STYRET FOR MOVAR IKS **NR. 6/2018**

Medlemmene i styret for MOVAR IKS innkalles til møte:

TORSDSAG 27. SEPTEMBER 2018 KL. 08:00
I MOVARs ADMINISTRASJONS LOKALER, HUGGENES

PROTOKOLL FRA STYREMØTET 31. AUAGUST 2018

Til behandling:

SAK NR. 9/2018
BEHANDLINGSRUTINE FOR VARSLING I MOVAR IKS
(UTSATT SAK)

SAK NR. 10/2018
BUDSJETT 2019 – ØKONOMIPLAN 2019 - 2022

O-SAK NR. 24/2018
DIREKTØRENS ORIENTERING
(Presenteres på møtet)

O-SAK NR. 25/2018
ORIENTERING OM INFORMASJONSSIKKERHET KNYTTET TIL FAGSYSTEMET YSI PA FRA NORCONSULT INFORMASJONSSYSTEMER AS

Rygge, 20. september 2018

Brit G. Plassen (sign.)
Adm. koordinator

MOVAR IKS STYREMØTE NR. 5 2018

Fredag 31. august 2018 holdt styret for MOVAR IKS møte i selskapets administrasjonslokaler på Huggenes.

8 medlemmer til stede av 8:

Av medlemmene møtte:	Ketil Reed Aasgaard, leder Nils-Anders Søyland, nestleder Hege Solberg Sandtrø Katrine Kerr Gammelsrød Aud Helen Wernberg Øyen Steinar Roos Tore Fredriksen Ole Martin Almvik
Varamedlem med fast oppmøte:	Bjørn Amundsen
Dessuten møtte:	Johnny Sundby, MOVAR IKS Kaj-Werner Grimen, MOVAR IKS Rolf-Ivar Buerengen, MOVAR IKS Rune Larsen, MOVAR IKS/MIB Freddy Tangen, MOVAR IKS Merete Ruud Tuskin, MOVAR IKS Jon Jerry Tveter, MOVAR IKS

Både leder og nestleder av representantskapet hadde meldt forfall til møtet.

Det var ingen innvendinger til innkallingen eller til sakslisten.
Det ble avtalt å bytte rekkefølge på behandling av O-sak 22/2018 og O-sak 13/2018.

Protokollen fra møte 15. juni ble enstemmig godkjent.

STYRESAK NR. 7/2018

FORESPØRSEL FRA MOSSEFOSSENS VENNER TIL MOVAR IKS

Direktørens forslag til vedtak:

1. MOVAR avstår fra å tre inn som avtalepart på vegne av Mossefossens Venner, i avtalen som fordrer istandsetting og vedlikehold av det gamle vannverket i fossen, jfr. foreningens forespørsel.
2. Mossefossens Venner oppfordres til å komme tilbake med en plan for istandsetting, finansiering og bruk av det gamle vannverket, og en konkret forespørsel om støtte.

Behandling:
Saken ble debattert og styret mente dette ikke var et prosjekt som vedrørte samtlige eier-kommuner, men var et anliggende for kun én eierkommune og ett privat eiendomsselskap. Styret ønsket å gi en klar tilbakemelding på henvendelsen og før votering foreslo styret å stryke pkt. 2 i forslag til vedtak.
Votering:
Det ble votert over pkt. 1 og dette ble enstemmig vedtatt. Det ble også under avstemningen enstemmig besluttet å stryke pkt. 2.
Vedtak:
MOVAR avstår fra å tre inn som avtalepart på vegne av Mossefossens Venner, i avtalen som fordrer istandsetting og vedlikehold av det gamle vannverket i fossen, jfr. foreningens forespørsel.

STYRESAK NR. 8/2018
REVIDERT MØTEPLAN FOR STYREMØTER I MOVAR IKS 2018

Direktørens forslag til vedtak:
Styret i MOVAR vedtar revidert møteplan for styremøtene i 2018.

Behandling:
Det ble bekreftet at dette kun gjaldt gjenstående møter i 2018, altså avtalte møter i september og november. Det kom frem at flere hadde utfordringer med å flytte allerede inngåtte avtaler.
Votering:
Det ble enstemmig besluttet å avholde styremøte i september til avtalt dato, og flytte møtet i november fra torsdag til fredag.
Vedtak:
Styremøte nr. 6/2018 avholdes som tidligere avtalt torsdag 27. september og styremøte 7/2018 flyttes til fredag 30. november.

STYRESAK NR. 9/2018
BEHANDLINGSRUTINE FOR VARSLING I MOVAR IKS

Direktørens forslag til vedtak:
Styret vedtar behandlingsrutine ved innkomne varsler i MOVAR IKS.

Behandling:
Adm. Direktør informerte om prosess frem til valgt løsning.
Tidlig i diskusjonen ble det avdekket at ikke fullstendig saksunderlag var distribuert til styret. Samtidig fremkom det at fagforening hadde synspunkter. Det ble besluttet å utsette saken, samt foreta avklaring med fagforeningene før ny behandling i styret.
Votering:
Det var enstemmig å utsette behandling av saken til neste møte.
Vedtak:
Saken ble utsatt og det ble følgelig ikke fattet noe vedtak.

O-SAK NR. 22/2018
REGNSKAPS- OG LIKVIDITETSSRAPPORTERING, INKL. PROGNOSE 2018
Økonomi- og administrasjonssjef orienterte om økonomien totalt og i de ulike sektorene pr. 31.05.2018, samt en oppdatert prognose for resultatet i 2018. En oversikt over likviditeten på samme tidspunkt ble også kommentert. Presentasjonen vedlegges protokollen.

O-SAK NR. 13/2018
DIREKTØRENS ORIENTERING MED SÆRLIG FOKUS PÅ BUDSJETTFORUTSETNINGER 2019
Adm. direktør oppdaterte styret på aktuelle prosesser og hendelser i selskapet og denne presentasjonen vedlegges protokollen. Budsjettforutsetninger for regnskapsåret 2019 inklusive mulige investeringer ble gjennomgått med styret, og dette legges ut på styrets portal i Admincontrol.

O-SAK NR. 23/2018
AVSLUTNING PROSJEKT 551 – SAP – DRENERING OG SLUK PÅ LAGERPLASS FOR HUSHOLDNINGSRNOVASJON

Direktørens forslag til vedtak:
Saken tas til orientering.
Behandling:
Det var ikke behov for informasjon utover fremlagte saksdokument.
Votering:
Innstilling enstemmig vedtatt.
Vedtak:
Saken tas til orientering**.**

EVENTUELT

Aud Helen Wernberg Øyen orienterte styret om sin bacheloroppgave som omhandler MOVAR og ledelse, og at hun derfor periodevis vil være i dialog med ansatte ved bedriften også utenom styremøtene.

Mer var ikke til behandling og møtet ble hevet kl. *11:10*.

Ketil Reed Aasgaard Leder	Nils-Anders Søyland
Aud Helen Wernberg Øyen	Hege Solberg Sandtrø
Katrine Kerr Gammelsrød	Steinar Roos
Tore Fredriksen	Ole Martin Almvik

DIREKTØRENS ORIENTERING 31.8.2018

Johnny Sundby, Adm. Direktør MOVAR IKS

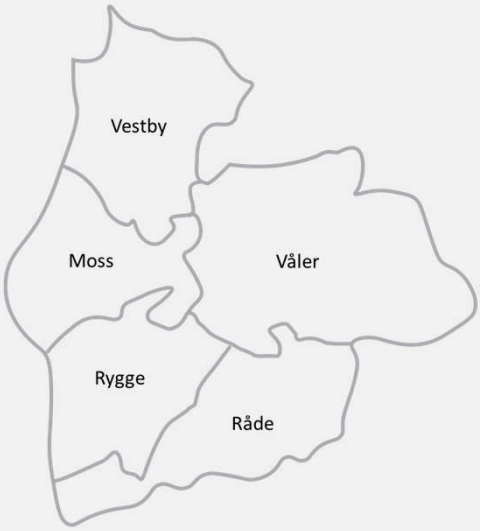
MOVAR

STATUS STYRESAKER:

Nummer	Tittel	Oppsummert vedtak	Status	Ansvar/frist
S-sak 12/15	Vestby gjenvinningsstasjon – Vurdering	Dialog med Vestby kommune for å finne løsninger som totalt sett er bedre enn dagens.	Diskutert i budsjettmøte med Rådmann i Vestby. Notat oversendt Vestby kommune, men tilbakemelding om at de ønsker å avvente.	Avventer Vestby kommune 2018?
~~S-sak 9/17~~	~~ROS-analyse reservekraft Vansjø Vannverk~~	~~Administrasjonen utreder mulighetene for alternative strømforsyning basert på reservekraft~~	~~Innarbeides i budsjettprosess 2018-2021.~~	~~ADM Sept. 2017 Prosjektet flyttes til 2019 pga kapasitet, men data som grunnlag for prosjektet fremskaffes ila 2018.~~
S-sak 10/17 og S-sak 3/18	Fremtidig avløpsløsninger	Søke utsettelse/harmonisering av krav FRA/KRA. KRA overføres til FRA. Søke å finne løsninger på slam.	Søknad innvilget, jfr. O-sak 9/18 Milepælsplanen følges opp I prosjektet.	ADM fortløpende.
S-sak 6/18	Evaluering av bereskapsøvelse	Adm. innarbeider sektorovergripende hendelser som en del av dagens beredskapsplaner. Styret ønsker å få fremlagt en sak om mulig fullmakt for Adm./styret ved krise-/beredskapssituasjoner.	Ikke påbegynt. Tas revisjon av beredskapsplanene. Tenkes presentert i styremøtet i sept. eller November.	Forventet oppstart høst 2018 Adm. Høst 2018
S-sak 7-18	Revidert styreinstruks	- Ta inn stedfortreder ved forfall fra styreleder eller nestleder ved årssamtale Adm. Direktør. - Styrets fullmakt ved kriser (se sak 6-18)	Sees i sammenheng med sak 6-18	Adm. Høst 2018

EIERSAMLING JELØY RADIO JUNI 2018

- Målsetning fra administrasjonen:
  - Gi deltakerne økt innsikt virksomheten, og ikke minst den store prosjektporteføljen.
  - Styret og administrasjonen ønsker å treffe og bli bedre kjent med eierne/rep.skapsmedlemmene.
- Resultat:
  - Positive tilbakemelding, som bekrefter at deltakerne har blitt bedre kjent med selskapet.
  - Ingen konkrete oppfølgningspunkter, foruten ønske om å gjenta dette.
  - Programmet var tett, men fra administrasjonens side opplevde vi å bli litt bedre kjent med eierrepresentantene som deltok.
  - Hva med dere i styret?



MOVAR

KORT ORIENTERING

- Ledningen på Fuglevik RA fløt opp igjen i sommer – Behov for en grundigere kontroll.
- IT organiseres under HR- og kommunikasjon fra 1.9.
- Vestby kommune har vedtatt gjennomføring av forprosjekt for å vurdere renovasjonsløsninger for sentrumsplanen, også Avfallssug.
- Samtlige områder har vært preget arbeid med budsjett siden i juni.

MOVAR

BYTTE AV REFERENT

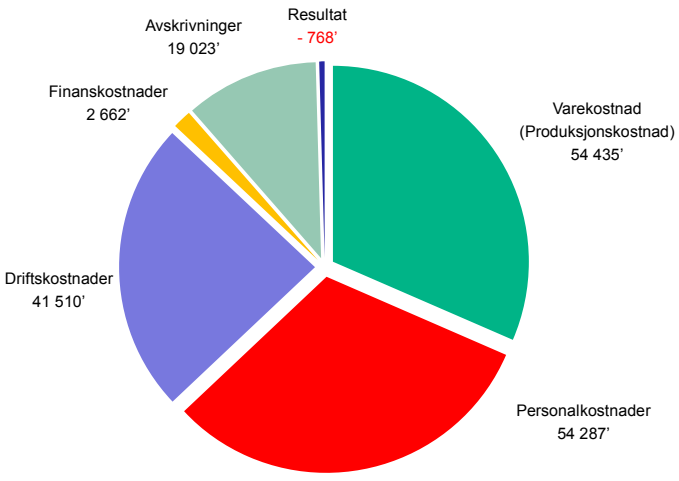
REGNSKAP 31.07.2018

Samt prognose for 2018

MOVAR

MOVAR IKS TOTALT PR.31.07.18

OMSETNING INKL. INTERNFAKTURERING KR 171 149'



MOVAR

LIKVIDITET PR.31.07.18

TALL I NOK 1000

	Pr. 31.07.18	Pr. 01.01.18
Innestående på bank (Inklusive skattetrekksmidler, eks etterbruksfond)	**31 684**	**42 223**
Kortsiktige fordringer	**10 163**	**25 601**
Påløpt prosjektkostnader i forhold til opptatt byggelån.	**2 045**	**4 840**
SUM	**43 892**	**72 664**
Kortsiktig gjeld , inkl. leverandører, FP og off. avg.	**20 562**	**53 796**
Arbeidskapital	**23 330**	**18 868**

Likviditeten har vært tilfredsstillende så langt i 2018 og arbeidskapitalen er der den har vært i tidligere oppstillinger.

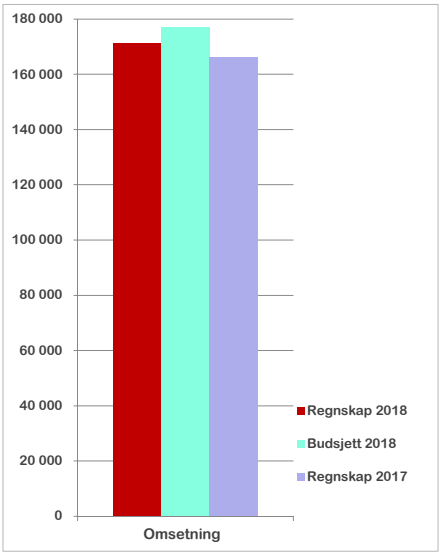
Alle lån som ble bevilget for 2017 er hentet inn, inklusive de som ble vedtatt som eget punkt om 2017 til budsjettet 2018.
Man har startet opplåning for noen av prosjektene som ble vedtatt startet og belånt for 2018, og hvor det har kommet prosjektkostnader av betydning.
Forutsatt at driften av de ulike sektorene går som budsjettert skal det være stram med tilfredsstillende likviditet i hele 2018.
Vi frigjorde en plasseringskonto vi har i KLP med virkning fra 10. juli som reserve gjennom sommeren. Det ble ikke behov for å benytte denne, og den vil settes inn med 30-dagers sperring i september/oktober etter fakturering av husholdningsrenovasjon for 2. halvår.

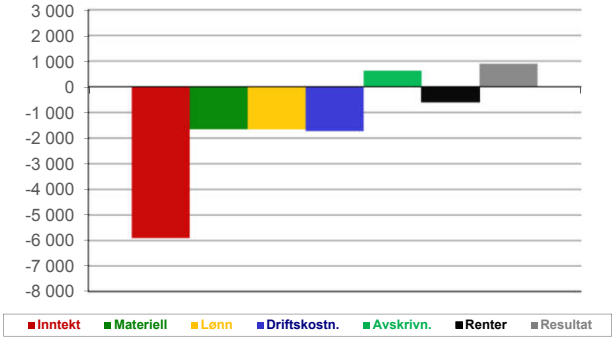
Selvkostfondene er pr. 01.01.18 på kr. 16 993, ned fra 26 541' pr. 01.01.17 og 36 901' pr. 01.01.16.

MOVAR

MOVAR IKS TOTALT

RESULTAT 31.07.18 I FORHOLD TIL BUDSJETT





Resultat 31.07.18	Prognose 2018	Budsjett 2018
- 768' (underskudd)	- 6 000' - - 7 500' (underskudd)	- 5 761' (underskudd)

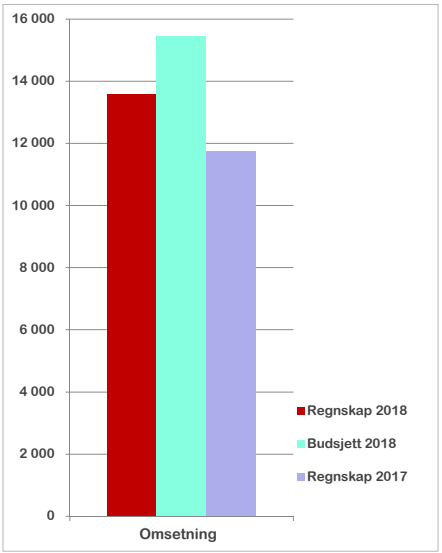
MOVAR

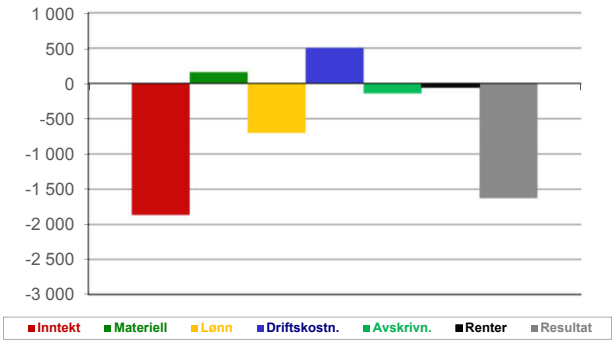
MOVAR IKS TOTALT

- Omsetning tydelig under budsjett, og Avløp er området med størst avvik.
- Totalt sett ikke så ulikt regnskapet pr. 31.07.17
- Periodiserings«problematikk», dvs at vi tar kostnaden først når vi mottar kravet.
- Ingen uventede hendelser utover det som et selskap av vår størrelse må påregne.

ADMINISTRASJON OG TEKNISK AVDELING

RESULTAT 31.07.18 I FORHOLD TIL BUDSJETT





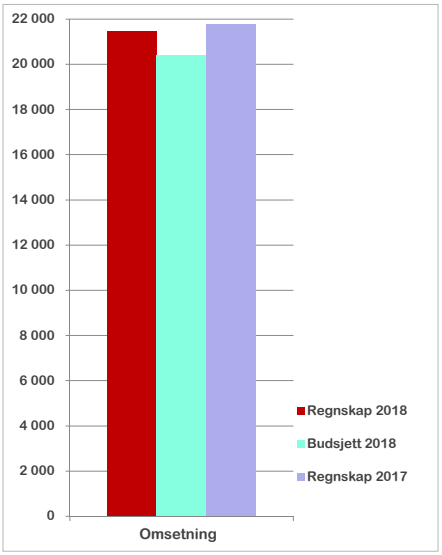
Resultat 31.07.18	Prognose 2018	Budsjett 2018
- 622' (underskudd)	350' (overskudd)	350' (overskudd)

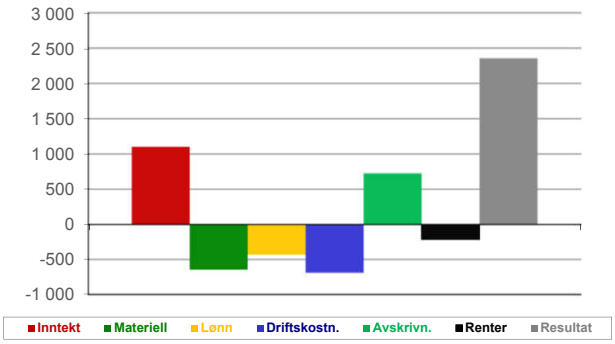
ADMINISTRASJON OG TEKNISK AVDELING

- Teknisk Avd faktureres samlet senere (Avventer en rasjonell rutine)
- (bl.a. ca 1 mill. til VV)
- Sykefravær med betydelige refusjoner både i avd 10 og i 11, uten at vakanser er dekket opp med innleie av personell.
- Periodiserings«problematikk», spesielt synlig på IT-lisenser.
- Avskrivninger lavere enn budsjett grunnet at adm.bygget er overflyttet til avd 20, Vansjø Vannverk. Ble iverksatt i årsoppgjøret, dvs etter at budsjett 2018 var vedtatt. («Betaler» husleie).

MOVAR

VANSJØ VANNVERK
RESULTAT 31.07.18 I FORHOLD TIL BUDSJETT





Resultat 31.07.18	Prognose 2018	Budsjett 2018
553' (overskudd)	- 2 000' – 3 000' (underskudd)	- 3 689' (underskudd)

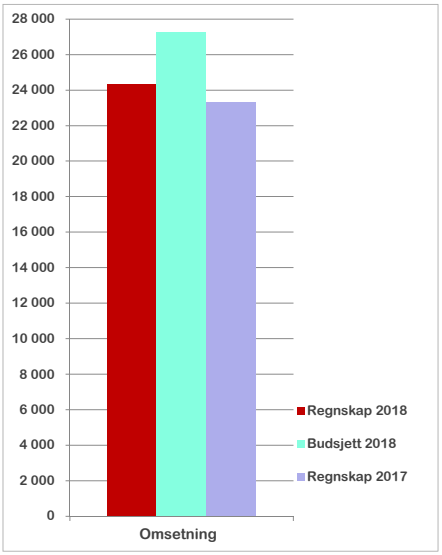
MOVAR

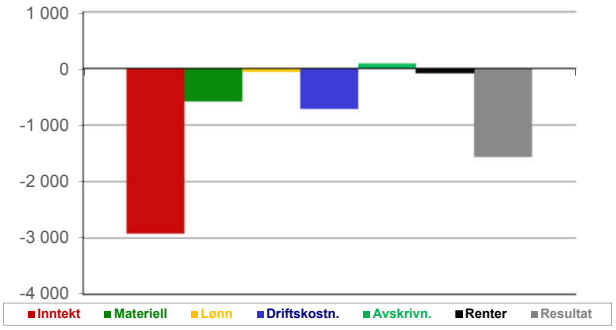
VANSJØ VANNVERK

- Omsetning; Moss og Råde (både beløp og i %) tydelig opp, de øvrige tett på budsjett.
- Leie av rørkapasitet av Moss ikke mottatt 1- 1,5 mill.
- Stor refusjon vedr sykepenger. Som styret er kjent med har det nå blitt ansatt ny operatør (intern ressurs).
- Venter intern faktura fra Teknisk på ca 1 mill.
- Avskrivninger for adm.bygget ikke budsjettert. Ble gjennomført etter budsjettet var vedtatt.(mottar «husleie»).

MOVAR

KAMBO, FUGLEVIK OG HESTEVOLD RA
RESULTAT 31.07.18 I FORHOLD TIL BUDSJETT





Resultat 31.07.18	Prognose 2018	Budsjett 2018
- 1 721' (underskudd)	- 3 000' – 4 000' (underskudd)	- 1 337' (underskudd)

MOVAR

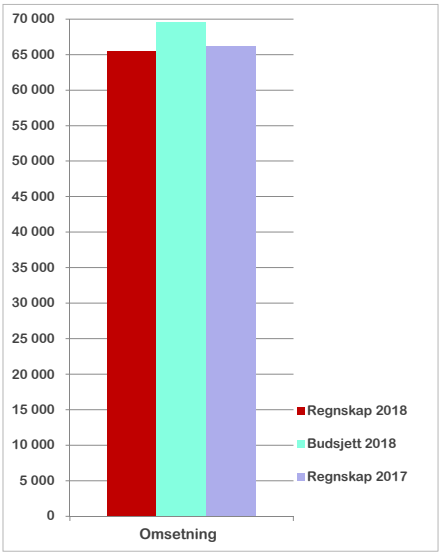
KAMBO, FUGLEVIK OG HESTEVOLD RA

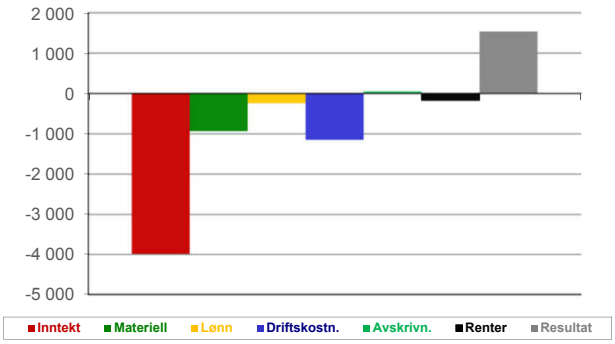
- Jevnt over lav tilrenning fra kommunene, men spesielt tydelig reduksjon fra Rygge. Kombinasjon av lite nedbør samt rør-sanering. (som betyr at overvann og ordinært avløpsvann blir adskilt ute i kommunen, og dermed er det lite av det vanlige regnvannet som kommer inn på anlegget.)
- Krav for leie av rørkapasitet hos Moss kommune ikke mottatt. Ca 500'.
- Driftskostnader; periodiserings«problematikk». (Tidspunkt for gjennomføring av vedlikehold.)
- Vi vil få et negativt selvkostfond for Avløp pr. 31.12.18. Ikke dramatisk, men slår negativt ut likviditetsmessig.

MOVAR

GJENBRUKSSTASJON OG RENOVASJON

RESULTAT 31.07.18 I FORHOLD TIL BUDSJETT





Resultat 31.07.18	Prognose 2018	Budsjett 2018
- 1 675' (underskudd)	- 500' (underskudd)	- 490' (underskudd)

MOVAR

GJENBRUKSSTASJON OG RENOVASJON

Ikke avregnet næringsvirksomhet (Movar Næring AS), noe som må foretas i etterkant.
Er dessuten svært variabel mhp tidspunkt for registrering av omsetning, da bl.a. mottak aske faktureres periodevis.
Mhp «ren» husholdningsrenovasjon følger vi rimelig tett på budsjett, med noe bedre resultat enn forventet, men unntak av Vestby som er jevnt med budsjett.

Kommunale renovasjonstjenester - Husholdningsrenovasjon

REGNSKAP 2018 (Prognose)

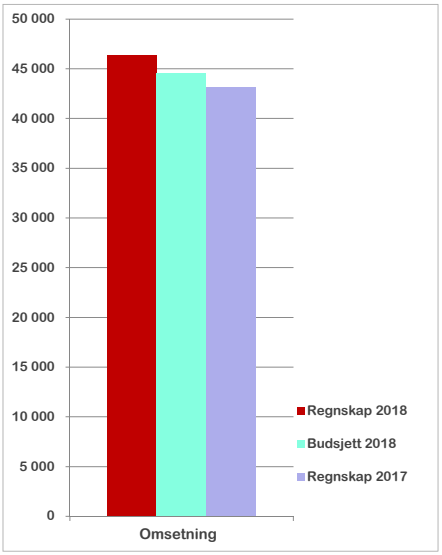
	Modell 2					
	Moss	*Rygge*	*Råde*	*Våler*	*Vestby*	*Vestby Gjenv.st.*
INNTEKTER						
Gebyrinntekter		15 950 000	7 680 000	5 370 000	17 100 000	490 000
Tjenesteinntekter	12 663 000					
Salgsinntekt. gjenvinning	1 830 000	790 000	410 000	230 000	900 000	100 000
Diverse inntekter	5 000	125 000	65 000	35 000	140 000	-
Sum inntekter	**14 498 000**	**16 865 000**	**8 155 000**	**5 635 000**	**18 140 000**	**590 000**
KOSTNADER						
Transport/tjenestekjøp/materialkost.	10 656 000	13 034 000	6 940 000	4 919 000	12 641 000	1 390 000
Andre driftskostnader, inkl. lønn	3 129 250	2 628 060	1 310 240	865 800	2 837 650	1 963 000
Avskrivninger/rentekostnader	165 915	548 512	192 445	184 260	608 906	-
Sum kostnader	**13 951 165**	**16 210 572**	**8 442 685**	**5 969 060**	**16 087 556**	**3 353 000**
Resultat 2018 (Prognose)	***546 835***	***654 428***	***-287 685***	***-334 060***	***2 052 444***	***-2 763 000***
Budsjettert resultat 2018	***0***	***307 000***	***-757 000***	***-185 000***	***1 871 000***	***-2 572 000***

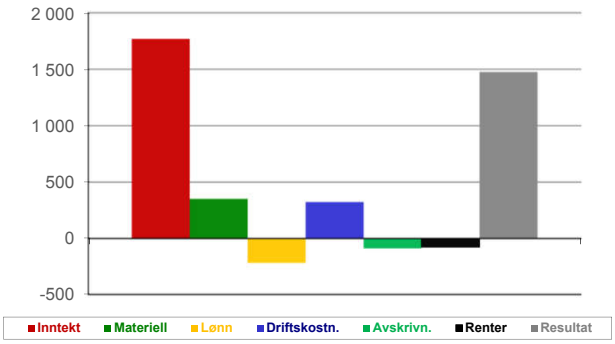
*) **Moss kommune** følger modell 2 - hvor bla. leveringskostnader av husholdningsavfallet belastes kommunen direkte med faktura fra MOVAR. Øvrige kostnader avregnes ved årets slutt med oppgjør mellom MOVAR og kommunen. Økonomien inngår i kommunenes egen selvkostregnskap.

MOVAR

MIB – MOSSEREGIONEN BRANN OG REDNING

RESULTAT 31.07.18 I FORHOLD TIL BUDSJETT





Resultat 31.07.18	Prognose 2018	Budsjett 2018
2 696' (overskudd)	- 595' (underskudd)	- 595' (underskudd)

MOVAR

MIB – MOSSEREGIONEN BRANN OG REDNING

- Leieinntekter ABØ v/oppsigelse, dvs for hele 2018 og 1. kvartal 2019.
- Fakturerer alarmtjenester selv, og har fakturert tom 3. kvartal (1,25' pr. kvartal)
- «Varekjøp»; høyere kostnad 110-sentralen i Ski («Brutto-føring», ref. alarmtjenesten ovenfor)
- Rene lønnskostnader høyere enn budsjett, spesielt i Beredskap grunnet høy aktivitet. Totalt i MIB (inkl. tilsyn/feiing) er det refusjon sykepenger på ca kr. 1 mill.
- God budsjettdisiplin på driftskostnader.

STYRET FOR MOVAR IKS

Styresak 9/2018

BEHANDLINGSRUTINE FOR VARSLING I MOVAR IKS

(UTSATT SAK)

Vedlagt:

- Behandlingsrutiner for innkomne varsler i MOVARs varslingstjeneste

Direktørens forslag til

V E D T A K :

Styret vedtar behandlingsrutine ved innkomne varsler i MOVAR IKS.

SAKSORIENTERING:

Styret hadde denne saken til behandling i sitt augustmøte, men saken ble utsatt, da vedlegget det vises til i saken ikke fulgte med. Administrasjonen vil først få beklage at dette ikke ble fanget opp.

Som styret er gjort kjent med tidligere, arbeider administrasjonen med å etablere et eksternt varslingsombud for virksomheten.

Dette har bl.a. sammenheng med endringen av arbeidsmiljøloven f.o.m. 1.7.2017, samt at ledergruppen ønsker en sikker og god behandling hvis saker varsles. For å få til dette ønsket ledergruppen å tilknytte seg en profesjonell aktør som kan bidra i behandlingen, samt et mottak av varsler som sikrer anonymitet hvis varsleren ønsker det.

BDO AS er valgt som leverandør, etter en tilbudskonkurranse.

Selskapets ledelse vil oppfordre organisasjonen til at varsling fortrinnsvis skjer til nærmeste leder og videre i linjen der det er mulig. Administrerende direktør, HR/kommunikasjonssjef og Hovedverneombud er definert som medlemmer i MOVARs interne varslingsmottak, som vil bli involvert dersom BDO mottar varsler gjeldende MOVAR.

Leverandøren tilbyr en digital, sikker varslingstjeneste. Denne sikrer anonymitet, personvern informasjonssikkerhet for varsleren.

Styrets leder vil være varslingsmottak og få ansvar for saksbehandlingen, ved inhabilitet for administrerende direktør, HR/kommunikasjonssjef og Hovedverneombud som følge av et varsel.

Administrasjonen legger med bakgrunn i dette frem de behandlingsrutinene som trer i kraft ved varsling for styret i MOVAR IKS.

Rygge, 22. august 2018

Johnny Sundby (sign.)
Adm. direktør

Rolf-Ivar Buerengen (sign.)
HR og kommunikasjonssjef

BEHANDLINGSRUTINER
for innkomne varsler i MOVARs varslingstjeneste

1. Innledning

Dette dokumentet beskriver behandlingsrutiner for varslingstjenesten hos MOVAR IKS (MOVAR). Dette dokumentet utgjør et tillegg til:

- MOVARs varslingsplakat

Disse behandlingsrutiner er referert til i ovenstående dokument.

2. Mottak av varsler

Det kan varsles via linjen, direkte til MOVARS eksterne varslingsmottak eller til selskapets interne varslingsmottak. De to sistnevnte benevnes heretter som «varslingsmottaket».

Varsler kan formidles til varslingsmottaket muntlig og skriftlig, fysisk eller elektronisk.

Det eksterne varslingsmottaket skal til enhver tid være en leverandør med kompetanse på håndtering av varslingssaker.

Det interne varslingsmottaket i MOVARs består av administrerende direktør, HR/kommunikasjonssjef og hovedverneombud. Dersom et varsel gjelder noen av disse funksjonene, vil det eksterne varslingsmottaket og styreleder i MOVAR IKS samlet overta funksjonen som varslingsmottak.

Det eksterne varslingsmottaket skal informere det interne varslingsmottaket i MOVAR senest dagen etter at et varsel er mottatt, med mindre det er åpenbart at varselet gjelder forhold som kan vente.

Alle innkomne meldinger/varsler registreres umiddelbart og tildeles et unikt saksnummer av det interne eller eksterne varslingsmottaket.

Varslingsmottaket

- har ansvar for saksbehandlingen av varselet gjennom hele prosessen, fra det mottas og til det er ferdig saksbehandlet med en rapport.
- skal påse at opplysningene i varslersaker behandles og oppbevares på betryggende måte i henhold til krav til personvern og informasjonssikkerhet. Informasjon om varsler som sendes per e-post skal sendes kryptert.
- skal påse at uvedkommende ikke får tilgang til informasjon fra varslersaker.

3. Undersøkelser

Varslingsmottaket gjennomfører undersøkelser om de faktiske forhold i ethvert varsel, innenfor de rammer som følger blant annet av arbeidsmiljøloven og personvernlovgivningen. I de innledende undersøkelsene skal varslingsmottaket:

- Vurdere hva varslet gjelder
- Vurdere varslets karakter, og alvorlighetsgrad
- Avklare om varselet er saklig begrunnet og om umiddelbare tiltak er påkrevet

- Klargjøre hvilke undersøkelser som kan utføres for ytterligere å belyse forholdet som varselet gjelder
- Utforme en kortfattet vurdering og anbefaling om hvordan saken skal håndteres av MOVAR

Saksbehandlingen skal omfatte de undersøkelser som er nødvendige for å avdekke de faktiske forhold det er varslet om, og avklare relevante konsekvenser av de faktiske forhold som avdekkes. I forbindelse med slike undersøkelser kan det være aktuelt å innhente dokumentasjon eller gjennomføre samtaler. Dersom varsler velger å være anonym, skal varslersaken allikevel saksbehandles så langt dette er mulig.

Søk og sikring av elektronisk lagret informasjon skal kun gjøres dersom det er saklig grunn til det, og dersom de lovbestemte vilkår for å gjennomføre slike undersøkelser er oppfylt.

Eventuell sikring og analyse av elektronisk lagret informasjon skal kun gjennomføres når vilkårene for slike undersøkelser er oppfylt. Ved undersøkelser av elektronisk lagret informasjon, skal det utarbeides rapport som viser hvordan elektronisk lagret materiale er sikret og hvilke undersøkelser som er gjort på elektronisk lagret informasjon.

4. Rapportering

Varslingsmottaket har ansvar for å utarbeide eller påse at det utarbeides rapport i enhver varslingssak. Formålet med rapporten er å ha et beslutningsgrunnlag for endelig avgjørelse i den enkelte varslersak.

Den skal normalt inneholde en gjengivelse av hovedpunktene i den informasjon som er mottatt fra varsler. Rapporten skal også angi eventuelle forslag til ytterligere undersøkelser som bør gjennomføres med bakgrunn i varselet, med mindre saken kan avsluttes uten ytterligere saksbehandling.

5. Avgjørelse i varslingssaker

MOVARs avgjørelser i varslingssaker, vil normalt gå ut på:

- Avslutning av saken
- Henvisning av saken til rette vedkommende hos MOVAR for videre håndtering
- Oversendelse av saken til offentlig kontrollmyndighet eller annen offentlig myndighet

Undersøkelser og avgjørelser i forbindelse med varslingssaker vil behandles i samarbeid med lokal ledelse, med mindre konkrete årsaker tilsier at dette ikke er hensiktsmessig.

6. Informasjon til varsler og den det er varslet om

Varslingsmottaket har ansvar for å informere varslere med kjent identitet om følgende forhold:

- Bekrefte at varselet er mottatt og registrert av varslingsmottaket.
- Resultatet av saken.

Varslingsmottaket skal også informere personen som det er varslet om, så langt dette kan gjøres uten å skade formålet med undersøkelsene. Informasjonen skal gis på en slik måte at varsleren ikke risikerer gjengjeldelse/ represalier.

7. Informasjonsplikt etter Personopplysningsloven

I tråd med kravene i Personopplysningsloven gir MOVAR følgende informasjon:

a) Behandlingsansvarlige for MOVAR er selskapets personvernombud.

b) Formålet med behandlingen er å oppfylle arbeidsmiljølovens bestemmelser om varsling, samt å legge forholdene til rette for forebygging og avdekking av kritikkverdige forhold, herunder økonomisk kriminalitet.

c) Opplysningene som samles inn vil etter omstendighetene kunne bli utlevert til påtalemyndigheten dersom det besluttes å anmelde forholdet, eller dersom påtalemyndigheten begjærer utlevering.

d) For den registrerte er det frivillig å gi fra seg opplysningene

e) Den registrerte har rett til å kreve innsyn og rett til å kreve retting/sletting, se ytterligere informasjon i egne punkter i denne rutinen.

Ved mottatte varsler skal MOVAR informere den/de varselet gjelder om hvilke opplysninger som samles inn, samt opplysningene som fremgår i punkt a-e ovenfor. Dette skal gjøres så snart opplysningene er innhentet/mottatt med mindre:

1) innsamlingen eller formidlingen av opplysningene er uttrykkelig fastsatt i lov,

2) varsling er umulig eller uforholdsmessig vanskelig, eller

3) det er på det rene at den registrerte allerede kjenner til informasjonen varslet skal inneholde

4) opplysningene er påkrevd å hemmeligholde av hensyn til forebygging, etterforskning, avsløring og rettslig forfølgelse av straffbare handlinger (POL § 23 første ledd bokstav b).

Når det unnlates å gi informasjon fordi det er umulig eller uforholdsmessig vanskelig, skal informasjonen likevel gis senest når det gjøres en henvendelse til den registrerte på grunnlag av opplysningene.

8. Overordnet rapportering

Varslingsmottaket rapporterer, minst en gang pr år, til styret i MOVAR. Rapporteringen oppsummerer:

- Antall varsler mottatt i perioden
- Type forhold det er varslet om uten å beskrive enkeltsaker
- Avgjørelsesmåtene i sakene
- Beskrivelse av tiltak som er iverksatt for å motvirke eventuelle kritikkverdige forhold det er varslet om
- Kjente tilbakemeldinger og kommentarer som kan beskrive tilliten til varslingsmottaket og effekten av varslingsordningen
- Eventuelle påstander om at varsler er utsatt for gjengjeldelse som følge av varslingen

All overordnet rapportering skal ta hensyn til varsleren, slik at enkeltsaker ikke identifiseres eller at det blir kjent hvem som har varslet.

9. Konfidensialitet

Dokumenter som gjelder varsling vil normalt være interne dokumenter som er konfidensielle.

10. Registrering/arkivering av varsler

Meldingen registreres og arkiveres i eget arkivsystem med begrenset tilgang hos varslingsmottaket. Saken skal arkiveres og for øvrig behandles i samsvar med det til enhver tid gjeldende regelverk og godkjente saksbehandlingsrutiner.

Saksopplysningene skal lagres på kryptert område hos MOVAR og/eller eksternt varslingsmottak, og skal kun være tilgjengelig for de ansatte som har et tjenstlig behov / arbeider med varslingssaker.

11. Sletterutiner

Når saksbehandlingen for et varsel er avsluttet, skal opplysninger som er vesentlig for sakens behandling og utfall sammenstilles i en sluttrapport. Deretter slettes/makuleres øvrige dokumenter og opplysninger som ble produsert i forbindelse med saksbehandlingen. Det er varslingsmottakets ansvar å gjennomføre dette.

Rapporten skal oppbevares for fremtiden med begrenset tilgang, kun for medlemmene i varslingsmottaket. Rapporten slettes i sin helhet når arbeidsforholdet opphører for den/de varselet var rettet mot, med mindre særlige forhold gjør det nødvendig å oppbevare opplysningene utover dette.

12. Innsynsrett for den eller de som varselet gjelder

Den som varselet gjelder skal informeres om forholdet i forbindelse med at saken undersøkes, med mindre slik informasjon kan ødelegge formålet med undersøkelsene.

Dersom varselet gjelder forhold som det kan tenkes at politi/påtale- eller tilsynsmyndigheter vil forfølge, skal disse gjøres kjent med forholdene, og den det er varslet mot informeres deretter i samråd med den aktuelle instansen.

Enhver som ber om det, skal få vite hva slags behandling av personopplysninger en behandlingsansvarlig foretar, og kan kreve å få følgende informasjon om en bestemt type behandling:

a) navn og adresse på den behandlingsansvarlige og dennes eventuelle representant,

b) hvem som har det daglige ansvaret for å oppfylle den behandlingsansvarliges plikter,

c) formålet med behandlingen,

d) beskrivelser av hvilke typer personopplysninger som behandles,

e) hvor opplysningene er hentet fra,

f) om personopplysningene vil bli utlevert, og eventuelt hvem som er mottaker.

Dersom den som ber om innsyn er registrert, skal den behandlingsansvarlige opplyse om:

a) hvilke opplysninger om den registrerte som behandles, og
b) sikkerhetstiltakene ved behandlingen så langt innsyn ikke svekker sikkerheten

Den registrerte kan kreve at den behandlingsansvarlige utdyper informasjonen i første ledd bokstav a - f i den grad dette er nødvendig for at den registrerte skal kunne ivareta egne interesser.

Forespørsler om innsyn til MOVARs eksterne varslingsmottak, skal videreformidles til MOVAR. MOVARs interne varslingsmottak er ansvarlig for at innsyn gis i tråd med det som er beskrevet ovenfor.

Før det gis innsyn skal den registrerte levere inn en skriftlig og undertegnet forespørsel. Av hensyn til kravet om konfidensialitet, må den registrerte også inngi en bekreftet kopi av legitimasjon.

Informasjon skal sendes skriftlig til den registrerte.

Hvis informasjonen skal sendes elektronisk, for eksempel ved bruk av e-post, må informasjonen krypteres eller sikres på annen måte. Dersom informasjonen sendes pr. post skal dette fortrinnsvis sendes til vedkommendes folkeregistrerte adresse.

Postsendinger som inneholder fødselsnummer skal være utformet slik at nummeret ikke er tilgjengelig for andre enn adressaten.

Det kan ikke kreves betaling for å gi informasjon etter forespørsel om innsyn.

Retting og/eller sletting av mangelfulle opplysninger

Dersom det er behandlet personopplysninger som er uriktige, ufullstendige eller som det ikke er adgang til å behandle, skal den behandlingsansvarlige av eget tiltak eller på forespørsel av den registrerte, rette de mangelfulle opplysningene. Den behandlingsansvarlige skal om mulig sørge for at feilen ikke får betydning for den registrerte, f.eks. ved å varsle mottakere av utleverte opplysninger.

Retting av uriktige eller ufullstendige personopplysninger som kan ha betydning som dokumentasjon, skal skje ved at opplysningene tydelig markeres og suppleres med korrekte opplysninger.

Sletting bør suppleres med registrering av korrekte og fullstendige opplysninger. Dersom dette ikke er mulig, og dokumentet som inneholdt de slettede opplysningene av den grunn gir et åpenbart misvisende bilde, skal hele dokumentet slettes.

Avvik på behandlingsrutiner og informasjonssikkerhet

Det skal registreres avvik dersom rutinene i dette dokumentet ikke følges, og ved brudd på personvern/informasjonssikkerheten i forbindelse med behandlingen av varselet.

Administrerende direktør i MOVAR er ansvarlig for at det føres oversikt over avviksmeldinger og at avviksmelding sendes Datatilsynet dersom særlig verneverdige personopplysninger er utlevert.

Disse retningslinjene er vedtatt av styret i MOVAR, den <sett inn dato>.

VEDLEGG
Arbeidsmiljøloven, Kapittel 2 A. Varsling

Arbeidsmiljøloven § 2 A-1. Rett til å varsle om kritikkverdige forhold i virksomheten
(1) Arbeidstaker har rett til å varsle om kritikkverdige forhold i arbeidsgivers virksomhet. Innleid arbeidstaker har også rett til å varsle om kritikkverdige forhold i virksomheten til innleier.

(2) Arbeidstakers fremgangsmåte ved varslingen skal være forsvarlig. Arbeidstaker har uansett rett til å varsle i samsvar med varslingsplikt eller virksomhetens rutiner for varsling. Det samme gjelder varsling til tilsynsmyndigheter eller andre offentlige myndigheter.

(3) Arbeidsgiver har bevisbyrden for at varsling har skjedd i strid med denne bestemmelsen.

Arbeidsmiljøloven § 2 A-2. Vern mot gjengjeldelse ved varsling
(1) Gjengjeldelse mot arbeidstaker som varsler i samsvar med § 2 A-1 er forbudt. Overfor innleid arbeidstaker gjelder forbudet både for arbeidsgiver og innleier. Dersom arbeidstaker fremlegger opplysninger som gir grunn til å tro at det har funnet sted gjengjeldelse i strid med første eller andre punktum, skal det legges til grunn at slik gjengjeldelse har funnet sted hvis ikke arbeidsgiveren eller innleieren sannsynliggjør noe annet.

(2) Første ledd gjelder tilsvarende ved gjengjeldelse mot arbeidstaker som gir til kjenne at retten til å varsle etter § 2 A-1 vil bli brukt, for eksempel ved å fremskaffe opplysninger.

(3) Den som er blitt utsatt for gjengjeldelse i strid med første eller andre ledd, kan kreve oppreisning uten hensyn til skyld hos arbeidsgiver eller innleier. Oppreisningen fastsettes til det beløp som retten finner rimelig under hensyn til partenes forhold og omstendighetene for øvrig. Erstatning for økonomisk tap kan kreves etter alminnelige regler.

Arbeidsmiljøloven § 2 A-3. Plikt til å utarbeide rutiner for intern varsling
(1) Dersom forholdene i virksomheten tilsier det, plikter arbeidsgiver å utarbeide rutiner for intern varsling i samsvar med § 2 A-1 i tilknytning til det systematiske helse-, miljø- og sikkerhetsarbeidet.

(2) Arbeidsgiver plikter alltid å utarbeide slike rutiner dersom virksomheten jevnlig sysselsetter minst 5 arbeidstakere.

(3) Rutinene skal utarbeides i samarbeid med arbeidstakerne og deres tillitsvalgte.

(4) Rutinene skal ikke begrense arbeidstakers rett til å varsle etter § 2 A-1.

(5) Rutinene skal være skriftlige og minst inneholde:

a) oppfordring til å varsle om kritikkverdige forhold,
b) fremgangsmåte for varsling,
c) fremgangsmåte for mottak, behandling og oppfølging av varsling.

(6) Rutinene skal være lett tilgjengelig for alle arbeidstakere i virksomheten.

Arbeidsmiljøloven § 2 A-4. Taushetsplikt ved varsling til offentlig myndighet

(1) Når tilsynsmyndigheter eller andre offentlige myndigheter mottar varsel om kritikkverdige forhold, plikter enhver som utfører arbeid eller tjeneste for mottakerorganet å hindre at andre får kjennskap til arbeidstakers navn eller andre identifiserende opplysninger om arbeidstaker.

(2) Taushetsplikten gjelder også overfor sakens parter og deres representanter. Forvaltningsloven §§ 13 til 13 e gjelder ellers tilsvarende.

STYRET FOR MOVAR IKS

Styresak 10/2018
Repr.sak 4/2018

BUDSJETT 2019 – ØKONOMIPLAN 2019 - 2022

Fremlagt:

- Budsjett 2019 samt økonomiplan 2019 - 2022 totalt og pr. avdeling, med kommentarer.

- *Saksfremlegget er et arbeidsdokument som distribueres styrets medlemmer/varamedlemmer, samt leder og nestleder i representantskapet elektronisk*.

Direktørens forslag til styrets innstilling til representantskapet;

- **Representantskapet i MOVAR IKS vedtar fremlagte som selskapets budsjett for 2019, samt økonomiplan for perioden 2019 – 2022, med investeringer og låneopptak ihht oppstillinger i økonomiplanen.**

SAKSUTREDNING:

Vedlagt oversendes forslag til budsjett 2019 og økonomiplan for perioden 2019 - 2022 for MOVAR IKS.

Utarbeidelsen av budsjettet involverer svært mange ansatte og tallene er godt forankret i de ulike avdelingene. Kostnadskontroll er en kontinuerlig prosess i selskapet, men det er under budsjettperioden ekstra fokus på utgifter og investeringer ned på detaljnivå. Eierkommunene ønsker tallmateriale/priser tidlig fra oss pga sin egen budsjettering. Følgelig starter budsjettprosessen i selskapet med første innleveringsfrist fra sektorene allerede før sommerferieavviklingen. Til tross for dette får vi tidvis tilbakemeldinger om at dette er noe sent i forhold til kommunenes behov for informasjon.

Under de enkelte avdelinger og sektorer er det kort kommentert om det er spesielle forhold som påvirker 2019. Videre er det vist til estimerte leveringsmengder kommende år, og de forutsetninger som er lagt til grunn for antatt utvikling i priser, lønn og rentenivå.

Budsjettet for 2019 gjøres opp med samlede driftsinntekter på kr. 326,9 millioner, og et underskudd etter finansposter på kr. 4,11 millioner.

Både *vann*, *renovasjon og feiertjeneste* budsjetteres med underskudd i 2019 for å nedregulere positive selvkostfond. De eldste saldoene på selvkostfondene vil dermed være utlignet, og samtlige avdelinger må i løpet av planperioden gå i balanse eller vise overskudd.

Produksjon av materiale til budsjettet har pågått helt frem til publiseringen i Admincontrol. Det kan derfor forekomme skrivefeil og at layoutmessige løsninger som ikke er optimale. Før budsjett og økonomiplanen sendes representantskapet vil slike feil bli forsøkt korrigert.

De endringer som eventuelt følger av styrets behandling vil innarbeides i dokumentet før oversendelse til representantskapet.

Administrasjonen er beredt til å besvare spørsmål under behandlingen.

Rygge, 19. september 2018

Johnny Sundby (sign.)
Adm. direktør

Merete Ruud Tuskin (sign.)
Økonomi- og administrasjonssjef

STYRET FOR MOVAR IKS

Orienteringssak nr. 25/2018

ORIENTERING OM INFORMASJONSSIKKERHET KNYTTET TIL FAGSYSTEMET YSI PA FRA NORCONSULT INFORMASJONSSYSTEMER AS

Fremlagt:

- Informasjonsbrev fra Norconsult
- Epost m/vedlegg mottatt fra varslerne
- Medieomtale digi.no, Moss Avis og Østlandets Blad
- Informasjon fra movar.no
- Brev til Norconsult fra MOVAR IKS

Direktørens forslag til

V E D T A K :

Saken tas til orientering

SAKSORIENTERING:

Norconsult Informasjonssystemer AS (Norconsult) er leverandør av fagsystemet ISY PA. IT-systemet benyttes for å administrere kundeinformasjon og logistikk knyttet til husholdningsrenovasjon i MOVAR IKS og 74 andre renovasjonsselskaper og kommuner i Norge.

Fredag 20. april 2018 mottar MOVAR IKS et informasjonsskriv fra leverandøren (vedlagt). Her fremkommer bl.a. følgende:

«Norconsult Informasjonssystemer (NoIS) har gjennomført kontroller vedrørende tilgang til tjenester som kan nås utenifra. Dere har installert ISY ProAktiv SyncService. Det er avdekket at det vil være teknisk mulig for 3. part å trekke ut informasjon fra denne tjenesten dersom man har den dype tekniske innsikten som kreves.

Det er viktig å presisere at dette ikke har skjedd, men at vi har satt i verk preventive tiltak»

Leverandøren opplyser at saken er meldt til Datatilsynet. Informasjonen fra Norconsult blir mottatt av sektorsjef renovasjon, og videresendt til IT-avdelingen mandag 22. april 2018.

For ordens skyld presiserer vi at mulige personopplysninger på avveie i denne sammenhengen, ikke dreier seg om åpent søkbare eller på andre måter lett tilgjengelige lister over personopplysninger. For å få tilgang til disse kreves det særskilt høy IT-teknisk kompetanse, der det bl.a. må gjøres manuelle spørringer ved hjelp av kommandoer.

ISY ProAktiv SyncService er en funksjonalitet som benyttes i forbindelse med Norconsults tømmekalenderen på nett. Av MOVARs fem eierkommuner, er denne kun benyttet av Moss kommune. Den gjør det mulig å søke opp informasjon for privatpersoner om når de ulike avfallsfraksjonene hentes på bostedsadresser, basert på fagsystemet ISY PA som datakilde. Tømmekalenderen fra Norconsult ble uavhengig av denne hendelsen avpublisert som planlagt på kommunens nettsider fra 1. mai 2018, og erstattet med en peker mot MOVARs nye tømmekalender som er felles for alle kommunene. Denne er ikke utviklet av Norconsult, og har ikke den samme sikkerhetssvakheten som førstnevnte.

23. april 2018 gjennomfører IT-avdelingen tiltak som begrenser tilgangen til fagsystemet for andre enn Norconsult, og tetter dermed sikkerhetshullet i IT-løsningen.

Basert på informasjonen vi har på dette tidspunktet, vet vi at leverandøren selv har avdekket et sikkerhetshull, og at de har kvalitetssikret at ingen personopplysninger er på avveie. Vi vurderer hendelsen som en del av det kontinuerlige vedlikeholds- og oppgraderingsarbeidet som utføres på enhver IT-plattform. I skrivende stund har vi siden da heller ikke mottatt noen ytterligere informasjon direkte fra Norconsult.

27. august 2018 klokken 15.13 publiserer nettavisen digi.no en sak, der MOVAR IKS omtales (vedlagt). Her fremgår det at to varslere har skaffet seg uautorisert tilgang til fagsystemet ISY PA fra Norconsult. Informasjonen på digi.no avviker fra det Norconsult informerte oss om i sitt brev i april. MOVAR IKS omtales to ganger i saken. Først som en av de mange opplistede kundene til Norconsult som benytter fagsystemet. I tillegg opplyses det at «… Ifølge en oversikt Solberg og Nygård har laget, var det Movar (Mosseregionen Vann, Avløp og Renovasjon) og Sandnes kommune som først fikk på plass en varig sikkerhetsfiks. Dette skjedde mellom den 20. og 25. april.»

Omtalen av selskapsnavnet, gjør at HR/kommunikasjonssjef mottar varsel om dette via en medieovervåkningstjeneste få minutter etter publisering. Den nærmeste halvtimen informeres administrerende direktør, sektorsjef renovasjon og IT-avdelingen.

28. august 2018 informerer vi Moss kommune om hendelsen og medieomtalen fra digi.no via epost, siden det er deres tjeneste som er berørt. De første interne undersøkelsene iverksettes, og pågår over de nærmeste dagene.

Natt til 5. september 2018 mottar MOVAR IKS en epost direkte fra varslerne som opprinnelig avdekket svakheten og varslet Norconsult (vedlagt). Først på dette tidspunktet får vi innsikt i vesentlige opplysninger som endrer vår oppfatning av hendelsen og informasjonen fra Norconsult:

- Det er ikke Norconsult, men to privatpersoner (tredjepart) som avdekket sikkerhetsbristen.
- Norconsult ble varslet om dette direkte fra privatpersonene den 15. april 2018.

- Hendelsen er ikke en ordinær programvareoppdatering fra leverandørens side, men et tiltak etter et reelt innbrudd i Norconsults IT-systemer.

Basert på utviklingen i saken kontakter vi vår kontaktperson i Norconsult.

På konkrete spørsmål til leverandøren, avdekker vi at de ikke har gått gjennom trafikkloggene til MOVAR IKS spesifikt, til tross for at de i april forsikret oss om at ingen personopplysninger har kommet på avveie. Leverandøren instrueres om å undersøke trafikkloggene og om å rapportere tilbake.

IT-avdelingen analyserer samme dag trafikkloggene tilbake til 2016. Resultatet viser kun ureglementert trafikk fra de to privatpersonene, i de tidsrommene de selv opplyser at de har hatt aktivitet.

6. september 2018 orienteres styret i MOVAR IKS om saken av administrerende direktør (vedlagt). Vi informerer også om hendelsen via våre nettsider.

Moss Avis publiserer saken på moss-avis.no kvelden den 6. september 2018, i papirutgaven av samme avis og på oblad.no den 7. september.

Det er ikke registrert øvrig medieomtale eller noen inngående henvendelser fra publikum via vår 1. linjetjeneste.

Oppsummering

Våre undersøkelser avkrefter at andre enn varslerne kan ha fått tilgang til personopplysninger om våre kunder.

Vi har valgt å informere åpent om saken via våre nettsider overfor våre kunder.

MOVAR IKS var en av landets første renovasjonsselskaper som tettet sikkerhetshullet i fagsystemet, basert på informasjonen fra leverandøren Norconsult. Allikevel er vi ikke tilfredse med Norconsults håndtering av saken, slik det fremgår av vårt brev til direktøren i Norconsult Informasjonssystemer AS den 19. september 2018.

Administrasjonen tar med seg følgende læringspunkter videre:

- Tømmekalenderen og den bakenforliggende funksjonaliteten som Moss kommune benyttet, ble en gråsone mellom Norconsult, Moss kommune og MOVAR IKS. drifter IT-serveren til løsningen driftes av MOVAR, som også gjennomførte den tekniske installasjonen, basert på instruksjoner fra leverandøren. Her burde vi vært mer kritiske og i sterkere grad ettergått/kvalitetssikret funksjonaliteten levert av Norconsult.
- Arbeidet med informasjonssikkerheten er et kontinuerlig arbeid. Vi vil fortsette å teste systemene våre ved hjelp av eksterne fagmiljøer, slik styret har blitt orientert om tidligere.
- I vår nylig lanserte tømmekalender (app og movar.no), har informasjonssikkerheten vært vurdert og er basert på en annen type teknologi/kommunikasjon.
- Leverandørenes kultur og praksis knyttet til informasjonssikkerhet, vil bli gjenstand for evaluering i fremtidige anskaffelsesprosesser.

- MOVAR viderefører arbeidet med oppnevnelse/anskaffelse av et personvernombud.
- Fremtidig valg av programvare for håndtering av renovasjonskundene vil bli vurdert som del av prosjekt 105, gitt at dette vedtas sammen med budsjettet.
- Våre erfaringer med Norconsult Informasjonssystemer AS i denne saken vil bli tillagt vekt ved fremtidige anskaffelser.

Rygge, 19. september 2018

Johnny Sundby (sign.)
Adm. direktør

Rolf-Ivar Buerengen (sign.)
HR & kommunikasjonssjef

Norconsult Informasjonssystemer

Movar IKS - Movar Mosseregionens VAR-Selskap
Att: Freddy Tangen
KJELLERØDVEIEN 30,
1580 RYGGE

Deres ref.	Vår ref.	Trondheim
	camen	20. april 2018

Tilgang til tjenester fra Norconsult Informasjonssystemer

Norconsult Informasjonssystemer (NoIS) har gjennomført kontroller vedrørende tilgang til tjenester som kan nås utenifra. Dere har installert ISY ProAktiv SyncService. Det er avdekket at det vil være teknisk mulig for 3.part å trekke ut informasjon fra denne tjenesten dersom man har den dype tekniske innsikten som kreves. **Det er viktig å presisere at dette ikke har skjedd, men at vi har satt i verk preventive tiltak.**

Vi ber om at det legges inn i brannmur hos dere at kall mot http://pasync.movar.no:81/SyncService/basic kun slipper gjennom fra spesifikke IP'er. Dersom dere har løsninger som bruker tjenesten som NoIS ikke har levert må dere åpne for kall fra IP'er der disse løsningene er installert.

For tekniske spørsmål kontakt Kjell Ivar Lønne (kjell.ivar.lonne@norconsult.com, 45404658)
For andre spørsmål kontakt Cathrine Marstein Engen (cathrine.marstein.engen@norconsult.com, 45404605)

Avviket er meldt til Datatilsynet.

Med vennlig hilsen
Norconsult Informasjonssystemer AS

Cathrine Marstein Engen
Avdelingsleder, GIS og kommunal forvaltning

ISY

Leak: Half a million Norwegians affected

Looking for an easy way to find out when the garbage was being picked up ended up in discovering a data leak affecting half a million people.

Published: Mon, September 3, 2018, 23:40

Category: Security

Tags: Security Monday, Information leak, Social Security numbers, OWASP 2013 A2, OWASP 2013 A3, OWASP 2013 A6, OWASP 2013 A10

Author: Hallvard Nygård & Roy Solberg

tl;dr

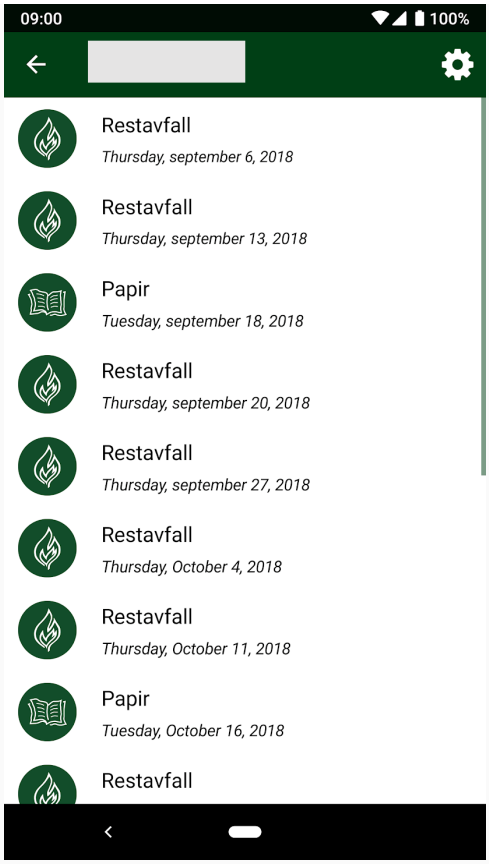
An app that was supposed to contain only addresses and a garbage collection calendar was actually using services that was leaking personal information like names and Social Security numbers for many, many persons.

Summary

Who:	Norconsult Informasjonssystemer (Nois)
Severity level:	Low to medium
Reported:	April 2018
Reception and handling:	Response time good, but slow on fixing. Notification to clients was faulty.
Status:	Fixed
Reward:	A thank you
Issue:	Information leak with personal data and usage data for up to 625,000 people. Data also contained waste disposal routes, sewage monitoring, and more. Likely that modification of some data was possible.

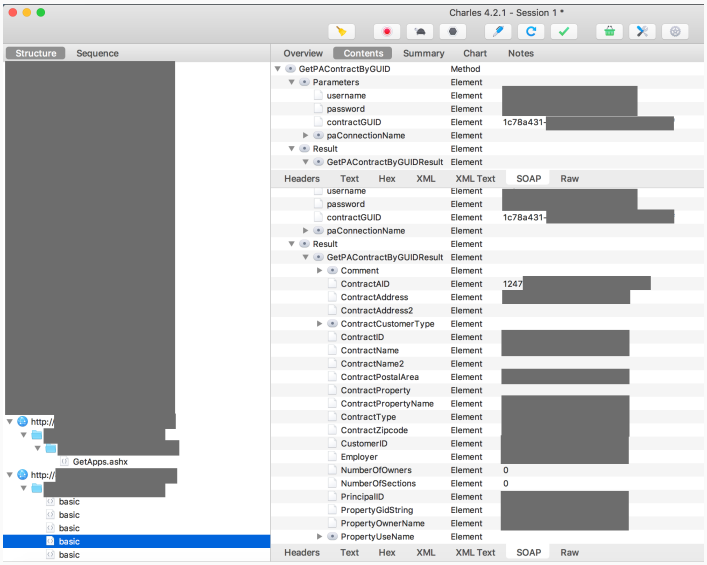
Background

A friend came up with an idea of having an Alexa skill/Google Assistant app where one could ask for *"when will the paper garbage be picked up"*? He saw that the website for BIR - our local waste management company - did not provide an easy way to fetch that data. He said there also was an app with the same data. Taking a look at the communication between the app and the server it quickly became clear that something was very wrong in regards of security.



Approach (technical stuff)

The app



Using the HTTP proxy application Charles it was easy to look at the traffic between the app and server. Surprisingly the app and server actually used SOAP for communication. SOAP is pretty painful to work with and not commonly observed in the world of apps (though it was used for the case with Tryg and Infotorg).

All the SOAP calls used the same simple username and password and all data was transferred unencrypted over HTTP.

Surprisingly, doing a search for a street name actually returned a list of properties including the full name of the owner.

Then, when selecting a property in the app there was a call getting more details about it. Even though the app did not show the data, the server response returned full name, address and Social Security number of the property owner.

SOAP service with the full access

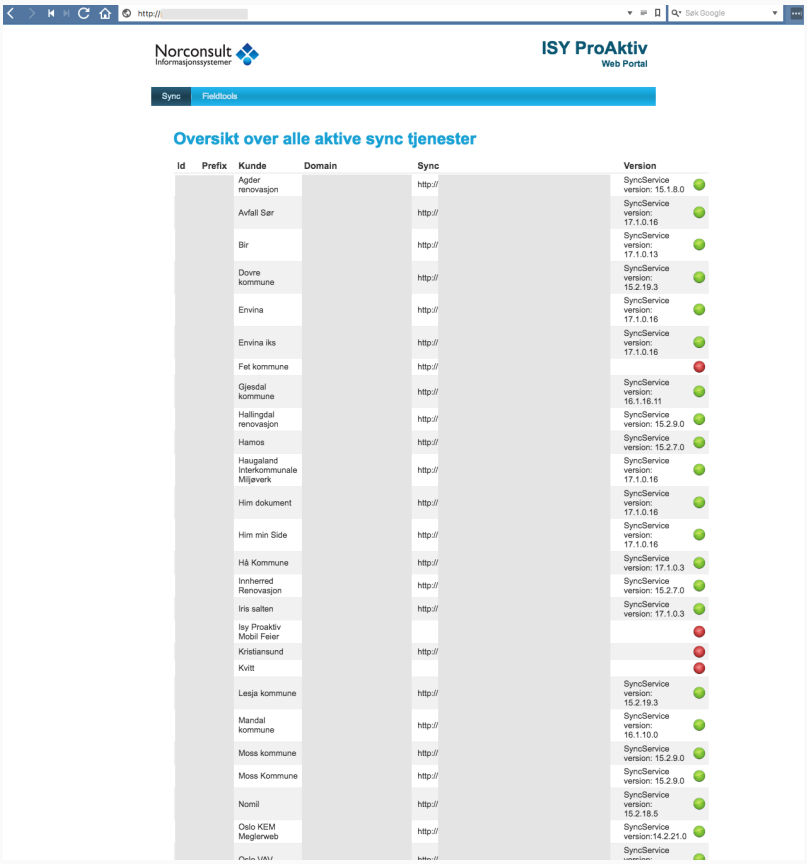
SOAP and related concepts

SOAP is a XML based messaging protocol. It can be used over HTTP, as in this case, or other protocols like JMS and SMTP. A SOAP server contains a lot over SOAP services. These are described in a WSDL file. With the WSDL (and corresponding XSDs) one can generate strongly typed classes for all endpoints that are easy to use. The WSDL/XSD files can contain comments that describe the parameters and possible values. This was not the case here. Using SoapUI or similar tool, one can easily execute different parameters for each service. SoapUI is like Swagger or Postman for REST.

The WSDL file for the service was accessible without any authentication or IP check. This means that all services that was available was listed with their parameters/definitions. Bringing up SoapUI from back in the days, we were able to create requests to services we did not know about from the app.

Using the username and password that was found in the app, we could do queries to the SOAP service. As we did not know the input values, some services was hard to use.

The system overview page



Nois has published quite a few apps, and one of the calls that the app made was one to get the configuration of these apps. Looking at the root of this URL revealed a public facing status page with URLs to many of Nois' web services. This page was even indexed by Google. The URLs gave out WSDL files for all services available.

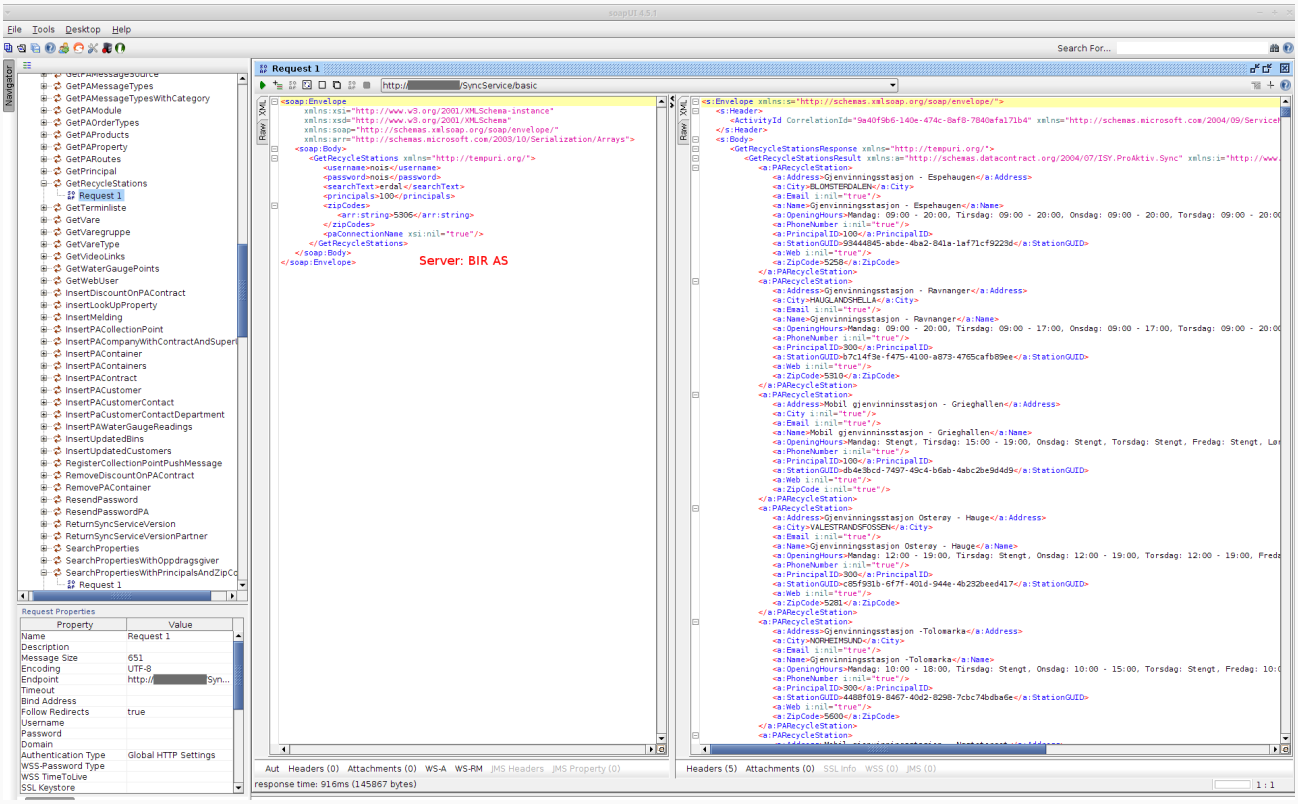
Based on the copyright statements on the page and source code it looked like the system overview page was last maintained in 2012.

Many more SOAP services

After dedusting SoapUI, we explored some of the "`GetXYZ`" services. We were able to get successful response on a subset of the once we tried. Main reason for failed requests was

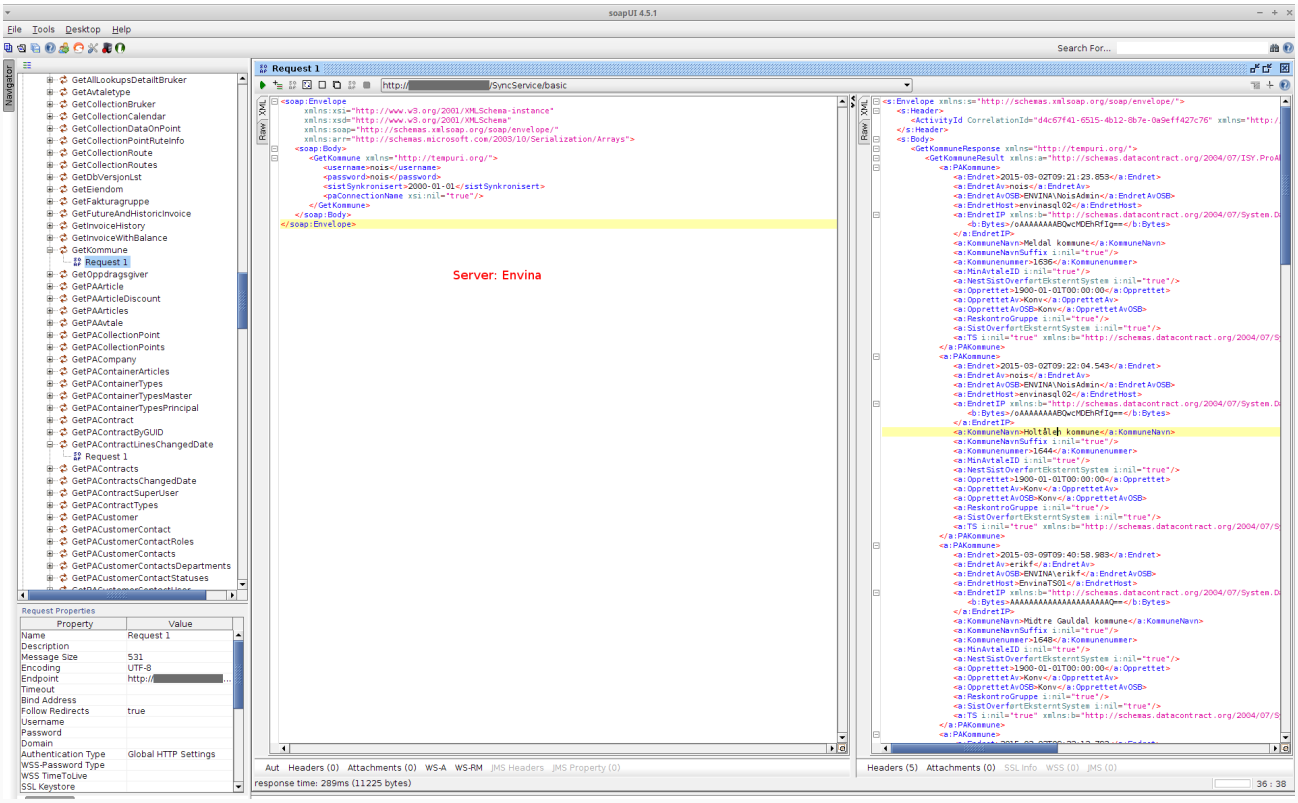
lack of examples of the input parameters. We did not try any write operations.

Example - `GetRecycleStations` (BIR AS)



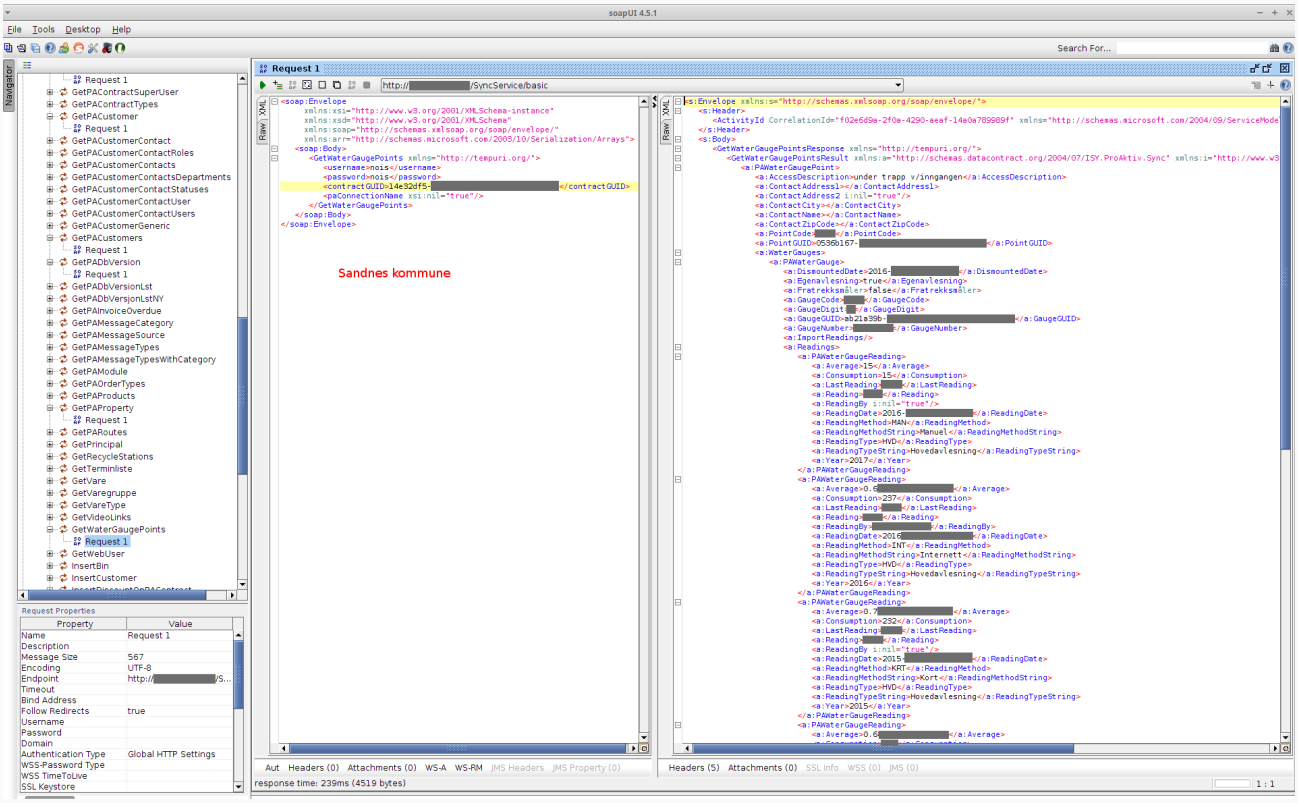
A SOAP service that might be called by a web page or app. Data we should have access to, in some way.

Example - `GetKommune` (`GetMunicipalities`) - Envina



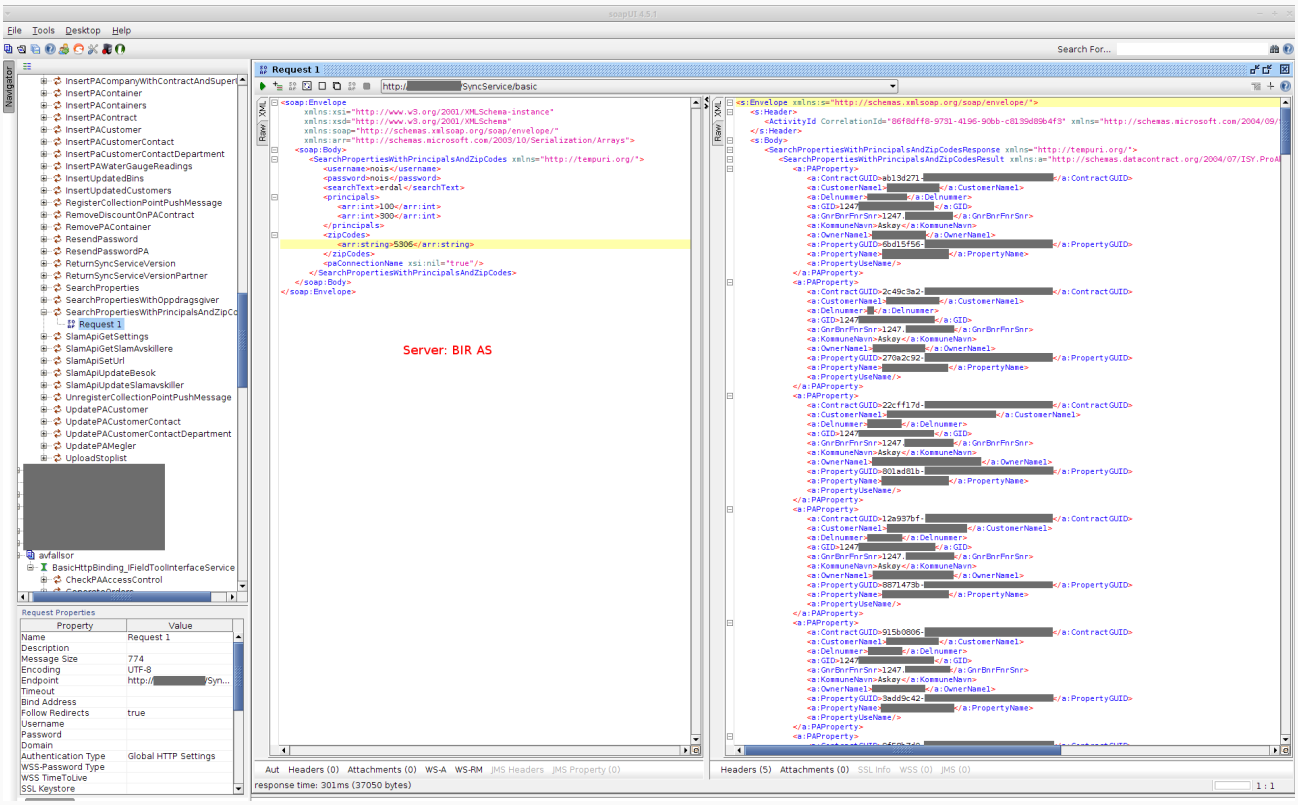
This service told which municipalities was available on the given server. We used it to create the below table of affected municipalities.

Example - `GetWaterGaugePoints` - Sandnes kommune



Some municipalities like Sandnes are billing water based on usage. This endpoint returns information about where a water gauge is located and what the last measurements were.

Example - `SearchPropertiesWithPrincipalsAndZipCodes` - BIR AS



Some services provided a search for customers. It should make it easy to get hold of all the customers.

Data available

Based on the list of SOAP services available, we figure the following data is available within the systems (given that they use that part of the system):

- Register of persons including Social Security number (used as customer id), name, address, e-mail, phone number, fax number, notes, created time, last changed, etc.
- Register of companies with the same data. Customer id is organization number.
- Who owns a property. Who is paying for waste disposal/water/etc.
- Who made changes (e.g. municipal employee, customer via Internet) and their IP address.
- Invoices including the contents of the invoice.
- Invoices not paid in time.
- Pick up spots for waste. Driving routes, work orders, etc.
- Water gauge usage data including description on where you can find it, history (timestamps, amount of water, measurement type, who did the reading).
- Register of both internal users and external users.

Verification

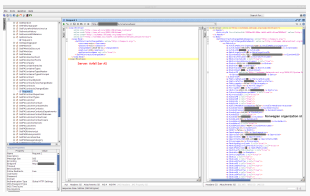
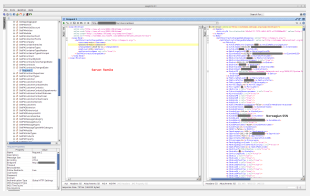
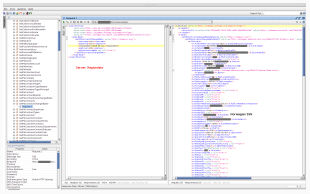
We created a list of servers we found on the system overview page. We also manage to find some using search engine (Googling for phrases from the application). From the overview page we identified some of the owners and it was also clear that some servers were offline.

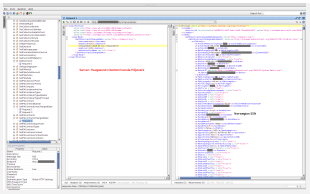
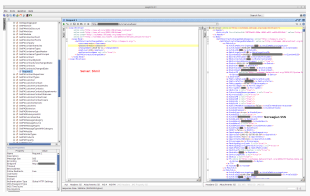
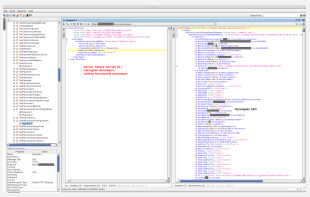
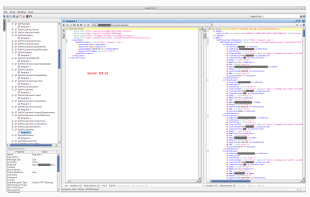
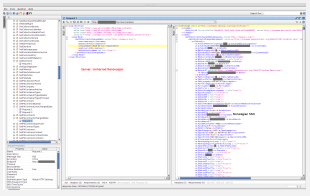
To exclude those that were not affected by this huge security flaw, we verified each and every server. Mainly two SOAP services were called, one that returned all municipalities on that server and one with the latest changes in customer data. The service with customer data revealed that our user (`nois/nois`) had access to customer data on that particular server AND that the server was currently being used (somebody edited some customer in the past week/month or so).

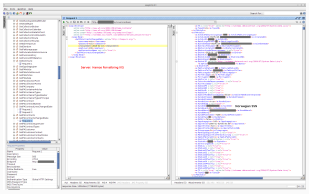
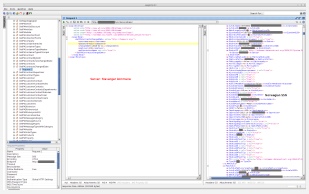
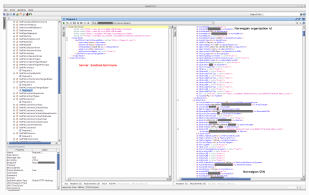
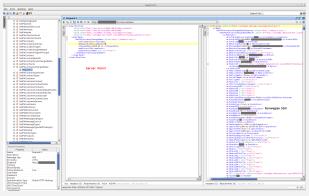
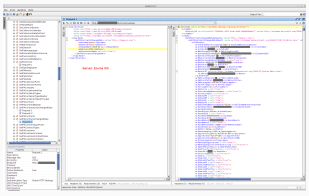
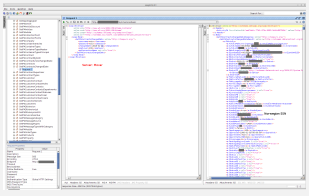
The servers were verified manually using SoapUI and we took screenshots as proof. The screenshots were edited to censor any personal data (we don't want to have that saved).

A few servers on the overview page did not work even if they showed status “green". One example of this is Gjesdal kommune. According to the overview page, the service was running but we could not reach it. This could be that they had firewalls that blocked our HTTP requests.

The owners were either a municipality or a cooperation of municipalities (Norwegian: IKS - interkommunalt selskap).

Municipality / company	**Municipalities**	**Inhabitants**	**Screenshot**
Avfall Sør AS	Kristiansand, Songdalen, Søgne, Vennesla	120,403 Customer estimate: 45-65,000	
Remiks	Tromsø, Karlsøy	76,814 Customer estimate: 30-40,000	
Regiondata	Dovre, Lesja, Sel, Vågå	14,820 Customer estimate: 5-8,000	
Haugaland Interkommunale Miljøverk (HIM)	Haugesund, Bokn, Tysvær, Vindafjord, Etne	62,026 Customers: 33,052	

			
Shmil	Hemnes * Server is responding with "Hemnes kommune", Shmil also responsible for Alstahaug, Brønnøy, Dønna, Grane, Hattfjelldal, Herøy, Leirfjord, Sømna, Vefsn, Vega, Vevelstad. Only Hemnes counted.	4,524 Customer estimate: 2,000	
Retura Val-Hall AS / Hallingdal renovasjon / Valdres Kommunale renovasjon	Hol, Ål, Gol, Hemsedal, Nesbyen, Flå, Krødsherad, Nord-Aurdal, Sør-Aurdal, Øystre Slidre, Vestre Slidre, Etnedal, Vang * Server is also responding with Gjøvik, Søndre Land and Sigdal. These are not counted.	40,915 Customer estimate: 15-22,000	
BIR AS	Askøy, Bergen, Fusa, Kvam, Os, Osterøy, Samnanger, Sund, Vaksdal	359,364 Customer estimate: 140-190,000	
Innherred Renovasjon	Selbu, Malvik, Meråker, Stjørdal, Frosta, Levanger, Verdal, Inderøy, Leksvik * Server is also responding with Moss, Oslo, Tolga, Bergen, Sula, Trondheim, Rissa, Bjugn, Orkdal, Melhus, Tydal, Steinkjer, Verran, Høylandet, Overhalla, Flatanger, Nærøy, Vefsn, Tydal, Indre Fosen, Innherred. These are not counted in the number of inhabitants.	92,563 Customers: 35,671	
Hamos Forvaltning IKS	Hemne, Agdenes, Meldal, Orkdal, Snillfjord, Skaun, Rindal, Hitra, Frøya, Rennebu, Surnadal	50,967 Customer estimate: 20-27,000	

			
Stavanger kommune (own server)	Stavanger * Server also responded with Sandnes, Hå, Klepp, Time, Gjesdal, Sola, Randaberg, Finnøy after we notified Nois about the issue. Not counted.	132,729 Customer estimate: 50-70,000	
Sandnes kommune (own server)	Sandnes	76,328 Customer estimate: 30-40,000	
Nordfjord Miljøverk IKS (NoMil)	Bremanger, Vågsøy, Selje, Eid, Hornindal, Gloppen, Stryn	32,932 Customer estimate: 12-18,000	
Envina IKS	Klæbu, Melhus, Midtre Gauldal * Server also responded with Meldal, Holtålen, Soknedal, Skaun. Not counted.	28,582 Customer estimate: 10-15,000	
Movar (Mosseregionen Vann, Avløp og Renovasjon)	Moss, Rygge, Råde, Vestby, Våler	76,391 Customer estimate: 30-40,000	

Total number of inhabitants in the municipalities: 1,169,358

It was hard to find good numbers of the amount of customers that are in the databases of the different municipalities. Innherred Renovasjon and Haugaland Interkommunale Miljøverk did have numbers on customers (Innherred)/waste disposal customers (HIM). They were respectively 2.6 inhabitants per customer and 1.87 inhabitant per customer. Based on those numbers we estimate 450,000 to 625,000 private persons possibly exposed with full name, address, Social Security number, contact information, etc.

Data from one municipal spans the whole country and more

Since people owns properties across the country, we checked one of the response (Regiondata) to check if that was true. An example is owning a cabin in Dovre kommune and paying the municipal a fee for waste disposal. This is mandatory and not possible to opt out of.

Some ZIP codes from a `GetEiendom` request to the server `Regiondata`:

- 0274 Oslo
- 0378 Oslo
- 0382 Oslo
- 0465 Oslo
- 0594 Oslo
- 0775 Oslo
- 1348 Rykkinn, Bærum kommune
- 1363 Høvik, Bærum kommune
- 1407 Vinterbro, Ås kommune
- 1555 Son, Vestby kommune
- 1816 Skiptvet
- 2013 Skjetten, Skedsmo kommune
- 2056 Algarheim, Ullensaker kommune
- 2319 Hamar
- 2322 Ridabu, Hamar kommune
- 2615 Lillehammer
- 2624 Lillehammer
- 2663 Dovreskogen, Dovre kommune
- 2670 Otta, Sel kommune
- 2672 Sel
- 2675 Otta, Sel kommune
- 2676 Heidal, Sel kommune
- 2677 Nedre Heidal, Sel kommune
- 2682 Lalm, Vågå kommune
- 2816 Gjøvik
- 6040 Vigra, Giske kommune (Møre og Romsdal)
- Danmark
- Sweden

This is not a complete list. We manually picked out some from the response in SoapUI to get a feeling for the data set.

ISY ProActive servers with no/minor issues found

Municipalities listed, but with a different service exposed:
- Dalane Miljøverk IKS, DIM (Eigersund, Sokndal, Bjerkreim)
- Ryfylke Miljøverk IKS, Rymi (Forsand, Finnøy, Strand, Hjelmeland, Suldal)
- Hadeland og Ringerike Avfallsselskap AS, HRA (Gran, Lunner og Jevnaker)
- Indre Hordaland Miljøverk, IHM (Eidfjord, Granvin, Jondal, Ullensvang, Ulvik, Voss)
- Iris Salten

We did not have a username/password that worked for this service. It doesn't seem wise to have these on the Internet. They should all add a firewall blocking access.

Municipalities listed, where our requests did not work:
- Agder Renovasjon IKS (Arendal, Froland og Grimstad)
- Hå kommune
- Steinkjær kommune
- Sykkylven Energi
- Ålesund kommune

We believe we shouldn't have been able to reach the servers of these municipalities. It doesn't seem wise to have these on the Internet. They probably should all add a firewall blocking access.

Municipalities listed where firewall blocked our request:
- Gjesdal kommune
- Fet kommune
- Skaun kommune
- Mandal kommune
- Kristiansund kommune

We consider all these secure.

Reception and handling

Day zero

Sunday night we sent an e-mail to the director of Nois and the head of department of the department responsible for the software in question.

A few hours later we got a pretty cold *"We confirm that the email has been received."* back.

Day 1

Just before midnight we sent an e-mail with some questions and information about another 7 municipalities affected by the issue.

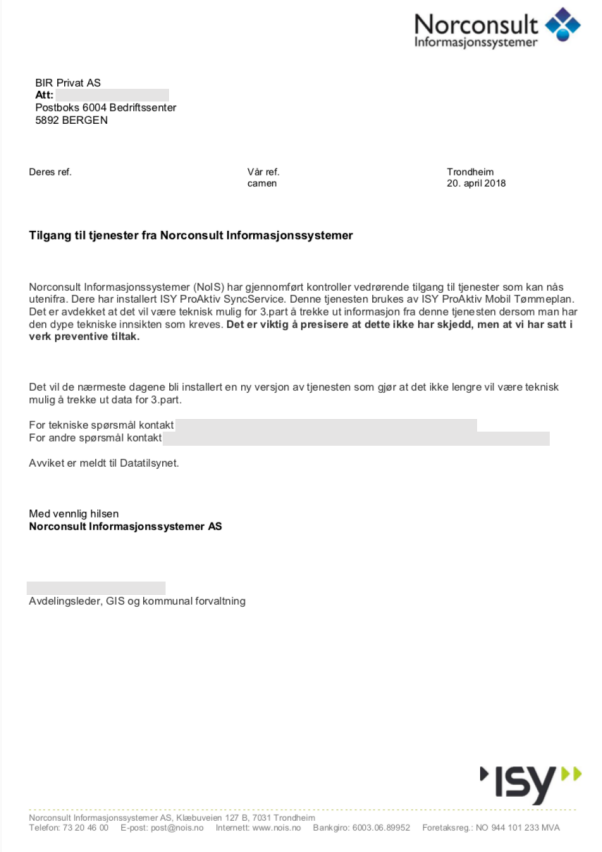
Day 5

Not having heard back we sent a new e-mail asking for a status.

We soon got a response telling that they had established a working group for the issue. They had fixed a couple of the issues and they had informed the The Norwegian Data Protection Authority (Datatilsynet) and the municipalities in question.

We used the freedom of information law to get a hold of the alerts and communication with the municipalities. The alert was a letter sent on day 5.

In addition to general information, this is was what the letter told:
"It has been discovered that it is technically possible for 3rd party to extract information from this service if you have the deep technical insight required. It is important to emphasize that this has not happened, but that we have implemented preventive measures."
They also said a new version would be rolled out during the next days.



Norconsult Informasjonssystemer

BIR Privat AS
Att:
Postboks 6004 Bedriftssenter
5892 BERGEN

Deres ref. | Vår ref. camen | Trondheim 20. april 2018

Tilgang til tjenester fra Norconsult Informasjonssystemer

Norconsult Informasjonssystemer (NoIS) har gjennomført kontroller vedrørende tilgang til tjenester som kan nås utenifra. Dere har installert ISY ProAktiv SyncService. Denne tjenesten brukes av ISY ProAktiv Mobil Tømmeplan. Det er avdekket at det vil være teknisk mulig for 3.part å trekke ut informasjon fra denne tjenesten dersom man har den dype tekniske innsikten som kreves. **Det er viktig å presisere at dette ikke har skjedd, men at vi har satt i verk preventive tiltak.**

Det vil de nærmeste dagene bli installert en ny versjon av tjenesten som gjør at det ikke lengre vil være teknisk mulig å trekke ut data for 3.part.

For tekniske spørsmål kontakt
For andre spørsmål kontakt

Avviket er meldt til Datatilsynet.

Med vennlig hilsen
Norconsult Informasjonssystemer AS

Avdelingsleder, GIS og kommunal forvaltning

ISY

Norconsult Informasjonssystemer AS, Kløbuveien 127 B, 7031 Trondheim
Telefon: 73 20 46 00 E-post: post@nois.no Internett: www.nois.no Bankgiro: 6003.06.89952 Foretaksreg.: NO 944 101 233 MVA

- BIR: Alerted by letter. ISY ProAktiv Mobil Tømmeplan affected.
  - No further follow up by BIR. They thougth the letter was clear and that no data was leaked.
  - Server was accessible about 2 months after the letter was sent.
- Stavanger kommune: Alerted by letter. Same as BIR but with ISY ProAktiv WebPortal also affected. Was also told to add firewall in front of the service.

Day 55

We saw that the issue still was open for many of the municipalities and asked for an ETA of a fix.

Day 58

Tuesday morning Nois said they expected everything to be OK by the end of the week.

Day 61

Friday night we asked if really was the case that everything was fixed.

We got a reply that they would work through the weekend to get it fixed.

Day 65

We informed that not everything was fixed yet. We sent an example query that returned a list of 1208 customers that had changed the last couple of months. The details returned from server included full name, social security number, property identifier and lots of other fields.

Nois told they were working on getting access to the necessary serves to fix it.

In the afternoon we got another response telling us that everything should be OK and they thanked us for informing them about it.

We replied that we still were getting personal data from one of their services.

They looked into the issue and they thought it could have been a service being restarted by an automatic scheduled job...

Day 66

We got another e-mail telling us that they had even more services automatically restarting during the night.

Day 112

We noticed that a service was back up running, and it returned information about more than 6,000 persons.

Day 113

The day after, a Sunday, we got a response that they would contact the customer the day after to make sure it was fixed.

Day 114

We got another response that the service in question now was removed.

Inaccurate report to the Data Protection Authority

We reported the incident to The Norwegian Data Protection Authority (DPA). After Nois gave their version of it, the DPA closed the case and said they were satisfied by the countermeasures implemented by Nois. We believe the report sent from Nois to the DPA to be inaccurate.

Nois claimed that it was not possible to get lists (supposedly one would have to ask for one at the time) of Social Security numbers or of properties that had not made their payments. Several services returned lists of SSN/customers/properties. (Property addresses are anyways public knowledge and one could easily just as for each property, one by one.)

Nois claimed that the issue was caused by a "technical failure". Not using encryption on any of their services, using both username and password "`nois`" and returning Social Security numbers when asking for which days the garbage is picked up is not a technical failure. The cause is ignorance by developers and lack of knowledge by any managers above them. Quite a few people must have been aware of this.

Nois claimed that the "deviation" was open from January 31st 2018 until April 16th 2018. The issue was not closed until the later part of June 2018 and start of August 2018 - and not at all when the report to the DPA was sent. While we discovered this mid April, Nois published BIR's "garbage collection calendar" app in August 2017. Looking at that exact version of the app reveals that the same services without encryption, with the same login and the fields for Social Security numbers, names and addresses were being used. Looking at Innherred Renovasjon's app we found the same to be true in a version released in October 2015. We don't understand why they would specify January 31st 2018 as the start date. If they will want to claim this, they should provide some evidence for the date being January 31st.

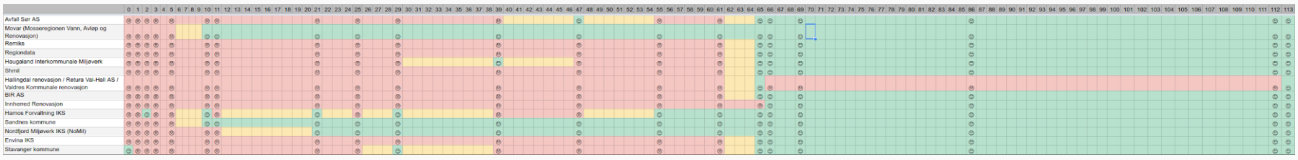
Nois claims that no personal information was leaked when looking at the logs. This claim is a bit hard to understand as Nois did not have operational responsibility of many of the servers and they have had a hard time getting access to the servers to do updates. At the time of the report they had not closed the issue on all servers. Also, as mentioned, the issue was seemingly open for much longer than they claim. And finally, the services were indeed leaking personal information for every request being made. It's impossible to know if a request came from the "garbage collection calendar" apps or from someone faking it and looking up a person's Social Security number. And for how long do they have logs for?

Timeline of fixed services

During the period from we notified the vendor to the time it was fixed, we monitored the servers from time to time using a small script. The monitoring was done by calling one of the SOAP services. We choose the `GetMunicipalities` (Norwegian: `GetKommune`) as this did not contain the personal information, required authentication and returned some data.

The smilies and colors below indicate if the service responded or not. There are two versions of this data set, one with just the days we tested and one with empty cells for days we did not test.

Owner of server	Day 0	Day 1	Day 2	Day 3	Day 5	Day 10	Day 11	Day 21	Day 25	Day 29	Day 39	Day 47	Day 55	Day 61	Day 65	Day 66	Day 69	Day 86	Day 112	Day 113
Avfall Sør AS	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😊	😟	😟	😊	😊	😊	😊	😊	😊
Movar (Mosseregionen Vann, Avløp og Renovasjon)	😟	😟	😟	😟	😟	😊	😊	😊	😊	😊	😊	😊	😊	😊	😊	😊	😊	😊	😊	😊
Remiks	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😊	😊	😊	😊	😊	😊
Regiondata	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😊	😊	😊	😊	😊	😊
Haugaland Interkommunale Miljøverk	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😊	😟	😟	😟	😊	😊	😊	😊	😊	😊
Shmil	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😊	😊	😊	😊	😊	😊
Hallingdal renovasjon / Retura Val-Hall AS / Valdres Kommunale renovasjon	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😊	😟	😟	😟	😟	😊
BIR AS	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😊	😊	😊	😊	😊	😊
Innherred Renovasjon	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😊	😊	😊	😊	😊
Hamos Forvaltning IKS	😟	😟	😊	😟	😟	😊	😟	😊	😟	😊	😟	😟	😊	😊	😊	😊	😊	😊	😊	😊
Sandnes kommune	😟	😟	😟	😟	😟	😊	😊	😊	😊	😊	😊	😊	😊	😊	😊	😊	😊	😊	😊	😊
Nordfjord Miljøverk IKS (NoMil)	😟	😟	😟	😟	😟	😟	😟	😊	😊	😊	😊	😊	😊	😊	😊	😊	😊	😊	😊	😊
Envina IKS	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😟	😊	😊	😊	😊	😊	😊
Stavanger kommune	😊	😟	😟	😟	😟	😟	😟	😟	😟	😊	😟	😟	😟	😟	😊	😊	😊	😊	😊	😊



Media

We sent this security issue out to the local media since there was 14 different corporations/municipalities involved. The main take away from it is that information security is higher on the agenda for a lot of these. We also got to know that the corporations (customers of Nois) did not view this as a security issue/breach of personal data. Norwegian headlines translated below.

- Remiks:
  - iTromsø - "Disclosed security hole: 30,000-40,000 Remiks customers social security numbers available online"
- Haugaland Interkommunale Miljøverk (HIM):
  - Haugesunds Avis - "Discovered leakage in information security at HIM"
- Hallingdal renovasjon / Retura Val-Hall AS / Valdres Kommunale renovasjon:
  - Hallingdølen
    - "Data security failure: Social security number in the open"
    - "Norconsult denies data being in the wrong hands."

- "-Possible to fool the DPA"
- Avisa Valdres - "Detected weakness in the systems of renovation company"

- BIR:
- Bergens Tidende - "Disclosed security hole - Social security number of waste customers available online for months"

- Innherred Renovasjon:
- Innherred - "Customers social security number available"

- Sandnes kommune, Stavanger kommune:
- Stavanger Aftenblad - "Disclosed security issue in Sandnes and Stavanger"

digi.no wrote a summary on a national level: "Renovation companies in many Norwegian municipalities leak personal data"

No media reported on these:
- Avfall Sør AS
- Movar
- Regiondata
- Shmil
- Hamos Forvaltning IKS
- Nordfjord Miljøverk IKS (Nomil)
- Envina IKS

Questions we still have

What is clear is that the municipality is responsible for the protection of the personal data they have. They are responsible for their database. It seems like Nois have full access to the system for upgrades and checking logs. We still wonder about who is responsible for the running of the systems. Who is responsible for not changing default configuration (default username and password with full access)? Who is responsible for not configuring the firewalls? Who is responsible for building apps on top of SOAP and using a user with full access for the communications?

After the media asked the municipalities responsible for the personal data and after we got to see the letter from Nois notifying their customer about the security issue, most of them did not react to this as a system leaking information. Why did Nois send such a vague letter to the customers and DPA (Datatilsynet)?

Nois claimed they checked the logs and that no data was actually leaked. They also claim the security issue was just present for 4 months. How was the access logs checked? Did they check back in time to at least 2015? Where is the report to their customers about this?

Conclusion

Who checks the security of an app that doesn't contain a login or any personal data at all? No one, because it just doesn't make sense to do that. It was just a coincidence that we discovered this one.

What sticks out in the end for us is that the reception and handling of the issue wasn't very good. Usually IT companies responds more quickly and are more open about the issue and handling of it. Here the customers got a vague description not telling much about what was going on.

It would be interesting to know if anyone really digged into how long the data was available for, because it seems like they have been there for quite a few years.

Finally, if you as a developer are told to use a service that returns much more data than what's intended to be used, **you should speak up**. Quite a few people have known about these personal data being transferred unencrypted over the wire.

15.04.2018

Norconsult Informasjonssystemer AS

Kopi: Datatilsynet **SLADDET FOR IP-ADRESSER!**

Varsling om sikkerhetshull i instanser av Isy Proaktiv og lekkasje av persondata fra 75 kommuner

Under følger 3 varslinger om sikkerhetshull og lekkasje av persondata fra Isy Proaktiv, lekkasje av persondata via webinar fra Norconsult Informasjonssystemer samt sikkerhetshull i supportløsning fra Norconsult Informasjonssystemer. Det følger også 3 vedlegg med teknisk informasjon om berørte Isy Proaktiv-servere.

Vi setter pris på å få tilsendt saksnummer hos de respektive kommunene/kommunale foretak når de er varslet.

Mvh.
Roy Solberg og Hallvard Nygård

Varsling 1 - Persondata fra 75 kommuner (ca 1,2 mill innbyggere) åpent tilgjengelig

Isy Proaktiv-servere er ubeskyttet med standard passord. Standard brukernavn og passord (nois / nois) eksponeres i mobilapper og er dermed tilgjengelig. Ca 1,2 millioner innbyggere hører til de 75 direkte berørte kommunene. I tillegg kommer eiere fra andre kommuner (f.eks. hytte i en av kommunene). Serverne er knyttet til 18 forskjellige kommuner og interkommunale foretak. Slik vi oppfatter det er det on-premise-løsninger hvor foretakene selv drifter serverne i samarbeid med Norconsult Informasjonssystemer. Vi anslår rundt 450 000 abonnenter sine persondata, vannmålerdata, fakturaer, med mer er tilgjengelig på disse tjenestene.

Liste over Isy Proaktiv-servere var å finne på https://XXXXX.isy.no og https://XXXXXX.isy.no/ (samt https://XXXXXXX.isy.no/ uten servere). Mange av disse var aktive med oppdatert versjon fra 2018. 14 av de brukte standard brukernavn og passord (nois / nois). 11 andre svarte på WSDL/SOAP-tjeneste, men virket ikke med standard brukernavn/passord. 11 servere svarte ikke på HTTP port 80. Enten er serverne satt opp med brannmur som har IP-sperre eller de er tatt ut av drift.

Alle 14 åpne serverne ble bekreftet via SOAP-tjenesten GetPAContractsChangedDate og GetKommune. Det ble søkt primært på 1 dato per server for å verifisere at det var persondata

tilstede og server var aktiv. Hvis denne ikke gav treff ble det byttet dato (tjenesten gav kun resultat hvis noen kunder var endret den dagen).

Følgende datoer ble forsøkt (totalt sett, men kun 1-3 per server):
- 11.04.2018
- 10.04.2018
- 10.01.2018
- 11.01.2018

Tar forbehold om andre requester også ble testet ut, men har ingen nedtegning av dette.

Hos BIR og Sandnes ble det forsøkt flere endepunkter. Blant annet vannmåler. For Sel kommune ble det kjørt spørring på GetEiendom med sistSynkronisert satt til 2000-01-01. Noen postnummer ble plukket ut.

Requestene ble primært gjort fra én IP-adresse. Noen fra en annen også. Ta kontakt for å få utlevert disse.

Ingen av serverne brukte SSL-kryptering. All trafikk over ukryptert kanal. Trolig bruker apper for innbyggere samt interne bruker (f.eks. renovatører) også samme ukrypterte kanal for å hente og oppdatere persondata i løsningen.

Alle persondata som vi har sett, er eller vil bli slettet eller obfuskert i bilder.

Følgende kommuner er direkte berørt:

Totalt 75 kommuner er trolig direkte berørt av åpne kommunale renovasjonsservere på nett. Innbyggertallet i disse kommunene er ca 1 160 000.

1. **Avfall Sør**
    a. Kristiansand, Songdalen, Søgne, Vennesla
2. **Remiks**
    a. Tromsø, Karlsøy
3. **Delt server - Dovre, Lesja, Sel, Vågå**
4. **Haugaland Interkommunale Miljøverk**
    a. Haugesund, Bokn, Tysvær, Vindafjord, Etne
5. **Shmil**
    a. Serveren svarer kun med "Hemnes kommune"
    b. Shmil har ansvar for Alstahaug, Brønnøy, Dønna, Grane, Hattfjelldal, Herøy, Leirfjord, Sømna, Vefsn, Vega, Vevelstad. Disse er ikke tatt med.
6. **Delt server**
    a. **Hallingdal renovasjon**
        i. Hol, Ål, Gol, Hemsedal, Nesbyen, Flå, Krødsherad

   b. **Retura Val-Hall AS**
      i. Ansvar for 13 kommuner i Hallingdal, Valdres
      ii. Server svarer "Valdreskommuner, Hallingdalskommuner, Gjøvik, Søndre Land, Sigdal, Ukjent" i tillegg til de som står under Hallingdal renovasjon og Valdres kommunale renovasjon. Disse er ikke med i totalen.
   c. **Valdres Kommunale Renovasjon**
      i. Nord-Aurdal, Sør-Aurdal, Øystre Slidre, Vestre Slidre, Etnedal, Vang
7. **BIR AS**
   a. Askøy, Bergen, Fusa, Kvam, Os, Osterøy, Samnanger, Sund, Vaksdal
8. **Innherred Renovasjon**
   a. Har ansvar for Selbu, Malvik, Meråker, Stjørdal, Frosta, Levanger, Verdal, Inderøy, Leksvik
   b. Server svarer også med "Moss, Oslo, Tolga, Bergen, Sula, Trondheim, Rissa, Bjugn, Orkdal, Melhus, Tydal, Steinkjer, Verran, Høylandet, Overhalla, Flatanger, Nærøy, Vefsn, Tydal, Indre Fosen , Innherred"
9. **Hamos Forvaltning IKS**
   a. Hemne, Agdenes, Meldal, Orkdal, Snillfjord, Skaun, Rindal, Hitra, Frøya, Rennebu, Surnadal
10. **Stavanger (egen server)**
11. **Sandnes (egen server)**
12. **Nomil**
   a. Bremanger, Vågsøy, Selje, Eid, Hornindal, Gloppen, Stryn
13. **Envina IKS**
   a. Har ansvar for Klæbu, Melhus, Midtre Gauldal
   b. Server svarer også med "Meldal, Holtålen, Soknedal, Skaun"
14. **Movar (Mosseregionen Vann, Avløp og Renovasjon)**
   a. Moss, Rygge, Råde, Vestby, Våler

Med direkte berørt menes at renovasjonsselskapet har åpen server. Serveren har en tjeneste for si hvilke kommuner den kjenner til/håndterer. I noen tilfeller er dette forskjellig fra hva selskapet har ansvar for. Alle server har hatt endringer på sine data i 2018 og vi antar derfor de er aktivt brukt.

I tillegg er person fra hele Norge og utlandet berørt:
Dette fordi alle eiere av eiendommer med renovasjon i en berørt kommune vil ligge inne i systemet med persondata (f.eks. Navn, adresse, fødselsnummer, fakturahistorikk, merknader). Eier man f.eks. hytte i en av de berørte kommunene, så vil man ha vært eksponert for sikkerhetshullet.

GetEiendom mot serveren http://XX-REGIONDATA-XX/SyncService/basic (Dovre/Lesja/Sel/Vågå) gir blant annet treff på følgende postnummer

- 0274 Oslo
- 0378 Oslo

- 0382 Oslo
- 0465 Oslo
- 0594 Oslo
- 0775 Oslo
- 1348 Rykkinn, Bærum kommune
- 1363 Høvik, Bærum kommune
- 1407 Vinterbro, Ås kommune
- 1555 Son, Vestby kommune
- 1816 Skiptvet
- 2013 Skjetten, Skedsmo kommune
- 2056 Algarheim, Ullensaker kommune
- 2319 Hamar
- 2322 Ridabu, Hamar kommune
- 2615 Lillehammer
- 2624 Lillehammer
- *2663 Dovreskogen, Dovre kommune*
- *2670 Otta, Sel kommune*
- *2672 Sel*
- *2675 Otta, Sel kommune*
- *2676 Heidal, Sel kommune*
- *2677 Nedre Heidal, Sel kommune*
- *2682 Lalm, Vågå kommune*
- 2816 Gjøvik
- 6040 Vigra, Giske kommune (Møre og Romsdal)
- Danmark
- Sverige

Blant annet følgende data er tilgjengelig på de åpne serverne:

- Personregister med fødselsnummer, adresse, opprettelsestidspunkt, sist endret tidspunkt, telefonnummer, fax, epost, merknader, med mer.
- Register for organisasjoner inneholder det samme (fødselsnummer byttet med organisasjonsnummer).
- Hvem som eier en eiendom. Hvem som betaler for renovasjon på eiendommen.
- Hvem som har utført endringer, hvilken IP de kommer fra, hvilken maskin de brukte
- Fakturaer med innhold.
- Register på for sent betalte fakturaer.
- Hentesteder for avfall. Tømmekalendre. Henteruter. Arbeidsordre for renovasjon. Med mer.
- Vannmåler inkludert beskrivelse av hvor måleren er og historikk (tidspunkt, mengde og hvem som avleste).
- Register over interne brukere. Register over eksterne brukere.

Se full liste over SOAP-endepunkter i vedlegg (lista over stammer fra dette). Endepunktene sier mye om omfanget på data tilgjengelig på tjenestene. Vi har testet noen, og brukernavn ser ut til å ha tilgang til samtlige.

Varsling 2 - Persondata i webinar fra Norconsult Informasjonssystemer

Webinar fra Norconsult Informasjonssystemer angående ny versjon av Isy Proaktiv inneholder persondata om kunder av Fosen Renovasjon. Dataene er fra et testmiljø. Videoen viser ny funksjonalitet i en ny versjon av Isy Proaktiv. Opptaket er tilgjengelig for alle som ønsker. Krever registrering med navn og epost.

En stikkprøve på ett av navn/fødselsnummer ble sjekket mot Vegvesen.no. Der kreves fødselsnummer + etternavn. Resultatet viser at dataene er reelle. Liste over kunder er etter 28:45 minutter i videoen. En enkeltkunde vises 38:54.

"Norconsult - Webinar - Ny kartløsning i ISY ProAktiv 09.03.18", 42:12 minutter
https://register.gotowebinar.com/register/XXXXXXXXXXXXXXX (LogMeIn platform)

Varsling 3 - Norconsult Informasjonssystemer supportløsning med enkelt admin-passord

På adressen https://XXXXXXXXXX.norconsult.no/ finnes det som ser ut som Norconsults supportløsning. Løsningen ser aktiv ut da forrige supporthenvendelse er på dagens dato (12.04.2018). Løsningen krever pålogging. En vanlig kombinasjon er brukernavn admin og passord admin. Dette virker fint.

En overfladisk titt er utført.

Responsible disclosure

Vi ønsker å offentliggjøre funnene våre gjennom såkalt "responsible disclosure". Det innebærer at vi ikke offentliggjør noe før dette er ordnet opp i - eventuelt etter 90 dager hvis dette ikke blir fikset.

Vi har ingen dumper av data og vil f.eks. ikke avsløre konkrete personopplysninger i offentliggjøringen. Likeledes har vi heller ikke endret noe data i noen av systemene.

Vi kommer til å varsle flere dager i forkant av offentliggjøring.

Vedlegg - liste med SOAP-endepunkter

- ActivateCustomer
- AddSmsSubscriptions
- AddrSearchPACollectionPoints
- AuthenticateCustomer
- AuthenticateWebUser
- CheckPAAccessControl
- CheckPASewageAccessControl
- DownloadLiftEvents
- ElemosSetRunUrl
- GenerateOrders
- GeoSearchPACollectionPoints
- GeoSearchProperties
- GetActivePALookupProperty
- GetAktivitet
- GetAktivitetFil
- GetAllLookups
- GetAllLookupsBruker
- GetAllLookupsDetailtBruker
- GetAvtaletype
- GetCancelledOrders
- GetCollectionBruker
- GetCollectionCalendar
- GetCollectionDataOnPoint
- GetCollectionPointRuteInfo
- GetCollectionRoute
- GetCollectionRoutes
- GetDbVersjonLst
- GetEiendom
- GetFakturagruppe
- GetFutureAndHistoricInvoice
- GetInvoiceHistory
- GetInvoiceWithBalance
- GetKommune
- GetOppdragsgiver
- GetPAArticle
- GetPAArticleDiscount
- GetPAArticles
- GetPAArticlesPerEmployer
- GetPAAvtale
- GetPAAvviksTyper

- GetPACollectionPoint
- GetPACollectionPointAdditionalServices
- GetPACollectionPointDeviations
- GetPACollectionPoints
- GetPACollectionPointsPerArea
- GetPACompany
- GetPAContainer
- GetPAContainerArticles
- GetPAContainerTypes
- GetPAContainerTypesMaster
- GetPAContainerTypesPrincipal
- GetPAContainers
- GetPAContainersPerArea
- GetPAContract
- GetPAContractByGUID
- GetPAContractLinesChangedDate
- GetPAContractSuperUser
- GetPAContractTypes
- GetPAContracts
- GetPAContractsChangedDate
- GetPAContractsPerArea
- GetPAContractsSewage
- GetPACustomer
- GetPACustomerContact
- GetPACustomerContactRoles
- GetPACustomerContactStatuses
- GetPACustomerContactUser
- GetPACustomerContactUsers
- GetPACustomerContacts
- GetPACustomerContactsDepartments
- GetPACustomerGeneric
- GetPACustomers
- GetPADbVersion
- GetPADbVersionLst
- GetPADbVersjonLstNY
- GetPADirectMessages
- GetPAFieldToolServiceVersion
- GetPAGTCEntities
- GetPAInvoiceOverdue
- GetPAMaterialValg
- GetPAMeldingKategorier
- GetPAMeldingKategorierElement
- GetPAMessageCategory

- GetPAMessageSource
- GetPAMessageTypeElements
- GetPAMessageTypes
- GetPAMessageTypesWithCategory
- GetPAModule
- GetPAOperationResults
- GetPAOrder
- GetPAOrderDetails
- GetPAOrderHeadsPerCategory
- GetPAOrderTypes
- GetPAOrders
- GetPAOrdersPerCategory
- GetPAOrdersPerCategoryDelta
- GetPAPlantTypes
- GetPAProducts
- GetPAProperty
- GetPARoute
- GetPARouteDelta
- GetPARoutePerArea
- GetPARoutes
- GetPARoutesContainer
- GetPARoutesDate
- GetPARoutesDateStatus
- GetPARoutesDelta
- GetPARoutesLight
- GetPARoutesPerArea
- GetPARoutesStatus
- GetPASewageDeviations
- GetPASewagePlant
- GetPASewagePlants
- GetPASeweragePlant
- GetPASewergePlants
- GetPAWorkList
- GetPAWorkListRoutePlanning
- GetPAWorkListSewage
- GetPAWorkLists
- GetPAWorkListsHead
- GetPAWorkListsHeadRoutePlanning
- GetPAWorkListsModule
- GetPAWorkListsNotSigned
- GetPrincipal
- GetRecycleStations
- GetTerminliste

- GetVare
- GetVareType
- GetVaregruppe
- GetVideoLinks
- GetWaterGaugePoints
- GetWebUser
- InsertDiscountOnPAContract
- InsertMelding
- InsertNewPARoute
- InsertPACollectionPoint
- InsertPACompanyWithContractAndSuperUser
- InsertPAContainer
- InsertPAContainers
- InsertPAContract
- InsertPACustomer
- InsertPACustomerContact
- InsertPAWaterGaugeReadings
- InsertPaCustomerContactDepartment
- InsertUpdatedBins
- InsertUpdatedCustomers
- RegisterCollectionPointPushMessage
- RegisterPATagCoupling
- RegisterPATagCouplings
- RemoveDiscountOnPAContract
- RemovePAContainer
- ReportPAWasteCollection
- ReportPAWasteCollections
- ResendPassword
- ResendPasswordPA
- ReturnFieldToolServiceVersion
- ReturnSignedOrderDetails
- ReturnSyncServiceVersion
- ReturnSyncServiceVersionPartner
- SearchProperties
- SearchPropertiesWithOppdragsgiver
- SearchPropertiesWithPrincipalsAndZipCodes
- SignPAOrder
- SignPAOrderDetail
- SignPAOrderDetails
- SignPAOrderLine
- SignPAOrders
- SignPAWorkListCompleted
- SignPAWorkListItem

- SignPAWorkListReceived
- SlamApiGetSettings
- SlamApiGetSlamAvskillere
- SlamApiSetUrl
- SlamApiUpdateBesok
- SlamApiUpdateSlamavskiller
- UnregisterCollectionPointPushMessage
- UpdatePACollectionPointPosition
- UpdatePACollectionPointStopPointID
- UpdatePACustomer
- UpdatePACustomerContact
- UpdatePACustomerContactDepartment
- UpdatePAMegler
- UpdatePAOrder
- UpdatePARoute
- UpdatePARoutes
- UpdatePASewagePlant
- UpdatePASeweragePlant
- UploadStoplist
- insertLookUpProperty

Vedlegg 2 - Liste over åpne servere og GetKommune

Under følger kall til tjenesten “GetKommune” hvor serveren selv identifiserer hvilke kommuner som er tilgjengelig.

http://XX-AVFALLSØR-XX/SyncService/basic
- Alle
- Næring

http://XX-MOVAR-XX/SyncService/basic
- Alle
- Moss
- Råde
- Rygge
- Våler
- Vestby

http://XX-REMIKS-XX/SyncService/basic
- Tromsø
- Karlsøy

http://XX-REGIONDATA-XX/SyncService/basic
- Alle
- Sel

http://XX-HIM-XX/SyncService/basic
- Alle kommuner
- Haugesund
- Bokn
- Tysvær
- Vindafjord
- Etne

http://XX-SHMIL-XX/SyncService/basic
- Hemnes kommune

http://XX-VARLDRES-HALLINGDAL-XX/SyncService/basic
- Alle kommuner
- Valdreskommuner
- Hallingdalskommuner
- Test
- test2
- Gjøvik
- Søndre Land
- Sør Aurdal
- Etnedal
- Nord Aurdal
- Vestre Slidre

- Øystre Slidre
- Vang
- Flå
- Nes
- Gol
- Hemsedal
- Ål
- Hol
- Sigdal
- Krødsherad
- Ukjent

http://XX-BIR-XX/SyncService/basic

- Alle
- Bergen
- Kvam
- Fusa
- Samnanger
- Os
- Sund
- Askøy
- Vaksdal
- Osterøy

http://XX-INNHERRED-RENOVASJON-XX/SyncService/basic

- Alle
- Moss
- Oslo
- Tolga
- Bergen
- Sula
- Trondheim
- Rissa
- Bjugn
- Orkdal
- Melhus
- Malvik (Gammelt nr.)
- Selbu (Gammelt nr.)
- Tydal (Gammelt nr.)
- Steinkjer
- Meråker (Gammelt nr.)
- Stjørdal (Gammelt nr.)
- Frosta (Gammelt nr.)
- Leksvik (Gammelt nr.)
- Levanger (Gammelt nr.)

- Verdal (Gammelt nr.)
- Verran
- Høylandet
- Overhalla
- Flatanger
- Nærøy
- Inderøy (Gammelt nr.)
- Vefsn
- Trondheim (Nytt nr)
- Steinkjer (Nytt nr)
- Bjugn (Nytt nr)
- Orkdal (Nytt nr)
- Melhus (Nytt nr)
- Malvik
- Selbu
- Tydal
- Meråker
- Stjørdal
- Frosta
- Levanger
- Verdal
- Verran (Nytt nr)
- Høylandet (Nytt nr)
- Overhalla (Nytt nr)
- Flatanger (Nytt nr)
- Nærøy (Nytt nr)
- Inderøy
- Indre Fosen
- Innherred

http://XX-HAMOS-XX/syncservice/basic

- Surnadal kommune
- Rindal kommune
- Hemne kommune.
- Snillfjord kommune.
- Hitra kommune.
- Frøya kommune.
- Agdenes kommune.
- Rennebu kommune.
- Meldal kommune.
- Orkdal kommune.
- Skaun kommune.
- Hemne kommune
- Snillfjord kommune

- Hitra kommune
- Frøya kommune
- Agdenes kommune
- Rennebu kommune
- Meldal kommune
- Orkdal kommune
- Skaun kommune

http://XX-SANDNES-XX/syncservice/basic

- Alle
- Sandnes kommune

http://XX-STAVANGER-XX/SyncService/basic

http://XX-NOMIL-XX/SyncService/basic

- Alle
- Bremanger
- Vågsøy
- Selje
- Eid
- Hornindal
- Gloppen
- Stryn

http://XX-ENVINA-XX/syncservice/basic

- Meldal kommune
- Holtålen kommune
- Midtre Gauldal kommune
- Soknedal kommune
- Melhus kommune
- Skaun kommune
- Klæbu kommune
- Meldal kommune (Nytt nr)
- Holtålen kommune (Nytt nr)
- Midtre Gauldal kommune (Nytt nr)
- Melhus kommune (Nytt nr)
- Skaun kommune (Nytt nr)
- Klæbu kommune (Nytt nr)

Vedlegg 3 - Andre servere

Følgende liste er servere fra portal.isy.no som responderer på HTTP og har tjenester kjørende. Noen av de har ikke “SyncService” (tjenesten med standard brukernavn og passord). Andre har tjenesten men svarer ikke på spørringene (trolig annet brukernavn/passord).

Dalane Miljøverk
http://XXXXXXXXXX/FieldToolService/basic

Rymi
http://XXXXXXXXXX/FieldToolService/basic

HRA
http://XXXXXXXXXX/FieldToolService/basic

Indre Hordaland Miljøverk
http://XXXXXXXXXX/FieldToolService/basic

Agder renovasjon
http://XXXXXXXXXX/FieldToolService/basic
http://XXXXXXXXXX/SyncService/basic

Iris salten
http://XXXXXXXXXX/FieldToolService/basic
http://XXXXXXXXXX/SyncService/basic

Maren
http://XXXXXXXXXX/FieldToolService/basic
http://XXXXXXXXXX/SyncService/basic

Hå Kommune
http://XXXXXXXXXX/ha/Syncservice/basic

Steinkjær kommune
http://XXXXXXXXXX/FieldToolService/Basic
http://XXXXXXXXXX/SyncService/basic

Sykkylven energi
http://XXXXXXXXXX/SyncServiceNY/basic

Ålesund kommune
http://XXXXXXXXXX/SyncService/basic

MOVAR IKS
Uttak 17.09.2018

Nyheter

ISY ProAktiv Renovasjonsforetak i mange norske kommuner lekket personopplysninger

Digi.no. 27.08.2018 15:13

Harald Brombach

Felles serverprogramvare var synderen.

Systemutviklerne Roy Solberg og Hallvard Nygård offentliggjorde i dag detaljer om deres hittil siste oppdagelse i forsøket på å forbedre sikkerheten til norske, internettbaserte og publikumsrettede tjenester i Norge.

Denne gang er det et system som brukes av renovasjonsforetakene til mange kommuner som omtales. Systemet lekket blant annet fødselsnummer over ukrypterte HTTP-forbindelser. Dataene var bare beskyttet med et brukernavn og passord som enkelt kunne avleses i trafikken fra en mobilapp.

Dette opplyser Solberg og Nygård i en pressemelding.

Systemet det er snakk om, heter ISY ProAktiv. Den ble opprinnelig utviklet av selskapet ProAktiv, som ble kjøpt av Norconsult Informasjonssystemer i 2006. Systemet kan også brukes til andre formål enn drift og fakturering av renovasjonsordninger.

75 kommuner

Programvaren brukes hos de interkommunale selskapene Avfall Sør, Remiks, Regiondata, Haugaland Interkommunale Miljøverk, Shmil, Retura Val-Hall AS, Hallingdal renovasjon, Valdres Kommunale renovasjon, BIR AS, Innherred Renovasjon, Hamos Forvaltning IKS, Nordfjord Miljøverk IKS (NoMil), Envina IKS og Movar, samt kommunene Stavanger og Sandnes.

Disse dekker til sammen 75 kommuner.

Det var Solberg som først oppdaget sårbarheten, da han undersøkte appen til renovasjonsselskapet BIR i Bergen. Han så at dataene som appen hentet fra serveren, var mer omfattende enn det som ble vist i appen.


digi.no

ISY PROAKTIV

Renovasjonsforetak i mange norske kommuner lekket personopplysninger

Felles serverprogramvare var synderen.

Norske sårbarhetsjegere fortalte om flere til nå ukjente funn

Standardpassord

Sammen med Nygård gikk Solberg i gang med å undersøke omfanget av sårbarheten. De fant etter hvert ut at også 13 andre aktører lekket kundedataene, blant annet ved at de brukte standard brukernavn og passord.

Hos elleve andre brukere av det samme systemet, fungerte ikke standardpassordet, og hos ytterligere elleve fikk ikke Solberg og Nygård noe svar på HTTP-port 80.

Dette omfattet navn, adresse, fødselsnummer, telefonnummer og e-post til kontaktpersoner til samtlige husstander og hytter i de aktuelle kommunene, i tillegg til fakturaer, bestillinger og annet.

Nygård opplyser til digi.no er at det er ukjent for ham og Solberg hvor lenge dette sikkerhetshullet har vært tilgjengelig.

Varslet i april

Solberg og Nygård varslet både Datatilsynet og leverandøren Norconsult Informasjonssystemer den 15. april i år. Selskapet oppgir i en avviksmelding som ble sent til Datatilsynet den 20. april, at sårbarhetene ble fjernet fra systemet den 16. april.

Dette er i første omgang gjort ved å begrense hvilke IP-adresser som får tilgang til servertjenesten som viser personinformasjon. For løsninger som ikke skal vise personinformasjon, slik som mobilapper, var planen i april å lage en separat tjeneste som ikke inkluderer personinformasjon.

Selskapet opplyste også at det skulle foreta intern revisjon av tiltakene og rutiner for utvikling og testing, samt kurse ansatte i sikker utvikling og innebygget personvern.

I et brev til Norconsult Informasjonssystemer, datert den 11. juni i år, skriver Datatilsynet at det er fornøyd med redegjørelsen som er gitt og tiltakene som er gjort. Tilsynet har dermed avsluttet saken.

Noen var tregere enn andre

Men selv om Norconsult Informasjonssystemer raskt rettet i programvaren, så måtte den oppdaterte utgaven tas i bruk av renovasjonsforetakene. Dette tok betydelig lenger tid. Ifølge en oversikt Solberg og Nygård har laget, var det Movar (Mosseregionen Vann, Avløp og Renovasjon) og Sandnes kommune som først fikk på plass en varig sikkerhetsfiks. Dette skjedde mellom den 20. og 25. april.

Hos enkelte av foretakene ser det ut til at sårbarhetene har kommet og gått i perioden. Først den 19. juni ble det registrert at sårbarhetene hadde forsvunnet helt hos de aller fleste av foretakene. Det skulle likevel gå nesten to ytterligere måneder før sikkerhetshullene ble registret lukket hos alle.

I avviksmeldingen fra Norconsult Informasjonssystemer bekreftes det at det har vært mulig å finne passordet til tjenesten ved å undersøke tilknyttede mobilapper. Selskapet skriver videre at dette krever inngående innsikt, samtidig som at det opplyser at det ikke vet hvordan Solberg og Nygård har fått til dette.

Norconsult Informasjonssystemer opplyser i avviksmeldingen også at det etter en gjennomgang av logger, ikke er noe tegn til at data har blitt hentet ut av parter som ikke skulle ha tilgang til dette.

Solberg og Nygård har bare gjennomført svært forsiktige stikkprøver.

Beklagelig

- Selv om dette var data som lå vanskelig tilgjengelig, er det beklagelig at det var hull i løsningen. Systemene ble raskt gjennomgått og det er ikke funnet unormal aktivitet annet enn på tidspunktene Nygård og Solberg har hatt aktivitet, sier leder for marked og kommunikasjon i Norconsult, Hege Njå Bjørkmann, i en uttalelse til BT, som omtalte saken allerede i forrige uke (bak betalingsmur).

Bekymret

Nygård mener at denne oppdagelsen gir grunn til å være bekymret over IT-sikkerheten hos kommunene.

- Jeg er svært bekymret for kommunal IT-sikkerhet. Vi har nå sett på noen kommuner, og det vi finner er hårreisende. Aller helst ville jeg bedt de om å slette meg fra registeret, men det er dessverre ikke mulig, sier han i en pressemelding.

- Opplysningene vi fant kan brukes til identitetstyveri, har Datatilsynet tidligere uttalt til media. Jeg ser også for meg at de kan brukes til utpressing. Kommunene og de interkommunale foretakene burde alle gjennomført sikkerhetstester, spesielt nå som den nye

personvernforordningen (GDPR) har trådt i kraft. Per nå får de stryk i IT-sikkerhet, avslutter Nygård.

En gjennomgang av sårbarheten skal publiseres i bloggen til Roy Solberg i nær framtid.

(Digi ekstra)

Image-text:

Datasystemene til en rekke norske renovasjonsforetak lekket personopplysninger. Dette gjaldt blant annet BIR AS i bergensområdet. Bildet viser renovatører på jobb hos selskapet. Personene på bildet har ingenting med denne saken å gjøre. (Illustrasjonsfoto: BIR AS/David Zadig) Hallvard Nygård og Roy Solberg fotografert under en OWASP Norge-meetup tidligere i år. Foto: Harald Brombach Eksempel på data som var tilgjengelige bak et standardpassord og via en ukryptert forbindelse. Her fra serveren til BIR. Skjermbilde: Roy Solberg og Hallvard Nygård I alle fall hos noen av foretakene var fødselsnummeret til kundene blant opplysningene som var svært mangelfullt beskyttet. Skjermbilde: Roy Solberg og Hallvard Nygård Tidslinje for når det ble oppdaget at de ulike foretakene hadde lukket sikkerhetshullet. Illustrasjon: Roy Solberg og Hallvard Nygård

Personinfo lå helt åpent hos Movar

Moss Avis. 07.09.2018. Side: 4-5

HELGE KJØNIKSEN

- Hele kunderegisteret til Movar lå ute med fullt navn, fødselsnummer og bruksog gårdsnummer. Trolig dreide det seg om mellom 30.00040.000 kunder, sier Roy Solberg som sammen med Hallvard Nygård fant informasjonen på nett.

Det var i april i år at Solberg og Nygård tok en nærmere titt på datasikkerheten hos interkommunale foretak i Norge.

- Det var egentlig helt tilfeldig at vi gjorde det. Det var en kamerat som lurte på hvordan han kunne finne ut når papirsøppelet ble hentet. Da vi så nærmere på hva vi kunne hente ut hos de ulike renovasjonsselskapene, var det ingen problemer med å hente ut fødselsnummer, fakturahistorikk, bruks- og gårdsnummer, telefonnummer, e-postadresser og mye annen forbrukerdata, forklarer Roy Solberg.

Det er Norconsult Informasjonssystemer AS som leverer fagsystemet for renovasjon, ISY ProAktiv, til en rekke kommuner - og i samtlige som ble sjekket av Solberg og Nygård, var samme informasjon tilgjengelig.

- Vi ble varslet om denne sikkerhetsbristen av Norconsult, som leverer systemet til 75 kommuner i Norge. Dette var i april, sier administrerende direktør Johnny Sundby i Movar (Mosseregionen vann, avløp og renovasjon), som har kunder i Moss, Vestby, Rygge Råde og Våler.

- Vi ser selvsagt alvorligheten i dette, og er glade for at det ble avdekket. Det ble raskt rettet opp i og nå skal ikke denne informasjonen være tilgjengelig lenger, legger Sundby til.

I ettertid har Movar gjort undersøkelser for å avdekke om informasjon har blitt hentet ut av uvedkommende.

- Vi har gått igjennom logger helt tilbake i 2016, og har ikke funnet noen treff på at informasjon skal være hentet ut. Vår konklusjon er at det ikke har blitt tappet persondata fra oss, bekrefter Sundby.

Roy Solberg er ikke enig i at det med sikkerhet stemmer.

- Selv skulle jeg ha klart å skjule dette for Movar. Hadde jeg vært inne og hentet ut persondata hos dem, ville de

Pokémon 11 timer hver dag

Stor helserisiko å jobbe natt

LEVE Østfold vil engasjere idrettsmiljøet

Rekord-opplæring

● Ville sjekke datasikkerheten hos norske renovasjonsselskaper ● Gjorde skokkerende funn

Personinfo lå helt åpent hos Movar

ikke funnet spor etter meg, kommenterer han.

- Norconsult har sagt til oss at ingen har misbrukt denne informasjonen, men de sier samtidig at de ikke har tilgang til å sjekke alle servere. Så helt sikkert er det nok ikke, legger han til.

Vet ikke hvor lenge

Movar har ikke varslet sine kunder om at det har vært et sikkerhetshull i datasystemet.

- Vi oppfattet ikke at dette var så alvorlig da vi ble varslet om dette i april. Det er først nå i ettertid at vi har fått informasjon som forteller om alvorlighetsgraden og vi vil varsle kundene våre om dette, sier Sundby.

- Som leverandør mener jeg at de forpliktet seg til å informere kundene sine så raskt som mulig etter at vi fant dette hullet. Det ville vært på sin plass å beklage. I saker som dette bør man spille med åpne kort, sier Roy Solberg.

Hvor lenge informasjonen har ligget ute, er det ingen som kan si noe spesifikt om.

- Vi har ikke klart å finne eksakte datoer, men vi kan snakke om lang tid. Det er ingen i Norconsult Informasjonssystemer som har gitt oss informasjon eller svar, sier Solberg.

Portalen hvor de aktuelle serverne sto ser ut til å ha stått stille siden 2012, og for hver enkelt kommune så er det avhengig av når kommunene har benyttet seg av fagsystemet som er levert av Norconsult Informasjonssystemer AS.

Datakunnskap

- Hva tenker du om denne informasjonen lå tilgjengelig, Solberg?

- Juridisk sett er ikke var det ikke sensitiv informasjon vi fant, men informasjon som dette vil i hvert fall ikke jeg ha liggende tilgjengelig på nettet. Det at Norconsult på vegne av kommunene har fjernet dette i etterkant viser vel at heller ikke de ønsker at dette er tilgjengelig informasjon, svarer Solberg.

Norconsults senior kommunikasjonsrådgiver Benedicte Bratt Jakhelln sier følgende til hendelsen:

- Selv om dette var data som lå vanskelig tilgjengelig, er det beklagelig at det var hull i løsningen. Systemene og logger ble raskt gjennomgått og det er ikke funnet unormal aktivitet annet enn på tidspunktene Nygård og Solberg har hatt aktivitet. Vi varslet umiddelbart Datatilsynet og kunden om forholdet. Deretter iverksatte vi både strakstiltak og tiltak på lengre sikt, og hadde en nøye gjennomgang av våre interne rutiner,

Personinformasjon lå åpent hos Movar

Østlandets Blad Pluss. 1 like treff. 07.09.2018 13:30

Helge Kjøniksen

- Hele kunderegisteret til Movar lå ute med blant annet fullt navn, fødselsnummer og bruks- og gårdsnummer. Trolig dreide det seg om mellom 30.00 kunder, sier Roy Solberg som sammen med Hallvard Nygård fant informasjonen på internett.

Det var i april i år at Solberg og Nygård tok en nærmere titt på datasikkerheten hos interkommunale foretak i Norge.

- Det var egentlig helt tilfeldig at vi gjorde det. Det var en kamerat som lurte på hvordan han kunne finne ut når papirsøppelet ble hentet. Vi gikk inn på nettstedet til BIR AS (Bergensområdets Interkommunale Renovasjonsselskap) hvor vi fant en app som ga oss den informasjonen. Da vi så nærmere på hva vi kunne hente ut hos de ulike renovasjonsselskapene, var det ingen problemer med å hente ut fødselsnummer, fakturahistorikk, bruks- og gårdsnummer, telefonnummer, e-postadresser og mye annen forbrukerdata, forklarer Roy Solberg til Moss Avis.

Det er Norconsult Informasjonssystemer AS som leverer fagsystemet for renovasjon, ISY ProAktiv, til en rekke kommuner - og i samtlige som ble sjekket av Solberg og Nygård var den samme informasjonen tilgjengelig.

- Vi ble varslet om denne sikkerhetsbristen av Norconsult, som leverer dette systemet til 75 kommuner i Norge. Dette var i april, sier administrerende direktør Johnny Sundby i Movar (Mosseregionen vann, avløp og renovasjon), som har kunder i Moss, Vestby, Rygge, Råde og Våler.

Skal ikke ha blitt tappet

- Vi ser selvsagt alvorligheten i dette, og er glade for at det ble avdekket. Det ble raskt rettet opp i og nå skal ikke denne informasjonen være tilgjengelig lenger, legger Sundby til.


Østlandets Blad

NYHET VESTBY DATAKRIMINALITET

Personinformasjon lå åpent hos Movar

I ettertid har Movar gjort undersøkelser for å avdekke om informasjon har blitt hentet ut av uvedkommende.

- Vi har gått igjennom logger helt tilbake i 2016, og har ikke funnet noen treff på at informasjon skal være hentet ut. Vår konklusjon er at det ikke har blitt tappet persondata fra oss, bekrefter Sundby.

Roy Solberg er ikke enig i at det med sikkerhet stemmer.

- Selv skulle jeg ha klart å skjule dette for Movar. Hadde jeg vært inne og hentet ut persondata hos dem, ville de ikke funnet spor etter meg, kommenterer han.

- Norconsult har sagt til oss at ingen har misbrukt denne informasjonen, men de sier samtidig at de ikke har tilgang til å sjekke alle servere. Så helt sikkert er det nok ikke, legger han til.

Vet ikke hvor lenge

Movar har ikke varslet sine kunder om at det har vært et sikkerhetshull i datasystemet hvor abonnentene er registrert.

- Vi oppfattet ikke at dette var så alvorlig da vi ble varslet om dette i april. Det er først nå i ettertid at vi har fått informasjon som forteller om alvorlighetsgraden og vi vil varsle kundene våre om dette, sier Sundby.

- Som leverandør mener jeg at de forpliktet seg til å informere kundene sine så raskt som mulig etter at vi fant dette hullet. Det ville vært på sin plass å beklage. I saker som dette bør man spille med åpne kort, sier Roy Solberg.

Hvor lenge informasjonen har ligget ute, er det ingen som kan si noe spesifikt om.

- Vi har ikke klart å finne eksakte datoer, men vi kan snakke om lang tid. Det er ingen i Norconsult Informasjonssystemer AS som har gitt oss informasjon eller svar på dette, sier Solberg.

Portalen hvor de aktuelle serverne sto ser ut til å ha stått stille siden 2012, og for hver enkelt kommune så er det avhengig av når kommunene har benyttet seg av fagsystemet som er levert av Norconsult Informasjonssystemer AS.

Datakunnskap

- Hva tenker du om denne informasjonen lå tilgjengelig, Solberg?

- Juridisk sett er ikke var det ikke sensitiv informasjon vi fant, men informasjon som dette vil i hvert fall ikke jeg ha liggende tilgjengelig på nettet. Det at Norconsult på vegne av kommunene har fjernet dette i etterkant viser vel at heller ikke de ønsker at dette er tilgjengelig informasjon, svarer Solberg.

- Hvor enkelt var det å finne denne informasjonen?

- Man skal ha en del datakunnskap for å finne den. Det er ikke slik at den automatisk kom opp ved å søke på et navn. Men personer med en del datakunnskap kunne enkelt finne fram til denne informasjonen.

- Dersom noen ønsker å misbruke informasjon som dette, så får de tak i den ved å bruke noen som er datakyndige. Det er alltid en risiko for at informasjon kan lekke ut, og derfor er datasikkerhet veldig viktig. Det er derfor Nygård og jeg sjekker om vi kan finne noen hull, fortsetter han.

Raske til å rette opp

Hallvard Nygård, som sammen med Solberg avdekket hullet hos blant annet Movar, sier følgende:

- Jeg er svært bekymret for kommunal IT-sikkerhet. Vi har nå sett på noen kommuner og det vi finner er hårreisende. Aller helst ville jeg bedt de om å slette meg fra registeret, men det er dessverre ikke mulig.

- Vi har påpekt overfor Norconsult at vi må ha større fokus på personvern og IKT-sikkerhet. Og på meg virker det som om de er skikkelig på den «ballen», kommenterer Johnny Sundby.

Han forteller også at de om ikke så lenge vil lansere en ny app, som ikke er levert av Norconsult Informasjonssystemer AS.

- Den vil ha en helt annen sikkerhet når det gjelder personsikkerhet. Dette er noe vi tar veldig alvorlig og seriøst, avslutter Johnny Sundby.

- Movar var sammen med Sandnes kommune de raskeste som fikset opp i dette hullet, avslutter Roy Solberg.

Norconsults senior kommunikasjonsrådgiver Benedicte Bratt Jakhelln sier følgende om hendelsen:

- Selv om dette var data som lå vanskelig tilgjengelig, er det beklagelig at det var hull i løsningen. Systemene

og logger ble raskt gjennomgått og det er ikke funnet unormal aktivitet annet enn på tidspunktene Nygård og Solberg har hatt aktivitet. Vi varslet umiddelbart Datatilsynet og kunden om forholdet. Deretter iverksatte vi både strakstiltak og tiltak på lengre sikt, og hadde en nøye gjennomgang av våre interne rutiner.

Image info:

DATA: I april ble det avdekket at man kunne finne mye persondata hos Movar-kunder.

FAKTA: Etter å ha søkt seg inn i databasen fant Roy Solberg mye informasjon som ikke burde vært tilgjengelig.

BEKLAGER: - Vi beklager at dette hullet ble funnet hos oss og vi skla gjøre alt vi kan for at dette ikke skjer igjen, sier administrerende direktør Johnny Sundby i Movar.

Oversikt over like treff

Personinformasjon lå åpent hos Movar
Moss Avis Pluss - 06.09.2018 19:18

Norconsult Informasjonssystemer AS
v/direktør Ola Greiff Johnsen

Deres ref.: Vår ref.: 18/447-3/JS Dato: 19.09.2018

Vedr. informasjonssikkerheten i ISY ProAktiv og Norconsults håndtering av saken

Viser til informasjon mottatt 20. april 2018 og telefonsamtale med Tor Kjetil Lisle den 5. september 2018.

Vi ønsker med dette å gi en tydelig tilbakemelding på hvordan vi opplever at saken har vært håndtert av Norconsult Informasjonssystemer AS. Vi ønsker også å få svar på de spørsmål som fortsatt står ubesvarte i sakens anledning.

I den første og eneste informasjonen vi har mottatt fra Norconsult i sakens anledning (20. april 2018) fremgår følgende:

> *«Dere har installert ISY ProAktiv SyncService. Det er avdekket at det vil være teknisk mulig for 3. part å trekke ut informasjon fra denne tjenesten dersom man har den dype tekniske innsikten som kreves.*
>
> *Det er viktig å presisere at dette ikke har skjedd, men at vi har satt i verk preventive tiltak.»*

Vi sitter på kopi av korrespondansen fra de to privatpersonene som varslet Norconsult og Datatilsynet om svakhetene i ISY ProAktiv (heretter omtalt som varslerne). Brevet er datert 15. april 2018. Fra og med da hadde Norconsult kjennskap til bl.a. følgende:

- At tredjepart hadde kommet seg inn og fått tilgang til informasjon lagret hos renovasjonskundene til Norconsult.
- At det benyttes et standard brukernavn og passord som eksponeres i mobilapplikasjoner, for de som benytter seg av Norconsults tømmekalender.
- Hvilke kunder som er indirekte eller direkte berørt, herunder MOVAR IKS.

- At saken ville bli offentliggjort, men at Norconsult fikk inntil 90 dager på seg til å rette feilen.
- At Norconsult ville bli varslet flere dager før offentliggjøring.

Hendelsen gjør at MOVAR IKS må vurdere om vi fortsatt kan tillit til Norconsult Informasjonssystemer AS i fremtiden.

1. Informasjonssikkerhet

1.1 Hvordan har Norconsult arbeidet med informasjonssikkerheten i ISY PA før hendelsen?

1.2 Hva er årsaken, slik Norconsult vurderer det, til at sikkerhetshullet i ISY PA oppstod i utgangspunktet?

1.3 Når oppstod det og hvor lenge var det åpent?

1.4 Hvorfor ble ikke sikkerhetshullet oppdaget av egne medarbeidere på et tidligere tidspunkt?

1.5 Hvilke konkrete tiltak har Norconsult gjennomført, for å bedre informasjonssikkerheten i ISY PA etter varslet om denne konkrete saken?

1.6 Hvilke tiltak planlegger Norconsult å gjennomføre i tiden fremover for å sikre en forsvarlig informasjonssikkerhet?

1.7 På hvilke områder tilfredsstiller ISY PA ikke den nye personvernforordningen, og hva er eventuelt fremdriftsplanen videre for å oppnå compliance med GDPR?

1.8 Hvordan følger Norconsult hendelsen overfor varslerne som avdekket og utnyttet sikkerhetsbristen?

1.9 Hvorfor ble ikke standard brukernavn / passord endret etter at dere ble gjort kjent med at dette var likelydende for mange av deres kunder? Hvem mener Norconsult burde endret dette passordet?

2. Informasjon

2.1 Innholdet i varslingen

MOVAR IKS ble kun informert om at Norconsult hadde avdekket en sikkerhetsutfordring, men at tredjepart ikke hadde utnyttet dette.

Hvorfor ble vi ikke informert om den faktiske hendelsen, som trigget informasjonen vi mottok fra dere den 20. april 2018?

2.2 Informasjonsflyt

Etter brevet mottatt 20. april 2018, har ikke MOVAR IKS mottatt noen ytterligere informasjon.

Hvorfor har vi ikke mottatt noen informasjon i etterkant?

2.2. Hva er årsaken til at vi ikke ble informert før den 20. april?

2.3 Rutiner for varsling

Vi kjenner som nevnt til at Norconsult ble varslet 15. april 2018. Vi mener derfor at Norconsult i sitt skriv den 20. april 2018 bevisst gir feil opplysninger til oss som kunde, i et forsøk på avdramatisere hendelsen og forhindre eget omdømmetap.

Overskriften i eposten fra Norconsult er «Tilgang til tjenester fra Norconsult Informasjonssystemer». Innholdet og måten informasjonen er utformet på, gir inntrykk av at dette nærmest er rutinebasert informasjon, med en oppfordring til å gjøre en teknisk endring.

I realiteten kjenner Norconsult til et alvorlig brudd på informasjonssikkerheten i systemet, og at de tekniske endringene må gjennomføres snarest for å begrense skadevirkninger og unngå at personopplysninger kommer på avveie.

Som kunde mener vi informasjonen som ble gitt er svært kritikkverdig og lite tillitsvekkende. Vår forventning fremover er full åpenhet og transparens. Vi forventer også bedre kommunikasjon, som gir oss et tydeligere bilde av alvorlighetsgraden i saken, så vi kan gjøre vurderinger og iverksette tiltak deretter.

Hva er Norconsult oppfatning om hvordan dere selv håndterte informasjonen til oss? Kan vi forvente at dere som leverandør oppfyller disse forventingene i fremtiden?

2.4 Medieomtale

I korrespondansen fra varslerne til Norconsult, fremgår det at Norconsult får 90 dager på seg til å rette feilen, før saken offentliggjøres.

Med andre ord må Norconsult siden midten av april 2018 ha hatt kjennskap til at dette ville bli en mediesak, der også deres kunder ville bli involvert. Til dags dato har vi fortsatt ikke blitt kontaktet eller mottatt ytterligere informasjon i sakens anledning.

Mottok dere varsel i dagene før saken ble offentliggjort?
Hvilke vurderinger ligger til grunn for at vi verken ble informert i april eller, om dere mottok varsling i forkant, før saken ble kjent offentlig i august/september?

2.5 «Tredjepart har ikke hatt tilgang»

De to som avslørte sikkerhetsbristen, er så langt vi vet personer uten tilknytning til Norconsult. Slik fremstår det i medieomtale og informasjonen vi har mottatt direkte fra de to varslerne. Det synes åpenbart at to privatpersoner som ikke har et ansettelsesforhold i Norconsult må regnes som «tredjepart».

Står Norconsult fast ved utsagnet i informasjonsskriv datert 20.04.18, om at tredjepart ikke har fått tilgang til informasjonen i ISY PA?

2.6 Varsling

Informasjonen vi mottok den 20. april 2018 fra Norconsult ble sendt via epost til, så langt vi kjenner til, kun én av våre medarbeidere fredag ettermiddag klokken 15.41.

Dette er ikke en tilfredsstillende varslingsløsning, fordi den er svært sårbar ved ferie og sykdom. I tillegg tilsier tidspunktet som informasjonen sendes ut på, at den i mange tilfeller først vil bli fanget opp etter helgen. Da har sikkerhetshullet vært åpent i ytterligere to dager.

Vi forventer en mindre sårbar og bedre varslingsrutine i fremtiden. Slike varsler må sendes til flere personer hos oss.

Hvordan vil Norconsult sikre at slike varslinger når frem til flere relevante mottakere i fremtiden?

MOVAR IKS er et selskap med høyt fokus på IKT-sikkerhet. I denne saken har vi selv vært nødt til å gjennomføre en grundig analyse av trafikkloggene inn mot ISY PA i MOVAR. Her fant vi ikke spor etter annen ureglementert trafikk, enn fra varslerne i de periodene de selv har oppgitt å ha vært aktive. Denne kvalitetssikringen var ikke gjennomført av Norconsult, da vi var i kontakt med dere på telefon 5. september 2018.

Upresis og manglende informasjon fra Norconsult, gjorde oss ikke i stand til å håndtere situasjonen på en god måte. I forsideoppslag og tilhørende artikkel, blant annet på nett og papirutgaven til Moss Avis den 6./7. september, fremstår MOVARs informasjonssikkerhet som lite tillitsvekkende. Dersom

Norconsult hadde håndtert informasjonsansvaret sitt på en bedre måte, ville MOVAR kunne håndtert situasjonen bedre, og unngått omdømmetap.

Erfaringene våre med Norconsult Informasjonssystemer AS, blant annet i denne saken, vil bli tillagt vekt i fremtidige anskaffelsesprosesser.

Vi ser frem til å motta Norconsults svar på våre spørsmål **senest innen 1. oktober 2018**.

Med hilsen

Johnny Sundby
Adm. direktør

Dette dokumentet er elektronisk godkjent og trenger dermed ingen underskrift.

Ingen personopplysninger har kommet på avveie for renovasjonskundene i Moss, Rygge, Råde, Vestby og Våler. Det er konklusjonen etter grundige undersøkelser i MOVAR IKS. I april i år ble det avdekket et sikkerhetshull i et fagsystem som administrerer kundeinformasjon for hele 75 renovasjonsselskaper i Norge.

- MOVAR IKS ble informert om sikkerhetshullet av vår leverandør Norconsult i april. Da satte vi umiddelbart i gang tiltak, og var en av de første som tettet dette sikkerhetshullet i Norge. Først de siste dagene har vi fått informasjon om at alvorlighetsgraden i hendelsen var høyere enn vi hadde grunn til å forstå. For eksempel at sikkerhetshullet ikke ble avdekket av vår leverandør, men av to som ikke jobber for vår leverandør, forteller administrerende direktør Johnny Sundby.

Svakheten ble avdekket av to personer med svært høy IT-teknisk kompetanse, som gir uttrykk for at de ønsker å sette fokus på informasjonssikkerhet i offentlig sektor. De meldte fra om svakheten til systemleverandøren Norconsult og Datatilsynet.

Følger opp leverandøren tett fremover
MOVAR har analysert all inngående datatrafikk på tjenesten tilbake til november 2016. Undersøkelsene har ikke avdekket annen unormal aktivitet, enn fra de de to personene som har jobbet med å dokumentere svakheten i programvaren fra Norconsult. Konklusjonen er derfor at ingen personopplysninger om våre kunder har kommet på avveie.

- Det er alvorlig når informasjonssikkerheten ikke er god nok, og det er vi de første til å beklage. Personopplysningene lå ikke åpent synlige eller søkbare for folk flest. Personer med særskilt høy teknisk kompetanse kunne allikevel utnytte svakheten i programvaren ISY PA fra Norconsult til å hente ut enkelte personopplysninger gjennom målrettede angrep. Da ville de eventuelt ikke fått ut opplysninger om våre kunders betalingshistorikk. Disse opplysningene er lagret i et annet datasystem, forteller Sundby.

MOVAR vil følger opp leverandøren av programvaren tett fremover, for å forsikre seg om at informasjonssikkerheten er ivaretatt.

Stort fokus på informasjonssikkerhet
MOVAR har hatt et stort fokus på informasjonssikkerhet over tid, og jobber aktivt på dette området. I 2016 engasjerte vi bl.a. et eksternt firma til å teste IT-sikkerheten eksternt og internt, gjennom såkalte penetrasjonstester og målrettede angrep. Rapporten viste at MOVAR IKS har en høy grad av informasjonssikkerhet, som følge av systematisk arbeid over tid, gode rutiner og en rekke sikkerhetstiltak.

MOVAR-appen er trygg
Vi lanserer i disse dager MOVAR-appen. Til tross for sikkerhetsbristen hos vår leverandør Norconsult, ville det ikke vært mulig å hente ut andre opplysninger via denne tjenesten, enn adresser, hentetidspunkt og avfallstype fra vår tømmekalender. Dette var tilfelle hos andre renovasjonsselskaper som var rammet av den samme svakheten.

Sist oppdatert 17. September 2018, kl 12:30

Opprettet 6. September 2018, kl 12:12