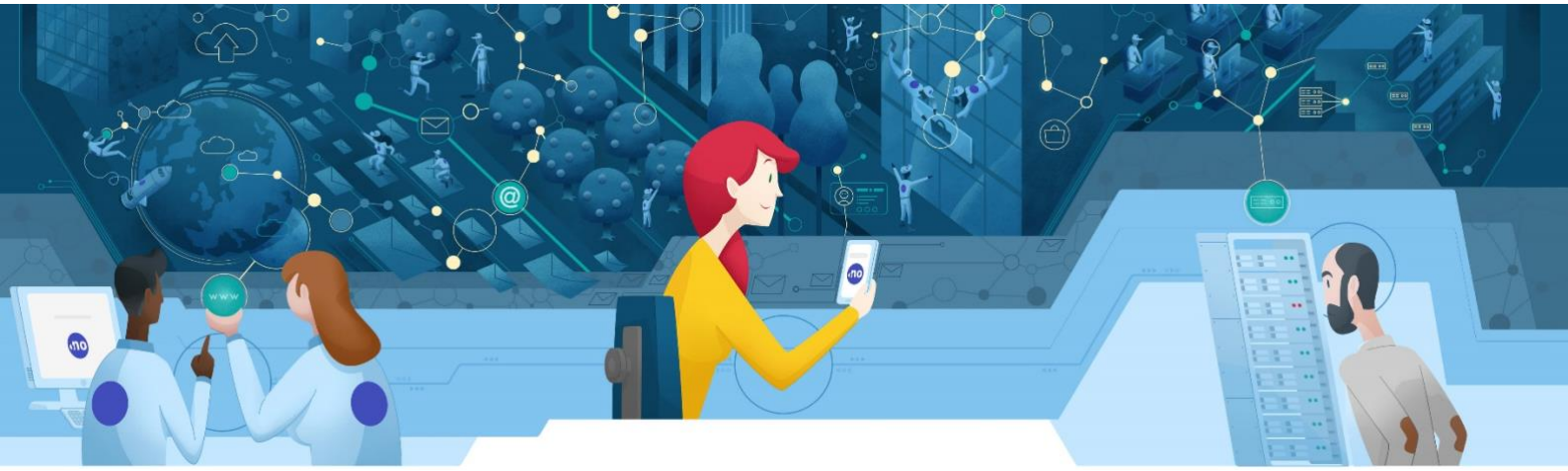


DOMENENAVN OG RISIKOHÅNDTERING

Veileder

Norid AS
2024

INNHOLD

1 INNLEDNING

1.1 HVA FINNER DERE I DENNE VEILEDEREN?

Denne veilederen hjelper dere å vurdere hvor avhengig virksomheten er av domenenavn, og hvilke tiltak dere kan gjøre for å sikre egne leveranser.

Veilederen gjelder alle domenenavn, selv om vi i eksemplene bare bruker domenenavn under det norske toppdomenet *.no*.

Veilederen er bygget opp slik:

- I kapittel 2 får du en innføring i hvordan domenenavnsystemet virker.
- I kapittel 3 får du vite hvilke konsekvenser det kan få hvis domenenavn skulle falle bort.
- I kapittel 4 får du vite hvordan dere kan vurdere hvor kritisk det er at domenenavnene dere benytter, er tilgjengelige. Du får også en oversikt over noen praktiske tiltak som virksomheter kan iverksette for å bli bedre rustet mot et bortfall av domenenavn.

1.2 HVEM KAN HA NYTTE AV DENNE VEILEDEREN?

Denne veilederen er laget for private og offentlige virksomheter der domenenavn spiller en rolle for å opprettholde viktige funksjoner i samfunnet eller normal omsetning og drift.

Personer som særlig kan ha nytte av veilederen, kan være IT-sikkerhetssjefer, risikoeiere og beredskapsansvarlige.

1.3 SENTRALE BEGREPER

Beredskap	Evne til å iverksette forhåndsplanlagte aktiviteter når det oppstår en ekstraordinær situasjon. Begrepet brukes spesielt om å være forberedt på å håndtere og redusere skadevirkninger av uønskede hendelser som kan føre til skade på eller tap av verdier. Beredskap omfatter menneskelige, teknologiske og organisatoriske tiltak.
DNS	Forkortelse for domenenavnsystemet. Domenenavnsystemet er en infrastruktur som knytter unike domenenavn til den relevante IP-adressen, slik at vi enklere kan kommunisere over internett.
Domenenavn	En unik, hierarkisk oppbygget navnestreng som benyttes til adressering på internett.
IP-adresse	Forkortelse for Internet Protocol-adresse. Internet Protocol er en felles protokoll for kommunikasjon mellom enheter som er tilknyttet internett. Alle enheter som er koblet på internett, har en unik IP-adresse, bestående av en lang tallrekke.
Kontinuitetsplanlegging	Planlegging for hvordan virksomheter kan opprettholde viktige leveranser ved uønskede hendelser som rammer samfunnet og virksomheten.
Kritikalitet	En funksjon av hvor avhengig en virksomhet er av noe, og hvilken mulighet virksomheten har til å påvirke eventuelle negative konsekvenser.
Kritiske samfunnsfunksjoner	Funksjoner som er nødvendige for å ivareta befolkningens og samfunnets grunnleggende behov der svikt raskt kan medføre tap og skade, og som det derfor er særlig viktig å unngå avbrudd i.[1] Kritiske samfunnsfunksjoner er også definert som funksjoner som samfunnet ikke kan klare seg uten i sju døgn eller kortere uten at det truer befolkningens sikkerhet og/eller trygghet. For at funksjonen skal regnes som kritisk, forutsettes det også at det skjer noe som medfører et behov for beredskapsressurser, i løpet av sjudøgnsperioden.
Risikovurdering	En vurdering av risikoene en virksomhet står overfor. En risikovurdering kan gjøres på mange ulike måter, men har generelt som formål å gi virksomhetens ledelse et grunnlag for å iverksette nødvendige tiltak.
Toppdomene	Den siste delen av et domenenavn. Det finnes både nasjonale toppdomener, som *.no*, *.se* og *.uk*, og generiske toppdomener, som *.com*, *.net* og *.org*.

Tabell 1: Sentrale begreper

[1] Direktoratet for samfunnssikkerhet og beredskap (2016). «Samfunnets kritiske funksjoner»

2 HVORDAN VIRKER DOMENENAVNSYSTEMET?

Alle datamaskiner som er koblet til internett, har en *IP-adresse* som består av en lang tallrekke. Utveksling av trafikk mellom tjenester og klientsystemer over internett er basert på disse adressene. For å forenkle bruken får en tjeneste ett eller flere *domenenavn*, som brukes både i brukergrensesnitt og i systemkonfigurasjoner. Dette gjør det også mulig å flytte en tjeneste til en ny maskin med en ny IP-adresse uten å måtte fortelle det til dem som bruker tjenesten.

Domenenavnsystemet (forkortet DNS) er en tjeneste som kobler unike domenenavn sammen med IP-adressen til en tjeneste eller maskin på internett. DNS kan også brukes til å formidle teknisk informasjon som trengs for å bruke en tjeneste over internett, som for eksempel sertifikatinformasjon eller mekanismer som beskytter e-post mellom e-posttjenere[2].

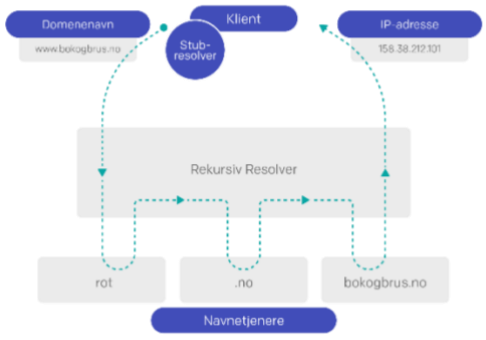
Alle domenenavn direkte under *.no* er registrert hos registerenheten Norid AS (Norid).

Norid behandler søknader om abonnement på domenenavn og sørger for at regelverket er i takt med behovene i samfunnet. I tillegg sørger Norid for teknisk drift og utvikling av tjenesten.

Tjenesten er regulert av en egen forskrift med Nasjonal kommunikasjonsmyndighet (Nkom) som tilsynsmyndighet.

2.1 Å SLÅ OPP TJENESTER VIA DOMENENAVNSYSTEMET

Domenenavnsystemet konverterer domenenavn til IP-adresser. Dette er en grunnleggende funksjonalitet som er nødvendig for at internettinfrastrukturen skal fungere. DNS har en hierarkisk oppbygging, noe som innebærer at hver konvertering forutsetter et samspill mellom flere uavhengige aktører. *Navnetjenerne* som sørger for stegene i konverteringen, befinner seg på alle nivåene i hierarkiet.



Figur 1: Oppslag av domenet bokogbrus.no i DNS

Når en bruker eller en maskin forsøker å kontakte en tjeneste, brukes en *stub-resolver* (DNS-klient). Dette er enkel programvare i brukerens datamaskin som tar imot henvendelser fra applikasjoner, for eksempel når en bruker taster inn «www.bokogbrus.no» i sin nettleser. Stub-resolveren er konfigurert med IP-adressen til en *rekursiv resolver* og tar kontakt med denne.

En *rekursiv resolver* er en navnetjener som er konfigurert til å fortsette å spørre navnetjenere gjennom hele hierarkiet til den finner IP-adressen til domenenavnet som stub-resolveren spør om. Hvis den rekursive resolveren nylig har slått opp dette domenenavnet, vil den ha IP-adressen i minnet (cache) og kan returnere adressen direkte. Hvis ikke sender resolveren henvendelsen til det øverste nivået i hierarkiet: DNS-roten.

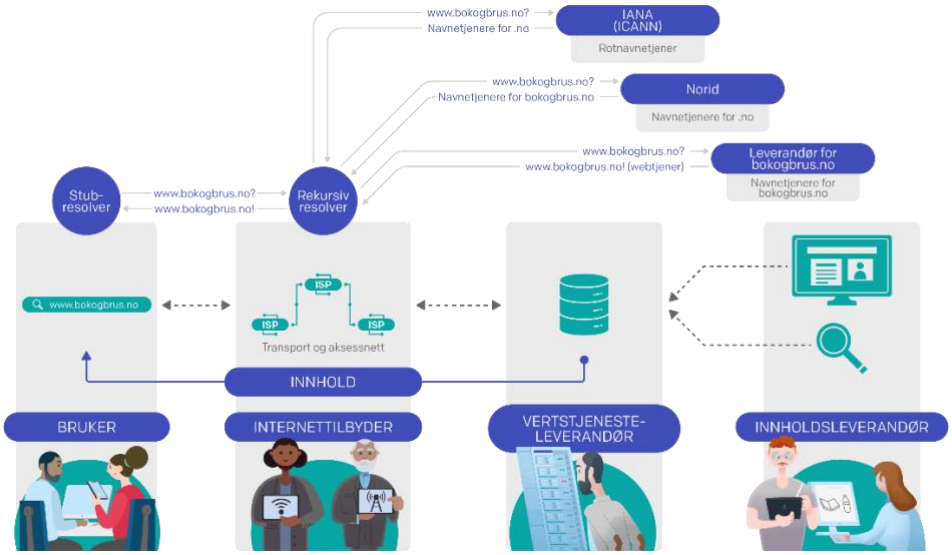
[2] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnleggende-tiltak-for-sikring-av-e-post/

Rotnavnetjenerne betjener DNS-roten. De tar imot henvendelser om domenenavn fra rekursive resolvere og returnerer et svar med en liste over navnetjenerne for toppdomenet til domenenavnet. Det finnes 13 rotnavnetjenere i verden, hver med flere instanser bak hvert navn, og det er ICANN (Internet Corporation for Assigned Names and Numbers) som har overoppsynet med disse.

Hvis den rekursive resolveren spør etter et domenenavn som slutter på *.no*, vil rotnavnetjenerne oppgi navnetjenerne for *.no*. Disse navnetjenerne kalles også for *autoritative navnetjenere*. Resolveren sender deretter en ny henvendelse til navnetjenerne for toppdomenet og får adressene til de autoritative navnetjenerne for domenenavnet i retur. En henvendelse til disse navnetjenerne returnerer en IP-adresse for tjenesten som brukeren forsøker å nå. Resolveren leverer denne til stub-resolveren, og deretter kan applikasjonen kontakte tjenesten. Det er på dette tidspunktet brukerens nettleser kan kontakte webserveren på for eksempel «www.bokogbrus.no» og spørre etter nettsiden.

De fleste bruker rekursive resolvere hos sin *internettleverandør (ISP)*, men en bruker kan også få tjenesten levert fra en lokal IT-avdeling eller velge offentlig tilgjengelige tilbydere, som Google eller andre. Den rekursive resolveren husker oppslag (cache) i en definert periode, og den slipper dermed å gjøre nye oppslag hvis den samme nettsiden blir besøkt flere ganger. Den navnetjeneren som gir informasjon om et domenenavn, bestemmer hvor lang «levetid» et oppslag skal ha før det må hentes på nytt.

For at en nettleser hos brukeren skal få IP-adressen til webserveren på «www.bokogbrus.no», må flere avhengigheter spille sammen: leveransene fra internettleverandøren (rekursiv resolver), fra ICANN (rotnavnetjenesten), fra Norid (navnetjenesten for .no) og til slutt leverandøren av nettsiden (navnetjenesten for «bokogbrus.no»). Hvis én av disse tjenestene ikke fungerer eller ikke kan nås på grunn av nettproblemer, vil nettleseren ikke få den IP-adressen den trenger for å kunne vise frem nettsiden.



Figur 2 Illustrasjon av de ulike aktørenes rolle

Det å vise frem en nettside kan i seg selv medføre en ny rekke DNS-oppslag for at alle elementene på nettsiden skal vises frem korrekt. Avhengig av hvilke servere og tjenester som finnes på siden, kan oppslagene skje mot mange forskjellige domenenavn. Disse kan være plassert under ulike toppdomener, noe som igjen genererer trafikk gjennom flere autonome systemer. I noen tilfeller skjer det hundrevis av ulike DNS-oppslag – mer eller mindre kritiske for å vise frem hovedinnholdet – før nettsiden vises i sin helhet.

3 HVILKE KONSEKVENSER KAN BORTFALL AV DOMENENAVN FÅ?

For å få tilgang til innhold eller andre tjenester på internett må brukerens maskin ha adressen til den serveren hvor innholdet er lagret eller tjenesten tilbys. Denne adressen hentes ut ved oppslag i domenenavnsystemet.

Hvis det ikke er mulig å hente ut adressen, enten fordi oppslag i domenenavnsystemet er ikke tilgjengelig, eller fordi selve domenenavnet er borte, så vil selve tjenesten oppfattes som utilgjengelig selv om for eksempel webservere med innhold kjører som normalt.

Om et domenenavn skulle bli borte, vil det få konsekvenser på mange ulike områder. Vi kan dele konsekvensene inn i tre kategorier:

- konsekvenser for kommunikasjon internt i virksomheten
- konsekvenser for kommunikasjon med andre virksomheter
- konsekvenser for kommunikasjon ut mot publikum

Kommunikasjon betyr i dette tilfellet ikke bare kommunikasjon mellom mennesker ved hjelp av datamaskiner, men også kommunikasjon mellom datamaskiner.

3.1 KONSEKVENSER FOR KOMMUNIKASJON INTERNT I VIRKSOMHETER

Eksempler på intern kommunikasjon som kan bli rammet av et bortfall av domenenavn (listen er avhengig av hvilke domenenavn som faller bort, og er ikke uttømmende):

- e-post
- intranett
- samarbeidsløsninger som Teams, Slack, Yammer, Workplace osv.
- skytjenester som Office 365, SharePoint, Dropbox, Google Drive osv.
- eksterne servere
- VPN-løsninger
- prosess- og styringssystemer
- logistikk- og fagsystemer
- saksbehandlingssystemer

For å illustrere konsekvensene som et bortfall av domenenavn kan ha på den interne kommunikasjonen i en virksomhet, har vi laget to eksempler: ett med en kommersiell aktør og ett med en offentlig aktør som leverer tjenester til et lokalsamfunn.

Eksempel 1 – Store økonomiske konsekvenser for en butikkjede

I det første eksempelet tar vi for oss en butikkjede som selger dagligvarer, la oss kalle den Matkjeden. Matkjeden fremstår med en helhetlig merkevare utad og har etablert felles løsninger for alle sine butikker. Det er imidlertid opp til hver enkelt butikk i kjeden å bestemme hvilke varer den skal ta inn, og hvilken beholdning den skal ha tilgjengelig. For å få påfyll av varer må hver enkelt butikk legge inn en bestilling i Matkjedens logistikksystem før hovedkontoret sender en samlet bestilling til hovedlageret. Matkjeden bruker et nettbasert logistikksystem slik at butikksjefene kan legge inn bestillinger fra både PC, iPad og telefon mens de jobber i butikken.

Dersom domenenavnet som Matkjedens logistikksystem er basert på, faller bort, vil dette systemet ikke lenger være tilgjengelig for verken butikksjefene, hovedkontoret eller hovedlageret. Butikksjefene får ikke meldt inn behov for varer, hovedkontoret får ikke sammenstilt bestillingene og sendt dem til hovedlageret, og hovedlageret mottar ingen liste

over hvilke varer som skal plukkes og sendes til butikkene. Konsekvensen blir en stans i vareflyten som relativt raskt vil påvirke tilgjengeligheten av varer ute i butikkene og dermed Matkjedens inntjening.

Eksempelet med Matkjeden kan også overføres til andre virksomheter med andre forretningsprosesser og verdikjeder. Så lenge virksomheten benytter seg av domenenavn i leveranser og tjenester, vil et bortfall av domenenavn påvirke virksomhetens mulighet for intern kommunikasjon.

Eksempel 2 – Systemer som ikke snakker sammen setter liv og helse på spill i en kommune

I vårt andre eksempel tar vi for oss IT-avdelingen i en kommune, la oss kalle denne Stormyra. IT-avdelingen i Stormyra kommune digitaliserer og effektiviserer prosesser og tjenester ved å utvikle, drifte og forvalte kommunens digitale tjenester. Blant annet har IT-avdelingen innført et felles saksbehandlingssystem som brukes på flere av kommunens tjenesteområder, for eksempel sosiale tjenester, skole og utdanning, bygg og eiendom og skatt og næring. Saksbehandlingssystemet er tilknyttet tjenesteområdenes fagsystemer slik at relevant informasjon overføres mellom saksbehandlingssystemet og fagsystemet.

Dersom domenenavnet som enten saksbehandlingssystemet eller fagsystemet baserer seg på, skulle falle bort, vil ikke disse systemene lenger kunne snakke med hverandre. Dette vil medføre forsinkelser i saksbehandlingen, siden saksbehandlerne ikke vil ha tilgang på nødvendig informasjon for å kunne behandle saken. Alle kommunens tjenesteområder som benytter seg av det samme saksbehandlingssystemet, vil bli rammet. Potensielt kan dette gå utover kommunens leveranser, økonomi, miljø og i verste fall liv og helse.

3.2 KONSEKVENSER FOR KOMMUNIKASJON MELLOM VIRKSOMHETER

Kommunikasjon mellom virksomheter foregår også i svært stor grad over nettbaserte løsninger, hovedsakelig e-post, men også direkte mellom ulike systemer.

Eksempler på kommunikasjon mellom virksomheter som kan bli rammet av et bortfall av domenenavn (listen er avhengig av hvilke domenenavn som faller bort, og er ikke uttømmende):

- e-post
- samarbeidsløsninger som Teams, Slack, Yammer, Workplace osv.
- utveksling av informasjon direkte fra system til system med samarbeidspartnere og underleverandører
- innhenting av data fra eksterne databaser, for eksempel kart- og værdata
- rapportering til tilsyns- og myndighetsorganer

Eksempel 1 – Sjåførene får ikke arbeidslistene sine

Matkjeden er avhengig av eksterne sjåfører for å frakte varene fra hovedlageret og ut til de enkelte butikkene. Siden behovet for transport av varer varierer, sendes det ut arbeidslister på e-post direkte til hver av de eksterne sjåførene. Dersom domenenavnet «matkjeden.no» skulle bli utilgjengelig, vil ikke e-posten fra Matkjeden nå gjennom til de eksterne sjåførene. Det vil bli mye vanskeligere for Matkjeden å kommunisere hvem som skal kjøre hva og når, noe som igjen vil få konsekvenser for vareflyten til butikkene.

Eksempel 2 – Fagsystemer som ikke snakker sammen går ut over innbyggerne

I vårt andre eksempel inngår Stormyra kommune og deres IT-avdeling i et interkommunalt samarbeid hvor de arbeider tett med sine nabokommuner innenfor sentrale tjenesteområder. Blant annet koordinerer kommunene helse- og omsorgtjenester seg imellom og sørger for at innbyggerne får tilstrekkelig oppfølging av helsepersonell og nødvendig støtte av kommunenes

spesialister når det trengs. Siden kommunene har hver sine sak- og fagsystemer, er det satt opp integrasjoner mellom disse slik at kommunene kan utveksle informasjon direkte fra system til system. Dersom domenenavnene som kommunenes informasjons- og kommunikasjonsteknologi baserer seg på, skulle falle bort, vil det blir vanskelig for kommunene å koordinere og samarbeide om de kommunale tjenestene, noe som vil påvirke kommunenes leveranser til innbyggerne.

3.3 KONSEKVENSER FOR KOMMUNIKASJON MOT PUBLIKUM

Dersom domenenavn skulle falle bort, vil det bli vanskelig for tilnærmet alle virksomheter å kommunisere med publikum, siden alle digitale former for massekommunikasjon vil slutte å fungere ved et bortfall av domenenavn.

Eksempler på ekstern kommunikasjon som kan bli rammet av et bortfall av domenenavn (listen er avhengig av hvilke domenenavn som faller bort, og er ikke uttømmende):

- e-post
- nettsider
- kundeportaler
- netthandel
- varslingstjenester

Eksempel 1 – Butikkjeden mister inntekter fra netthandel

Man kan tenke seg at Matkjeden har store deler av sin omsetning fra nettbutikken «matkjeden.no». Denne nettbutikken er godt etablert i markedet og har en høy daglig inntjening. Dersom domenenavn faller bort, vil kundene fortsatt kunne skrive inn «matkjeden.no» i sin nettleser, men nettleseren vil ikke finne veien til Matkjedens nettside. Dette betyr at all trafikk til nettbutikken umiddelbart vil falle bort, med konsekvensene det får for Matkjedens inntjening.

Eksempel 2 – Kommunen når ikke ut til befolkningen med viktig informasjon

Stormyra kommune oppdaterer regelmessig sine hjemmesider med all informasjon som innbyggerne kan ha behov for i det daglige. I tillegg legger de ut informasjon om blant annet ekstremvær, vaksinering, stenging av vann og avløp og andre spesielle situasjoner som kan oppstå.

Dersom domenenavn faller bort, vil ikke innbyggerne kunne nå Stormyras nettside for å finne den informasjonen de er på jakt etter, og Stormyra vil få utfordringer med å nå ut til befolkningen med viktig informasjon.

4 SLIK VURDERER DU HVOR KRITISK DOMENENAVN ER FOR DIN VIRKSOMHET

De aller fleste virksomheter gjennomfører risikovurderinger i en eller annen form, enten som en formell prosess der risikovurderinger er en del av virksomhetsstyringen, eller som en mer uformell prosess der risikoer analyseres etter hvert som de oppdages.

Det kan være imidlertid være vanskelig å identifisere risikoer på områder som er lite fremtredende i det daglige. Domenenavnsystemet er et slikt område. Det er en del av internetts grunnmur, men er lite kjent. Oppslag mot ulike registre for domenenavn foregår i stor grad automatisk og i bakgrunnen av de aktive prosessene i en virksomhet. Dermed er det som regel kun de som arbeider med dette til daglig, som er klar over denne infrastrukturen og den potensielle sårbarheten den utgjør.

I kapittel 4.1 til 4.4 skisserer vi hvordan virksomheter kan analysere risikoer og sårbarhet knyttet til bortfall av domenenavn. I kapittel 4.5 til 4.8 presenterer vi noen tiltak som kan gjøre virksomheten bedre rustet mot et bortfall av domenenavn.

4.1 KARTLEGG RISIKOEN

Mange virksomheter vurderer ikke hvor avhengige de er av domenenavn, i sine eksisterende risikovurderinger. Konsekvensen kan bli at en potensielt kritisk avhengighet ikke blir vurdert på en systematisk og god måte. Dette kan føre til at virksomheten ikke iverksetter nødvendige tiltak, noe som igjen kan få direkte påvirkning på virksomhetens måloppnåelse, enten det dreier seg om samfunnskritiske leveranser eller en positiv bunnlinje.

Spørsmål virksomheter bør stille seg:

- Hvordan kan vi gjennomføre en systematisk og god risikovurdering som inkluderer hvor kritisk internett generelt og domenenavn spesielt er for vår virksomhet?

Vi anbefaler at dere inkluderer en vurdering av hva som vil skje hvis sentrale domenenavn skulle falle bort, i deres eksisterende prosesser for risikostyring.

4.2 VURDER KRITIKALITETEN TIL DOMENENAVNENE

For det neste steget i risikoanalysen kan det være nyttig å ta i bruk en forenklet versjon av metoden for identifisering av kritisk infrastruktur og skjermingsverdige objekter, slik den er beskrevet i NOU 2006:6 *Når sikkerheten er viktigst*. Denne metoden hjelper dere å vurdere hvilken infrastruktur som må til for å opprettholde viktige leveranser. Metoden tar utgangspunkt i en kvalitativ vurdering av de tre kriteriene *avhengighet*, *alternativer* og *tett kobling* som til sammen indikerer at en infrastruktur er kritisk[3].

Under går vi nærmere inn på disse tre kriteriene og foreslår noen spørsmål som virksomheten kan stille seg. Listen over spørsmål er ikke uttømmende og må tilpasses situasjonen til hver enkelt virksomhet.

[3] NOU 2006:6 Når sikkerheten er viktigst, side 33

Avhengighet

Hvis virksomheten ikke er avhengig av domenenavn, vil det heller ikke oppstå noen uønskede konsekvenser ved et bortfall av disse, og domenenavn er dermed ikke kritisk. I tillegg til å kartlegge åpenbare avhengigheter bør dere også tenke over om det kan være noen skjulte avhengigheter som dere ikke tenker over til daglig. Det er viktig å kartlegge hele verdikjeden og ha en forståelse av hvordan tjenesten produseres.

Spørsmål virksomheter bør stille seg:

- Hvor avhengig er vi av domenenavn i vår interne kommunikasjon?
- Bruker vi DNS-oppslag når vi sender e-post internt?
- Bruker vi logistikk- eller fagsystemer som kommuniserer ved hjelp av DNS, eller har vi automatiserte systemer som kommuniserer seg imellom ved hjelp av DNS?

- Hvor avhengig er vi av domenenavn i vår kommunikasjon med andre virksomheter?
- Innhenter vi informasjon fra eller rapporterer vi til andre virksomheter over internett?
- Samarbeider vi med eller har vi underleverandører på våre viktigste leveranser?
- Har vi automatiserte systemer som kommuniserer med andre virksomheter ved hjelp av DNS?

- Hvor avhengig er vi av domenenavn i vår kommunikasjon mot publikum?
- Er det å kommunisere med publikum over internett en sentral del av vår virksomhet (netthandel, banktjenester, digitale medier)?
- Er vi på andre måter avhengig av å få informasjon ut til publikum over internett (markedsføring, tjenesteavbrudd, kundehenvendelser)?

Alternativer

Siden de aller fleste virksomheter er avhengige av domenenavn i en normalsituasjon, vil kritikaliteten av et bortfall av domenenavn i stor grad bestemmes av hvor gode alternativer som finnes til denne funksjonaliteten, og i hvor stor grad de negative konsekvensene ved et bortfall kan begrenses.

Alternativer påvirker kritikalitet ved at de kan gi virksomheten større mulighet til å påvirke utfallet av en hendelse. Hvis funksjonen til domenenavnene kan erstattes, vil påvirkningsmuligheten være større og kritikaliteten lavere.

Spørsmål virksomheter bør stille seg:

- Bruker vi andre systemer i en krise (krisehåndteringsverktøy, varslingskanaler e.l.)? Kan noen av disse være avhengig av domenenavn for å fungere?
- Hva med beredskapsplaner? Er disse tilgjengelige lokalt, eller er de på internett?
- Kan vi bruke alternative kommunikasjonsløsninger som telefon eller fysisk oppmøte?
- Kan vi utføre prosessene våre manuelt?
- Kan vi opprette direkte linjer som ikke er avhengig av domenenavn, til de nærmeste samarbeidspartnerne våre?

Tett kobling

Tett kobling påvirker også kritikalitet gjennom virksomhetens påvirkningsmulighet. Hvis alvorlige konsekvenser inntreffer raskt, vil påvirkningsmuligheten være mindre og kritikaliteten høyere. Samtidig blir kritikaliteten høyere hvis flere leveranser påvirkes samtidig, uavhengig av hvor alvorlig det er at enkeltleveranser blir påvirket.

Spørsmål virksomheter bør stille seg:

- Hvor lenge kan *.no* eller andre domenenavn falle bort før det påvirker oss?
- Hvor lang tid vil det ta fra domenenavn faller bort, til det påvirker leveransene våre? Har vi mulighet til å påvirke eventuelle konsekvenser i dette tidsrommet?
- Vil et bortfall av domenenavn kun ramme enkelte deler av virksomheten, eller er det mange deler som vil bli rammet samtidig?

4.3 KARTLEGG HVEM VIRKSOMHETEN ER AVHENGIG AV

Med stadig flere systemer som må kommunisere med hverandre på tvers av virksomheter, øker avhengigheten av internett generelt og domenenavn spesielt. Samtidig vil det være mer utfordrende å sørge for nødvendige kommunikasjonslinjer og tilpasninger i en krise i tilfeller der en virksomhet kun har eierskap til deler av infrastrukturen som den er avhengig av i sine leveranser. Det er altså helt sentralt å vite hvem dere er avhengig av. Dette gjelder særlig hvis dere er en del av en kompleks verdikjede.

Spørsmål virksomheter bør stille seg:

- Har vi samarbeidspartnere eller andre som vi er avhengig av, på våre viktigste leveranser? Kan det finnes skjulte avhengigheter eller komplekse verdikjeder som bør nøstes opp?
- Har vi noen samarbeidspartnere som er så sentrale for å ivareta de viktigste leveransene våre at vi bør legge planer for kommunikasjon som ikke er avhengig av domenenavn?
- Kan andre virksomheter være avhengige av våre domenenavn?

Vi anbefaler alle virksomheter å kartlegge hvem dere samarbeider med, og vurdere om det er noen av disse samarbeidspartnerne som er så sentrale for virksomhetens viktigste leveranser at dere bør legge planer for hvordan dere kan kommunisere uten domenenavn.

4.4 FÅ OVERSIKT OVER ABONNEMENTSFORHOLDENE

I dette kapitlet beskriver vi hvordan du skaffer deg oversikt over abonnementsforholdene for *.no*. Bruker du andre toppdomener må du undersøke hvordan registreringsordningen er hos dem. For *.no* er domeneforhandlerne Norids kanal for salg av domenenavn og oppfølging av abonnentene. Det er domeneforhandleren som bestiller abonnementet på domenenavnet hos Norid, og som hjelper domeneabonnentene med endringer som gjelder abonnementet, for eksempel oppdatering av kontaktinformasjon. Forhandleren sørger for at abonnementet forlenges så lenge domeneabonnenten ønsker å ha det.

De fleste forhandlere tilbyr forskjellige tjenester knyttet til bruk av domenenavnet, blant annet webhotell, e-post og verktøy for å lage websider, men det er også mulig å sette opp disse tjenestene selv eller kjøpe dem fra en tredjepartsleverandør.

Det er viktig å merke seg at det som Norid tilbyr via en domeneforhandler kun er et abonnement på selve domenenavnet. Norid er ikke involvert i opprettelsen av eventuelle ekstratjenester som nettsider eller e-post – dette avtales mellom domeneabonnenten og den som leverer tjenesten, i hvert enkelt tilfelle. Dersom virksomheten har bygget viktige tjenester med utgangspunkt i sitt domenenavn, er det ekstra viktig å velge en domeneforhandler og/eller tjenesteleverandør som tilbyr et tilstrekkelig høyt servicenivå.

Norid anbefaler at man velger en domeneforhandler som gir tydelige, skriftlige vilkår for kundeforholdet. Avtalen bør minimum omfatte forhold som priser, responstid, mangler ved tjenesten og oppsigelse av avtalen. Med en god avtale er det lettere for virksomheten å komme med krav hvis det skulle oppstå problemer.

Både Norid og domeneforhandlere sender ut informasjon om abonnementet ditt. Det er derfor viktig at e-postadressen som dere har registrert hos Norid og domeneforhandleren, er riktig. I verste fall kan domeneabonnementet deres blir slettet hvis dere ikke reagerer på et varsel.

Spørsmål virksomheter bør stille seg:

- Har vi oversikt over hvem som er domeneforhandler for vårt domenenavn, hva som er registrert informasjon om vår virksomhet, og hvem hos oss som kan ta beslutninger knyttet til dette domenenavnet?
- Har vi oversikt over hvem som leverer de ulike tjenestene (webhotell, e-post, verktøy) til oss?
- Har vi sikret oss en avtale med en domeneforhandler/tjenesteleverandør som gjenspeiler hvor viktige tjenestene vi har bygget på domenenavnet, er? Dette kan være krav til responstid, krav til robusthet, reserveløsninger mm.
- Har vi riktig e-postadresse knyttet til våre domenenavn?

4.5 LAG KONTINUITETSPLANER

Virksomheter som har laget kontinuitetsplaner og planlagt for uønskede hendelser, klarer seg bedre gjennom kriser og kommer raskere tilbake til normal drift. Dette fordi kontinuitetsplanlegging bidrar til å sikre virksomhetens evne til å opprettholde driften på et akseptabelt nivå selv under ekstraordinære hendelser. En kontinuitetsplan vil derfor redusere sannsynligheten for at viktige leveranser enten blir forsinkede eller mangelfulle.

En sentral del av en kontinuitetsplan er en vurdering av hvilke alternativer virksomheten har tilgjengelig dersom sentrale verdier eller innsatsfaktorer skulle falle bort. For noen virksomheter vil domenenavnet eller tilgjengelighet til DNS være spesielt viktig, og de trenger å planlegge ut i fra hvor gode alternative løsninger de har eller kan etablere.

Flere av reserveløsningene vil kunne fungere internt i en virksomhet, men hvis dere er avhengig av å kommunisere med eksterne, blir bildet straks mer komplisert. En del av de mer manuelle løsningene kan fort bli veldig ressurskrevende. Hvor godt et alternativ vil fungere, er dermed avhengig av virksomhetens forretningsmodell og den funksjonen domenenavn er satt til å fylle.

Spørsmål virksomheter bør stille seg:

- Hvilke alternative løsninger kan vi iverksette hvis domenenavn vi benytter, faller bort?
- Hvor ressurskrevende vil de alternative løsningene være, og hvor lenge har vi kapasitet til å opprettholde disse løsningene?

I kontinuitetsplanleggingen bør dere vurdere hva virksomheten tåler av nedetid, hvordan dere skal sikre fortsatt drift, og hvordan dere skal opprettholde kvaliteten på driften dersom sentrale domenenavn skulle falle bort. For en nærmere beskrivelse av hvordan dere kan jobbe med kontinuitetsplanlegging, anbefaler vi DSBs veileder i kontinuitetsplanlegging.[4] Denne veilederen fokuserer på temaet høyt personellfravær, men metoden kan overføres til andre temaer.

4.6 LAG BEREDSKAPSPLANER

Ved hjelp av gode beredskapsplaner vil dere være i forkant av uønskede hendelser når de inntreffer, og vil på best mulig måte kunne håndtere hendelsen for å begrense skadevirkningen. Bortfall av domenenavn er et scenario som i liten grad inkluderes i virksomheters beredskapsplaner i dag.

Dere kan gjerne lage generelle beredskapsplaner og tiltakskort, men vi anbefaler å inkludere et eget scenario for bortfall av domenenavn eller oppslag i DNS. Tiltakskortet som går spesifikt på dette scenarioet, bør inneholde en strategi for å håndtere bortfallet, inkludert informasjon om hvem i organisasjonen som har ulike roller og ansvar under hendelsen, hvilke tiltak som skal iverksettes, og i hvilken rekkefølge.

Enkelte generelle beredskapstiltak som dere definerer, kan også være avhengig av at domenenavn er tilgjengelig. For eksempel kan etablerte varslings- og rapporteringskanaler via intranett eller e-post bli utilgjengelige ved et bortfall av domenenavn.

Spørsmål virksomheter bør stille seg:

- Har vi inkludert bortfall av domenenavn som et scenario i vår beredskapsplan, og har vi egnede tiltakskort?
- Er noen av våre andre beredskapstiltak avhengig av domenenavn?

[4] Direktoratet for samfunnssikkerhet og beredskap (2009, oppdatert i 2020). Veileder i kontinuitetsplanlegging – Opprettholdelse av kritiske funksjoner ved høyt personellfravær.

4.7 GJENNOMFØR ØVELSER

Øvelser er et viktig virkemiddel for å øke krisehåndteringskompetansen i en virksomhet og styrke samarbeidet med andre aktører. Ved å øve på å bruke beredskaps- og kontinuitetsplanene får de involverte virksomhetene kartlagt hvor godt tiltakene de har planlagt, vil fungere i praksis. Øvelser bidrar også til økt bevissthet og kompetanseheving på både individnivå, virksomhetsnivå og på tvers av virksomheter dersom det er flere virksomheter involvert i øvelsen. Aktører og virksomheter med ansvar for kritiske samfunnsfunksjoner som er avhengige av fungerende elektronisk kommunikasjon, har i tillegg et eget ansvar for å gjennomføre øvelser på området. Både departementene og underliggende etater, samt aktører på regionalt og lokalt nivå, skal gjennomføre nødvendige øvelser.

Beredskap som fungerer godt internt i en virksomhet, fungerer ikke nødvendigvis like godt mellom virksomheter som operer sammen i komplekse verdikjeder. Det er derfor viktig å både øve på egne planer og å øve sammen med andre aktører i verdikjeden, slik at utfordringer på tvers av virksomhetene blir belyst.

DSB har gitt ut en veileder i planlegging, gjennomføring og evaluering av øvelser,[5] som gir en grunnleggende introduksjon til øvelser og rammeverk for hvordan dere kan utføre øvelser.

Spørsmål virksomheter bør stille seg:

- Har vi øvd på scenarioet som går på bortfall av domenenavn, og har vi inkludert våre sentrale samarbeidspartnere i øvelsen?
- Har virksomheten evaluert og justert kontinuitets- og beredskapsplanene etter erfaring fra øvelsene?

[5] Direktoratet for samfunnssikkerhet og beredskap (2006). Veileder i planlegging, gjennomføring og evaluering av øvelser. Grunnbok: Introduksjon og prinsipper

4.8 RISIKOREDUSERENDE TILTAK

Før dere vurderer å sette inn tiltak, er det viktig at dere definerer problemet som skal løses. Tiltakene dere lander på, vil være svært forskjellige om dere vil sikre at et internt overvåkingssystem skal kunne nå et internt produksjonssystem, eller om dere vil sikre at publikum skal kunne sende e-post til en gitt kontaktadresse.

Domenenavnsystemet har som fordel at informasjon om hvordan man når en tjeneste, kan vedlikeholdes på ett sted, og så tar DNS seg av å spre denne informasjonen til klientene som trenger informasjonen.

Skal dere oppnå en tilsvarende robusthet med andre løsninger, må samme informasjon registreres og vedlikeholde flere steder, enten som navn/IP-adressepar på klientene eller i form av IP-adresser for navnetjenere som dere skal hente sonedata fra. Hvis dere ønsker å endre på noe av dette, så må det gjøres koordinert med alle brukere av denne informasjonen. Dette gjør at alle endringer blir mer omstendelige, og hvis noe blir glemt, vil man likevel kunne oppleve feil med tjenestene.

Alle grep dere tar for å sikre dere mot utfall i DNS, må dermed veies opp mot ulemper og risiko som dere påfører dere selv og samarbeidspartnerne deres. Dersom dere velger å ta i bruk noen av disse teknikkene, må dere også vurdere om dere er best tjent med å ha dette som en permanent del av eget driftsregime, eller om det er et tiltak dere har forberedt og kan ta i bruk i skarpe situasjoner.

Vi kan dele de tekniske tiltakene inn i to hovedkategorier:

1. tiltak som fjerner eller reduserer avhengigheten av DNS-oppslag
2. tiltak som øker robustheten og tilgjengeligheten av DNS-tjenesten for de domenenavnene som er viktige for virksomheten

Tiltakskategori 1 – Fjerne behovet for eksterne DNS-oppslag

Et mulig tiltak for å unngå DNS-oppslag er å i stedet eller i tillegg bruke mekanismer for å angi IP-adressen til en tjeneste. For noen tjenester er det mulig å angi IP-adressen der tjenesten kjører, direkte i konfigurasjonen til klientprogramvaren som skal bruke tjenesten. Klienten vil i slike tilfeller ikke være avhengig av DNS for å kunne bruke tjenesten. Dette er ikke alltid mulig for alle tjenester, og dersom IP-adressen konfigureres inn mange steder, blir det vanskelig å flytte tjenesten til en annen adresse om det skulle være nødvendig. Men i liten skala kan dette være en nyttig teknikk.

Mange systemer støtter alternative måter å vedlikeholde navn-til-adresse-informasjon på. Dette kan være et alternativ til å angi IP-adresser direkte. Dere kan da bygge en virksomhetsintern infrastruktur for å distribuere denne informasjonen.

Tiltakskategori 2 – Øke robustheten og tilgjengeligheten av DNS-oppslag

Dere kan velge å implementere en DNS-tjeneste internt i virksomheten, som kan fungere uten eksterne avhengigheter. Mange virksomheter har dette allerede i form av nettverksteknologi for kontorstøttesystemer. Med en intern DNS-tjeneste med egne domenenavn konfigurert vil virksomhetens klienter gjøre oppslag uten å være avhengig av ekstern DNS.

For tjenester som er avhengige av andre virksomheters domenenavn, kan dere vurdere å etablere en permanent kobling mellom navnetjenerne til virksomhetene, der dere kontinuerlig overfører sonen som inneholder data om de kritiske tjenestene til den interne DNS-tjenesten. Dere kan etablere denne løsningen på permanent basis, eller dere kan sørge for at tiltakene kan iverksettes om situasjonen skulle kreve det. Hvordan dere velger å

organisere dette, vil måtte bero på en konkret risikovurdering og hvor langvarige utfall dere tåler for de forskjellige tjenestene.

Dette må dere tenke over før dere iverksetter tekniske tiltak

Felles for løsningene over er at dere må være i stand til å påvirke konfigurasjonen på klientsystemene. Disse tiltakene passer derfor best for kommunikasjon internt i virksomheten. De kan også være aktuelle der virksomheter samarbeider tett.

Spørsmål virksomheter bør stille seg:

- Er tiltakene nevnt over relevante for den kritiske tjenesten?
- Kan virksomheten styre konfigurasjonen på eget utstyr som skal bruke tjenesten?
- Har virksomhetene kapasitet og driftsapparat til å vedlikeholde og distribuere adresseinformasjon om tjenesten til sine klienter?
- Har virksomhetene kapasitet og driftsapparat til å vedlikeholde og distribuere adresseinformasjon om tjenesten til andre virksomheter/samarbeidspartnere?
- Skal tiltakene være en permanent del av eget driftsregime, eller være en del av bedriftens beredskapsplaner?
- Vil de risikoreduserende tiltakene fungere etter hensikten, eller vil dere øke risikoen og kompleksiteten i andre systemer slik at tiltakene ikke gir en netto gevinst?

5 SJEKKLISTE

☐ Vi har gjennomført en systematisk og god risikovurdering som inkluderer hvor kritisk internett generelt og domenenavn spesielt er for vår virksomhet.

☐ Vi vet hvilke andre virksomheter vi er avhengige av – både samarbeidspartnere og leverandører.

☐ Vi vet hvilke alternative løsninger vi kan iverksette dersom *.no* faller bort. Vi vet også hvor ressurskrevende disse vil være, og hvor lenge vi har kapasitet til å opprettholde disse løsningene.

☐ Vi har inkludert bortfall av domenenavn som et scenario i vår beredskapsplan, og vi har egnede tiltakskort.

☐ Vi har øvd på scenarioet som går på bortfall av domenenavn, og vi har inkludert våre avhengighetsforhold i øvelsen.

☐ Vi har angitt sentrale IP-adresser internt.

☐ Vi har begrenset behovet for eksterne DNS-oppslag så langt det er hensiktsmessig.

☐ Vi har etablert en intern DNS-infrastruktur der det er hensiktsmessig.

☐ Vi har etablert nødvendige tekniske tiltak ut mot andre virksomheter vi er avhengig av.

☐ Vi har sjekket at vi har registrert riktig e-postadresse hos Norid og domeneforhandlerne for de domeneabonnementene vi har under *.no*.[6]

☐ Vi har avklart hvem som har ansvar for hvilke domenenavn hos oss.

[6] https://www.norid.no/no/domeneoppslag/