittring och minska förtroendet för myndigheter och de styrande. Detta för att göra det till en svagare och mer formbar konkurrent, så att ens egna intressen gynnas. Ett aktuellt exempel kan vara överbelastningsangrepp (som kanske möjliggjorts av ett botnät som rekryterat undermåligt skyddade IoT-enheter) mot viktiga webbsidor. Den faktiska konsekvensen kan vara att webbsidor är otillgängliga under en period, vilket kan ställa till med besvär men inte nödvändigtvis behöver påverka organisationens förmåga att leverera sina tjänster eller produkter. För att minska risken för att en aktör utnyttjar en sådan incident och använder den i narrativ om samhällets kollaps kan myndigheter och andra relevanta organisationer snabbt och löpande förmedla korrekt information som förklarar läget. Detta kan bidra till att perceptionen av såväl hot som konsekvenser av angrepp är proportionerliga.

Med det sagt: svenska myndigheter och företag är bland de mest digitaliserade i världen – i FN:s digitaliseringsindex ligger Sverige på en femteplats[67] medan landet 2020 befann sig på plats 26 avseende cybersäkerhet enligt Internationella Teleunionens Global Security Index[68]. I takt med att funktioner i samhället, ekonomiska värden och ytterst människors liv och hälsa knyts till sammankopplade system riskerar cyberangrepp att få allvarligare konsekvenser än besvär orsakade av överbelastningsangrepp[69]. Om styrsystemen för elkraft, vatten, fjärrvärme, telefoni, myndigheter, flygledning, och banker blir angripna kan konsekvenserna i samhället bli omfattande. Det är därför av vikt att parallellt **implementera basala åtgärder** som ger grundläggande skydd mot angrepp, såsom överbelastningsskydd och genomlysning av IoT i verksamheten, samtidigt som konkreta åtgärder från aktörer inom både myndigheter och näringsliv tas för att minska sårbarheter, som en del av förberedelserna för potentiella framtida hotscenarion.

# 5. Källor


1 (2022) European Cyber Security Organisation. ECSO Technical Paper on Internet of Things (IoT). S. 7. https://mcusercontent.com/dd08496e1863c5ea11d77abac/files/06beb5b6-221f-9fc2-97cd-696ea85a2a88/ECSO_WG6_IoT_Technical_paper_final.02.pdf

2 Hull Wiklund, C., Faria, D., Johansson, B., Öhrn-Lundin, J. (2017) FOI Strategisk utblick 7. Närområdet och nationell säkerhet. S. 57 https://www.foi.se/rest-api/report/FOI-R--4454--SE

3 (2022) Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride! https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030

4 (2023) Must årsöversikt 2022. s. 38 https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/musts-arsoversikter/must-arsoversikt-2022.pdf

5 (2023) Must årsöversikt 2022. s. 13 https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/musts-arsoversikter/must-arsoversikt-2022.pdf

6 (2018-02-08) The Internet of Things: A technical primer https://www2.deloitte.com/us/en/insights/focus/internet-of-things/technical-primer.html

7 2016) Sundström, T. Internetguide #43 Internet of things: En guide till sakernas internet. S. 14 https://internetstiftelsen.se/app/uploads/2021/01/internet-of-things.pdf

8 (2019-06-18) The Growth in Connected IoT Devices is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast https://www.businesswire.com/news/home/20190618005012/en/The-Growth-in-Connected-IoT-Devices-is-Expected-to-Generate-79.4ZB-of-Data-in-2025-According-to-a-New-IDC-Forecast

9 (2017-05-06) The world's most valuable resource is no longer oil, but data. The Economist https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

10 Det vill säga regler och processer för hur beslut som rör data fattas. Källa: https://infohub.delltechnologies.com/l/edge-to-core-and-the-internet-of-things-2/internet-of-things-and-data-placement

11 The Internet of Things: A technical primer (2018-02-08) https://www2.deloitte.com/us/en/insights/focus/internet-of-things/technical-primer.html

12 (2016) Sundström, T. Internetguide #43 Internet of things: En guide till sakernas internet. S. 17 https://internetstiftelsen.se/app/uploads/2021/01/internet-of-things.pdf

13 (2016) Sundström, T. Internetguide #43 Internet of things: En guide till sakernas internet. S. 17 https://internetstiftelsen.se/app/uploads/2021/01/internet-of-things.pdf

14 (2016) Sundström, T. Internetguide #43 Internet of things: En guide till sakernas internet. S. 20 https://internetstiftelsen.se/app/uploads/2021/01/internet-of-things.pdf

15 Lagercrantz, S. (2014-01-17) Kontaktlinser ska mäta blodsocker. Dagens Medicin. https://www.dagensmedicin.se/specialistomraden/medicinsk-teknik/kontaktlinser-ska-mata-blodsocker/

16 Ansiktsigenkänning och dataskydd – Integritetsskyddsmyndigheten https://www.imy.se/verksamhet/kamerabevakning/ansiktsigenkanning-och-dataskydd/

17 Dobos, L. (2019-08-24) Ny teknik för anonymiserad ansiktsigenkänning lanseras i svenska butiker Computer Sweden. https://computersweden.idg.se/2.2683/1.722396/anonymiserad-ansiktsigenkanning

18 Smarta städer: Framtidens städer https://www.microsoft.com/sv-se/industry/government/resources/smart-cities

19 Vad är Sakernas internet? Definition och förklaring https://www.kaspersky.se/resource-center/definitions/what-is-iot

20 Hur smart jordbruk och elektrifiering är nyckeln till hållbarhet https://www.harting.com/SE/sv/topics/how-smart-farming-and-electrification-key-sustainability AIoT i jordbruket – med allt fler fördelar https://www.bosch.se/nyheter/agriculture/

21 Sundström, T. (2016) Internetguide #43 Internet of things: En guide till sakernas internet. S. 32 https://internetstiftelsen.se/app/uploads/2021/01/internet-of-things.pdf

22 Internet of things för vattenverk och vattenkraftstationer https://www.induo.com/a/va-system/internet-of-things-vattenverk-kraftstationer/

23 Dahlqvist, F., Patel, M., Rajko, A., Schulman, J. (2019-07-22) Growing opportunities in the Internet of Things https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things

24 The Internet of Things: A technical primer (2018-02-08) https://www2.deloitte.com/us/en/insights/focus/internet-of-things/technical-primer.html

25 Moen, J., Persson, H. (2022-11-03) Del 1: Internet of Things – vår tids "game-changer"? https://www.soprasteria.se/blogg/internet-of-things--var-tids-game-changer/

26 Hjerpe, R. (2022-06-21) 5G:s 3 faser för IoT– så kommer utvecklingen att se ut Ny Teknik https://www.nyteknik.se/5gs-3-faser-for-iot-sa-kommer-utvecklingen-att-se-ut/968927

27 The Internet of Things: A technical primer (2018-02-08) https://www2.deloitte.com/us/en/insights/focus/internet-of-things/technical-primer.html

28 Hull Wiklund, C., Faria, D., Johansson, B., Öhrn-Lundin, J. (2017) FOI Strategisk utblick 7. Närområdet och nationell säkerhet. S. 60 https://www.foi.se/rest-api/report/FOI-R--4454--SE

29 (2023) Säkerhetspolisen 2022 – 2023. s. 38 - 39 https://www.sakerhetspolisen.se/download/18.36cda2851868025da5b2b/1677241538918/SP_A%CC%8Arsbok_2022__Anpassad.pdf

30 https://azure.microsoft.com/sv-se/resources/cloud-computing-dictionary/what-is-iot/security/

31 (2022) European Cyber Security Organisation. ECSO Technical Paper on Internet of Things (IoT). S. 19. https://mcusercontent.com/dd08496e1863c5ea11d77abac/files/06beb5b6-221f-9fc2-97cd-696ea85a2a88/ECSO_WG6_IoT_Technical_paper_final.02.pdf

32 Hedtjärn Swaling, V., Johansson, J. (2018) NCS3 Studie – IoT-relaterade risker och strategier. Risker relaterade till Internet of Things (IoT) och vad myndigheter kan göra för att motverka dem. S. 25 https://www.msb.se/RibData/Filer/pdf/28550.pdf

33 Hedtjärn Swaling, V., Johansson, J. (2018) NCS3 Studie – IoT-relaterade risker och strategier. Risker relaterade till Internet of Things (IoT) och vad myndigheter kan göra för att motverka dem. S. 25 https://www.msb.se/RibData/Filer/pdf/28550.pdf

34 Heiding, F., Süren, E., Olegård, J. Lagerström, R. (2022) Penetration testing of connected households Computers & Security. s.1 https://www.sciencedirect.com/science/article/pii/S016740482200459X

35 (2022) Ethical and societal challenges of the approaching technological storm. https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729543/EPRS_STU(2022)729543_EN.pdf s. 18

36 https://www.infosecurity-magazine.com/news/smart-home-experiences-cyber/

37 En adapter som kan kopplas in i en bil för att förbättra dess uppkopplade funktionalitet
Heiding, F., Süren, E., Olegård, J. Lagerström, R. (2022) Penetration testing of connected households. Computers & Security. s.3 https://www.sciencedirect.com/science/article/pii/S016740482200459X

38 Heiding, F., Süren, E., Olegård, J. Lagerström, R. (2022) Penetration testing of connected households Computers & Security. s.1 https://www.sciencedirect.com/science/article/pii/S016740482200459X

39 Söderholm, E. (2022-12-05) Allvarlig brist avslöjad i uppkopplad biltjänst. Vi Bilägare https://www.vibilagare.se/nyheter/allvarlig-brist-avslojad-i-uppkopplad-biltjanst
Söderholm, E. (2023-01-12) Mängder av sårbarheter hittade hos flera bilmärken. Vi Bilägare https://www.vibilagare.se/nyheter/mangder-av-sarbarheter-hittade-hos-flera-bilmarken

40 Campanello, S. (2018-08-31) Forskare hackar låset på en Tesla på några sekunder. Ny Teknik. https://www.nyteknik.se/model-s-sakerhet-tesla/forskare-hackar-laset-pa-en-tesla-pa-nagra-sekunder/1239142

41 Hern, A. (2017-08-31) Hacking risk leads to recall of 500,000 pacemakers due to patient death fears. The Guardian https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update

42 Hedtjärn Swaling, V., Johansson, J. (2018) NCS3 Studie – IoT-relaterade risker och strategier. Risker relaterade till Internet of Things (IoT) och vad myndigheter kan göra för att motverka dem. S. 32 https://www.msb.se/RibData/Filer/pdf/28550.pdf

43 Valassi, C., Karresand, M. (2019) NCS3 - Komponenter på avstånd: Säkerhetsbeaktanden för direkt adresserbara trådlöst nätverksanslutna komponenter i
i ndustriella informations- och styrsystem. s. 45 https://www.msb.se/contentassets/6840a9f762184a869b39954f670c8e77/ncs3---komponenter-pa-avstand.pdf

44 Hedtjärn Swaling, V., Johansson, J. (2018) NCS3 Studie – IoT-relaterade risker och strategier. Risker relaterade till Internet of Things (IoT) och vad myndigheter kan göra för att motverka dem. S. 32 https://www.msb.se/RibData/Filer/pdf/28550.pdf

45 Hedtjärn Swaling, V., Johansson, J. (2018) NCS3 Studie – IoT-relaterade risker och strategier. Risker relaterade till Internet of Things (IoT) och vad myndigheter kan göra för att motverka dem. S. 33 https://www.msb.se/RibData/Filer/pdf/28550.pdf

46 Hedtjärn Swaling, V., Johansson, J. (2018) NCS3 Studie – IoT-relaterade risker och strategier. Risker relaterade till Internet of Things (IoT) och vad myndigheter kan göra för att motverka dem. S. 33 https://www.msb.se/RibData/Filer/pdf/28550.pdf

47 Hedtjärn Swaling, V., Johansson, J. (2018) NCS3 Studie – IoT-relaterade risker och strategier. Risker relaterade till Internet of Things (IoT) och vad myndigheter kan göra för att motverka dem. S. 29 https://www.msb.se/RibData/Filer/pdf/28550.pdf

48 En anordning som används för att styra en mekanism eller mekaniskt system. Ställdonet styrs av en signal och omvandlar denna signal till en mekanisk rörelse eller en annan fysisk förändring. Källa: https://iotsverige.se/om-oss/iot-sa-funkar-det

49 Hedtjärn Swaling, V., Johansson, J. (2018) NCS3 Studie – IoT-relaterade risker och strategier. Risker relaterade till Internet of Things (IoT) och vad myndigheter kan göra för att motverka dem. S. 33 https://www.msb.se/RibData/Filer/pdf/28550.pdf

50 IMY, Integritetsskyddsapport - - redovisning av utvecklingen på IT-området när det gäller integritet och ny teknik 2020 s. 69 källa: https://www.imy.se/globalassets/dokument/rapporter/integritetsskyddsrapport2020.pdf

51 Hull Wiklund, C., Faria, D., Johansson, B., Öhrn-Lundin, J. (2017) FOI Strategisk utblick 7. Närområdet och nationell säkerhet. S. 59 https://www.foi.se/rest-api/report/FOI-R--4454--SE

52 Hedtjärn Swaling, V., Johansson, J. (2018) NCS3 Studie – IoT-relaterade risker och strategier. Risker relaterade till Internet of Things (IoT) och vad myndigheter kan göra för att motverka dem. S. 30 https://www.msb.se/RibData/Filer/pdf/28550.pdf

53 Hedtjärn Swaling, V., Johansson, J. (2018) NCS3 Studie – IoT-relaterade risker och strategier. Risker relaterade till Internet of Things (IoT) och vad myndigheter kan göra för att motverka dem. S. 28 https://www.msb.se/RibData/Filer/pdf/28550.pdf
samt IoT-relaterade risker, uppdaterad version: Begrepp och kategorisering (MSB Publ.nr MSB1523 – mars 2020)

54 2023) Årsöversikt 2022 MUST. S. 48 https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/musts-arsoversikter/must-arsoversikt-2022.pdf

55 (2023) Årsöversikt 2022 MUST. S. 47 https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/musts-arsoversikter/must-arsoversikt-2022.pdf

56 (2022) Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride! https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030

57 IoT-säkerhet – en översikt https://azure.microsoft.com/sv-se/resources/cloud-computing-dictionary/what-is-iot/security/ Säkerhetsarkitektur för IoT-lösningar (2023) https://learn.microsoft.com/sv-se/azure/iot-fundamentals/iot-security-architecture#security-starts-with-a-threat-model

58 En digital tvilling är en virtuell representation av en fysisk sak, baserad på realtidsdata från sensorer som är placerade på den fysiska saken. En mycket komplext virtuell modell skapas, vilken ska vara den exakta motsvarigheten till den fysiska saken. Modellen kan sedan ge realtidsinformation om den fysiska sakens tillstånd, medan den samtidigt låter användare testa olika scenarion eller förutser framtiden genom att driva modellen som skapats.
Källa: (2022) Ethical and societal challenges of the approaching technological storm. https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729543/EPRS_STU(2022)729543_EN.pdf s. 9

59 Hedtjärn Swaling, V., Johansson, J. (2018) NCS3 Studie – IoT-relaterade risker och strategier. Risker relaterade till Internet of Things (IoT) och vad myndigheter kan göra för att motverka dem. S. 37 https://www.msb.se/RibData/Filer/pdf/28550.pdf

60 Hedtjärn Swaling, V., Johansson, J. (2018) NCS3 Studie – IoT-relaterade risker och strategier. Risker relaterade till Internet of Things (IoT) och vad myndigheter kan göra för att motverka dem. S. 37 https://www.msb.se/RibData/Filer/pdf/28550.pdf

61 Sammanfattning av Förordning (EU) 2019/881 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (cybersäkerhetsakten) https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=LEGISSUM:4398780 och IVA-rapporten, s.23

62 EU Cyber Security Act—vad innebär det och vilka regler gäller? (2023-02-02) https://www.ri.se/sv/eu-cyber-security-act-vad-innebar-det-och-vilka-regler-galler

63 Rättsakt om cyberresiliens (2022-09-15) https://digital-strategy.ec.europa.eu/sv/library/cyber-resilience-act

64 Vilken effekt kommer EU Cyber Resilience Act ha? (2023-02-02) https://www.ri.se/sv/vilken-effekt-kommer-eu-cyber-resilience-act-ha
Vissa undantag gäller, för bland annat medicintekniska produkter, luftfart och bilar som redan omfattas av existerande EU-lagstiftning. Källa: https://www.vinge.se/nyheter/europeiska-kommissionen-foreslar-en-cyber-resilience-act/

65 (2018) Säkrare IoT - Rekommendationer till myndigheter. https://rib.msb.se/filer/pdf/28545.pdf

66 (2023) Must årsöversikt 2022. S. 42 - 43 https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/musts-arsoversikter/must-arsoversikt-2022.pdf

67 (2023) Must årsöversikt 2022. S. 53 https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/musts-arsoversikter/must-arsoversikt-2022.pdf

68 (2020) International Telecommunication Union Global Cybersecurity Index 2020. S. 25 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

69 (2023) Säkerhetspolisen 2022 – 2023. s. 36 https://www.sakerhetspolisen.se/download/18.36cda2851868025da5b2b/1677241538918/SP_A%CC%8Arsbok_2022__Anpassad.pdf

**Sakernas internet (IoT, Internet of Things) är en ledande komponent i digitaliseringen av samhället, industrin och ekonomin. Rapporten syftar till att belysa risker kopplade till tekniken samt vara ett stöd för chefer och beslutsfattare i den offentliga och privata sektorn.**

**RISE – Research Institutes of Sweden**
ri.se / info@ri.se / 010-516 50 00
Isafjordsgatan 22, 6 tr | SE-164 40 Kista

Grants Office/Informationscenter
RISE Rapport: 2023:mars