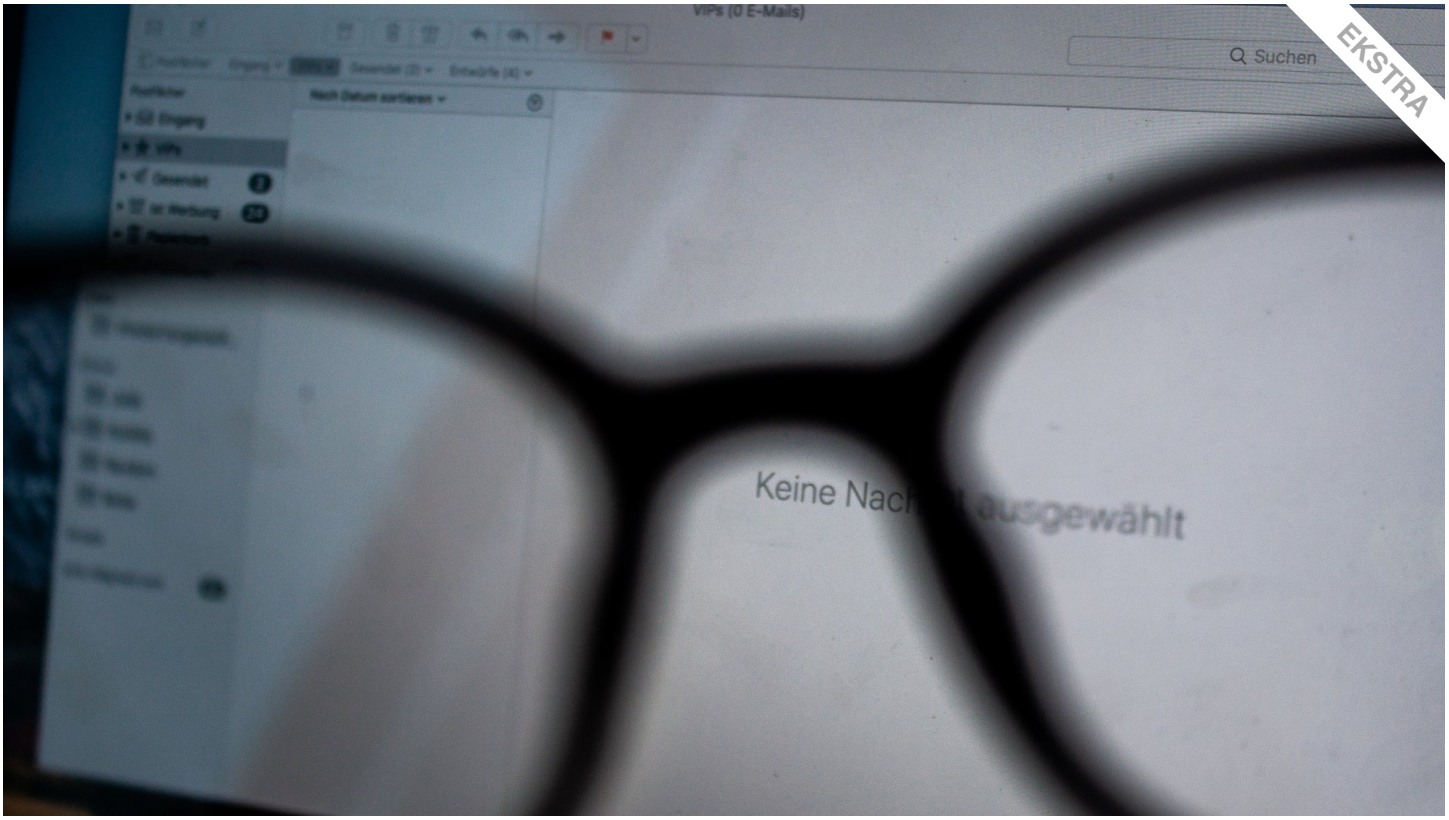


Apples mail-tjeneste. (Foto: Eirik Tangeraas Lygre)

Dropp Gmail, Outlook og Icloud: Norsk utfordrer klart best på personvern

Stor gjennomgang.

AV: EIRIK TANGERAAS LYGRE | PERSONVERN | PUBLISERT: 21. JUNI 2018 - 13:17

Den er helt grunnleggende i det moderne arbeidslivet. Arbeidsdagen består for mange av å være avsender og mottaker av e-poster. Her lagres alt du foretar deg på jobb, og mye av det du gjør ellers også.

Men kan en alltid stole på e-postklienten sin? En rekke søksmål mot Google tyder på at svaret er nei.

I 2016 kom det frem at studenter ved University of California, Berkeley hadde reist søksmål mot internettgiganten. Bakgrunnen var at Google uten samtykke hadde fanget opp og skannet e-postkontoer av reklamehensyn.

Skanningen skal ha funnet sted mellom 2010 og 2014.

Dette hele skal ha foregått i Google sine «Apps for Education», der Gmail er en av kjerneapplikasjonene. 30. april 2014 annonserte selskapet at de skulle avslutte praksisen. Mange tolket dette som at Google vedgikk at skanningen før den tid var lovstridig.

Datatilsynet kjent med praksisen

– Vi er kjent med at Google har skannet e-postene til vanlige brukere og brukt det til reklameformål, sier juridisk rådgiver i Datatilsynet Tobias Judin.

– Heldigvis har de nå sluttet med å skanne vanlige Gmail-kontoer av markedsføringshensyn. Nå gjør de det bare av andre årsaker slik som å oppdage spam.

(Saken fortsetter under bildet)

Tobias Judin er juridisk rådgiver i Datatilsynet. (Foto: Eirik Tangeraas Lygre)

Judin håper at den kommende EU-forordningen Eprivacy Regulation legger ytterligere begrensninger for skanning av e-post.

Strengere krav til samtykke vil trolig føre til at e-postbrukere i framtiden kan være trygge på at e-postene deres bare blir gjennomgått av sikkerhetsformål, spår han.

Norsk tjeneste på topp

En rapport utført ved Wirtschaftsuniversität Wien er nedslående lesning for alle som bruker Gmail, Outlook eller Icloud.

Den er derimot oppløftende for det vesle selskapet Runbox i Oslo. E-postleverandøren med tre ansatte kommer nemlig vesentlig bedre ut enn Google, Microsoft og Apple med sine mellom 74 000 og 124 000 ansatte.

Årsaken er delvis at Runbox leverer e-posttjenester mot betaling, og dermed ikke har en forretningsmodell som er avhengig av informasjonen din, skriver rapportforfatterene.

> **«Alle tjenester har sin pris, enten i kroner eller personopplysninger eller begge deler»**

– Dette er et dilemma. Alle tjenester har sin pris, enten i kroner eller personopplysninger eller begge deler. Da vil mange ønske å heller betale i kroner, sier Judin.

– Samtidig ønsker vi ikke å ha et A-lag og B-lag, der de med minst å rutte med må ta til takke med dårligere personvern. Personvern er en menneskerett, og reglene skal verne om alles personvern, ikke bare de som kan betale mer, mener Datatilsynet-rådgiveren.

En del aktører – inkludert Google – har ikke fullstendig kryptert e-post-trafikken sin. Det betyr at sensitiv informasjon enklere kan fanges opp av uvedkommende.

Gmail svakest på personvern

I gjennomgangen blir fem e-postleverandører vurdert langs parametrene som står listet opp i faktaboksen til høyre. Digi.no har plukket ut de som angår personvern.

Gmail skårer aller svakest på personvern ved standardinnstillinger. Google-tjenesten kommer også dårlig ut på informasjonskontroll og brukermedvirkning.

Hakket bedre ser det ut på personvern ved utforming og atferdskontroll.

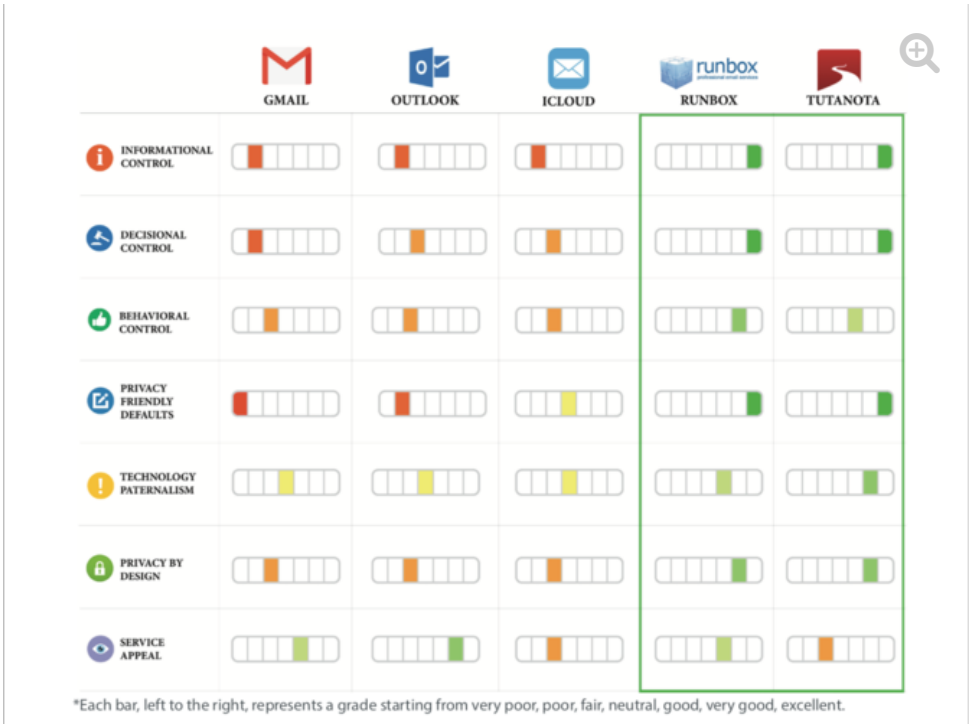
Kort om kriteriene:

- **Informasjonskontroll**: Vurderer hvorvidt tjenesten informerer fullstendig og sannferdig om praksisen deres for databehandling.
- **Brukermedvirkning**: Vurderer i hvilken grad bruker informeres om og kan nekte deling, behandling og videresalg av egen persondata uten å «straffes» for det i form av dårligere funksjonalitet.
- **Atferdskontroll**: Ser på hvorvidt tjenesten respekterer brukernes valg og implementerer deres preferanser i tjenesten, eller om det ganske enkelt sendes nye forespørsler om datainnsamling.
- **Personvern ved utforming**: Vurderer hvor mye vekt som ble lagt på personvern ved utformingen av tjenesten. Er dataoverføringene gjennomgående kryptert og bare tilgjengelig for avsender og mottaker?
- **Personvern ved standardinnstillinger**: Ser på i hvilken grad tjenesten ivaretar personvernet uten at brukeren endrer på innstillingene. Vurderer om leverandøren kun samler inn det minimum av data som kreves for å levere meldingstjenesten.

Outlook og Icloud blir plassert en hårsbredde foran, men Apple og Microsoft-appene ligger hestehoder bak norske Runbox og tyske Tutanota.

De to sistnevnte blir trukket frem som gode alternativer for personvernbevisste brukere. Tutanota er basert på åpen kildekode, og tilbyr kryptering ende-til-ende – også av kontaktlister og vedlegg som ofte blir utelatt kryptering.

(Artikkelen fortsetter under bildet)



Gjennomgangen fra Wien-universitetet viser at norske Runbox kommer aller best ut. (Foto: Skjermdump)

Slik sikrer du deg

Dersom du vil sikre e-posten din bedre finnes det heldigvis råd, viser Wien-rapporten til. Her er noen tips til hvordan personvernbevisste kan beskytte seg – i starten heller elementære ting, til slutt mer tidkrevende og omfattende grep.

- Se til at passordet ditt er sikkert. Bytt med jevne mellomrom.
- Bruk en sikker forbindelse. E-postleverandører tillater deg å bytte til en kryptert «HTTPS»-forbindelse i stedet for «HTTP».
- Aldri åpne vedlegg eller lenker fra mistenkelige avsendere. Dobbeltsjekk når du er i tvil.
- Bytt til en betalt e-postleverandør som ikke krever informasjon om deg for å levere tjenesten.
- Registrer e-posten din i landet som til en hver tid har strengest personvernlovgivning. Se til at all trafikken din skjer over VPN.
- Bruk PGP for e-post-trafikk. Slik sikrer du at alt innholdet er kryptert.
- Den skuddsikre løsningen: Dersom du har fagkunnskapen som trengs kan du fint sette opp din egen e-post-server og lage din egen kryptering. Da trenger du i svært liten grad å bekymre deg for angrep eller bakdører, og du kan være sikker på at ingen uvedkommende kikker deg over skuldrene.

Forbrukerteknologi | It-bransjen | Personvern