Trusselsvurdering

Cybertruslen mod Danmark 2025

November • 2025

Styrelsen for Samfundssikkerhed

”Cybertruslen mod Danmark” udarbejdes af Styrelsen for Samfundssikkerhed og er blevet til i tæt samarbejde med blandt andet FE og inddrager tjenestens vurderinger om statslige aktører.

Trusselsvurderingen har til formål at informere beslutningstagere i det danske samfund om cybertruslen mod Danmark. Vurderingen kan bl.a. tjene som input til danske organisationers risikovurderinger på cybersikkerhedsområdet. Trusselsvurderingen erstatter Center for Cybersikkerheds ”Cybertruslen mod Danmark”, der udkom i september 2024.

Indhold

Styrelsen for Samfundssikkerhed

Datavej 20
3460 Birkerød
Telefon: + 45 4516 1666
E-mail: samsik@samsik.dk

Forsidefoto: AdobeStock af Alex Stemmer

November 2025

Indledning

Danmark står over for det mest alvorlige risiko- og trusselsbillede siden anden verdenskrig. Det gælder ikke mindst i forhold til truslen fra cyberangreb, som har været stigende siden Ruslands invasion af Ukraine i 2022. Cybertruslen mod Danmark er alvorlig. Danske myndigheder, virksomheder og borgere udsættes dagligt for cyberangreb. Angrebene kommer fra både statslige og ikke-statslige aktører.

Den 3. oktober 2025 fremlagde Forsvarets Efterretningstjeneste (FE) vurderingen af den hybride trussel mod Danmark. Cyberangreb er et centralt værktøj i den hybride værktøjskasse, og forskellige typer af cyberangreb kan undergrave samfundets sammenhængskraft ved at forstyrre eller standse kritiske samfundsfunktioner.

I vores gennemdigitaliserede samfund er it en del af samfundets infrastruktur, som vi alle sammen er i berøring med. Med alle digitaliseringens fordele følger desværre også sårbarheder. Det ser vi, når danske organisationer får stjålet kritisk information, når vandforsyningen afbrydes som følge af hackerangreb eller når borgere via svindel på nettet får franarret penge af kriminelle i ind- og udland.

Trusselsvurderingen *Cybertruslen mod Danmark 2025* fastholder, at cybertruslen er blevet et grundvilkår. Derfor skal vi kende truslerne, så vi kan målrette vores indsats bedst muligt. Og selvom truslen i mange år har været alvorlig, ændrer den løbende karakter, ligesom hackerne hele tiden tager nye værktøjer og metoder i brug. Derfor fastholder vi i årets udgave trusselsniveauerne for formålskategorierne fra Cybertruslen mod Danmark 2024.

Cybertruslen mod Danmark er blevet udgivet siden 2016, og dette års udgave indeholder mange velkendte elementer, men også en række nye tiltag.

I årets vurdering fokuserer vi i højere grad på, *hvordan* hackerne angriber os, og i mindre grad på *hvorfor*. Derfor er trusselsvurderingen bygget op omkring de mest aktuelle angrebstyper. Det gør vi, fordi vi mener, at vi dermed kan formidle truslen mere målrettet til en bred vifte af modtagere på tværs af myndigheder, virksomheder og borgere. Med den nye opdeling er håbet, at vores vurdering som et konkret redskab kan medvirke til at styrke beredskabet og samfundets modstandsdygtighed. Den skal bruges og benyttes aktivt til at værne Danmark mod kriser. Under angrebstyperne vil vi fortsat analysere og beskrive, hvorfor de forskellige aktører handler, som de gør.

Selvom vi i år i højere grad fokuserer på typen af angreb end formålet, er den underlæggende analyse foretaget ud fra samme metodiske principper. Den nye ramme er altså alene en ny måde at formidle analysen på. Derfor er det stadig muligt at sammenligne med tidligere udgivelser og trusselsniveauer.

I de følgende kapitler om de forskellige angrebstyper findes analysen af, hvilke aktører og formål, der kan være på spil for de respektive angrebstyper. Trusselsvurderingen behandler følgende former for angreb:

- Ransomware-angreb
- Datatyveri
- Digital svindel
- DDoS
- Manipulation af operationel teknologi
- Wiper-angreb

I Styrelsen for Samfundssikkerhed tilbyder vi en bred vifte af vejledning og rådgivning om it-sikkerhed og cyberangreb, beredskabsplanlægning og meget andet, vi som samfund skal forholde os til. Det gør vi for at styrke Danmarks sikkerhed, og vi håber, at I som læsere vil medvirke til den vigtige opgave med at imødegå både nuværende og fremtidige trusler.

Laila Reenberg, direktør i Styrelsen for Samfundssikkerhed

Hovedvurderinger

Aktuelle trusselsniveauer

- Truslen fra cyberkriminalitet er **MEGET HØJ.** Cyberkriminelle rammer hele tiden ofre i Danmark med forskellige cyberangreb, fra omfattende ransomware-angreb til tyveri af sensitiv viden og svindel af den enkelte borger.

- Truslen fra cyberspionage er **MEGET HØJ**. Særligt Rusland og Kina retter løbende cyberangreb mod danske organisationer i forsøg på at få adgang til viden af bl.a. udenrigs- og sikkerhedspolitisk karakter samt indsigt i informationer med betydning for Danmarks forsvar.

- Truslen fra cyberaktivisme er **HØJ.** Særligt pro-russiske hackere rammer løbende danske mål med DDoS-angreb, og i nogle tilfælde gøres også forsøg på at manipulere operationel teknologi (OT), som f.eks. da et dansk vandværk blev ramt i slutningen af 2024. Det er sandsynligt, at nogle pro-russiske hackergrupper har forbindelse til den russiske stat.

- Truslen fra destruktive cyberangreb er **MIDDEL.** Det er særligt Ruslands risikovillighed i forhold til brugen af hybride virkemidler, der kan komme til udtryk i form af wiper-angreb og angreb mod operationel teknologi med begrænsede effekter.

- Truslen fra cyberterror er **INGEN**. SAMSIK vurderer, at ingen militante ekstremister aktører aktuelt har kapacitet til eller intention om at udføre cyberterror mod Danmark.

Angrebstyper

Styrelsen for Samfundssikkerhed vurderer, at følgende seks angrebstyper er de mest aktuelle, som danske organisationer skal forholde sig til:

- Det er meget sandsynligt, at danske organisationer vil blive udsat for forsøg på **ransomware-angreb**. Kriminelle hackergrupper retter løbende ransomware-angreb mod danske organisationer. Angrebene har ofte betydelige omkostninger for offeret, som bliver ramt, og kan potentielt også få alvorlige konsekvenser for samfundet, hvis kritisk infrastruktur eller samfundsvigtige funktioner påvirkes.

- Det er meget sandsynligt, at danske organisationer vil blive ramt af forsøg på **datatyveri**. Truslen kommer både fra fremmede stater, der løbende bedriver cyberspionage mod organisationer i Danmark, og kriminelle, der eksfiltrerer store mængder data fra deres ofre for enten at afpresse dem eller sælge data på det mørke internet.

- Det er meget sandsynligt, at danske organisationer og borgere vil blive udsat for forsøg på **digital svindel**. Kriminelle forsøger løbende at svindle danske organisationer og enkeltpersoner via digitale midler, og digital svindel udgør i dag et stigende samfundsproblem.

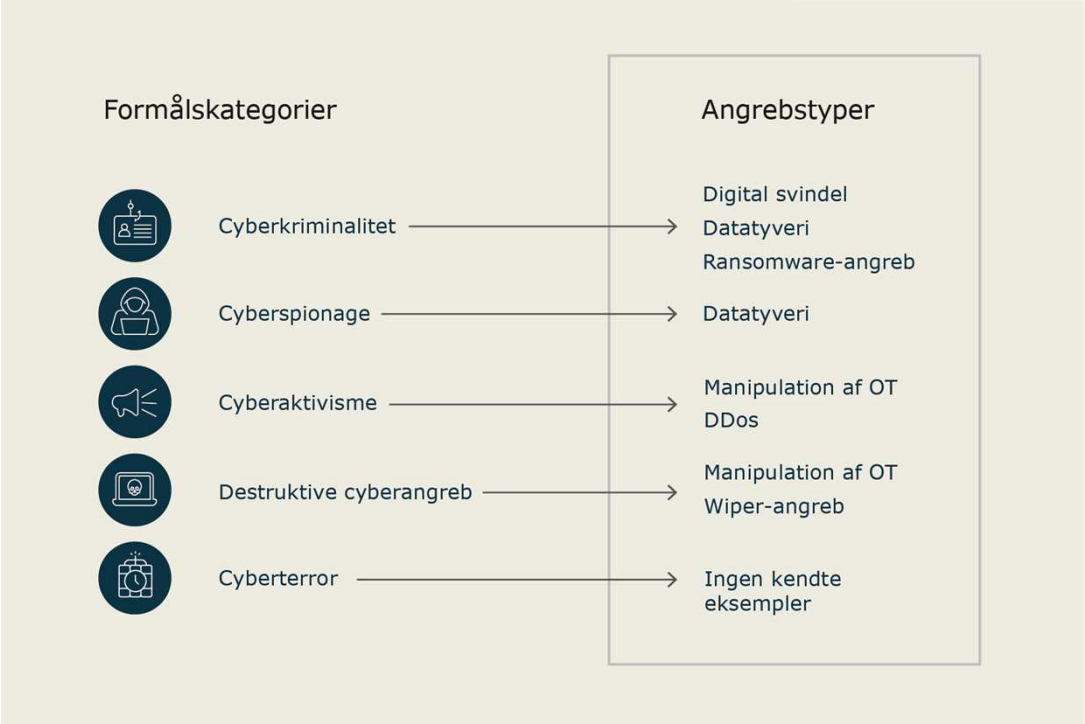
- Det er meget sandsynligt, at danske organisationer vil blive mål for **DDoS-angreb**, hvor hackere udnytter kompromitterede enheder til at overbelaste hjemmesider eller netværk. Især hackergrupper, som støtter Rusland, rammer løbende danske organisationer med DDoS-angreb i et sådant omfang, at det er blevet en fast del af trusselsbilledet. Nogle af disse pro-russiske hackere har sandsynligvis forbindelser til den russiske stat.

- Det er muligt, at danske organisationer vil blive udsat for forsøg på **manipulation af operationel teknologi (OT).** Truslen er især rettet mod dårligt beskyttet OT, idet pro-russiske hackere løbende forsøger at kompromittere og manipulere denne type OT i Vesten. Der er dog også en trussel fra statslige angreb mod OT.

- Det er muligt, at danske organisationer vil blive mål for mindre omfattende **wiper-angreb** som følge af Ruslands risikovillighed i forhold til anvende hybride virkemidler med destruktive effekter. Wiper-angreb sletter eller overskriver data på offerets systemer. Særligt Rusland har tidligere anvendt wiper-angreb i forbindelse med angreb mod Ukraine.

Sammenhæng mellem formåls-kategorier og angrebstyper

Ny struktur, samme analyse
I dette års trusselvurdering formidles cybertruslen på en ny måde, men den underliggende analyse er foretaget ud fra samme metodiske principper og med samme fokus. Figuren herunder Illustrerer sammenhængen mellem formålskategorierne og angrebstyperne.



Hvorfor nu?
Med den nye struktur for cybertrusselsvurderingen bevæger SAMSIK sig i en retning, som særligt organisationer indenfor kritisk infrastruktur har efterspurgt. Vi lægger større fokus på, *hvad* der kan ramme den enkelte organisation, og dernæst på *hvem*, der står bag angrebet. Den nye struktur medfører også mere fleksibilitet, såfremt nye angrebsmetoder og –teknologier vinder frem, da angrebstyperne løbende kan opdateres.

Det er vores håb, at det nye format vil gøre trusselsvurderingen endnu mere anvendelig for alle dem, der bruger den til at styrke cybersikkerheden i vores samfund.

Ransomware-angreb

Det er meget sandsynligt, at organisationer i Danmark vil blive udsat for forsøg på ransomware-angreb.

Truslen kommer primært fra kriminelle hackergrupper, som løbende retter ransomware-angreb bredt mod organisationer i både Danmark og i udlandet. Formålet er at kryptere it-systemer og data, der er kritisk for offerets drift, og derefter afkræve en løsesum for at gøre dem tilgængelige igen.

Hvad er ransomware-angreb?

Ransomware-angreb er cyberangreb, hvor hackere ved hjælp af malware (kaldet ransomware) krypterer it-systemer og data hos et offer og derved gør systemer og data utilgængelige. Ransomware-angreb kan variere i form og udførsel, men har det tilfælles, at data teoretisk set kan gendannes via dekryptering med den rette dekrypteringsnøgle. På den måde adskiller ransomware-angreb sig fra wiper-angreb, hvor data som udgangspunkt slettes permanent.

Ransomware-angreb udføres primært af kriminelle hackergrupper i forsøg på at kryptere deres ofres it-systemer og afkræve en løsesum. Ransomware-angreb kan dog potentielt også udføres af andre aktører.

Rekordmange ransomware-angreb rammer danske organisationer
SAMSIK vurderer, at antallet af ransomware-angreb mod virksomheder, myndigheder og andre organisationer i Danmark i 2024 var rekordhøjt. Således fortsatte antallet af ransomware-ofre i Danmark med at vokse fra 2023, der tidligere har været beskrevet som året med det højeste antal i Danmark.

Ransomware-angreb har ofte betydelige konsekvenser for organisationerne, som bliver ramt, uanset om der betales løsesummen eller ej. Eksempelvis i form af udgifter til hændelseshåndtering og genopretning af systemer, driftsforstyrrelser eller tab af tillid hos virksomheders kunder. I nogle tilfælde kan omkostningerne være så store, at organisationerne ikke kan overleve. Det gælder ikke mindst, hvis man som lille eller mellemstor organisation har begrænsede økonomiske ressourcer til rådighed.

De mest anvendte ransomware-varianter i Danmark

SAMSIK har kendskab til, at flere varianter af ransomware har været anvendte i forbindelse med ransomware-angreb i Danmark det seneste år. I de tilfælde, hvor ransomware-varianten er kendt, har de mest anvendte været:

Udover de omkostninger, som ransomware-angreb kan have for det enkelte offer, kan de også få alvorlige konsekvenser for samfundsvigtige funktioner. Det kunne f.eks. ske, hvis et angreb rammer it-systemer hos et energiselskab eller et teleselskab og påvirker samfundsvigtige ydelser. Det kunne også ske, hvis angreb rammer andre systemer og ydelser, som de kritiske it-systemer er afhængige af.

"Vi har været nødt til at gå helt manuelt til værks. De seneste dage har vi brugt papir og kuglepen for at få varerne ekspederet."

Jørn Johansen, adm. direktør hos Skanlog, til Finans efter et ransomware-angreb ramte virksomheden i 2024

Dansk hospital påvirket af ransomware-angreb mod leverandør

Det danske hostingselskab, IT-hotellet, var i sommeren 2024 udsat for et ransomware-angreb. Angrebet betød, at IT-hotellets systemer og data blev krypteret og dermed gjort utilgængelige. Da virksomheden ikke havde ressourcer til at få hackerne ud af systemerne og genoprette driften, måtte IT-hotellet til sidst lukke ned. Flere af virksomhedens kunder blev også påvirket af angrebet. Blandt kunderne var bl.a. Odense Universitetshospital. Hospitalet mistede adgangen til et centralt overvågningssystem, som de bl.a. anvendte til at justere varmen på hospitalet. Hændelsen havde ifølge hospitalet ikke konsekvenser for patienter, men understreger alligevel de tværgående afhængigheder, der karakteriserer et digitalt samfund, samt de potentielle konsekvenser, ransomware-angreb kan have.

Alle kan blive udsat for et ransomware-angreb

SAMSIK vurderer, at alle organisationer i Danmark, uanset størrelse og branche, risikerer at blive ofre for ransomware-angreb. Det omfatter også organisationer inden for samfundsvigtige sektorer.

Årsagen er, at de kriminelle hackere, som løbende udfører ransomware-angreb verden over, generelt er opportunistiske og drevet af muligheden for at opnå en økonomisk gevinst. Hackerne vil derfor typisk også gribe de muligheder, der byder sig, og rette ransomware-angreb mod en organisation, hvis de vurderer, at organisationen er sårbar for et angreb, samt at det er muligt at opnå en økonomisk gevinst.

Det er dog ofte små og mellemstore organisationer, som bliver ramt af ransomware-angreb. Det kan blandt andet skyldes, at små og mellemstore organisationer ikke altid har mulighed for at afsætte de samme ressourcer til cybersikkerhed som større organisationer. Derfor kan de også have et lavere beskyttelsesniveau end store organisationer og være mere sårbare over for potentielle angreb.

Det er dog ikke ensbetydende med, at større organisationer med stærke cyberforsvar ikke kan blive ramt. Eksempelvis går nogle kriminelle grupper målrettet efter at kompromittere organisationer med høje omsætninger, fordi de forventer, at de kan opnå et større udbytte ved angreb mod den type virksomheder. Samtidig har den stigende specialisering, professionalisering og effektivisering af det cyberkriminelle miljø også styrket de kriminelle hackeres samlede kapacitet til at gennemføre cyberangreb – herunder også mod velbeskyttede organisationer. Det ses bl.a. ved, at nogle kriminelle hackere selv afdækker eller køber sig til nul-dags-sårbarheder (også kaldet "zero-days-sårbarheder"), altså sårbarheder, der endnu ikke er offentligt kendte, med henblik på at udnytte dem i cyberangreb.

Sårbarheder anvendt i ransomware-angreb

Når ransomsware-grupper indleder et angreb, anvender de nogle gange tekniske sårbarheder. For at give organisationer et overblik over hvilke sårbarheder hackerne anvender, opdaterer det amerikanske agentur for cyber- og infrastruktursikkerhed (CISA) løbende deres katalog *Known Exploited Vulnerabilities* med kendte sårbarheder. Kataloget anvender det standardiserede system for kategorisering af sårbarheder, kaldet *Common Vulnerabilities and Exposures* (CVE), og indeholder bl.a. en beskrivelse af hver sårbarhed, årstallet for hvornår den er blevet opdaget samt en vurdering af, om sårbarheden har været anvendt i forbindelse med ransomware-angreb.

Siden januar 2024 er følgende sårbarheder, som har været anvendt i forbindelse med ransomware-angreb, blevet tilføjet til CISA's katalog:

CVE-2025-29824	CVE-2024-38094	CVE-2023-24955
CVE-2025-31161	CVE-2024-40711	CVE-2023-48788
CVE-2025-24472	CVE-2024-6670	CVE-2024-27198
CVE-2025-26633	CVE-2024-40766	CVE-2024-21338
CVE-2018-8639	CVE-2017-1000253	CVE-2024-1709
CVE-2024-55591	CVE-2024-23897	CVE-2020-3259
CVE-2023-48365	CVE-2024-37085	CVE-2023-22527
CVE-2024-55956	CVE-2024-26169	CVE-2023-35082
CVE-2024-50623	CVE-2024-4577	CVE-2023-29357
CVE-2024-51378	CVE-2024-24919	CVE-2023-29300
CVE-2024-11667	CVE-2024-30051	CVE-2023-38203
CVE-2023-28461	CVE-2024-3400	

Kilde: CISA, Known Exploited Vulnerabilities Catalog

Begrænset brug af ransomware-angreb blandt øvrige aktører

Selvom truslen fra ransomware-angreb primært kommer fra kriminelle hackere, kan nogle statslige og aktivistiske hackere også have kapacitet til samt intention om at udføre denne type angreb. Ransomware-angreb fra disse aktører udgør derfor også en begrænset trussel.

Eksempelvis har Microsoft i en offentlig rapport beskrevet, hvordan statslige russiske hackere i efteråret 2022 udførte et cyberangreb mod organisationer i transportsektoren i Ukraine og Polen. Ifølge Microsoft skulle angrebet ligne et kriminelt

ransomware-angreb i et forsøg på at skjule, at Rusland stod bag. Microsoft vurderede dog, i modsætning til kriminelle ransomware-angreb, at hackerne bag dette angreb ikke havde intention om at afpresse ofrene eller dekryptere offerets filer mod betaling. Dermed havde angrebene reelt en effekt, som mindede om et wiper-angreb.

Derudover er der også eksempler på cyberaktivistiske hackere, som enten har hævdet at have udført ransomware-angreb eller på anden vis udvist interesse for at udføre ransomware-angreb med aktivistiske formål.

SAMSIK vurderer dog, at omfanget af statslige og aktivistiske ransomware-angreb har været yderst begrænset sammenlignet med antallet af kriminelles ransomware-angreb. Blandt andet derfor vurderer SAMSIK, at det er mindre sandsynligt, at danske organisationer vil blive ramt af ransomware-angreb fra disse aktører.

Datatyveri

Det er meget sandsynligt, at danske organisationer bliver udsat for forsøg på datatyveri.

Forskellige aktører udøver forsøg på datatyveri med forskellige motiver for øje. Fremmede staters efterretningsbehov inden for særligt det udenrigs-, sikkerheds- og forsvarspolitiske område samt teknologiudvikling er fortsat en drivkraft bag meget datatyveri i form af cyberspionage. Samtidig udnytter cyberkriminelle i stor stil datatyveri til økonomisk berigelse.

Hvad er datatyveri?

SAMSIK definerer datatyveri som cyberangreb, hvor formålet er at indsamle data og information, som er sensitivt af karakter og ikke er frit tilgængeligt. Trusselsaktøren bruger denne data til at berige sig selv eller fremme egne økonomiske og politiske interesser, eller til at opnå viden om systemer, som kan anvendes til andre typer angreb.

Når fremmede stater udfører datatyveri, benytter SAMSIK udtrykket "cyberspionage".

Stater bedriver cyberspionage mod udenrigs-, sikkerheds- og forsvarspolitik
Det er meget sandsynligt, at fremmede stater, herunder særligt Rusland og Kina, forsøger at få adgang til data om dansk udenrigs-, sikkerheds- og forsvarspolitik.

Danmark er sandsynligvis et mål for cyberspionage på linje med andre vestlige lande qua Danmarks status som EU- og NATO-medlem. Det skyldes, at Rusland og Kina er bredt interesserede i Vestens udenrigs-, sikkerheds- og forsvarspolitik samt syn på internationale dagsordener. Truslen er ikke kun rettet mod myndigheder, men også virksomheder og andre organisationer som på forskellig vis understøtter dansk engagement og opgavevaretagelse inden for disse områder.

Der er også forhold, som bidrager til en mere specifik interesse for Danmark. Det er sandsynligt, at Danmarks geografiske placering i Østersøen bidrager til truslen fra cyberspionage fra Rusland. Samtidig er det meget sandsynligt, at Rusland og Kinas forsøg på cyberspionage mod Danmark er drevet af Kongerigets geografiske placering og rolle i Arktis.

Endelig vurderer SAMSIK, at dansk opgavevaretagelse i internationale fora kan drive interessen for danske positioner og sikkerhedspolitiske prioriteter. Den 12. maj 2025 overtog Kongeriget Danmark formandskabet i Arktisk Råd frem til 2027, fra den 1. juli 2025 og året ud varetager Danmark EU-formandskabet og den 1. januar 2025 tiltrådte Danmark som midlertidigt medlem af FN's Sikkerhedsråd indtil udgangen af 2026. Danmark er således i særlig høj grad involveret i og med til at præge dagsordenen på den internationale scene, hvilket kan skabe en yderligere interesse fra fremmede staters hackere.

Russiske hackere udgav sig for at være EU-parlamentsmedlem

Cybersikkerhedsvirksomheden Volexity har beskrevet, hvordan russiske hackere i starten af 2025 udførte en spear phishing-kampagne med det formål at kompromittere ofrenes Microsoft 365-konti.

Hackerne udgav sig i nogle tilfælde for at være medlem af Europa-Parlamentet. Under dette påskud kontaktede hackerne bestemte organisationer med henblik på at afholde et Teams-møde om eksempelvis EU's forhold til Trump-administrationen. Offeret modtog dernæst en falsk invitation med en af hackeren genereret verifikationskode. Hvis offeret indtastede denne kode og dernæst loggede ind, fik hackerne adgang til offerets Microsoft 365-miljø. Det skyldes, at verifikationskoden i virkeligheden var en anmodning om at tilknytte Microsoft 365-kontoen til en anden enhed.

Hackerne anvendte dermed en fremgangsmåde, mange vil kende fra processen ifm. tilknytning og login til en streamingtjeneste på et smart-TV.

Alle sektorer kan i princippet komme i fremmede staters søgelys. Det skyldes bl.a., at statslige hackere løbende forsøger at kompromittere et stort antal ofre på opportunistisk vis. Eksempelvis udnytter fremmede stater kendte sårbarheder i stor stil, bl.a. fordi mange ældre enheder ikke længere understøttes af sikkerhedsopdateringer, eller fordi disse opdateringer ikke implementeres i tide. Fremmede stater anvender i nogle tilfælde også nul-dags sårbarheder, der endnu ikke findes sikkerhedsopdateringer til. Er software bredt anvendt, kan udnyttelse af både kendte og ukendte sårbarheder i denne potentielt give adgang til mange mål på én gang.

Skift og strømninger i den geopolitiske udvikling og i staters efterretningsbehov kan også medføre, at særlige emner bliver interessante for fremmede stater. De seneste år har temaer som sundhed, energi, transport og handel eksempelvis været udsat for en øget trussel fra cyberspionage som følge af bl.a. Covid-19-pandemien og krigen i Ukraine.

Cyberspionage bruges til at opnå fordele i tilfælde af en konfliktsituation

Hackergrupper knyttet til Rusland forbereder sig løbende på at kunne udføre cyberangreb mod den kritiske infrastruktur i Danmark.[1] Gennem cyberspionage kan hackere få indsigt i organisationers systemer og netværk samt etablere bagdøre. På

[1] For mere information om truslen fra Rusland henviser SAMSIK til FE's "UDSYN".

den måde kan hackerne udføre yderligere cyberangreb mod disse mål med kort eller uden varsel i tilfælde af f.eks. en eskalerende krise eller krig.

Cyberspionage bruges også aktivt i forbindelse med krigsførelse. Eksempelvis er det meget sandsynligt, at hackere med tilknytning til russiske efterretningstjenester udfører denne form for cyberangreb mod militære mål og kritisk infrastruktur i Ukraine med det formål at understøtte fysiske angreb og dermed opnå en operationel fordel på slagmarken.

Cyberspionage understøtter økonomiske interesser
Det er meget sandsynligt, at fremmede stater også udfører cyberspionage med det formål at fremme egne økonomiske og teknologiske interesser inden for en række kritiske sektorer. Eksempelvis har Kina historisk set udøvet cyberspionage med henblik på teknologioverførsel.

SAMSIK vurderer, at dual use-teknologier er særligt interessante for fremmede stater. Dual use-teknologier kan bruges i både civile og militære sammenhænge og kan dermed understøtte et lands militære kapaciteter samt områder i civilsamfundet. Danske virksomheder og forskningsinstitutioner er i nogle tilfælde langt fremme inden for deres felt i internationalt perspektiv. Det er sandsynligt, at fremmede stater i flere tilfælde har forsøgt at ramme danske universiteter samt organisationer inden for bl.a. forsvarsteknologi de seneste år.

Handelspolitik er også et efterretningsbehov

Det amerikanske finansministerium, U.S. Department of the Treasury, blev ifølge amerikanske myndigheder kompromitteret af kinesiske hackere i december 2024. Ifølge flere åbne kilder fik hackerne adgang til en række arbejdsstationer i ministeriet samt tusindvis af ikke-klassificerede dokumenter. Hackerne gik bl.a. målrettet efter ministeriets Office of Foreign Assets Control (OFAC), som varetager amerikanske sanktioner inden for handel og økonomi.

Det amerikanske justitsministerium, U.S. Department of Justice (DOJ), anklagede i marts 2025 tolv navngivne kinesiske statsborgere for at stå bag angrebet. Hackerne har ifølge DOJ tråde til bl.a. hackergruppen APT27.

Cyberspionage kan bidrage til at opnå adgang til viden og teknologi, som kan omsættes til et lands egen fordel. På den korte bane kan denne viden eksempelvis afbøde konsekvenserne ved eksportrestriktioner, sanktioner og flaskehalse i forsyningskæder. På længere sigt kan illegitim videns- og teknologioverførsel bl.a. skævvride internationale markedsandele og landes konkurrenceevne. De seneste års teknologiske kapløb inden for bl.a. kvanteteknologi og kunstig intelligens understreger vigtigheden af udvikling af og kontrol med kritiske teknologier.

Cyberkriminelle stjæler data for økonomisk vinding
Det er meget sandsynligt, at danske organisationer også bliver udsat for forsøg på datatyveri fra cyberkriminelle. Cyberkriminelle forsøger at omsætte stjålne data og adgange til økonomisk udbytte på forskellige måder.

Ransomware er, som beskrevet i forrige kapitel, blevet en fast del af trusselsbilledet. Desværre sker det ofte, at de kriminelle ikke alene krypterer systemer, men lægger yderligere pres på offeret ved at stjæle data fra offeret. Ved disse angreb stjæler de cyberkriminelle ofte følsomme data såsom kontrakter, finansielle oplysninger, forretningshemmeligheder og personoplysninger, hvorefter de truer offeret med at lække disse til offentligheden, hvis ikke offeret betaler en løsesum. Ud over disse "dobbelte afpresningsangreb" er der også tilfælde, hvor de kriminelle alene stjæler data, og altså ikke krypterer systemer. Også danske organisationer har været udsat for afpresningsangreb i løbet af de seneste år.

De cyberkriminelles datatyveri kan også ske uden at ofrene opdager det. Eksempelvis specialiserer nogle cyberkriminelle sig i at kompromittere organisationers systemer for dernæst at sælge datasæt eller systemadgange såsom login-oplysninger videre på kriminelle markedspladser. Hackere, der sælger adgange videre, kaldes for Initial Access Brokers. Køb af login-oplysninger, såkaldte credentials, giver ikke bare hackere direkte systemadgang. Valide login-oplysninger kan dels spare hackerne for at bruge tid og ressourcer på selv at finde huller i systemet, dels kan udnyttelse af et legitimt login uden brug af malware eller brute force - det vil sige et angreb, hvor hackerne forsøger at kombinere forskellige tal, tegn og bogstaver, der kan indgå i et password - være sværere for en organisation at opdage.

Russiske cyberkriminelle afpresser adskillige ofre

I december 2024 angreb hackere fildelingsoftware fra virksomheden Cleo. Hackerne udnyttede en nul-dags-sårbarhed i softwaren, som Cleo ikke kendte til.

Den russiske cyberkriminelle gruppe, CLOP, har sidenhen været ude at tage ansvaret for angrebet. Gruppen har på sit Dedicated Leak Site (DLS) hævdet at have stjålet data fra adskillige ofre og truet med at offentliggøre dette. Biludlejningsvirksomheden Hertz bekræftede i april 2025, at personfølsomme oplysninger på nogle af deres britiske kunder var blevet kompromitteret i angrebet.

CLOP har gjort det til et kendetegn at angribe digitale knudepunkter såsom fildelingssoftware. Hackergruppen har tidligere stået bag lignende angreb, hvor danske virksomheder også er blevet kompromitteret.

Statslige hackere udnytter datatyveri til økonomisk berigelse
Der er også eksempler på, at stater udnytter datatyveri til økonomisk berigelse. Nordkorea er et særligt tilfælde i den forbindelse. Det er meget sandsynligt, at den nordkoreanske stat mobiliserer store dele af sine cyberkapaciteter til systematisk at udføre datatyveri for at generere penge til regimet.

SAMSIK vurderer, at truslen fra nordkoreansk datatyveri primært gælder for danske borgere og virksomheder, der beskæftiger sig med kryptovaluta og for visse organisationer, som ansætter medarbejdere på distancen.

Milliarder til Kim Jong Un

Kryptovaluta anvendes i store dele af den internationale cyberkriminalitet. Kryptovalutas decentrale natur, mulighed for anonymitet samt områdets begrænsede regulering og tilsyn gør dette digitale aktiv attraktivt for både statslige og ikke-statslige hackere med økonomiske motiver. Digitale røverier af kryptobørser- og wallets er ligeledes blevet en lukrativ indtægtskilde for det nordkoreanske regime.

I februar 2025 lykkedes det eksempelvis nordkoreanske hackere at stjæle kryptovaluta af typen Ethereum for en samlet værdi af USD 1,46 milliarder fra kryptobørsen ByBit. Ved at manipulere ByBits transaktionsprotokol samt den digitale signaturproces, der autoriserer en transaktion, kunne hackerne overføre kryptovaluta fra ByBits såkaldte ”wallet” til hackernes egen wallet. Derfra flyttede hackerne midlerne videre til tusinder af forskellige wallets på andre platforme for at konvertere beløbet til andre typer kryptovaluta.

Cyberaktivister kan også anvende hack-og-læk angreb

Cyberaktivister verden over påstår med jævne mellemrum at have stjålet data i form af såkaldte ”hack-og-læk”-angreb. Truslen fra datatyveri begået med aktivisme for øje har dog indtil nu været meget begrænset i en dansk kontekst.

Digital svindel

Det er meget sandsynligt, at danske organisationer og borgere vil blive udsat for forsøg på digital svindel. Danskere bliver løbende udsat for svindel på digitale platforme, og det er meget sandsynligt, at omfanget af svindlen vil stige i de kommende år.

Truslen adskiller sig fra de øvrige angrebstyper, idet den ofte rammer den inviduelle borger. Det foregår dog i et sådant omfang, at det potentielt kan medvirke til at ødelægge tilliden til digitale løsninger. Den form for angreb er derfor både et problem for de enkelte ofre såvel som et samfundsproblem.

Hvad er digital svindel?

Digital svindel er en samlebetegnelse for bedrageri, hvor kriminelle med henblik på at opnå en økonomisk gevinst via digitale kanaler eller systemer forsøger at manipulere ofre til at afgive penge, oplysninger eller adgangskoder. Svindlen kan både foregå ved at vildlede offeret til frivilligt at gennemføre transaktioner i god tro, eller ved at kriminelle franarrer offeret oplysninger, som de kriminelle kan misbruge til at gennemføre ubrettigede transaktioner.

For den enkelte borger opleves svindlen ofte i forbindelse med online handel, hvor ca. hver tredje dansker har oplevet at blive udsat for svindel. Andre svindelsformer er dog også udbredte, såsom investeringssvindel samt forskellige typer kontaktbedrageri, hvor de kriminelle bagmænd opbygger en relation til deres ofre og narrer dem til at overføre penge eller udlevere personlige oplysninger.

For virksomheder er det især direktørsvindel (CEO-fraud), der fylder i trusselsbilledet. Ved denne type svindel udgiver de kriminelle sig for at være fra virksomhedens ledelse og overtaler derved medarbejdere til at overføre større beløb – ofte ved at sende mails, der fremstår som om, de kommer fra direktøren. Andre svindelformer omfatter bl.a. også fakturasvindel, hvor kriminelle fremsender falske regninger for varer eller ydelser, de aldrig har købt, i håb om at disse bliver betalt.

Store omkostninger for både den enkelte og samfundet

De samlede konsekvenser af digital svindel kan være vanskelige at opgøre. Ifølge Nationalbanken udgjorde den samlede svindel og misbrug med digitale betalingsløsninger i Danmark ca. 627 mio. kr. i 2023, mens Finans Danmark estimerer det samlede tab til 464 mio. kroner for samme år.

Selvom de fleste ofre for digital svindel mister relativt små beløb, er tabene for nogle betydelige og kan i særlige tilfælde overstige millioner af kroner. For eksempel lykkedes det i december 2023 kriminelle hackere at svindle Guldborgsund Kommune for mere end 1,3 mio. kr. ved først at kompromittere en medarbejders mail-konto og dernæst, ved hjælp af denne mail-konto, at sende fakturaer til betaling hos kommunens økonomiafdeling.

Udover de økonomiske tab kan det at blive udsat for digital svindel også have alvorlige sociale og psykologiske konsekvenser, som kan mindske ofrenes selvværd samt tilliden til andre mennesker og samfundets institutioner, herunder banker og digitale løsninger. Over tid kan udbredt digital svindel også svække tiltroen til myndighedernes handlekraft samt samfundets evne til at beskytte borgerne.

Afsløring af kriminelt svindelnetværk i Norden

Bag digital svindel står kriminelle bagmænd, ofte organiseret i netværk med internationale forbindelser, som høster udbyttet. Kriminaliteten udføres i særlig grad af bander og grupper, der opererer via callcentre eller online-forbindelser.

I november 2024 blev en række danske statsborgere anholdt i Finland i en sag om kontaktbedrageri mod ældre i Norden. To af dem har forbindelse til den forbudte bande Loyal to Familia (LTF).

De anholdte er blandt andet sigtet for at forsøge at svindle 9.000 danskere via falske opkald eller beskeder, der fremstod som at komme fra MitID, Nets, politiet eller banker. Denne metode kaldes også spoofing. Det er uvist, hvor mange penge, det lykkedes dem at svindle for, men vurderingen er, at det er flere millioner kroner.

Afsløringen bygger på over 100.000 hackede filer, som TV 2 og TjekDet har verificeret gennem et sikkerhedsfirma, og materialet er overleveret til politiet.

Nogle gange udgiver de kriminelle sig for at være banken eller politiet og lokker borgeren til at overføre penge til en særlig sikkerhedskonto med den falske begrundelse, at den forurettedes konto er i fare. Derefter fragmenteres beløbene i mange små overførsler eller sendes til udlandet.

Pengene fra svindlerne kanaliseres typisk hurtigt videre via et stort net af såkaldte "muldyr", som er personer, der modtager ofrenes overførsler på deres konti og videresender dem. Der er også eksempler på, at svindlerne går direkte ind og overfører ofrenes penge til kryptovalutabørser under deres kontrol for siden at veksle pengene til digitale valutaer, hvor hvidvask er sværere at spore.

DDoS-angreb

Det er meget sandsynligt, at danske organisationer vil blive udsat for forsøg på DDoS-angreb.

Det skyldes, at hackergrupper, som støtter Rusland, løbende forsøger at gøre danske hjemmesider utilgængelige ved hjælp af DDoS-angreb. Det er sandsynligt, at nogle af disse pro-russiske hackergrupper har forbindelse til den russiske stat. Selvom nogle af de pro-russiske hackere derfor ikke entydigt kan betragtes som cyberaktivister, som handler uafhængigt af stater, kategoriserer SAMSIK fortsat deres aktiviteter som "cyberaktivisme", fordi de bruger en angrebsmodus, der ligner cyberaktivisme.

Hvad er et DDoS-angreb?

DDoS står for Destributed Denial of Service og er et overbelastningsangreb.

Hackere udnytter kompromitterede enheder til at generere usædvanligt store mængder datatrafik mod en hjemmeside (webserver) eller et netværk, så hjemmesiden eller netværket overbelastes.

Imens angrebet står på, er hjemmesiden eller netværket utilgængelig for legitim trafik.

DDoS-angreb har potentielt en synligt forstyrrende effekt, som aktørerne bag f.eks. kan bruge til at chikanere og skabe opmærksomhed omkring et specifikt budskab. Samtidigt er DDoS en relativt simpel angrebsform, og udøveren behøver derfor ikke at udvikle komplicerede tekniske færdigheder for at gennemføre dem. "DDoS-for-hire"-og "botnets-for-hire"-tjenester øger desuden tilgængeligheden af DDoS-kapaciten for flere aktører.

Fra ét minut til flere dages nedetid

DDoS-angreb gør potentielt en hjemmeside utilgængelig for legitim trafik i kortere eller længere perioder, men angrebet er ikke ødelæggende for de ramte systemer. Oftest kan angrebet udbedres inden for kort tid og uden større konsekvenser.

Der er dog store forskelle i angribernes tekniske kapaciteter, og de angrebsmetoder, de bruger.[2] Selvom DDoS-angreb oftest skaber ingen eller meget kort nedetid, har der inden for de seneste år været eksempler på mere velkoordinerede og udfordrende DDoS-angreb, der har skabt væsentligt længere nedetid på ofrenes systemer.

Det skete f.eks., da kraftige DDoS-angreb ramte finanssektoren i og uden for Danmark i efteråret sidste år. I Danmark måtte Nordea mitigere DDoS-angreb, hvor banken ikke i sig selv var målet, men som Nordea anså som et angreb på civilsamfundet med det formål at skabe uro og usikkerhed. Nordea lykkedes med at mitigere 90 pct. af

[2] Se SAMSIK "Temaartikel: DDoS-angreb mod hjemmesider"

angrebene, der blandt andet periodisk påvirkede kundernes adgang til netbank i 25 dage. DDoS-angreb kan altså i nogle tilfælde påvirke netværkets drift samt koste tid og ressourcer.

DDoS-angreb mod hjemmesider under kommunal- og regionalvalget

En række danske hjemmesider blev i forbindelse med kommunal- og regionalvalget den 18. november 2025 udsat for DDoS-angreb fra pro-russiske hackere. Angrebene blev bl.a. rettet mod hjemmesider ved kommuner og politiske partier og betød, at nogle af siderne i perioder var utilgængelige. Angrebene havde dog ikke betydning for gennemførslen af valget.

SAMSIK udgav sammen med Politiets Efterretningstjeneste og Forsvarets Efterretningstjene forud for valget en fælles vurdering af truslen mod kommunal- og regionsrådsvalget. I denne fremgik det blandt andet, at det var sandsynligt, at pro-russiske hackere ville rette DDoS-angreb mod danske hjemmesider. Blandt andet fordi pro-russiske hackere tidligere har udført denne type angreb mod Danmark og andre lande i Europa i forbindelse med valg.

DDoS-angreb mod danske hjemmesider er en del af normalbilledet

Den høje trussel fra DDoS-angreb mod organisationer i Danmark er en del af normalbilledet. Det skyldes som nævnt pro-russiske hackere, som i konteksten af krigen i Ukraine løbende retter DDoS-angreb mod danske hjemmesider.

De pro-russiske grupper retter typisk deres DDoS-angreb mod hjemmesider, der tilhører myndigheder og virksomheder i kritisk infrastruktur, og ofte bliver de samme mål forsøgt ramt gentagne gange. Det drejer sig især om organisationer i finans- og transportsektoren, men også virksomheder i energisektoren og telesektoren er blevet udsat for forsøg på DDoS-angreb i 2024 og 2025. Selvom der er mønstre i angrebsmodus, rammer DDoS-angreb også bredere og mere tilfældigt, både i forhold til tid og ofre. Derfor er enhver organisation med internetvendte systemer og hjemmesider et potentielt mål for DDoS-angreb.

Truslen fra de pro-russiske grupper skal både ses i kontekst af Danmarks rolle som bidragsyder af militær støtte til Ukraine og som medlemsland af EU og NATO. De pro-russiske hackere italesætter typisk deres angreb mod danske hjemmesider som en straf mod Danmark som land, og ikke mod den enkelte virksomhed. Nogle grupper udnytter gerne konkrete lokale begivenheder, såsom et valg eller en politisk udmelding, til at rette DDoS-angreb mod hjemmesider. Eksempelvis er hjemmesider tilhørende myndigheder og virksomheder i en række europæiske lande blevet ramt af DDoS-angreb i forbindelse med både lokale og nationale valg i det seneste år.

Foruden den pro-russiske dagsorden kan andre storpolitiske konflikter også drive cyberaktivistiske DDoS-angreb mod Danmark. Eksempelvis rettede en cyberaktivistisk gruppe, hvis politiske motivationer angiveligt er at støtte op om Hamas, i marts 2025 DDoS-angreb mod danske myndigheders hjemmesider.
Grupperne overlapper ofte i motiver, ligesom de samarbejder og støtter hinandens angrebs- og kommunikationskampagner på sociale medier. Det er muligt at

samarbejdet påvirker gruppernes kapaciteter, selvom det primære formål sandsynligvis er at få cybertruslen samt opbakningen til gruppernes politiske formål til at fremstå større.

Grupperne overdriver for at skabe opmærksomhed

Hackeres kommunikation omkring deres aktivistiske angreb er ofte misvisende og overdreven. Dette betyder, at der i mange tilfælde er usikkerhed om, hvorvidt et angreb har fundet sted, samt hvilken effekt angrebene har haft.

SAMSIK vurderer, at hackernes kommunikation om både falske og reelle angreb har til hensigt at skabe offentlig opmærksomhed omkring deres dagsorden samt at skabe utryghed og usikkerhed i befolkningen i de lande, hvis hjemmesider er mål for DDoS-angrebene. Disse grupper, ikke mindst de pro-russiske grupper, søger således omtale i vestlige medier og deler typisk vestlige, herunder danske, mediers artikler om gruppernes egne angreb som en del af deres kommunikation på sociale medier.

Selvom SAMSIK er bekendt med gruppernes navne, bliver de derfor ikke nævnt i publikationer, medmindre det er afgørende for at give et retvisende trusselsbillede.

DDOS-angreb kan bruges til mange formål

DDoS-angreb bruges også af hackere med andre formål. Eksempelvis bruger cyberkriminelle grupper til tider DDoS-angreb for at tilføje pres ved et ransomware-angreb.

DDoS-angreb kan også bruges til at aflede offerets opmærksomhed fra angribernes egentlige hensigter, såsom at foretage datatyveri i offerets systemer.

Omfattende DDoS-angreb mod centrale systemer vil desuden kunne afbryde eller forstyrre samfundsvigtige funktioner i kortere eller længere tid. Den type angreb vil derved potentielt kunne påvirke befolkningen og beslutningstagere.

Manipulation af operationel teknologi (OT)

Det er muligt, at organisationer i Danmark vil blive udsat for cyberangreb, der har til formål at kompromittere og manipulere operationel teknologi (OT).

Truslen fra manipulation af OT er især rettet mod udstyr og systemer, som har et lavt beskyttelsesniveau og kan identificeres og tilgås direkte via internettet. Det skyldes, at denne type OT løbende forsøges identificeret, kompromitteret og manipuleret af pro-russiske hackere, hvoraf nogle sandsynligvis har forbindelse til den russiske stat. Angrebene har foreløbigt haft en simpel karakter, men kan alligevel få omfattende konsekvenser, hvis de f.eks. rammer OT i kritisk infrastruktur.

Fremmede stater har både kapaciteten til simple og mere avancerede angreb mod OT. Det er dog mindre sandsynligt, at fremmede stater, herunder Rusland, aktuelt har intention om at udføre angreb mod OT med alvorlige, samfundsmæssige konsekvenser.

Hvad er manipulation af OT?

Ved manipulation af OT forsøger hackere at få adgang til operationelle teknologier (OT) med henblik på at manipulere systemet og de processer, som systemet styrer. Operationelle teknologier dækker over alle former for systemer anvendt til monitorering, styring og indsamling af data i fysiske miljøer og kan bl.a. være systemer, der bruges til at justere vandtrykket hos et vandværk, eller systemer der anvendes til at monitorere og styre produktion i industrien.

Truslen er særligt rettet mod dårligt beskyttet OT

SAMSIK vurderer, at det især er OT, der har et lavt beskyttelsesniveau, og som kan tilgås direkte via internettet, som er udsat for en trussel. Det skyldes, at der sandsynligvis har været en stigning i pro-russiske hackeres forsøg på at kompromittere og manipulere denne type OT-systemer i Vesten de seneste par år.

Angrebene foregår typisk ved, at hackerne scanner internettet for OT med eksponerede fjernadgange. Herefter forsøger de at tiltvinge sig adgang til systemer, som de vurderer er interessante, f.eks. ved at afprøve standardpasswords. Såfremt det lykkes, vil hackerne derefter forsøge at manipulere systemerne og dokumentere det ved at dele et skærmbillede eller en video på sociale medier, ofte med en overdreven eller misvisende beskrivelse af angrebet.

Det er sandsynligt, at måludpegningen er opportunistisk i den forstand, at hackerne primært går efter OT systemer, der er beskyttet i så ringe grad, at hackerne kan identificere og let få adgang til dem. Pro-russiske hackere har f.eks. hævdet at have kompromitteret og manipuleret alt fra klimanlæg i private hjem til OT ved vandværker og biogasanlæg. Hackerne anser således de fleste OT-systemer som legitime mål, og

udviser også en relativt høj risikovillighed ift. at angribe OT, der potentielt udgør kritisk infrastruktur.
Eksempelvis har norske myndigheder anklaget pro-russiske hackere for at stå bag et cyberangreb på en dæmning i Bremanger i Norge i april 2025. Hackerne tog kontrol over dæmningens styresystem, hvorefter de åbnede for ventilerne og sendte store vandmængder ud af anlægget i flere timer.

En pro-russisk aktivistgruppe offentliggjorde dette opslag på X efter et angreb mod et dansk vandværk. Opslaget indeholder bl.a. en video, hvor hackerne klikker rundt i systemerne. SAMSIK har sløret gruppens navn, fordi formålet med angrebet bl.a. er at skabe opmærksomhed omkring gruppens aktiviteter. Navne på danske organisationer er ligeledes udeladt.

Pro-russiske hackere manipulerede OT ved dansk vandværk

Et mindre danske vandværk blev i slutningen af 2024 ramt af et cyberangreb fra pro-russiske hackere. Ved angrebet kompromitterede hackerne vandværkets OT-systemer og manipulerede dernæst vandtrykket. Angrebet medførte bl.a., at 450 husstande kortvarigt ikke havde vand på grund af lavt vandtryk. Vandværket har efter angrebet udtalt, at man kunne tilgå deres OT fra internettet, hvis man kendte eller gættede koden ”1234”.

Hackerne ved ikke altid, hvilke systemer de angriber, eller hvilke organisationer, der anvender systemerne. De er imidlertid ofte opmærksomme på, i hvilke lande de udvælger OT som mål. For eksempel begrunder pro-russiske hackere ofte deres angreb mod OT med, at det pågældende land har doneret militærstøtte til Ukraine. Et angreb kan også ske ud fra et ønske om at støtte op om en anden gruppes angreb

mod samme land. Disse dynamikker ses bl.a. også i forbindelse med de pro-russiske DDoS-angreb.

Manipulation af OT kan potentielt få omfattende konsekvenser
SAMSIK vurderer, at de pro-russiske cyberangreb, der foreløbigt har været rettet mod OT i Vesten, har haft begrænsede konsekvenser for samfundet. Således har angrebene ramt OT-systemer i mindre organisationer eller steder, hvor de har haft en begrænset effekt.

Det kan dog ikke udelukkes, at selv simple angreb mod OT kan få mere omfattende konsekvenser for både ofre såvel som for samfundet. Eksempelvis ville det potentielt kunne få alvorlige konsekvenser for samfundet, såfremt hackere får mulighed for at angribe OT, der understøtter samfundsvigtige funktioner.

Pro-russiske hackere ønsker at skabe opmærksomhed
Truslen fra manipulation af OT skal ses i sammenhæng med de DDoS-angreb, som pro-russiske hackere løbende har rettet mod hjemmesider i Danmark og resten af Vesten de seneste år. For eksempel er det sandsynligt, at de pro-russiske angreb mod OT, ligesom DDoS-angrebene, generelt har til formål at skabe utryghed og usikkerhed i de lande, som bliver ramt. Desuden har angrebene sandsynligvis til formål at straffe vestlige lande og signalere opbakning til Rusland.

Det er sandsynligt, at de pro-russiske hackere i stigende grad gør brug af cyberangreb mod OT, fordi DDoS-angreb ikke længere genererer den opmærksomhed og utryghed, som de ønsker.

Statslige russiske hackere udgør en begrænset trussel mod OT
Det er meget sandsynligt, at flere fremmede stater også har mere avancerede kapacitet til at kompromittere og manipulere OT, end de pro-russiske hackere foreløbigt har vist. For eksempel har Ruslands statslige hackere tidligere illustreret deres evne til at udføre mere avancerede cyberangreb, bl.a mod kritiske OT-systemer i Ukraines energisektor.

Truslen fra denne type angreb mod Danmark er dog for nuværende begrænset. Det skyldes, at det er mindre sandsynligt, at Rusland aktuelt vil rette cyberangreb mod OT, som har til formål at skabe alvorlige og omfattende konsekvenser for samfundsvigtige funktioner.[3] I stedet vil et eventuelt angreb fra Ruslands statslige hackere mod OT i Danmark sandsynligvis medføre mindre omfattende effekter og have til formål at påvirke befolkningen og beslutningstagere. Altså angreb, hvis ønskede effekt kan sammenlignes med de pro-russiske hackeres.

Det er dog sandsynligt, at der foregår russisk cyberaktivitet mod kritisk infrastruktur i Danmark, der har til formål at muliggøre mere alvorlige cyberangreb, f.eks. i forbindelse med en evt. fremtidig skærpet konflikt. Dette kan også omfatte evnen til at udføre mere alvorlige cyberangreb mod OT-systemer.

[3] For mere information om truslen fra Rusland henviser SAMSIK til FE's "UDSYN".

Wiper-angreb

Det er muligt, at danske organisationer vil blive udsat for forsøg på wiper-angreb.

Forsvarets Efterretningstjeneste vurderer, at Rusland er villig til at anvende hybride virkemidler med destruktive effekter i europæiske NATO-lande. SAMSIK vurderer, at denne risikovillighed også omfatter cyberangreb med destruktive effekter, herunder visse former for wiper-angreb.

Hvad er wiper-angreb?

I et wiper-angreb slettes eller overskrives data, så det bliver utilgængeligt eller er umuligt at genskabe. Wiper-angreb kan være en alvorlig trussel mod den ramte organisation og, afhængigt af målet, potentielt også det omkringliggende samfund. Ved at destruere kritisk information og systemer kan angriberne besværliggøre eller stoppe en organisations arbejde og derved potentielt afbryde samfundsvigtige funktioner.

Wiper-angreb kan have flere formål end blot at slette systemer og data. Stater kan således benytte wiper-angreb både for konkrete, taktiske formål som at forhindre en modstander i at få adgang til et givent system, men også for at skabe usikkerhed og dermed påvirke befolkninger og beslutningstagere. Kriminelle kan ligeledes benytte wiper-angreb for at slette deres spor i jagten på profit.

Truslen kommer især fra Rusland

Det er sandsynligt, at truslen fra wiper-angreb særligt kommer fra Rusland, og at eventuelle wiper-angreb vil være med begrænsede konsekvenser og have påvirkning som formål. Ligesom det er tilfældet med angreb, der manipulerer med OT, vurderer SAMSIK aktuelt, at de mest avancerede kapaciteter vil blive gemt til en evt. fremtidig skærpet konflikt.[4]

Russiske statslige hackergrupper har i årevis haft kapacitet til at udføre wiper-angreb, og har flere gange udført sådanne angreb, særligt mod mål i Ukraine. Selvom det altså er muligt, at danske organisationer bliver udsat for forsøg på wiper-angreb, er det mindre sandsynligt, at Rusland i den nuværende sikkerhedspolitiske situation vil gennemføre wiper-angreb, hvor hensigten er at skabe alvorlige og omfattende konsekvenser for samfundsvigtige funktioner.

SAMSIK vurderer alligevel, at wiper-angreb med omfattende konsekvenser er en type cyberangreb, som samfundet skal forholde sig til. Det er sandsynligt, at Rusland løbende gennemfører forberedende aktivitet for at kunne udføre mere ødelæggende angreb, herunder wiper-angreb. Disse angreb vil i givet fald kunne iværksættes, såfremt man fra russisk side vurderer, at konflikten er eskaleret tilstrækkeligt til, at det er en passende handling. En del af denne forberedelse kan bl.a. være at udføre cyberspionage mod kritisk infrastruktur for at kortlægge systemer. Truslen fra mere

[4] For mere information om truslen fra Rusland henviser SAMSIK til FE's "UDSYN".

alvorlige wiper-angreb kan derfor stige med kort eller uden varsel, såfremt Ruslands intention ændrer sig.

Andre stater benytter også wiper-angreb

Ifølge åbne kilder har Albanien ad flere omgange været mål for iranske hackeres wiper-angreb. I juni 2025 blev flere af hovedstaden Tiranas offentlige digitale systemer ramt af cyberangreb. Hackergruppen Homeland Justice, som tidligere er blevet attribueret til Irans Revolutionsgarde, påstod bl.a. at have wipet flere servere.

Det amerikanske agentur for cyber- og infrastruktursikkerhed (CISA) og FBI har tidligere beskrevet, hvordan iranske hackere gennem 14 måneder havde adgang til den albanske regerings netværk, hvor hackerne bl.a. udførte datatyveri, inden de i juli 2022 iværksatte destruktive cyberangreb ved brug af wiper-malware.

NATO-landet Albanien har siden 2013 huset tusindvis af iranske dissidenter med tilknytning til organisationen Mojahedin-e-Khalq (MEK). Iran betegner MEK som en terrororganisation.

Erfaringen fra Ukraine

Wiper-angreb kan bl.a. udføres i forsøget på at opnå taktiske militære fordele i en konkret situation, hvilket sandsynligvis har været formålet med flere russiske wiper-angreb mod ukrainske mål. Et eksempel er angrebet, der er blevet omtalt som "AcidRain". Angrebet fandt sted på dagen for Ruslands invasion af Ukraine i februar 2022 og var sandsynligvis målrettet de ukrainske militære styrkers satellitkommunikation. Acid Rain-angrebet slettede opsætningen på tusindvis af satellitmodemmer fra den amerikanske virksomhed Viasat og påvirkede også organisationer udenfor Ukraine.

Wiper-angreb målrettet Ukraine har både fundet sted i tiden op til invasionen samt efter krigens udbrud. Det er meget sandsynligt, at Ruslands wiper-angreb har til hensigt at destabilisere det ukrainske samfund og landets forsvarsevne. Wiper-angreb indgår altså også som en del af Ruslands aktive krigsførelse mod Ukraine.

Wiper-angreb mod Ukraines største teleudbyder

Ukraines største teleudbyder, Kyivstar, blev den 12. december 2023 ramt af et omfattende, destruktivt wiper-angreb. Angrebet efterlod en stor del af selskabets 24 millioner kunder uden adgang til mobilnettet i flere dage og påvirkede bl.a. luftalarmsystemer for missiler og hæveautomater. Ukraines sikkerheds- og efterretningstjeneste har meldt ud, at Ruslands militære efterretningstjeneste stod bag angrebet, nærmere bestemt hackergruppen Sandworm.

Ikke-statslige aktører benytter sig også af wiper-angreb
Wiper-angreb er dog ikke alene forbeholdt statslige aktører. Særligt kriminelle, men også aktivister, udfører wiper-angreb med henblik på at opnå et økonomisk afkast eller omtale.

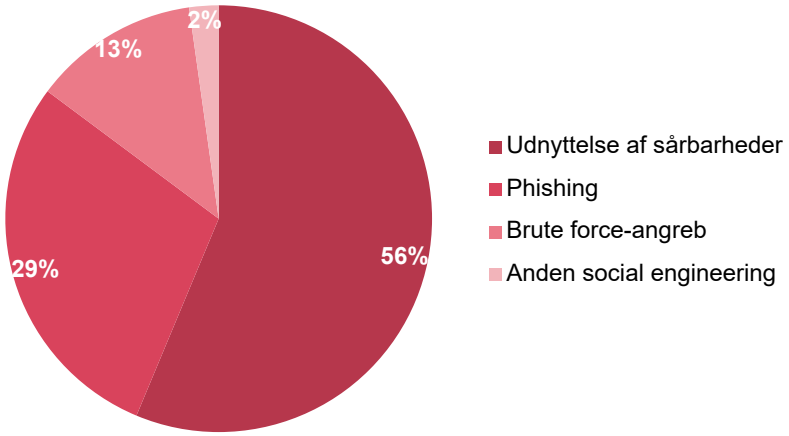
Cyberkriminelle aktører benytter sig i nogle tilfælde af wiper-angreb, eksempelvis i forbindelse med et ransomware-angreb. Ved at slette logs og backups søger hackerne bl.a. at besværliggøre detektion og attribuering af angrebet. Sletning af backups kan samtidig besværliggøre genopretning af data, hvilket kan lægge yderligere pres på offeret. Ved denne type hændelser indgår wiper-angreb som et delmiddel til at opnå et mål om økonomisk vinding.

Hackernes angrebsteknikker

Cybertruslen udvikler sig løbende, og hackere finder hele tiden på nye måder at udføre cyberangreb på. Ikke desto mindre er der nogle teknikker, som hackere ofte anvender til at få indledende fodfæste i en organisations netværk. I dette afsnit beskriver SAMSIK derfor de angrebsteknikker, som er særligt relevante for organisationerne at beskytte sig mod.

Angrebsteknikker fordelt på cyberhændelser

Forsvarets Efterretningstjeneste (FE) monitorerer løbende cyberangreb mod danske og grønlandske organisationer. I de tilfælde, at cyberangreb registreres, noterer FE så vidt muligt også, hvilke angrebsteknikker hackerne benyttede sig af i den indledende fase af angrebene. I nedenstående diagram ses andelen af FE's registrede cyberangreb fordelt på angrebsteknikker.



Kilde: Forsvarets Efterretningstjeneste

Note: Grafikken er udarbejdet med afsæt i data fra FE's situationscenter fra de seneste to år. Bemærk, at fordelingen i grafikken af tekniske årsager kan afvige fra det reelle aktivitetsbillede.

Phishing-beskeder

Phishing har længe været en populær angrebsteknik blandt hackere og er det fortsat. Det skyldes blandt andet, at phishing både er billigt, skalerbart, relativt nemt at udføre og samtidig er effektivt. Det er derfor meget sandsynligt, at hackere forsat vil anvende phishing mod danske organisationer i de kommende år.

Ved phishing forsøger hackerne ved hjælp af mails, sms'er eller andre kommunikationsformer at narre en modtager til at foretage en specifik handling. Denne handling kan f.eks. være at få modtageren til at åbne en vedhæftet fil, klikke på et link eller scanne en QR-kode og derved aktivere malware, der giver hackerne uretmæssig adgang til offerets systemer. Det kunne også være at videregive fortrolige oplysninger eller betale en falsk faktura.

I modsætning til mange andre angrebsteknikker er formålet med phishing ikke alene at udnytte tekniske sårbarheder, men i lige så høj grad menneskelig natur. Af denne grund anvendes der i phishing ofte en række psykologiske greb, som skal gøre modtagerne mere tilbøjelige til at udføre den ønskede handling. Disse greb kaldes også *social engineering,* og kan f.eks. komme til udtryk i form af, at hackere i phishing-beskeder tilskriver en handling en hastende karakter. På den måde vil nogle ofre ubevidst komme til at fokusere på handlingens udførsel, snarere end hvorfor handlingen skal udføres.

Phishing kan især være overbevisende for modtagerne, når det udføres af statslige eller dygtige kriminelle hackere. Det skyldes, at disse hackere har omfattende cyberkapaciteter, som de bl.a. anvender til at tilpasse deres phishing-forsøg til deres ofre. På den måde fremstår phishing-beskederne mere troværdige over for offeret og har en større chance for at lykkes.

Denne form for målrettet phishing kaldes også spear phishing og kan f.eks. være en phishing-mail med et bestemt emne, som hackere sender til medarbejdere i specifikke organisationer, fordi de forventer, at de vil være tilbøjelige til at reagere på mails med netop dette indhold. SAMSIK har kendskab til eksempler, hvor organisationer i Danmark har været udsat for denne type spear phishing.

Det er dog ikke kun spear phishing-forsøg, som rammer danske organisationer. Et meget højt antal phishing-kampagner med mere generisk indhold rammer ligeledes danske borgere og organisationer hver dag, og desværre lykkes det også i nogle tilfælde at snyde modtagerne. Det gælder f.eks. i forbindelse med digital svindel, som fylder meget i trusselsbilledet, og som tre ud af fire danskere har været udsat for.

SAMSIK, Danske Regioner og KL udgav den 6. juni 2025 rapporten Danskernes Informationssikkerhed 2024. Rapporten indeholder bl.a. statistik på en række områder inden for digital kriminalitet i Danmark, heriblandt omfanget af phishing.

Rapporten kan læses på SAMSIK's hjemmeside: www.samsik.dk.

En af de former for phishing, som især har været i stigning de seneste år, er phishing via telefonen. SAMSIK har i rapporten *Danskernes informationssikkerhed 2024* beskrevet, at der både har været en stigning i antallet af phishing-forsøg via sms'er (smishing) og via opkald (vishing). Således steg andelen af danskere, der har været udsat for smishing-forsøg, ifølge rapporten fra 28 pct. i 2022 til 51 pct. i 2024, mens andelen for vishing-forsøg steg fra 17 pct. i 2022 til 29 pct. i 2024. På samme måde kunne cybersikkerhedsvirksomheden Crowdstrike i deres *Global Threat Report 2025* berette, at de det seneste år havde set en stigning i vishing på 442 pct.

En anden tendens, som har haft betydning for truslen fra phishing, og som sandsynligvis også vil fortsætte med at påvirke truslen de kommende år, er udviklingen af kunstig intelligens. Hackere kan bl.a. anvende kunstig intelligens til at forbedre og målrette deres phishing-beskeder, så de bliver sværere for ofrene at identificere. Samtidig kan hackerne også spare en stor mængde tid ved f.eks. at få sprogmodeller til at udfærdige phishing-beskeder for dem. Det er derfor også muligt, at phishing både vil blive mere sofistikeret, mere udbredt og mere succesfuldt i fremtiden.

Udnyttelsen af sårbarheder

En anden angrebsteknik, som hackere ofte anvender, er udnyttelsen af sårbarheder. Ved disse angreb udnytter hackerne en eller flere tekniske fejl i software eller hardware til at omgå sikkerhedsforanstaltningerne på en enhed og få uretmæssig adgang til enheden. Herefter kan hackerne typisk foretage en række handlinger på enheden, og fortsætte deres angreb mod enhedens netværk.

Sårbarheder varierer generelt meget i karakter og kritikalitet. Det skyldes, at den software og hardware, som kan være sårbar, har meget forskellige design og funktioner. Det er derfor heller ikke alle sårbarheder, som er lige kritiske. Fælles for mange sårbarheder er dog, at de ofte skyldes en fejl i den måde software eller hardware er designet eller anvendt på, samt at fejlen typisk muliggør misbrug af en eksisterende funktionalitet.

Der findes i dag et stort antal kendte sårbarheder i den software og hardware, som anvendes på globalt plan. Disse forsøger både statslige og ikke-statslige hackere i høj grad at udnytte til at få indledende adgang til deres ofres systemer og netværk. En af årsagerne er sandsynligvis, at brugen af kendte sårbarheder kræver forholdsvist få ressourcer for hackerne at anvende, ligesom de – på trods af at være offentligt kendte – stadig ofte er effektive.

Sidstnævnte skyldes blandt andet, at mange organisationer ikke får mitigeret sårbarhederne i den mellemliggende tid fra offentliggørelse, til at sårbarheden udnyttes. I nogle tilfælde er der f.eks. tale om minutter, fra en sårbarhed offentliggøres, til at angrebsforsøg registreres. I andre tilfælde er der blot tale om, at organisationer ikke prioriterer at få patchet sårbare systemer, hvorfor de således står eksponeret i lang tid.

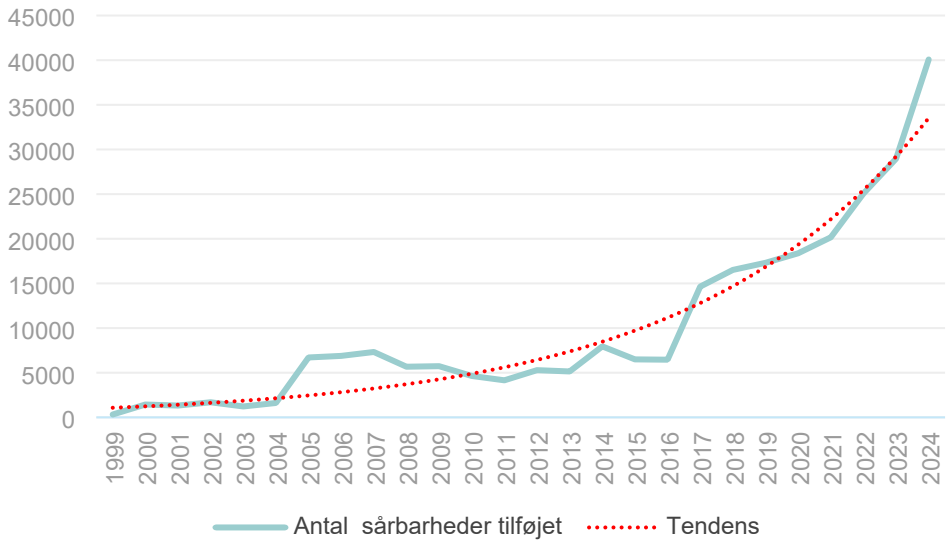
Derudover er det også en generel problemstilling, at mange sårbare enheder har nået deres "end of life", hvilket betyder, at de ikke ikke længere understøttes med sikkerhedsopdateringer fra producentens side. Brugere af det sårbare udstyr vil derfor i nogle tilfælde ikke kunne patche deres systemer for at mitigere sårbarheden, men vil

i stedet være nødt til at udskifte deres enheder eller finde alternative mitigeringsløsninger. Dette kan i nogle tilfælde være omkostningsfuldt.
Udover de kendte sårbarheder anvender nogle hackere også sårbarheder, som endnu ikke er offentligt kendte. Disse sårbarheder kaldes også nul-dags-sårbarheder (på engelsk *zero days*) og er generelt meget effektive, fordi sårbarheden kun kendes af hackerne, og dermed ikke er kendt af hverken systemejere eller producenten. Hackerne vil derfor ofte have mulighed for at kompromittere et stort antal ofre med denne type sårbarheder, før sårbarheden opdages.

Nul-dags-sårbarheder anvendes primært af stater og velorganiserede kriminelle hackere. Det skyldes, at det især er dem, der har kapaciteterne og ressourcerne til selv at identificere nul-dags-sårbarheder eller alternativt at købe sig til dem på digitale undergrundsmarkeder. Selvom både statslige og ikke-statslige hackere dermed har kapaciteten til at identificere og anvende nul-dags-sårbarheder, er det dog ikke ensbetydende med, at det er disse, som oftest anvendes. I stedet vurderer SAMSIK, at disse hackere i høj grad også anvender de kendte sårbarheder.

Rekordhøjt antal nye sårbarheder i 2024

Den amerikanske nonprofitorganisation, MITRE, vedligeholder en offentligt tilgængelig, fællesskabsbaseret database over sårbarheder (CVE'er). Databasen opdateres løbende i takt med, at nye sårbarheder de opdages. I 2024 var antallet af nye sårbarheder tilføjet til databasen det højeste nogensinde med i alt 40.077 sårbarheder. Til sammenligning var antallet i 2023, der ligeledes var et rekordår, i alt 28.961. Det svarer til en stigning på ca. 72 pct. Det stigende antal sårbarheder skyldes blandt andet, at der hele tiden udvikles nye enheder verden over, som kan indeholde sårbarheder.



Udnyttelsen af svage og kendte passwords
Hackere misbruger i høj grad også legitime loginoplysninger til at kompromittere deres ofres enheder, netværk og konti. En af de angrebsteknikker, som især anvendes i den forbindelse, er brute force-angreb.

Ved brute force-angreb forsøger hackere at få adgang til enheder og konti ved at gætte sig til det rette brugernavn og password. Dette sker typisk ved hjælp af computerprogrammer, der gør hackerne i stand til systematisk at afprøve et stort antal brugernavne og passwords. Teknikken kan anvendes mod mange forskellige systemer og konti og bliver bl.a. anvendt mod mailkonti, virtual private network-løsninger samt systemer og enheder, der kan tilgås via fjernadgange som Secure Shell (SSH) og Remote Desktop Protocol (RDP).

Brute force-angreb varierer i karakter og kan have forskellige grader af kompleksitet. I sin simpleste form kan hackerne eksempelvis forsøge at gætte loginoplysningerne ved systematisk at afprøve forskellige kombinationer af tilfældige tal, bogstaver og tegn. Denne fremgangsmåde kan dog tage lang tid og kræve store ressourcer for hackerne, hvis loginoplysningerne er tilpas lange. Derfor anvender hackere ofte også andre former for brute force-angreb.

Én af disse er password spraying, hvor hackerne forsøger at få adgang til en stor mængde konti ved skiftevis at afprøve forskellige kombinationer af kendte brugernavne (såsom alle mailadresser i en organisation) og hyppigt anvendte passwords (såsom ”12345678”). En anden er credential stuffing, hvor hackerne afprøver loginoplysninger, som de har fundet i tidligere datalæk.

I tillæg til brute force-angreb forsøger nogle hackere også at få adgang til systemer og netværk ved købe sig til legitime loginoplysninger på digitale undergrundsmarkeder. Det kan f.eks. være legitime loginoplysninger fra de mange Initial Access Brokers, der er kriminelle hackere, som har specialiseret sig i at skabe adgang til systemer for derefter at sælge adgangen videre til interesserede købere.

Mange angreb, der udnytter svage og kendte passwords, kan effektivt imødegåes ved implementering af ordentlig fler-faktor-godkendelse.

Angreb via leverandører
Leverandører er generelt attraktive mål for hackere. Det skyldes blandt andet, at hackerne kan udnytte leverandører til at få adgang til enheder og netværk hos deres kunder. Denne angrebsteknik kaldes også supply chain-angreb og foregår typisk ved, at hackerne først kompromitterer en leverandør og dernæst udnytter den tillid og de adgange, som eksisterer mellem kunden og leverandøren, til at kompromittere leverandørens kunder.

En form for supply chain-angreb, der har været flere eksempler på de seneste år, er software supply chain-angreb. Ved denne angrebsteknik forsøger hackerne først at kompromittere leverandøren af et software-program. Lykkes de med dette, vil hackerne dernæst forsøge at udnytte adgangen til at indlejre malware i leverandørens legitime softwareopdateringer. Når leverandøren senere skubber opdateringen ud som

planlagt, bliver malwaren også installeret på kundernes systemer, hvilket potentielt også giver hackerne adgang til deres netværk.

SAMSIK vurderer, at supply chain-angreb er en mindre udbredt angrebsteknik end phishing, brute force-angreb og udnyttelsen af sårbarheder. Ikke desto mindre er der løbende eksempler på supply chain-angreb mod organisationer verden over, og når det sker, har det ofte omfattende konsekvenser. Det gælder særligt, når større internationale software-leverandører kompromitteres, da de typisk har et meget højt antal kunder. Supply chain-angreb mod sådanne leverandører risikerer derfor at få et meget stort antal kompromitterede ofre.

Software-leverandør ramt af supply chain-angreb

Den verdensomspændende ip-telefoni-udbyder, 3CX, blev i foråret 2023 ramt af et omfattende supply chain-angreb. Ifølge cybersikkerhedsvirksomheden, Mandiant, som undersøgte angrebet, havde nordkoreanske hackere indledningsvist kompromitteret en leverandør til 3CX og derved fået adgang til 3CX's netværk. Hackerne havde derefter udnyttet denne adgang til at indarbejde en bagdør i 3CX's kommende opdatering til deres ip-telefoni software. Handlingen betød, at hackerne potentielt fik adgang til kundernes enheder, da 3CX udrullede opdateringen af softwaren. Ifølge 3CX var der på daværende tidspunkt mere end 350.000 organisationer, heriblandt danske organisationer, som var kunder hos 3CX.

Insidere

En anden måde hackere kan få adgang til systemer og netværk er gennem insidere. Man skelner ofte mellem bevidste og ubevidste insidere, hvor sidstnævnte er personer, som ubevidst har givet hackere adgang til organisationens systemer, f.eks. ved at have åbnet en ondsindet fil i en phishing-mail. Bevidste insidere er derimod personer, som bevidst understøtter hackere i deres forsøg på at kompromittere organisationers netværk.

Organisationer i Danmark har de seneste år også været udsat for kompromitteringer begået af bevidste insidere. SAMSIK har ikke kendskab til det præcise omfang af brugen af insidere i Danmark. Det skyldes, at der sandsynligvis er mørketal på området, som SAMSIK ikke kender til.

Løbende hændelser i udlandet vidner dog om, at brugen af insidere er en angrebsteknik, som hackerne anvender. De digitale undergrundsmarkeder forsøger også at appellere til bevidste insidere. Her tilbydes medarbejdere en anseelig mængde penge for at hjælpe hackerne med at stjæle oplysninger fra deres organisation eller understøtte cyberangreb mod deres netværk.

Nordkoreanske hackere søgte job i virksomhed

Flere medier og cybersikkerhedsvirksomheder har i 2024 og 2025 beskrevet, hvordan nordkoreanske hackere har forsøgt at kompromittere virksomheder i bl.a. USA og Storbritannien ved at søge ledige stillinger i de pågældende virksomheder.

Ifølge én af disse virksomheder, Kraken, der beskæftiger sig med kryptovaluta – et kendt mål for nordkoreanske hackere – havde ansøgerne bl.a. fremvist falske CV'er og falsk ID, ligesom de havde tilgået den virtuelle jobsamtale via fjernskrivebord og VPN.

Ifølge en anden unavngiven virksomhed havde angrebet mod deres virksomhed været succesfuldt, idet hackeren efter ansættelsen havde downloadet sensitive data og krævet en løsesum for ikke at lække denne data.

Råd og vejledning

Styrelsen for Samfundssikkerhed tilbyder en bred vifte af rådgivning, bl.a. til organisationer i Danmarks kritiske infrastruktur. Vi udarbejder også vejledninger, som alle organisationer kan bruge til at styrke den digitale sikkerhed. Vejledningerne kan tilgås styrelsens hjemmeside – www.samsik.dk – og omfatter bl.a. følgende:

Cyberforsvar der virker
SAMSIK's grundlæggende vejledning om cyberforsvar og håndtering af cyberangreb. Hvis vejledningens trin implementeres, vil det være muligt at forhindre en markant del af de cyberangreb, som danske organisationer løbende er udsat for, samt være i stand til effektivt at håndtere de angreb, der lykkes.

Beskyt din organisation mod phishing-angreb
Giver en række konkrete anbefalinger til ledelsen, der kan bidrage til organisationens arbejde med at beskytte sig mod phishing-angreb.

Passwordsikkerhed
Vejledningen præsenterer en række anbefalinger og tips til, hvordan sikkerheden i og omkring passwords højnes og derved øge organisationens sikkerhedsniveau.

Beskyt mod DDoS-angreb
Vejledningen giver med en række forholdsregler, som en organisation kan tage for at beskytte sig mod DDoS-angreb.

Cybersikkerhed i leverandørforhold
Indeholder gode råd til, hvordan man kan oprette og bibeholde et godt og sikkert samarbejde mellem kunden og leverandøren af it-driften, gennem hele samarbejdsperioden. Fra valg af leverandør til ophør af samarbejdet.

Reducér risikoen for ransomware
Vejledningen giver en række anbefalinger, som organisationer kan følge for at reducere sandsynligheden for at blive ramt af ransomware-angreb. Vejledningen giver desuden råd til, hvordan et ransomware-angreb kan håndteres, når skaden er sket.

Logning – en del af et godt cyberforsvar
Logning er afgørende for at opdage og håndtere et cyberangreb. Vejledningen giver gode råd til, hvor i netværket man skal logge og hvad man bør logge. Den bygger på erfaringer fra bl.a. it-sikkerhedsfirmaer i forbindelse med bistand ved hændelseshåndtering.

Sådan imødegås digital svindel
Digital svindel er en alvorlig trussel mod både borgere, virksomheder og myndigheder. På sikkerdigital.dk kan du læse råd om sikre adgangskoder, hvordan man undgår svindel som CEO-fraud og fakturasvindel. Her findes også tjeklister, kampagner, guides og værktøjer målrettet forskellige målgrupper, som gør det nemt at komme i gang med en mere sikker digital adfærd.

Trusselsniveauer

Styrelsen for Samfundssikkerhed anvender i sine trusselsvurderinger følgende trusselsniveauer:

INGEN	Der er ingen tegn på en trussel. Der er ingen aktør, der både har kapacitet til og intention om angreb/skadelig aktivitet.
LAV	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men enten er kapaciteten eller intentionen eller begge dele begrænset.
MIDDEL	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men der er ikke indikationer på specifik planlægning af angreb/skadelig aktivitet.
HØJ	En eller flere aktører har kapacitet til og foretager specifik planlægning af angreb/skadelig aktivitet, eller har allerede gennemført eller forsøgt angreb/skadelig aktivitet.
MEGET HØJ	Der er enten oplysninger om, at en eller flere aktører iværksætter angreb/skadelig aktivitet, herunder oplysninger om tid og mål, *eller* en eller flere aktører iværksætter kontinuerligt angreb/skadelig aktivitet.

Et givent trusselsniveau er udtryk for SAMSIKs vurdering af aktørers intention, kapacitet og aktivitet på baggrund af de tilgængelige oplysninger. Niveauerne svarer til Forsvarets Efterretningstjenestes (FE) trussels- og sandsynlighedsniveauer.

SAMSIK bruger denne skala for sandsynligheder i analyser:

En sandsynlighedsgrad er udtryk for et skøn, ikke en beregnet statistisk sandsynlighed.
"SAMSIK vurderer" svarer til "Sandsynligt", medmindre en anden sandsynlighed er angivet.