Policy för hantering av sårbarheter och sårbarhetsinformation

Nulägesbeskrivning och analys sammanställdes i oktober 2025. Dessa kommer att uppdateras i det vidare arbetet med policyn.

Definitioner

Definitioner av begrepp av central betydelse för att förstå policyn.

Coordinated Vulnerability Disclosure (CVD) - en process där arbetet med att ta fram åtgärder för samt informera om en upptäckt sårbarhet koordineras mellan upptäckaren och leverantören/tillverkaren av produkten eller tjänsten, bl.a. angående tidpunkt för publicering av sårbarheten. Den svenska översättningen i NIS2 är ”samordnad delgivning av information om sårbarheter”.

Vulnerability Management, hantering av sårbarheter – en metodik för att löpande identifiera, klassificera, prioritera och åtgärda eller mildra konsekvenser av sårbarheter som uppträder i den it-miljö man hanterar.

Upptäckare av sårbarheter innebär i denna policy etiska hackare, säkerhetsintresserade personer, brottsförebyggande myndigheter, undrerättelsemyndigheter, försvarsmakten.

Rapportörer är de som hör av sig om sårbarheter till leverantör eller koordinerande part.

Introduktion

Den här policyn rör av samordnad delgivning av information av sårbarheter samt hantering av sårbarheter hos enskilda organisationer. Dessa områden är båda väsentliga beståndsdelar för att stärka samhällets cybersäkerhet och minimera risken för att sårbarheter får skadliga följder.

Samordnad delgivning av information av sårbarheter (Coordinated Vulnerability Disclosure på engelska) är en process för att på ett effektivt sätt ta fram säkerhetsuppdateringar eller andra åtgärder som avser underlätta för enskilda organisationer att undanröja sårbarheter innan något går snett eller utnyttjas av hotaktörer.

Flera aktörer behöver medverka i CVD-processen. Det inkluderar de som upptäcker sårbarheter, rapporterar sårbarheter, leverantörer och användare av mjukvaror samt de aktörer som koordinerar och stöttar arbetet i processen.

Samordnad delgivning av information av sårbarheter kan ske på olika nivåer samt mellan olika parter. Ett sätt är att upptäckare av sårbarheter vänder sig direkt till leverantören eller tillverkaren av programvaran eller leverantören av tjänsten ifråga som innehar sårbarheten och informerar om sin upptäckt. Ett alternativt sätt är att upptäckaren rapporterar information om sårbarheten till en betrodd förmedlare, en koordinerande part.

Enligt NIS2-direktivet ska varje land utse minst en nationell CSIRT-enhet som kan inneha rollen som koordinator och vara en betrodd förmedlare av information om sårbarheter.

Den nationella CVD-policyn ska vara harmoniserad med nationella policyer om sårbarhetshantering i andra länder inom EU.

Nulägesbild för policyområdet om samordnad delgivning av information om sårbarheter samt hantering av sårbarheter

Sårbarheter upptäcks löpande av mjukvaruleverantörerna själva, it-säkerhetsintresserade personer och hotaktörer; manuellt och med hjälp av automatisering. Nya metoder och tekniker för att exploatera sårbarheter utvecklas kontinuerligt. En noterbar trend är att generativ artificiell intelligens används i allt större utsträckning i syfte att både identifiera och utnyttja sårbarheter. Efterforskandet av sårbarheter och hur dessa kan utnyttjas är därtill en del av tjänsteutbudet på den globala marknaden för cyberbrottslighet. Utnyttjandet av orättade sårbarheter är idag det näst vanligaste sättet för en angripare att få fotfäste i en it-miljö efter phishing (nätfiske). Vidare utnyttjar antagonistiska cyberaktörer, underrättelsemyndigheter och brottsbekämpande myndigheter s.k. zeroday-sårbarheter[1] i allt högre utsträckning än tidigare. Det ska understrykas att trots en ökad förekomst och uppmärksammande av zeroday-sårbarheter så utnyttjas sårbarheter genom hela sårbarhetens livscykel[2]. Det innebär att det är även vanligt förekommande att gamla sårbarheter utnyttjas.

Låg kännedom om CVD-process och varför den är viktig för samhället

Organisationer i samhället har generellt en låg kännedom och kunskap om vad samordnad delgivning av information om sårbarheter innebär, varför processen är viktig och varför det är viktigt att fler deltar i den.

Mogna leverantörer och särskilt it-säkerhetsintresserade personer känner till processen och dess roller. På grundval av mängden frågor och den låga frekvensen av sårbarhetsärenden är Sverige underutvecklat på området.

[1] sårbarheter som utnyttjas innan dessa publikt är konstaterade, finns buggrättning och är allmänt tillkännagivna
[2] https://cybersecuritynews.com/768-vulnerabilities-exploited/

Rollerna som ”upptäckare” och ”rapportör” är otydligt beskrivna och reglerade. Viss vägledning om CVD och skillnaden mellan överenskommen undersökning på uppdrag respektive kontakt med leverantörer eller andra berörda när sårbarheter upptäckts i samband med annan verksamhet, kan fås i de få utbildningar i etisk hackning som finns i Sverige.

I september 2026 börjar bestämmelserna om rapportering i EU:s Cyberresiliensförordning (CRA) att gälla. I artikel 15 beskrivs frivillig rapportering av bl.a. sårbarheter till den nationella koordinerande CSIRT-enheten, vilket kan göra det tydligare för upptäckare vart de kan vända sig avseende produkter som tillgängliggörs i EU.

Koordinatorrollen för sårbarhetsärenden är välbeskriven och har stöd i dokumentation från främst CERT/CC, men även branschorganisationen FIRST, och är därmed en roll som t.ex. en nationell CSIRT-enhet förväntas kunna ta. SITIC (vid PTS från 2004) och senare CERT-SE (vid MSB från 2011) är den verksamhet i Sverige som motsvarar en nationell CSIRT och MSB är formellt utpekad som sådan i Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster. I NIS2-direktivet kravställs den nationella CSIRT-enhetens uppgifter till bl.a att:

- ta emot sårbarhetsrapporter,
- stödja rapportören,
- identifiera och kontakta berörda parter,
- fungera som en betrodd mellanhand och
- förhandla tidsramar samt samordna arbetet.

Hela processen för samordnad delgivning av information om sårbarheter är dock fortsatt oreglerad. MSB förbereder för ett ökat inflöde av CVD-ärenden.

En typ av koordinerande roll har de s.k. bug bounty-plattformarna, som knyter leverantörer till sig som kunder och tar emot sårbarhetsrapporter från upptäckare. Plattformen förmedlar sedan rapporter till leverantörerna, faciliterar ibland efterföljande dialog och betalar ut ersättning (s.k. Bug Bounty).

Leverantörer hittar stöd för sin roll bl.a. i ISO-standarder[3] som beskriver processen och hur man som leverantör förbereder för att effektivt åtgärda egenupptäckta eller rapporterade sårbarheter i sin produkt. Enligt branschstandard (RFC 9116) bör företag publicera kontaktinformation för sårbarhetsärenden på sin webbplats. De kan där även beskriva förväntningar på dem själva och på upptäckare, en egen CVD-policy och/eller eget bug-bounty-program, d.v.s. vilka produkter som avses och villkoren för utbetalning av belöning för värdefulla rapporter. När EU:s cyberresiliensförordning (CRA) träder i kraft ställs krav på företag som säljer produkter på EU-marknaden, se avsnittet om rättsliga förutsättningar för rollerna i sårbarhetshanteringen.

[3] Främst ISO/IEC 27002:2013, ISO/IEC 29147 och ISO/IEC 30111 samt ISO/IEC TR 5895:2022

Nationellt och internationellt samarbete

I Sverige finns enstaka forum eller samarbeten där sårbarhetsrättning diskuteras som t.ex. Nordic Software Security Summit[4].

CERT-SE deltar i CVD-relaterade diskussioner i EU:s nätverk för nationella CSIRT:s.

Rättsliga förutsättningar för upptäckare och nationell CVD-koordinator

Den som gör sig skyldig till dataintrång, dvs olovligen tränger sig in i ett it-system där data blir behandlad, lagrad eller överförd elektroniskt kan enligt 4 kap. 9 c brottsbalken (1962:700) bli straffad med böter och fängelse. När det gäller genomförande av penetrationstester eller etisk hackning som på förhand godkänts av organisationen vars it-system testas och uppdragstagaren (den etiska hackaren) håller sig inom överenskomna ramar handlar det inte om dataintrång.

Det saknas i dagsläget ett tydligt legalt skyddsnät för den som begår s.k. ”etisk hackning” eller genomför penetrationstestning utanför överenskomna ramar eller genom ett uppdrag från en organisation i syfte att upptäcka en sårbarhet och för den rapporterande parten kan mötas av rättsliga konsekvenser, t.ex. genom stämning från tillverkare eller leverantörer av programvaran som innehar sårbarheten. Utförandet av etisk hackning kan även innebära överträdelser inom dataskyddsområdet (GDPR), immaterialrätten (t.ex. åtkomst till kod) samt bryta mot användarvillkor.

Offentlighets- och sekretesslagen (2009:400) kan komma att kompletteras med nya sekretessregler för att säkerställa konfidentialitet vid inrapportering av sårbarheter till myndigheter. Sådan inrapportering ska ske både enligt artikel 14 cyberresiliensförordningen och artikel 21 i NIS2-direktivet.

Hantering av sårbarheter

Organisationer förlitar sig idag på en stor mängd programvaror och system för att kunna bedriva egen verksamhet samt för att erbjuda tjänster och produkter. Mängden och variationen av programvaror och system ökar över tid.

Resultat i MSB:s cybersäkerhetsmätning Cybersäkerhetskollen[5] visar på att offentliga organisationer i stor utsträckning saknar ett systematiskt cybersäkerhetsarbete. En bakomliggande grundläggande orsak är att organisationer inte avsätter tillräckligt med ekonomiska och personella resurser till arbetet. Det får även påverkan på förmågan att hantera, prioritera och åtgärda sårbarheter i programvaror.

Vanligt förekommande bristande förmågor på området kan sammanfattas i följande övergripande kategorier:

• **Kunskap och kompetens**: utmaningar kring saknad kunskap om behovet av utförande av säkerhetsuppdateringar och om beaktandet av sådan information från CSIRT-enheten r leverantören ifråga.
• **Organisatoriska utmaningar**: utmaningar med otydlig organisationsstruktur med oklara roller och arbetssätt för prioritering av genomförande av säkerhetsuppdateringar.

• **Processuella utmaningar**: utmaningar kring användning av ett ändamålsenligt och holistiskt arbetssätt för att både kunna prioritera och hantera sårbarheter. Avsaknad av processer och tekniska system för att ha god kännedom om organisationens programvaror och programvaruversioner.

• **Resurser:** utmaningar kring otillräckliga ekonomiska eller personella resurser för genomförande av säkerhetsuppdateringar eller vidtagande av andra nödvändiga säkerhetsåtgärder för att minimera risker för incidenter och att ekonomiska resurser för säker hantering säkerställs även över tid.

Nya föreskrifter om säkerhetsåtgärder enligt Cybersäkerhetslagen innehåller bl.a. närmare krav på förändringshantering och säker livscykelhantering. Vidare uppställer EU:s regleringar Cybersäkerhetsförordningen och Cyberresiliensförordningen krav på bl.a. inbyggd säkerhet liksom på säker livscykelhantering i programvaror.

CERT-SE informerar ett antal tillfällen per vecka om aktuella sårbarheter genom bl.a. veckobrev och s.k. blixtmeddelanden när kritiska sårbarheter finns att informera om. Allt fler organisationer prenumererar på dessa informationsutskick, men flertalet organisationer gör det inte.

Analys av nuläget

Låg kännedom om samordnad delgivning av information om sårbarheter i samhället

Det är positivt att det finns internationell branschpraxis, ISO-standarder och stödmaterial för samtliga roller i processen. Att utbildning inom etisk hackning samt information och råd som publiceras av MSB (www.cert.se i januari 2026) ökar kännedomen om dessa är bra, men den alltjämnt låga kännedomen om samordnad delgivning av information om sårbarheter i Sverige leder till att:

- Onödigt få personer kommer på tanken att utnyttja sina tekniska färdigheter att söka efter sårbarheter som finns i produkter och system. En möjlig orsak till detta kan vara att det saknats främjandeåtgärder på området eller att främjandeåtgärderna inte har varit lyckosamma. En annan orsak kan vara att det saknats och saknas tillräckligt rättsliga förutsättningar för att kunna delta i processen på ett säkert sätt.
- Onödigt få upptäckta sårbarheter rapporteras till leverantör eller berörd driftsansvarig eller till koordinerande part, som nationell CSIRT eller bug bounty-plattformar. Möjliga orsaker till detta bedöms vara desamma som i den första punkten.

- Onödigt många ärenden för att åtgärda sårbarheter i produkter eller tjänster kör fast eller brister i effektivitet och resultat.

Att kännedomen är låg beror på att området är nischat och att inte gemene person har kunskap om kodutveckling, attackmetoder. Ytterligare orsaker är att kodunderhåll och omhändertagandet av sårbarheter inte är fullt lika engagerande som att utveckla kod från start.

Nationellt och internationellt samarbete

Det är positivt att visst nationellt och internationellt utbyte förekommer men det är en missad chans att inte fler möjliga samarbeten utnyttjas. Att dessa möjligheter går förbi beror på att de inte är kända för de som skulle kunna engagera sig i dem, samt att det finns få faciliterande aktörer på området.

Rättsliga förutsättningar

Det är positivt att samordnad delgivning av information om sårbarheter delvis formaliseras i Sverige genom genomförandet av Cybersäkerhetslagen och Cyberresiliensförordningen i svensk rätt, samt att nya sekretessregler kring anonyma rapportörer och inrapporterad information kan komma i offentlighets- och sekretesslagen (2009:400), OSL.

Det är negativt att det saknas ett tydligt lagrum för den ”etiska hackning” som kan leda till upptäckten av både nya sårbarheter och instanser av kända sårbarheter. Människor som har vilja och förmåga att utforska mjukvara och internetexponerade system i jakt på sårbarheter att informera om innan samma sårbarheter utnyttjas av hotaktörer riskerar exempelvis att åtalas för dataintrång. Det får till följd att etiska hackare avstår från verksamhet som hade kunnat komma såväl organisationer som samhället till stor säkerhetsnytta. Orsaken till att sådant lagrum saknas har att göra med att digitaliseringen har gått mycket fortare än både statens säkerhetsarbete och lagstiftningsprocessen.

Hantering av sårbarheter hos den egna verksamheten

Cybersäkerhetslagen med tillhörande föreskrifter om säkerhetsåtgärder som träder i kraft 2026 bidrar positivt till området. Dessa ställer krav på bl.a. förändringshantering, inbyggd säkerhet och säker livscykelhantering av programvaror, vilket kommer att stärka organisationers förmåga att hantera sårbarheter. Vidare kommer ikraftträdandet och tillämpningen av cyberresiliensförordningen driva utvecklingen mot ökad inbyggd säkerhet i programvaror, förbättrad säker livscykelhantering från leverantörer och en ökad rapportering av sårbarheter. Att bestämmelser om administrativa sanktionsavgifter får tas ut i händelse av överträdelser enligt Cybersäkerhetslagen bidrar till att organisationer behöver vidta säkerhetsåtgärder på ett mer systematiskt och riskbaserat sätt än tidigare.

- Det är dock i nuläget och inom de närmaste åren allvarligt att många organisationer inte avsätter tillräckliga ekonomiska och personella resurser till arbetet med att identifiera, prioritera och åtgärda sårbarheter. Detta leder till att sårbarhetshanteringen ofta blir reaktiv snarare än proaktiv, vilket i utsträckning

kan leda till en ökad risk för att cybersäkerhetsincidenter med potentiellt stora konsekvenser sker. Resursbristen påverkar även förmågan att upprätthålla nödvändiga rutiner och kontinuitet. Det kan finnas flera olika orsaker till att organisationer inte avsätter tillräckliga resurser. Exempel är att organisationen inte känner till eller har bedömt vilka faktiska ekonomiska, affärs- och konkurrensmässiga, samhällsviktiga eller förtroende- och integritetsmässiga konsekvenser incidenter kan medföra för den egna verksamheten, samhället eller enskilda människor i händelse av att incidenter inträffar. Ett annat exempel är att säker hantering av programvaror bedöms vara it-avdelningens ansvar, en viss verksamhets och inte ledningens.

- Det är negativt att många organisationer har en låg grad av kännedom om sina installerade programvaror, versioner och beroenden. Detta försvårar möjligheten att identifiera vilka system som kan påverkas när nya sårbarheter offentliggörs. Bristande överblick leder möjligen till att uppdateringar kan missas eller genomföras osystematiskt, särskilt i miljöer där ”skugg-it” eller äldre system förekommer och att cybersäkerhetsincidenter sker i värsta fall. Det kan finnas flera orsaker till detta, exempelvis att organisationen inte har kunskap om varför det är viktigt att ha en samlad och uppdaterad bild över samtliga sina programvaror och programvaruversioner, att organisationen inte har haft resurser för att införskaffa och använda ändamålsenliga system och processer för att kunna säkerställa en god överblick över detta.
- Det är vidare problematiskt att ansvarsfördelningen för säkerhetsuppdateringar ofta är otydlig och ofullständig mellan exempelvis verksamhetens olika delar och it-avdelningen. När ansvaret ligger på roller utan tillräcklig teknisk kompetens finns en risk att uppdateringar inte prioriteras eller görs i tid. En orsak till detta kan vara att ledningen behöver avsätta mer tid för frågor avseende styrning, prioritering och uppföljning av ett systematiskt säkerhetsarbete.
- Det är negativt att många organisationer saknar eller inte använder ändamålsenliga och dokumenterade processer för hur sårbarheter ska hanteras och prioriteras. I praktiken innebär detta att beslut om uppdateringar ofta tas ad hoc eller utan ett helhetsperspektiv på sårbarheter som kan utnyttjas bland organisationens system och programvaror. Ett sådant arbetssätt medför att hanteringen av sårbarheter inte sker systematiskt och att olika slags system kan lämnas oskyddade längre än nödvändigt. Flera etablerade modeller och ramverk för sårbarhetshantering finns att tillämpa, men de behöver anpassas till verksamhetens förutsättningar och risknivå. Det kan finnas flera orsaker till detta. En är att organisationer inte har haft tillräckligt med resurser för att identifiera eller saknar kunskap om ändamålsenliga processer på området.
- Många organisationer saknar ett helhetsperspektiv på vilka programvaror, system och tjänster som är mest kritiska för verksamheten. Utan tydlig prioritering finns risk att resurser riktas mot de delar av organisationen som gör mest väsen av sig snarare än mot de mest samhälls- eller verksamhetskritiska systemen. Ett systematiskt arbetssätt för att klassificera system utifrån affärs- och

informationssäkerhetskriterier behövs för att möjliggöra effektiv prioritering av åtgärder.

- Det är positivt att CERT-SE löpande informerar om aktuella sårbarheter via veckobrev och blixtmeddelanden. Det finns även osäkerheter kring hur väl informationen når fram till rätt mottagare inom organisationerna, och om den uppfattas som tillräckligt tydlig och handlingsinriktad. En bristande förståelse av budskapet riskerar att fördröja eller helt förhindra nödvändiga uppdateringar.