NRK Trusselvurdering

2023

Klassifisering: Åpen

En alvorlig situasjon

Foto: Eskil Wie Furunes/NRK

For andre gang kan NRK presentere en egen trusselvurdering. Det er krig i Europa og media spiller en nøkkelrolle gjennom å bringe analyser og rapportere fra krigshandlingene. Kampen om sannheten var et uttrykk NRK benyttet i fjorårets trusselvurdering, og det kan også brukes i år. Desinformasjon og påvirkning er en del av trusselbildet hvor media har et stort ansvar gjennom å utøve kildekritikk og ha et kritisk blikk på alt som publiseres.

Trusselnivået er høyt og møter NRK på mange områder. Våre journalister rapporterer fra krigen og vi driver undersøkende journalistikk for å løfte frem saker som ikke kommer frem i det daglige nyhetsbildet. NRK håndterer hver dag ulike former for digitale hendelser og vi erfarer at den digitale trusselen i perioder har økt i intensitet. Det er vanskelig å vite om små og store hendelser kan være knyttet til statlige aktører, eller om det er andre aktører som ønsker å utnytte ustabiliteten rundt krigen i Ukraina, til å påføre skade eller hente ut informasjon.

Det vi har sett er at medier utsettes for digitale angrep og at det finnes grupper på sosiale medier som avtaler hva som er neste mål for angrep på vestlig digital infrastruktur. NRK har som andre virksomheter blitt utsatt for DDoS-angrep og vi forventer at det vil skje igjen.

Vi har bare sett starten på bruk av kunstig intelligens (KI). Slik teknologi kan utfordre journalistikken og vil kunne være et verktøy for trusselaktører som ønsker å spre falske nyheter. Videoer med kjente fjes fra nyhetene kan spres på sosiale medier med riktig stemme, men med falskt budskap. Dette er en ny hverdag for NRK, som vi må forholde oss til.

Spørsmålet vi må stille oss i NRK er om vi er godt nok forberedt på det økte trusselnivået. Er vi bevisste nok i det daglige og bruker vi ressursene riktig? Det er stor etterspørsel etter digitale kompetanse i det norske samfunnet og ulike virksomheter konkurrerer om de beste hodene. Kanskje må vi dele på erfaringer, samarbeide mer på tvers og dele på ressurser med andre?

For NRK er arbeidet med å utarbeide trusselvurderingen, og ta den i bruk i organisasjonen, en metode for å styrke sikkerheten og gjøre alle medarbeidere mer bevisste på ansvaret alle har. Trusselnivå fastsettes på en skala med fem nivåer. Det øker modenheten i vår organisasjon og bidrar til at vi blir mer bevisste på hvilke trusler vi står overfor. Vi håper trusselvurderingen kan være til glede for andre også.

Vibeke Fürst Haugen
Kringkastingssjef

Øyvind Vasaasen
Sikkerhetssjef

Innholdsfortegnelse

Aktuelt

NRKs korrespondenter i Ukraina, Kari Skeie og Gunnar Bratthammer.

Foto: Andrii Ovid

Trusselen sett fra nord

av Nina Einem, regionredaktør, Region Nord

Illustrasjon: U.S Departement of State

En bil stopper utenfor NRK-huset i Tromsø en onsdag i februar. Ut trår en mann som raskt begynner å ta bilder av bygget, før han forsvinner like fort som han dukka opp. Hvem er han? Og hvorfor tar han bilder av bygget vårt?

For et år siden hadde vi neppe lagt merke til han. Nå blir han fotografert av en ansatt, som leverer bildet videre til sin leder. Vi publiserer jevnlig saker om spionasje, mistenkelig aktivitet og følgene krigen i Ukraina har for oss som lever tett på Russland. Har vår egen virksomhet blitt gjenstand for økt oppmerksomhet? Sannsynligvis er svaret på det; ja.

Kart og terreng

Kart kan fortelle mye om Nord–Norge. Når vi ser oss rundt er vårt perspektiv et helt annet enn det andre i Norge har. Vi har supermaktene tett på oss.

Kartet forteller også at Kautokeino ligger sør for Tromsø og Vardø lengre øst enn Istanbul. Vi bruker færre timer på å kjøre til både Helsinki, Stockholm og St. Petersburg enn til Oslo. Murmansk er vår nærmeste storby. Velger du å se verden fra nord, utfordres din virkelighetsoppfatning. Flere burde prøve det.

Vår beliggenhet definerer også vår tilnærming til innholdsproduksjon i NRKs nordligste region. Vi skal lage innhold bare vi kan, fordi bare vi er der vi er. Fra det utgangspunktet har serier som Klar til strid, 113, Puckers, Kald krig og Kortbaneliv kommet– for å nevne noen.

Den russiske bjørnen

Det er en ny tid nå. Vi som jobbet her på 1990 – og 2000 tallet reiste ganske fritt over russergrensen. Vi har etablert kontakt med kollegaer i Murmansk. Deltatt på mediefestivaler og fagdebatter, og fått gode bekjente, sågar venner, over grensen. Vi har selvsagt alltid visst at den russiske bjørnen holdt et øye med oss. Vi finnes nok alle i russiske arkiver. Selv har jeg opplevd påfallende interesse for min familie – og dagligliv og NRKs organisasjon, fra administrativt ansatte i media styrt av russiske myndigheter. Det var en del av spillet, og vi kunne kjenne det igjen. Da så vi på det som en rest fra den kalde krigen. Nå har den russiske bjørnen våknet av dvalen.

Det vi så på som kuriosa har blitt en reell fare som vi må snakke med våre ansatte om. De fleste av dem har aldri opplevd en tilspissa sikkerhetssituasjon, eller den kalde vinden som igjen siver inn over grenseområdene i nord. Er de i stand til å kjenne igjen forsøk på påvirkning? Kan de la seg overtale til å gi fra seg opplysninger om seg selv og NRK som kan misbrukes, eller brukes for å presse dem?

Hva om...?

NRK har et særskilt ansvar som er beskrevet allerede i første linje i forskriften NRK under beredskap og krig. *Norsk rikskringkasting plikter å treffe særskilte beredskapstiltak for å sikre at informasjon fra regjeringen når befolkningen under beredskap og i krig.* Vi er ikke i en beredskapssituasjon i Nord-Norge nå. Men ordene leses med fornyet alvor.

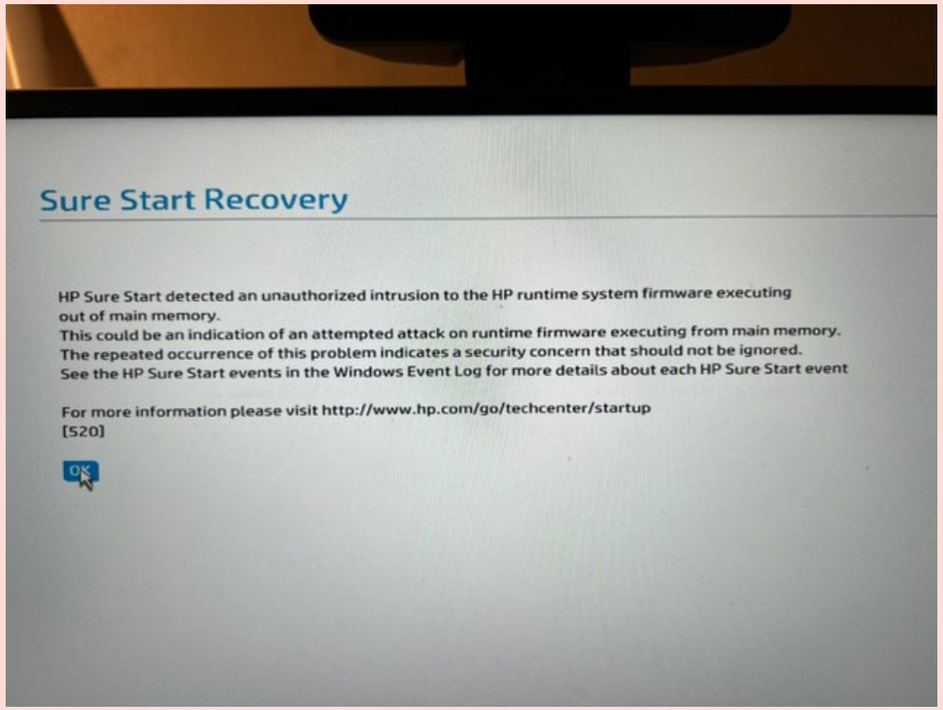
Europa har blitt destabilisert. Samtidig rapporterer vi om mystiske kabelbrudd utenfor kysten i nord, lager saker om ulovlig droneflyving og økte forstyrrelser på mobilnettet øst i Finnmark. Kan vi oppfylle forpliktelsene våre i et samfunn som har gjort seg avhengig av strøm, mobil – og dataløsninger? Har vi gode og stødige nok alternativ dersom viktig digital infrastruktur svikter? Vi har nok å sjekke, dobbeltsjekke og sikre. Jeg har aldri i min tid som leder brukt så mye tid på spørsmålet «Men hva om...?».

Likevel føles det meningsfylt. Fordi NRKs beredskapsoppdrag, og vår rolle for befolkningen i en krisesituasjon, er betydningsfull og viktig.

PS: Mannen med kamera var elektriker.

God sikkerhet er et felles ansvar

av Bjørn Mathias Helseth, IT-sikkerhetsgruppe



Skjermbildet viser eksempel på et varsel nylig meldt inn av en NRK-medarbeider til Operativ IT-sikkerhet. Varselet førte til en grundig undersøkelse over flere dager, og er et typisk tilfelle som ønskes rapportert.

Visste du at også du er en sikkerhetsmedarbeider i NRK?

Hver dag opplever vi at sikkerheten til NRK blir satt på prøve. Enten du er på jobb ute i felt, i produksjon eller jobber fra kontoret, er du en viktig brikke i sikkerhetsarbeidet vårt.

Vi i operativ IT-sikkerhet håndtere en rekke hendelser hver dag. Én enkelt IT-sikkerhetshendelse kan i seg selv binde opp flere av oss i flere dager. Ofte skjer ikke en hendelse alene, så det kan virkelig «koke» når det står på. Da jeg startet i NRK i fjor høst forventet jeg en spennende jobb, men jeg forventet ikke en så stor pågang av saker hele tiden, som jeg har opplevd frem til nå.

Hver gang NRK blir utsatt for et tjenestenektangrep (DDoS) er det en oppgave å holde NRK tilgjengelig for publikum gjennom angrepet. Når en tjeneste går ned, gjelder det å få den raskest mulig opp igjen. Får en medarbeider ett sikkerhetsvarsel på maskinen, må vi sjekke hva det betyr både for den berørte og for NRK. Vi sjekker om e-poster er ekte eller inneholder skadevare, og vi følger opp alarmer fra egne og eksterne sikkerhets-og varslingssystemer. Når NSM varsler om at en alarm har gått på VDI-sensoren de har i NRK, må vi kanskje kalle inn ekstra mannskap for å få oversikt over hva alarmen betyr for NRK. I forbindelse med store produksjoner som Nobelsendingen, valg-sendinger, VM i Qatar eller OL i Beijing, setter vi inn ekstra IT-sikkerhetstiltak, som f.eks. ekstra overvåking.

I jula oppdaget vi at det på en underside av nrk.no var lagt ut lenker til reklame. Siden ble raskt stengt og lenke etterhvert fjernet fra forsida, men vi måtte sjekke hva som hadde skjedd og om flere undersider var blitt angrepet. I slike situasjoner abonnerer vi heldigvis på noen tjenester som hjelper oss, men det er likevel mye manuelt arbeid. Det betyr ett ekstremt press på oss som jobber her. Det er en spennende og viktig jobb å holde NRK oppe, men vi klarer ikke det alene. Trusselaktører benytter seg av alle mulige digitale inngangsporter, og inngangen via en medarbeider er ofte den enkleste. Vi er avhengige av at alle medarbeidere gjør sitt for å sikre NRK.

Som sikkerhetsmedarbeider er det viktig at du har bevissthet, god sikkerhetshygiene og en god rapporteringskultur.

- Vær varsom på hva du trykker på av lenker og vedlegg.
- Rapporter mistenkelige varsler (se Portalen)
- Ha ett eget unikt passord for innlogging til NRK
- Bruk nrk.no e-post kun i jobbsammenheng
- Oppdater PC og mobil jevnlig
- Installer og benytt kun godkjent programvare
- Vær oppmerksom på hvilke mobilapper du installerer og hvilke tilganger du gir
- Husk å låse skjermen når du forlater plassen

God sikkerhet og en sunn sikkerhetskultur er summen av alt vi i fellesskap gjør, eller ikke gjør, hver eneste dag!

NRK på flyttefot

av Øyvind Vasaasen, sikkerhetssjef

NRK bygger nytt i Trondheim.
Foto: Morten Andersen/NRK

NRK skal de neste årene flytte inn i nye lokaler flere steder i landet. Samtidig skal også hele produksjonskjeden moderniseres. Det byr på mange store utfordringer knyttet til sikkerhet, men også mulighet til å styrke sikkerheten i NRK.

Det største prosjektet er etableringen av et nytt hovedkontor på Normannsløkka på Ensjø i Oslo. Før det skal NRKs virksomhet i Trondheim flytte fra Tyholt og inn i et nytt mediehus i Holtermannsvei på Elgseter, som skal stå ferdig i 2025. Arbeidet på tomta er i gang og detaljplanleggingen foregår parallelt. Tomten på Normannsløkka skal først reguleres og det er ikke satt en konkret dato for flytting.

NRK på Marienlyst består av sju bygg og er utviklet gjennom 70 år, fra ren radiovirksomhet, til TV-produksjon og nye medier. Behovene har endret seg underveis og sentrale funksjoner og infrastruktur er plassert der hvor det har vært hensiktsmessig uten at sikkerhetsperspektivet har trengt å være en del av vurderingen. Dermed er produksjons- og publikumsaktiviteter over tid blandet sammen med kritiske rom og kritisk infrastruktur og spredd over flere bygninger. Ved flytting kan dette samles i større grad .

NRK benytter Norsk Standard 5834:2016 som veileder for sikkerhetsplanleggingen både i Trondheim og i Oslo. Det betyr at planleggingen starter tidlig, slik at byggene blir utformet og får en funksjonalitet som gir mest mulig naturlig sikkerhet. Sikkerhetsarbeidet i forbindelse med nytt hovedkontor startet i 2019 ved å kartlegge hvilke verdier som skal sikres. Det er viktig at sikkerhet kommer inn i prosjekter fra starten av, hvis ikke kan det påføre prosjektene økte kostnader og forsinkelser.

Begge flytteprosjektene skjer i en tid hvor mye teknologi flyttes ut av virksomheten og inn i eksterne datasentre. Tjenester som NRK tidligere håndterte selv, leveres nå av eksterne leverandører. Kravene til god og profesjonell styring av leverandører vokser og NRK må styrke egen kompetanse til å håndtere dette.

I sin trusselvurdering for 2023 peker Nasjonal sikkerhetsmyndighet, NSM, på at fremmede aktører investerer og kjøper seg inn i norske virksomheter og eiendom for å få sensitiv informasjon og skaffe seg strategisk viktig teknologi. I 2022 ble nær 50 slik saker avdekket. Det betyr at det både er en prosjektrisiko knyttet til selve planleggingen, til oppføringen av NRKs nye kontorer i Oslo og Trondheim , og til driften av den nye digitale produksjonskjeden som etableres parallelt med dette. Eksterne datasentre kan bli kjøpt opp og i så fall kan NRK risikere å miste kontroll over egne data som er lagret. Behovet for redusere risiko og sikre oppetid gjennom en kontinuitetsplan krever at flere datasentre benyttes. NSM anbefaler fire.

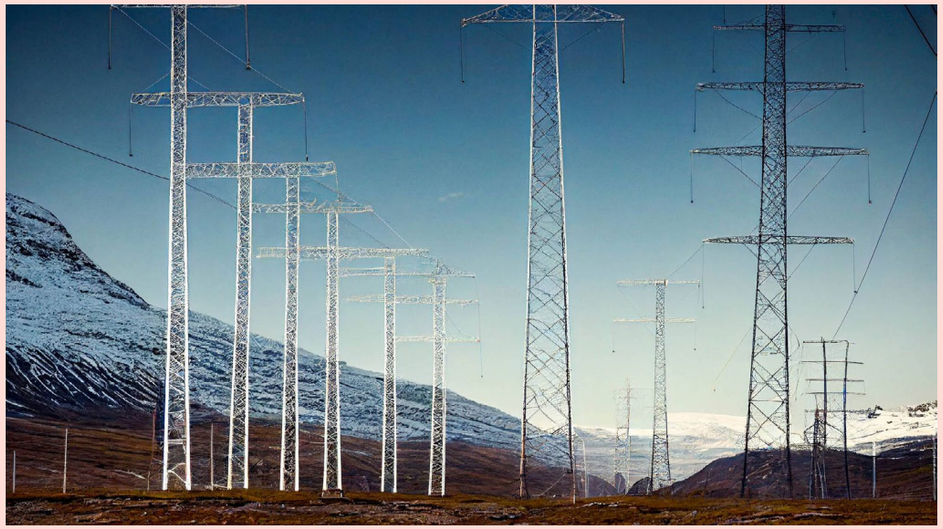
NRKs nye kontorer skal gjennom god planlegging bli et flott sted å jobbe, et hyggelig sted for publikum og samarbeidspartnere å komme til, samtidig som sikkerhet skal ivaretas på en god måte.

Når kunstig intelligens utfordrer sannheten

av ChatGPT-4 etter innspill fra Lars Eirik Berg,
fung. CISO/Informasjonssikkerhetsleder

Denne artikkelen er i sin helhet generert av OpenAIs ChatGPT-4, som er et chatteverktøy drevet av maskinlæring og elementer av KI.

Maskinlæring er en metode hvor datamaskiner læres opp til å utføre spesifikke oppgaver ved å analysere store datamengder og konstruere modeller av informasjonen. KI refererer til evnen til et dataprogram å utføre oppgaver som normalt krever menneskelig intelligens, som å løse problemer eller lære av erfaringer. Maskinlæring er derfor en teknikk som brukes for å forsøke å oppnå KI, men vi har i dag ennå ikke oppnådd et nivå av KI som kan regnes som likt eller bedre enn menneskelig intelligens og kreativitet.



Dette KI-genererte bildet laget av tjenesten Midjourney, ble brukt av NRK som et ekte bilde i oktober 2022.

I en verden der kunstig intelligens (KI) blir stadig mer avansert, står journalistikken overfor nye utfordringer. KI-teknologi kan nå produsere falske nyheter, manipulerte bilder og realistiske deepfakes som kan skape forvirring og undergrave tilliten til media. Journalister må navigere i dette landskapet for å opprettholde sannheten og forsvare den frie pressen.

Deepfakes, eller hyperrealistiske digitale manipulasjoner av foto, video og lyd, er et av de mest bekymringsfulle eksemplene på hvordan KI kan utfordre sannheten. Med enkle verktøy kan man nå lage falske videoer som ser ut som om de inneholder ekte uttalelser fra kjente personer. Dette kan ha alvorlige konsekvenser for politikk, næringsliv og samfunnet generelt.

Men KI kan også hjelpe journalister med å avsløre falske nyheter og manipulerte medier. Avanserte analyseverktøy kan identifisere tegn på manipulering og hjelpe til med å bekrefte kilders pålitelighet. KI kan også bistå med å overvåke store mengder data for å oppdage mønstre og avsløre historier som ellers kunne gått ubemerket.

For å beskytte sannheten og opprettholde tilliten til journalistikken, må bransjen selv ta ansvar og utvikle etiske retningslinjer for bruk av KI i journalistikk. Dette inkluderer å være transparent om hvordan KI brukes, og å sikre at teknologien ikke brukes til å forvrenge sannheten eller manipulere publikum.

Det er også viktig å samarbeide med teknologiselskaper, forskere og regulatorer for å skape en felles forståelse av utfordringene og mulighetene som KI bringer. Dette vil bidra til å sikre at teknologien utvikles på en ansvarlig måte og brukes til å styrke journalistikkens integritet snarere enn å undergrave den.

Til syvende og sist er det avgjørende at journalister fortsetter å utdanne seg selv og publikum om KI-teknologi og dens potensielle innvirkning på sannheten. I en verden der KI kan utfordre sannheten på stadig mer sofistikerte måter, er det mer nødvendig enn noen gang å bevare en fri, uavhengig og ansvarlig presse.

Journalistikk står overfor en ny æra der kunstig intelligens både kan være en alliert og en motstander. Det er opp til journalistene å navigere i dette komplekse landskapet og holde fast ved sannheten, uansett hvor vanskelig det måtte bli.

Trusler

Foto: Christian Fougner/NRK

Påvirkning og desinformasjon

«Vi trenger alle å være oppmerksomme på faren for påvirkning i vårt daglige arbeid.»

Vibeke Fürst Haugen, kringkastingssjef

Nord Stream2-lekkasjen ved Bornholm i september 2022.
Foto: Dansk Forsvarskommando/NTB

I februar avviste FNs sikkerhetsråd et krav fra Russland om internasjonal etterforskning av Nord Stream-sabotasjen. Bakgrunnen var en bloggartikkel der det ble hevdet at USA, med hjelp av Norge, stod bak sabotasjen. Artikkelen ble direkte sitert i flere anerkjente internasjonale medier. Norske medier som utøvde kildekritikk, fant konkrete feil i artikkelen. Nettavisen var en av få norske medier som omtalte saken i første omgang. I ettertid kom påstander om at manglende omtale i norske medier skyldes sensur. Norsk UD karakteriserte saken som en påvirkningsaksjon i Russlands pågående krigføring mot Ukraina. Senere har det kommet flere ulike teorier om hvem som stod bak sabotasjen.

Den manglende militære fremgangen for Russland innebærer at konflikten forsterkes på andre områder, hvor desinformasjon og påvirkning mot vestlige land er blant virkemidlene. Desinformasjonskampanjer kan for eksempel ha som mål å svekke vestlige demokratiers vilje til å bidra med våpen til Ukraina.

Langsiktige påvirkningsaksjoner handler i første rekke om å svekke befolkningens tillit til myndigheter og demokratiske prosesser. Norske journalister kan bli forsøkt brukt i slike aksjoner. Ett annet middel er å forsterke polariserende temaer i kommentarfelt og skape usikkerhet rundt myndighetenes styringsevne og evne til å håndtere kriser. Debattklimaet blir hardere og myndighetenes evne til å styre reduseres. Selve diskusjonen om hva som er påvirkning eller ikke, kan i seg selv virke polariserende.

Russland har i mange år drevet påvirkningsaksjoner, for eksempel forsøkt å påvirke politikk og valg i andre land. I Fokus 2023 peker Etterretningstjenesten på at Russland sprer skreddersydde budskap og desinformasjon via egne kontrollerte mediekanaler og til utvalgte målgrupper. «Uavhengige» nyhetskilder kan i realiteten være kontrollert av russiske myndigheter. På den måten spres russiske budskap i vestlige informasjonsmiljøer uten at den som videreformidler nyhetene kjenner det egentlige opphavet. Etterretningstjenesten sier spørsmål knyttet til forsvars- og sikkerhetspolitikk er spesielt utsatt, dette kan være verdt å merke seg for journalister som jobber med disse spørsmålene. Andre temaer i Norge som kan virke polariserende og benyttes i påvirkningsaksjoner fremover kan være miljø, vindmøller, urfolks rettigheter, klima, samt priser på strøm, mat og drivstoff.

Et internasjonalt graveprosjekt med over 100 journalister fra 30 medier avslørte i februar et israelsk selskap som skal ha påvirket 33 presidentvalg gjennom å forstyrre og sabotere valgkamper. Selskapet hadde utviklet en programpakke (Aims) som kunne operere tusener av falske profiler på sosiale medier.

NRK vurderer trusselnivået som høyt.

Misbruk av NRK som merkevare

NRK toppa hausten 2022, for andre år på rad, Ipsos si årlege måling av omdøme i Noreg. Det var 31. gongen omdømet av til saman 252 etatar, verksemder og organisasjonar vart kartlagt.

NRK vert regelmessig misbrukt i falske nettartikler, slik dette skjermbilete syner.

Merkevara NRK scorar høgt og kan difor vere attraktiv å misbruke. Gjennom aktive handlingar vel både personar og grupperingar som ikkje har noko med NRK å gjere, å bruke NRK-namnet eller NRK-logoen for å lure til seg pengar, merksemd eller truverd. Det finns ei rekkje eksempel på slik misbruk. Falske nettsider spreidd i sosiale medium og som reklame i nettaviser, gjev seg ut for å vere frå NRK. Det same gjeld videoar som ser ut som reportasjar frå NRK Nyheiter. NRK-artiklar blir feil omsett og publisert med signatur frå NRK-journalisten på heilt andre nettstader enn NRK sine. Falske kontoar vert oppretta i sosiale medium, slik at dei ser ut som kontoane til NRK-profilar. Det vert publisert og delt videoar i sosiale medium, der aktøren bak gjev seg ut for å jobbe i NRK utan å gjere det, og det vert rapportert om folk som «luskar» rundt i nabolag under dekke av å vere på utkikk etter passande stad å produsere, utan at NRK har informasjon som kan stadfeste at dette er korrekt.

Tekst, bilete, video og grafikk har vore brukt for å etterlikne NRK. Videoar og falske nettsider har så langt hatt tydelege økonomiske motiv, der NRK si truverd vert brukt til bedrageri. Etter at norske medieleiarar i fellesskap varsla riksadvokaten om denne trusselen, har Økokrim etablert eit arbeid for å motverke og førebygge denne typen kriminalitet.

«Lusking» i nabolag er nærliggjande å tru har vinnings hensikt. Falske kontoar kan ha ulike motiv. Uavhengig av motiv, slike aktivitetar utgjer ein trussel mot NRK som merkevare. Det er grunn til å tru at vi framover vil sjå auka brukt av datagenerert tale og datagenerert video med NRK-profilar som verkemiddel i forfalsking av NRK-produkt. Parallelt med utvikling av dataverktøy og kunstig intelligens, vert slike verkemiddel meir og meir effektfulle. I kombinasjon med konspirasjonsteoriar og feilinformasjon utgjer slik misbruk av NRK sine merkevarer ein trussel mot NRK sitt truverd.

Ein type misbruk av merkevare som kom med krigen i Ukraina er misvisande bruk av skjermdump frå nrk.no. Ekte artiklar eller overskrifter blir brukt som bevis på at historier fortalt av russisk statsmedie, er sanne. I eit valår som 2023 kan ikkje NRK sjå bort frå at merkevara NRK kan bli misbrukt i produkt eller tenester etablert for å påverke kommune- og fylkestingsvalet, eller auke polarisering i samfunnet.

Misbruk av merkevara *NRK* kan utgjere ein trussel mot NRK sitt omdømme og truverd.

NRK vurderer trusselnivået som høgt.

Tilliten til vårt innhold

Integritet er en av de tre hovedprinsippene i informasjonssikkerhet, sammen med konfidensialitet og tilgjengelighet. Integritet betyr at informasjonen skal være pålitelig og nøyaktig, noe som er viktig for å opprettholde tilliten til NRK. Vi må derfor beskytte all vår publiserte og upubliserte informasjon og innhold mot uautoriserte endringer, sletting, eller uautorisert tilgang.

Innholdet på en nettside fra NRK ble endret av uvedkommende i desember 2022.

I desember 2022 kunne overskriften «NRK hacket – Falsk propaganda fikk spre seg i ukevis!» dessverre blitt realitet. En kombinasjon av tilfeldigheter og rask respons fra NRKs IT-sikkerhetsmiljø forhindret dette.

NRK-plakaten setter krav til at NRK skal verne om sin integritet og troverdighet for å kunne opptre fritt og uavhengig i forhold til personer eller grupper som av politiske, ideologiske, økonomiske eller andre grunner vil øve innflytelse på det redaksjonelle innholdet. Dette betyr at NRK må beskytte både upublisert og publisert innhold mot endring, selv om informasjonen er ansett som åpen og ikke sensitiv.

Gjennom høsten og vinteren har vi sett at kampen om sannheten har blitt viktigere og viktigere. Cyberkrigen mellom de pro-ukrainske og pro-russiske hacktivist-gruppene har i hovedsak bestått av tjenestenektangrep mot nettsider i Russland og i Vesten. I 2022 er det i tillegg registrert en rekke dataangrep hvor formålet har vært å spre propaganda direkte ved å avbryte TV- og radiosendinger, samt manipulere nyhetsnettsider med falske artikler og propaganda. Dette så vi også under protestene i Iran høsten 2022, hvor det var flere hendelser der statlige iranske TV-kanaler ble avbrutt med propagandainnslag som så ut å komme fra regimekritiske demonstranter.

Tilliten til at nyhetsartikler og annen informasjon på NRKs nettsider er uavhengig og korrekt fremstilt, er kritisk for samfunnsoppdraget. I desember 2022 hadde NRK en hendelse med potensiale til å kunne bli den mest alvorlige IT-sikkerhetshendelsen som er avdekket til nå i bedriften. En undernettside av NRK.no var blitt endret og det var lagt ut ti falske reklameartikler tilgjengelig for publikum. Angriper har utnyttet en kjent sårbarhet på siden i et antatt automatisert angrep for å spre reklameartikler opp mot julesalget. Nettsiden ble deaktivert øyeblikkelig etter at hendelsen ble rapportert. Interne undersøkelser konkluderte med at angriper med høy sannsynlighet ikke har tatt seg videre inn på NRKs andre nettsider, og at angrepet med høy sannsynlighet ikke var bevisst rettet mot NRK. Potensialet her, om angriper var bevisst at dette var en NRK-nettside som kunne benyttes til spredning av eksempelvis skadevare eller propaganda, kunne vært kritisk for NRKs troverdighet og integritet. Denne gangen gikk det heldigvis bra...

NRK vurderer trusselnivået som høyt.

Oppetid og publiseringsevne

Direktesending fra studio på Marienlyst.
Foto: Christian Fougner/NRK

Fem effektive tiltak mot dataangrep

1. Installer sikkerhetsoppdateringer så fort som mulig, og mest mulig automatisk
2. Ikke tildel administratorrettigheter til sluttbrukere
3. Ikke tillat bruk av svake passord, og bruk to-/multifaktorautorisering der det er mulig
4. Fas ut eldre IKT-produkter
5. Tillat kun programvare som er godkjent av virksomheten eller enhetsleverandøren

(Kilde: NSM)

Bare i januar 2023 ble NRK utsatt for minst fire digitale angrep som hver utgjorde en trussel mot NRKs evne til å publisere innhold. NRK har preventive tiltak som stoppet disse DDoS-angrepene.

Trusler mot NRKs evne til å publisere innhold omfatter ulike former for digitale angrep. Dette kan være destruktive digitale angrep fra hacktivist-grupper eller cyberkriminelle som ønsker å forstyrre eller skade NRKs evne til å nå publikum med innhold, eller med rent økonomiske motiv. NRK kan være et norsk symbolmål eller rammes som et tilfeldig mål.

Skadevareangrep som løsepengevirus anses fortsatt som en av de største truslene mot NRK.

Flere rapporter fra 2022 viser en nedgang i virksomheter som betaler løsepenger etter kryptovirusangrep. En av årsakene kan være økt bevissthet om at man ikke har noen garanti for å få tilgang til alle sine krypterte filer, selv om det betales. Man har heller ingen garanti for at data ikke videreselges selv om man betaler. Løsepengeangrep som en tjeneste (ransomware-as-a-service) har blitt mer profesjonalisert det siste året. Det er observert en endring i flere av angrepene, hvor bedriftens backup først er målet før hovedangrepet finner sted. Utviklere av skadevare selger nå tjenestene til kriminelle grupperinger eller til enkeltpersoner, mot prosenter av innbetalte løsepenger. Slike angrep har derfor blitt mye mer tilgjengelige, på lik linje med det vi tidligere har sett ved tjenestenektangrep (DDoS).

Tjenestenektangrep/DDoS (Distributed Denial of Service) dominerer likevel statistikken som den vanligste angrepsform mot media i fjor (se side 18) NRK blir selv regelmessig utsatt for slike angrep, men har avverget de fleste uten påvirkning på våre publikumstjenester. DDoS-angrep gjennomføres ved at det sendes et stort antall forespørsler mot en nettside for å overbelaste den, og dermed hindres ordinære besøkende tilgang. Angrepene er som oftest raskt over, men varighet og styrke begrenses bare av hvor mange ressurser som settes inn. Selv om angrep som oftest kun er forstyrrende, kan de på feil tidspunkt få alvorlige konsekvenser, ved å eksempelvis hindre tidskritiske publiseringer eller viktige direktesendinger.

Leverandører kan også direkte og indirekte utgjøre en trussel mot NRKs publiseringsevne. NRK er avhengig av tredjepartsleveranser i lange digitale verdikjeder i produksjon, og cyberangrep mot dem kan få kritiske konsekvenser for NRKs tjenester. Dette gjelder både der NRK kjøper en tjeneste og der NRK kjøper utstyr eller komponenter som inngår i produksjonskjeden. Leverandørens egne sårbarheter kan gjøre de utsatt for cyberangrep som igjen kan ramme NRK. Det er derfor også viktig med kartlegging samt risikovurderinger i forbindelse med anskaffelser og kontraktsinngåelser.

NRK vurderer trusselnivået somhøyt.

Datalekkasjer og informasjonstyveri

Fra fremleggelsen av de nasjonale trusselvurderingen til Etterretningstjenesten, PST og NSM.
Foto: Fredrik Varfjell/NTB

Person- og kildeopplysninger, upublisert materiale og tilsvarende sensitiv informasjon fra datainnbrudd eller lekkasjer, er ettertraktet salgsvare på det mørke nettet. Slik informasjon kan tenkes benyttes av kriminelle til utpressing. For NRK kan dette bety bøter og omdømmetap, og mulig utpressing for å få oss til å endre journalistikk.

Russland, Iran og Kina har i år igjen blitt fremhevet av norske myndigheter som de største etterretningstruslene mot Norge, både i det fysiske og det digitale domenet. NRK er med vårt samfunnsoppdrag i en særstilling i medie-Norge, og kan derfor antas å være et attraktivt etterretningsmål for innsamling av upublisert materiale og informasjon om sensitive regimekritiske saker, kilder med mer.

Russisk etterretning forventes i stor grad å operere på norsk jord, mens det kinesiske regimet benytter en rekke andre virkemidler. "Made in China 2025" er en strategisk 5-årsplan med formål å redusere Kinas avhengighet av utenlandsk teknologi og fremme kinesiske teknologiske produsenter på det globale markedet. Masseinnsamling av mulig interessant informasjon er en del av denne strategien.

Den kinesiske etterretningsloven forplikter enhver kinesisk borger, virksomhet og organisasjon til å dele informasjon med myndighetene, eller utføre andre tjenester om de blir bedt om det. Derfor er det i praksis ikke mulig å skille private aktører fra statlige, siden kinesiske selskaper eller statsborgere som i utgangspunktet har gode hensikter, kan pålegges å spionere for staten.

TikTok og muligheten kinesiske myndigheter har for å benytte den til etterretningsformål har den siste tiden hatt stort fokus. Alle apper samler inn en mengde data om brukerne, men i Vesten har vi en lovfestet rett til personvern og et mer velfungerende maktfordelingsprinsipp som gjør at bruken av dine data har ett større rettsvern enn det som er tilfelle i Kina. Ved en tilspisset konflikt med Vesten er det fullt mulig at de politiske behovene for å få tilgang til all informasjon samlet inn av kinesiske apper, overstyrer de opprinnelige uttalte formålene.

Iran pekes også på i PSTs trusselvurdering. Qatars tette tilknytning til blant annet Iran var en av hovedårsakene til at NRK under fotball-VM ikke tillot å bruke de offisielle appene på NRK-tilknyttede telefoner.

NRKs økende digitalisering skaper i seg selv nye og større angrepsflater for digitale kriminelle. Nye sårbarheter vil introduseres via ny teknologi, som betyr at vi har behov for sikkerhetskompetanse på nye områder. Enhver nettverkstilkoblet komponent eller IT-tjeneste er en ny potensiell vei inn for de som ikke vil oss vel.

NRK vurderer trusselnivået som høyt.

TikTok, WeChat og Alibaba statskontrollerte

«Golden Shares» er et virkemiddel Kina har tatt i bruk for å få direkte kontroll i strategisk viktige private virksomheter. Ordningen gir staten 1% eierandel med lovfestet kontroll og vetorett i alle større beslutninger. «Golden Shares» ble effektuert i TikToks morselskap Bytedance i 2021, og en egen representant fra partiet ble da satt inn i styret. Det samme har også skjedd i flere av tek-gigantene, som Tencent og Alibaba.
(Kilder: Financial Times / International Finance – 2023)

Trusselen fra innsiden

”Igjen er VG full av sitat frå Workplace og igjen blir eg minna om kvifor eg mest aldri gidder å ytra meg her. Det er **UKOLLEGIALT** og **ILLOJALT** å springe til konkurrentane når du er usamd.”

Fra Workplace 1. mars 2023

En innsider er en person som har, eller har hatt, legitim tilgang til virksomhetens verdier, og som misbruker denne tilgangen for å utføre handlinger som påfører virksomheten skade eller tap.

TV-resepsjonen i NRK.
Foto: Sidsel Avlund/NRK

Medarbeidere, ansatte og tidligere ansatte har informasjon, kunnskap eller tilgang som kan være av interesse for en trusselaktør. Det er derfor viktig at alle som jobber i NRK er bevisste på hva vi kan dele og ikke dele til eksterne for ikke å utsette NRK for skade. I perioder med omorganisering er det viktig med gode prosesser slik at alle berørte føler seg godt ivaretatt. I NSM sitt arbeid med innsidetrusler pekes det på omstillinger og organisasjonsendringer som situasjoner der misfornøyde medarbeidere kan være lette å påvirke til å gi fra seg intern informasjon, eller på andre måter skade egen bedrift. Summen av stadige lekkasjer fra innsiden, for eksempel fra debatter på Workplace, er en trussel mot det interne ordskiftet og i ytterste konsekvens mot NRK.

Enkelte ansatte kan være utsatte for å bli påvirket, forsøkt manipulert eller sågar rekruttert av et annet lands etterretning, enten på grunn av sin funksjon i NRK eller sitt statsborgerskap. Norske myndigheter peker spesielt mot etterretning fra Kina og Russland, og deres støttespillere. - Russiske borgere i Norge kan i større grad oppleve press om å samarbeide med russisk etterretning, sa PST-sjef Beate Gangås ved fremleggelsen av PSTs trusselvurdering for 2023. I følge kinesisk lov plikter enhver kinesisk borger, virksomhet og organisasjon å bistå etterretningstjenestene dersom de blir bedt om det.

Trusselaktører tilnærmer seg over tid og det kan være lett å bli utnyttet og lurt til å gi fra seg sensitiv informasjon også uten å være klar over det. Saken mot den tidligere ansatte i DNV viser at russiske diplomater er villige til å betale penger for informasjon. Spionsiktelsen er henlagt, men han ble i desember 2022 dømt for grov korrupsjon. Han har anket saken.

Dagens Nyheter har avslørt hvordan forskerstudenter og gjesteforskere som er tatt opp via et kinesisk studieprogram på universiteter i Sverige, tvinges til å skrive under på at de skal være lojale mot kommunistpartiet og tjene regimets interesser. I følge avtalen risikerer de ”konsekvenser” om de ikke gjør som kinesiske myndigheter vil.

Det er viktig for NRK å ha en kultur for at dersom en ansatt blir forsøkt presset, truet eller på annen måte fristet til å begå en innsidehandling, er det naturlig å melde fra, enten til egen leder eller til sikkerhetsavdelingen. NRK skal støtte medarbeidere som stiller spørsmål med det de har opplevd eller mistenker at de kan ha blitt forsøkt manipulert.

NRK vurderer trusselnivået som moderat.

Vold, trusler og uønsket oppmerksomhet

"Jeg vil ikke ta på meg verv i forbindelse med barna mine fordi jeg ikke vil at kontaktinfo om meg skal spres til noen flere enn de som må vite hvor jeg bor."

Sitat fra intern NRK-undersøkelse

56 journalister ble drept i 2022. Flest i Mexico (11) og Ukraina (8).

550 journalister er i fengsel pr. 1. mars 2023. Flest i Kina (101) og Myanmar (75). I Tyrkia sitter 24 journalister fengslet.

(Kilde: Reportere uten grenser)

Politiet tilstede for å sikre en demonstrasjon i forbindelse med krigen i Ukraina.
Foto: Heiko Junge/NTB

Utenriks, pandemi, vaksine, kriminalitet, politikk og urfolksproblematikk er temaer som ofte utløser trakasserende eller truende respons fra eksterne. Journalister blir påvirket av ubehag de opplever gjennom jobben og det innebærer en fare for at NRKs journalistikk også kan bli påvirket.

I Europa har vi de siste årene sett målrettede angrep på journalister i forbindelse med demonstrasjoner og på grunn av gravende journalistikk mot kriminelle miljøer. I Norge er det svært sjelden fysiske angrep på journalister, men NRK-journalister beskriver opplevelser der de blir omringet av ungdommer som filmer, og trusler om at kamera eller "trynet" skal knuses. Det fortelles også om digitale ubehagelige henvendelser fra publikum, både fra vanlige folk, næringslivsfolk og politikere, om alt fra anklager om å være i ledtog med verdens legemiddelindustri og mørke krefter, til trusler om at man ikke har livets rett. Journalister med flerkulturell bakgrunn kan i noen tilfeller være ekstra utsatt for hets og sjikane både fra "egne" minoritetsmiljøer som har spesielle forventninger til dem og fra høyreradikale miljøer.

Internasjonalt forfølges journalister i stadig større grad fra myndighetshold. Gjennom endring i lovverk kan journalister fengsles om de finner behov for dette. Tydeligst er dette i Russland der lovverket er endret flere ganger siden invasjonen av Ukraina, men også i Polen, Hellas og Tyrkia har vi sett at loven er blitt brukt til å pågripe journalister. I Finland ble to journalister fra avisen Helsingin Sanomat i januar 2023 funnet skyldige i å ha avslørt statshemmeligheter gjennom en artikkel publisert i 2017. Norsk redaktørforening har uttalt bekymring for at denne typen etterforskning og dommer mot journalister fort kan ha en nedkjølende effekt på journalistikken.

Norge er fortsatt best på pressefrihet i verden, ifølge Reportere uten grenser. NRK har journalister på jobb også i land som scorer lavt på pressefrihet og i land med høy risiko, blant annet korrespondenter i Russland, Kina, Tyrkia og Libanon. I februar 2023 ble korrespondentkorpset utvidet med reporter og fotograf i Ukraina. Et NRK-team på jobb i Afghanistan opplevde tilbakeholdelse ogt aggresjon fra Taliban under reportasjereise høsten 2022. Fra å kunne jobbe relativt fritt i landet etter at Taliban tok makten høsten 2021, er forholdene for journalister nå svært vanskelige.

NRK vurderer trusselnivået for vold som lavt, for trusler og uønsket oppmerksomhet som høyt.

Uvedkommende og aksjonisme

«Aktører med uærlige hensikter kan forsøke å påvirke vår dekning og aksjonister kan forsøke å prege våre direktesendte arrangementer. Derfor tenker vi sikkerhet fra start når vi planlegger sendinger».

Laurie MacGregor, prosjektleder Valg 2023

Klimaaksjon under TV-sendt skirenn fra Lillehammer (skjermbilde fra NRK).

NRKs direktesendinger fra arrangementer kan være et middel eller et mål for aksjonister som ønsker oppmerksomhet.

Under et TV2-sendt skirenn plasserte aktivister seg i løypene i Lillehammer og sperret skisporet for utøverne. Det siste året har vi i Norge også sett klimaaktivister grise til statuer og forsøke å lime seg til kjente kunstverk. Andre har aksjonert ved å sette seg ned i veibanen for å hindre morgentrafikken eller ved å sette seg ned foran offentlige bygninger for å hindre adgang til bygget.

I en klimadebatt på NRK i november 2022, ble det sagt fra en klimaaktivist at voldsbruk kan være aktuelt for å fremme sin sak. Norske klimaorganisasjoner har tatt avstand fra dette utsagnet.

NRK har 50 kontorer spredd over hele landet. Infrastruktur, eiendeler og informasjon i lokalene kan være av interesse for uvedkommende som ønsker å ta seg inn i bygningsmassen. Uvedkommende inne i NRKs lokaler skaper utrygghet for medarbeidere og gjester. Det har vært hendelser hvor personer har forsøkt å komme seg inn uten avtale for å kontakte journalister eller for å oppsøke en NRK profil.

Uvedkommende inne i lokalene kan bevisst eller ubevisst gjøre skadeverk på infrastruktur, dører eller vinduer. Innbrudd og skadeverk med vinnings hensikt, som tyveri av utstyr, kan påvirke NRKs sendinger. Det er i dag ingen stor trussel mot NRK, men påfører NRK ulempe og kostnader til reparasjoner når det skjer. NRK ser i dag ingen økende tendens. Det er likevel verdt å merke seg at aktivitet som skjer utenfor NRKs bygningsmasse som ikke håndteres raskt, kan medføre situasjoner som ikke er ønskelig. NRK kjenner til at det sporadisk foregår sykkeltyveri, bruk av narkotika og det som framstår som flaskesamling på NRKs eiendom. NRK kan ikke se bort fra at disse vil ta seg inn i bygningsmassen om muligheten er der. Tyveri av NRKs eiendeler forekommer, men er på et lavt nivå.

Nyhetsbildet og ulike sendinger bidrar til at truslene mot NRK endrer seg i takt med dette. NRK må ta høyde for at sendinger kan bli forsøkt avbrutt for å fremme et budskap.

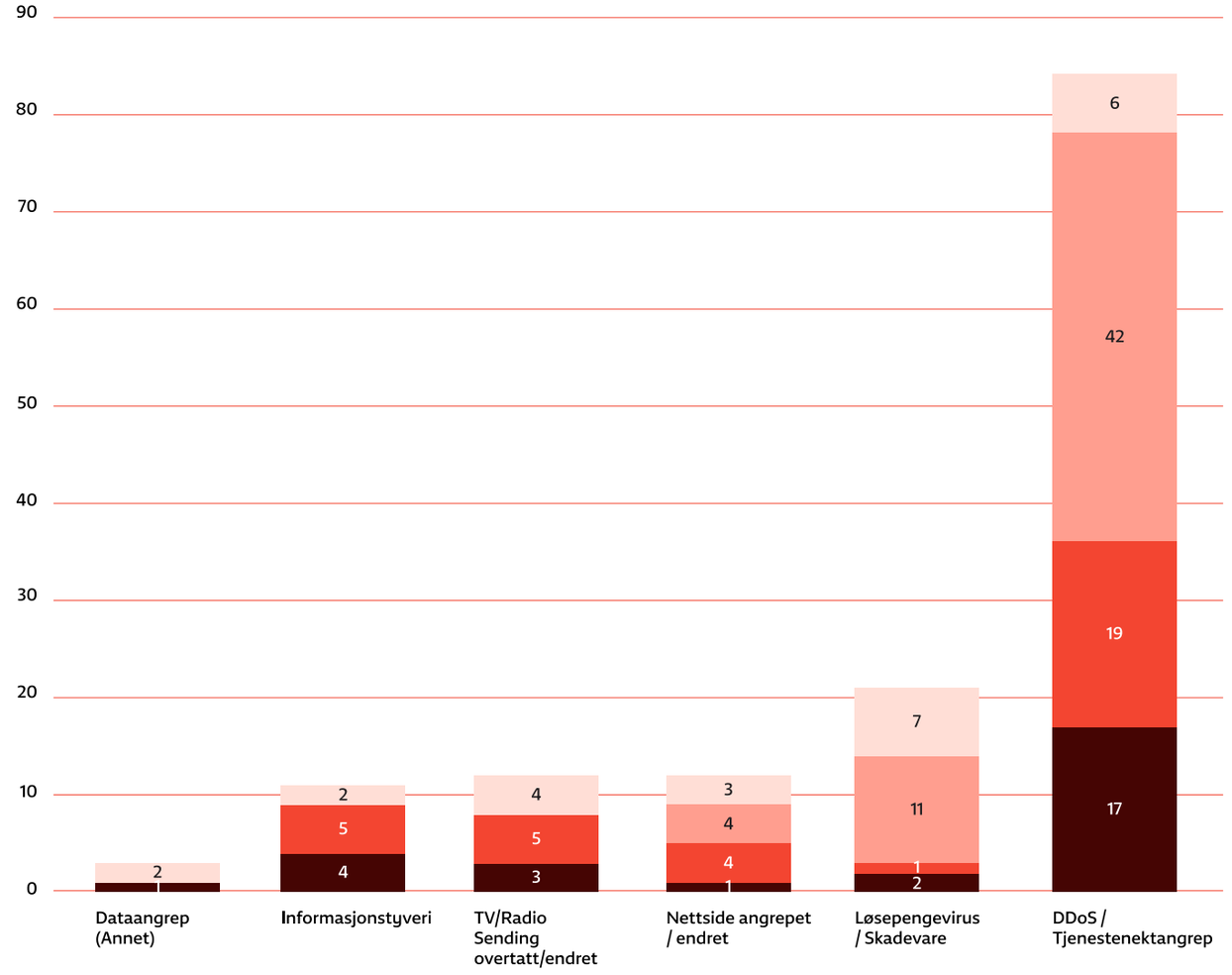
NRK vurderer trusselnivået som moderat.

Kjente dataangrep mot media i 2022

NRK har gjennom året sammenstilt en oversikt over alle kjente dataangrep rettet mot medierelaterte nettsider og virksomheter. I 2022 ble det avdekket over 140 angrep, en økning fra rundt 40 året før. Mørketallene er forventet å være store for begge år. Oversikten viser antall angrep, hvor flere angrep kan være rettet mot en rekke virksomheter så de reelle tallene er høyere.

DDoS fra pro-russiske og pro-ukrainske hacktivistgrupper står for hovedtyngden av angrep. DDoS utføres i hovedsak for å skape oppmerksomhet i media samt på egne kanaler, og antall angrep har holdt seg stabilt utover 2023. Mediefokus har avtatt noe og flere Europeiske mediehus, inkludert NRK, har begynt å utelate navn på grupperingene for å redusere eksponering. Den siste tiden er det observert en dreining mot andre former for angrep, som informasjonslekkasjer og endring av nettsider (”defacement”), antatt som følge av redusert oppmerksomhet av DDoS alene.

Informasjonen er hentet fra en rekke kilder, primært fra nyhetsartikler og virksomhetenes egne uttalelser og pressemeldinger.



Om NRKs trusselvurdering

Foto: Henrik Bergman

Om NRKs trusselvurdering

Foto: Rita Nottveit/NRK

NRKs trusselvurdering er utarbeidet av Sikkerhetsavdelingen med bidrag fra andre fagmiljøer i NRK. Vurderingen dekker forventede relevante trusler mot NRK som virksomhet ett til to år fremover i tid.

Trusselnivå fastsettes på en skala med 5 nivåer:
Svært høyt – Høyt – Moderat – Lavt – Ubetydelig.

Nivå baseres på en kombinasjon av analyse og faglige vurderinger av opptil fem indikatorer, satt for relevante trusselaktører innen hver trusselkategori, og kan i perioder øke som følge av interne og eksterne forhold.

- **Tilstedeværelse:** Er aktøren antatt til stede eller kan den nå verdiene på andre måter (digitalt, via tredjepart eller tilsvarende)?
- **Kapasitet:** Er det antatt eller demonstrerte evner hos aktører til å utføre handlingene som kan ramme NRKs verdier?
- **Intensjon:** Eksisterer det, eller antas det å eksistere en vilje eller ønske om å ramme NRKs verdier?
- **Historikk:** Eksisterer det påviselig aktivitet over tid, mot NRK eller tilsvarende virksomheter?
- **Målvalg:** Eksisterer det ny og pålitelig informasjon som indikerer forberedelse av et nært forestående angrep direkte rettet mot NRK?

Trusselnivå er ikke det samme som risikonivå. Risikonivå i NRK fastsettes ut fra sannsynlighet og konsekvens. Vi kan for eksempel ha et høyt trusselnivå, men gode sikkerhetstiltak kan være med å redusere sannsynligheten for at hendelsen inntreffer, slik at samlet risiko igjen kan være lavere. Trusselnivå benyttes som en av faktorene i en risikovurdering for å anslå sannsynlighet for at en tilsiktet uønsket hendelse kan inntreffe. I dette arbeidet vil trusselvurderingen for fjoråret også være aktuell å se til.

Forsidefoto viser Roger Sevrin Bruland rapportere direkte fra Ukraina, og er tatt av NRKs fotograf Oleh Balaban.

Helikopterbildet viser Cineflex-kameraet til NRK Luftfoto etter debutturen i oktober 2022.

Bidragsytere:
Christian Fougner, Gerd Fredriksen, Lars Eirik Berg, Rita Nottveit, Sidsel Avlund, Tor Willy Laursen og Øyvind Vasaasen.

Eksterne kilder:
PST - Trusselvurdering 2023
E-tjenesten - Fokus 2023
NSM - Risiko 2023
CyberPeace Institute
KonBriefing

Interne kilder:
NRKs spørreundersøkelse om vold, trusler og uønsket oppmerksomhet, mai 2022.
Eksempler brukt i rapporten er ikke uttømmende.

Arbeidet ble ferdigstilt 21. mars 2023.

Design: ANTI