TEMASERIE FRA IT-AVDELINGEN VED UNIVERSITETET I BERGEN / NUMMER 2 › 2009

E-POST VED UIB

LEDER

Dette er nr 2 i IT-avdelingens nye temaserie. Tilbakemeldingene på første nummer (lagring og backup) har vært veldig positive og det har gitt oss tro på at informasjonen er både nyttig og ikke minst brukervennlig. Vi blir og motivert av tilbakemeldinger, både ris og ros og forslag til hva universitetets ansatte og studenter vil vite mer om. Hovedhensikten med informasjonsserien er å skape en merverdi for flertallet av brukere av IKT-tjenester ved UiB.

Dette nummer handler primært om tjenesten e-post og litt om sikkerhet ifm tjenesten. E-post er en av UiBs viktigste IKT-tjenester. Tjenesten vil blant annet bli inkludert i UiBs nye IKT kontinuitetsløsning når denne blir fullt operativ i løpet av 2010.

Tidligere i år ble arbeidsgivers rett til innsyn i blant annet ansattes e-post regulert i ny lov. Loven gir arbeidsgiver rett til å søke tilgang til ansattes e-post dersom det er nødvendig for å ivareta den daglige driften eller andre berettigede interesser ved virksomheten. UiB har og vil ha en mer restriktiv politikk for innsyn enn det loven gir anledning til. UiBs regler for innsyn er dokumentert i det reviderte IKT-reglement (UiB regelsamling) som er forelagt for godkjenning av UiB styret i desember 2009.

Selv om UiB har en restriktiv politikk for innsyn bør alle ansatte ved UiB vise varsomhet med privat bruk av sin UiB e-post adresse. IT-avdelingen anbefaler at alle ansatte som ikke har en privat e-post adresse skaffer seg dette. I dag er det ingen problemer med å opprette gratis private e-post kontoer som er stabile og driftssikre.

I mars planlegger vi neste nummer om "klientdriftede PC-er". Dette vil inkludere Windows, Linux og Mac. Før sommeren vil vi også skrive om tjenester for utskrift, kopi og OCR. Til høsten vil vi fokusere på programvare / filformater.

God lesing!

Thomas Evensen
IT-direktør

POSTEN SKAL FRAM..ELLER?

Visste du at det meste av e-posten som sendes aldri når fram? Eller at e-post er en olding i IT-verden?

E-post runder 40 år i 2010, og det er en høy alder for en IT-tjeneste. Opprinnelsen var enkel, åpen og basert på gjensidig tillit. Moderne e-postklienter har fått utvidet funksjonalitet og integrasjon med andre programmer og tjenester. Om dette ikke brukes riktig, kan det gå utover både effektivitet og sikkerhet.

Selv om denne tjenesten er svært mye brukt, har utviklingen vært liten. Dette innebærer også at e-post blir utsatt for en del misbruk. De som ønsker å utnytte svakhetene har en relativt lett jobb, et stort marked, og har hatt god tid på seg til å utvikle sine metoder.

To enkle regler for å begrense dette er å ikke svare på uønsket e-post, og å unngå ukritisk spredning av egen og andres e-postadresse.

EN RYDDIG INNBOKS

Utstrakt bruk av e-post og vedlegg av dokumenter kan føre til at e-postkontoen fort kan bli fylt opp. Men lagringsplassen er ikke ubegrenset, og e-posten går generelt treigere med store datamengder i systemet. Derfor er det lurt å sortere ut e-post fra innboksen din.

En grei måte å arkivere e-post er å lage egne mapper som du overfører e-post til. Dette kan være basert på tema, dato, avsender etc, og hjelper deg til å ha en bedre oversikt. Sletting av e-post med lite relevans kan med fordel gjøres hyppig. På denne måten sørger du for å holde innboksen slank og smidig. Opplever du at e-postklienten din går tregt kan en stor innboks være årsaken til det.

Andre tips rundt en stor innboks: Konsentrer deg om de største e-postene. Vanligvis kan du klikke på kolonneoverskriften "Størrelse" i e-postklienten din slik at de største e-postene vises samlet.

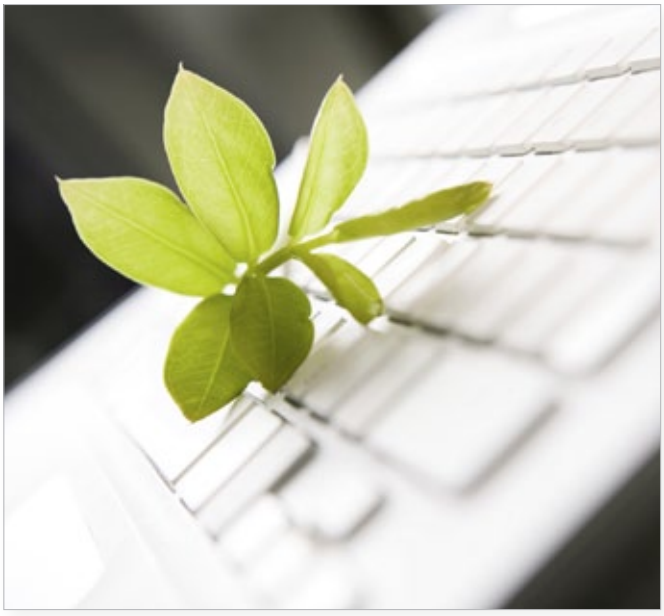
Vedlegg i e-post tar ofte stor plass. Disse kan du lagre på hjemmekatalogen din og så slette meldingen. Husk å fjerne e-posten fra mappen "Slettet e-post". Ellers ligger e-posten fortsatt på serveren.

En Outlook-bruker kan ha inntil 1 gigabyte (1000 megabyte) med e-post liggende på Exchange-serveren. I dette inngår alle mappene; innboksen og andre mapper du har laget. Hvis du når denne grensen, må du arkivere e-post lokalt på hjemmekatalogen din. Fremgangsmåten finner du på nettsiden: **it.uib.no**, under "E-post" og "Overskredet lagringsplass".

Bruker du EXIM vil begrensingen være gitt av størrelsen på hjemmekatalogen din. Denne er i utgangspunktet på 10 gigabyte.

HUSK!

Vedlegg tar mye plass. Rydd i postboksen og bruk e-postlister og/eller vedlegg på vev.



GRØNT IT–TIPS: SPAR PLASS

La oss si at du ønsker å sende en e-post med et vedlegg til en større gruppe mottakere. Kanskje vedlegget er en kombinasjon av tekst og bilde. La oss tenke oss et vedlegg med størrelse på rundt 2 megabyte. E-postlisten du sender det til har kanskje 100 mottakere. Dette gir et lagringsbehov på e-postserverne våre på rundt 400 megabyte bare på denne ene forsendelsen. Dette er med på å øke behovet for disker, belastning på systemet, ytterligere kjøling av serverne etc. – altså kostnads- og energikrevende.

Alternativet er å lagre vedlegget på et åpent område og sende en lenke til denne filen på e-post. Da tar e-posten bare brøkdeler av plassen, mottakerne får den sammen filen, og vi sparer litt på den tekniske siden. Les mer på: **https://tjinfo.uib.no/vedlegg.html**

Flere filer kan også pakkes til en enkelt som tar mindre plass.

SENDER DU OFTE E-POST TIL MANGE MOTTAKERE?

Kanskje opprettelse av en sentral e-postliste kan lette administrasjon av mottakere? Da administrerer du listen via vev. Du kan gjøre en del valg selv, som blant annet om det skal gå an å melde seg på og av listen selv, og hvem som kan sende til listen. Du vil også spare deg en del feilmeldinger. Registrer en sak i **bs.uib.no** om dette er noe for deg. Sentrale lister sparer også e-postsystemet for ressurser ved at en e-post sendes i stedet for en til hver mottaker.

For flere e-posttjenester, se **https://tjinfo.uib.no**

HVEM KAN LESE E-POSTEN?

Når du har sendt en e-post, har du ikke lenger kontroll med hva som skjer med den. Mottaker kan for eksempel videresende den. Dette gjelder uavhengig av e-postsystem.

I Outlook går det an å dele e-post, kalender, oppgaver og kontakter med andre. Det du da gjør, er at du lar andre få lov til å se og eventuelt endre det som ligger i din personlige Outlook-konto. Det er du som styrer hvem du vil dele innhold i Outlook med. I utgangspunktet ser ikke andre Outlook-brukere innholdet i din e-post, dine personlige avtaler osv.

Det er du som styrer hvem du vil dele innhold i Outlook med

For lett å kunne finne passende møtetidspunkt, kan andre se når du er ledig i følge kalenderen. Mange synes også det er praktisk at de som vil kalle inn til møter kan se innhold i avtaler. Det kan jo være nyttig å vite om vedkommende er på nabokontoret, på forelesning eller i Tanzania.

HUSK!

Vær obs på at Outlook-brukere kan dele e-post, kalender osv. med andre

Noe ikke alle tenker over er at de som har tilgang til en delt kalender også får se det eieren mottar fra tredjepart. Dette inkluderer blant annet vedlegg til møteinnkallinger via Outlook. Kaller du inn til møte og for eksempel legger ved personalsaker, så er dette tilgjengelig også for alle som møtedeltagerne deler kalender med. Hemmelig eller sensitiv informasjon bør derfor aldri legges ved møteinnkallinger i Outlook.

MISBRUK AV E-POST

E-post er et billig kommunikasjonsmiddel som lett kan misbrukes. Disse fremmedordene beskriver metoder som teknisk sett er lett å gjennomføre:

SPAM

er uønsket e-post sendt ut i store mengder, typisk reklame for produkter med et tvilsomt ry eller med uhederlige baktanker. Avsender er normalt forfalsket.

PHISHING

er e-post, som regel masseutsendt og med forfalsket avsenderadresse, som prøver å lure hemmelig informasjon fra mottakerne

SNIFFING

er innhenting av (e-post)informasjon på vei fra avsender til mottaker

SPOOFING

er forfalsking av avsenderadresse

HOAX

er falsk virusvarsel som ber deg videresende til alle du kjenner

NOEN RÅD FOR SIKKER E-POST

Oppgi aldri passord på e-post

Ikke svar på eller følg instruksjoner i en spam-melding. Du bekrefter bare at adressen din er i bruk. Bare slett e-posten.

Vær varsom med å oppgi sensitiv informasjon på e-post

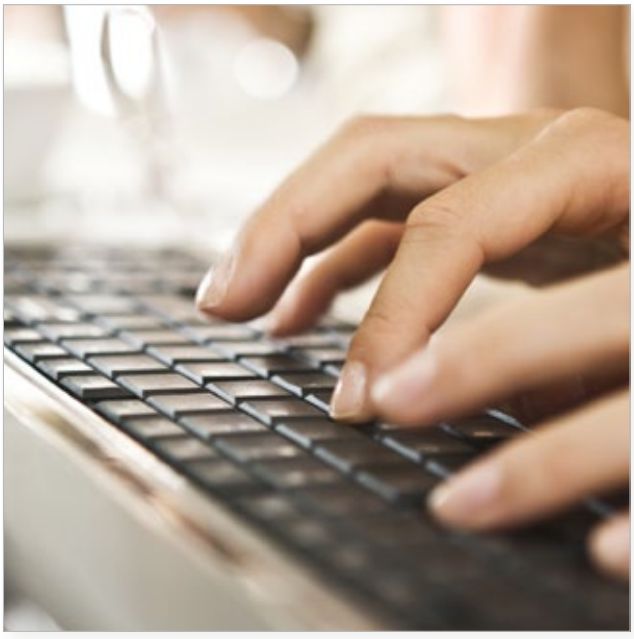
Vær skeptisk til vedlegg du ikke forventer fra avsender

Husk at både avsenderadresse og svaradresse kan være endret

Ikke videresend kjedebrev eller masseutsendelser til venner og bekjente

Vær forsiktig med hvor du oppgir din eller andres e-postadresse

Unngå automatisk videresending fra privat e-postadresse til UiB-kontoen



HVOR ER E-POSTEN DIN?

All e-post som sendes inn og ut av UiB går gjennom Exim. Her blir e-posten filtrert for spam og virus før meldingene sorteres for levering til mottaker. Det kan være til eksterne adresser, til interne lister eller personlige brukerkontoer.

Fra Exim går meldingen enten til Exchange, kalendersystemet som blir brukt av mange tilsatte med Outlook, eller til de tradisjonelle unix-serverne for ansatte og studenter, henholdsvis alf og rasmus, hvor e-posten blir tilgjengelig med standardprotokollen IMAP ved hjelp av Dovecot.

Om noe av e-posten ikke når frem til deg, kan det være at det ene e-postsystemet er feilinformert om hvilket system du bruker. Du kan sjekke dette i det andre e-postsystemet via **webmail.uib.no**, og eventuelt kontakte BRITA.

E-post kan også leses på mobilen. Men kjøp da en modell som er testet og godkjent av IT-avdelingen.

UIBS E-POSTSYSTEMER

EXCHANGE
Microsofts integrerte løsning

EXIM
Open source internet-mailer fra Cambridge Universitet

DOVECOT
Open source IMAP-server fra finsk ildsjel

FØR E-POSTEN HAVNER I INNBOKSEN DIN

Emner vi tradisjonelt har forbundet med uønsket e-post, er i stor grad erstattet av organisert kriminell virksomhet som id-tyveri og økonomisk svindel. Oppfinnsomhet og omfang gjør at det kan være vanskelig å spore og stanse all denne e-posten, spesielt også når en tar hensyn til den enorme mengden e-post som forvaltes av UiBs postsystem.

Daglig behandler UiB godt over 1 million e-poster. Det aller meste, rundt 1 million, blir umiddelbart forkastet pga. ukjent mottaker. Av den øvrige e-posten vil rundt 200.000 e-poster vurderes som uønsket og stanses. Vi står igjen med ca. 100.000 e-post som daglig leveres til mottaker her på UiB. I snitt regnes det med en avvisning av e-post på ca. 70% på virkedager og ca. 90% på helligdager.

Før det blir avgjort om en e-post skal leveres til mottaker, eller avvises, går den gjennom flere tester.

Først sjekkes avsenders ip-adresse (maskinens unike adresse på nettet) mot interne og eksterne svartelister. Hvis ip-adressen aksepteres vil e-postens avsenderadresse bli kontrollert. Da sjekkes brukerdelen (til venstre for '@'), domene/organisasjonsdelen (til høyre for '@') og hele adressen mot lister over uønskede avsendere. »

Hvis det tidligere ikke er levert e-post til UiB fra ip-adressen e-posten kommer fra, vil vi gjøre et forsøk på å finne ut om maskinen bak ip-adressen er en ekte e-posttjener eller en infisert hjemmemaskin. Dette gjøres ved å bruke to teknikker kjent som hhv. tarpit og grålisting. Tarpit går ut på å bevisst legge inn en forsinkelse i kommunikasjonen mellom e-posttjener og klient, noe som er fullt lovlig. Grålisting går ut på at e-posttjeneren, i prosessen med å motta en e-post, svarer; "Beklager, men det har oppstått en temporær feil, prøv igjen senere". Klienten må da vente en viss tid før e-posttjeneren vil akseptere en ny oppkobling og motta e-posten.

Begge disse tiltakene utnytter det faktum at virus og programvare som sender ut spam ofte er av lav kvalitet og ikke har all den funksjonaliteten som er definert for behandling av e-post.. Dette virker. 10% av uønsket e-post blir avvist på denne måten.

Til slutt prøver vi å verifisere om avsenders e-postadresse er gyldig. Dette gjøres ved å sende en forespørsel til den e-posttjeneren som er oppført som eier av avsenders e-postadresse, og spør om den aksepterer e-post til denne brukeren.

E-posten vil nå bli gjenstand for en innholdstest. Det er viktig å presisere at det er en helt maskinell prosess som bare leter etter ord og ordkombinasjoner, webadresser (url), og andre predefinerte mønster, for å avgjøre om dette er e-post som skal avvises som spam eller leveres til mottaker.

Innholdstesten går ut på å vekte forekomsten av ulike ord, ordkombinasjoner, webadresser o.l. Webadresser sjekkes mot eksterne svartelister. Hver e-post får nå en rangering som avgjør om e-posten blir levert til mottaker eller avvist som spam. Selv om en e-post blir avvist på denne måten, så tas det kopi av e-posten slik at den kan etterleveres hvis mottaker ønsker det. Denne innholdstesten gjennomføres daglig på rundt 300.000 e-post. Når en vet at enkelte av registrene som benyttes for testing, har millioner av innslag, forstår en at det er et stort apparat i sving hele tiden. Kompleksiteten økes ytterligere ved at det for et 10-talls tabeller med regler også finnes mange tabeller med unntaksregler. Dette krever en tett oppfølgning fra IT-avdelingens systemansvarlige for å justere, oppdatere og vedlikeholde funksjonaliteten i disse løsningene. Alt dette for at du skal slippe å få uønsket e-post i innboksen din.

I snitt regnes det med en avvisning av e-post på ca. 70% på virkedager og ca. 90% på helligdager

HUSK!

Vær forsiktig med hvor du oppgir din eller andres e-postadresse

HVORFOR STOPPES E-POST TIL MEG?

Som bruker av e-post opplever vi innimellom at forventet e-post ikke dukker opp. Dette kan selvsagt ha med avsender å gjøre, men det er også en mulighet for at e-post blir stoppet hos oss.

Siden det er mest maskiner (ip-adresser) som svartelistes, så er det nok at en bruker på en del av nettverket har vært uforsiktig og fått infisert maskinen sin. Den delen av nettverket maskinen står på kan da bli svartelistet. UiB vil da, som mange andre, ikke ta i mot e-post fra denne nettverksdelen, selv om den kommer fra en maskin som ikke er infisert. Dette er først og fremst et problem for folk som sender e-post fra hjemmemaskiner og for mindre organisasjoner som deler nettverk med mange andre. Det skal likevel mye til for at seriøse organisasjoner og partnere skal bli svartelistet.

Det er kun den enkelte e-postmottaker som alltid kan være helt sikker på hvilke e-post hun ønsker å motta. Uansett hvor gode systemer spamkontrollen har, vil alltid noen få meldinger havne feil. Noen e-post havner i innboksen selv om mottaker ikke ønsker dem. De kan lett slettes. Verre er det om ønsket e-post ikke når frem. Postmaster er rask med å stanse levering når avsender er svartelistet eller e-posten vurderes som spam. Men på forespørsel er de også raske med å reversere hvis vurderingen var feil.

Noen har satt opp private e-postkontoer slik at deres e-postadresse på UiB står som avsender. I slike tilfeller er det ikke UiBs servere som står for utsendelse av e-post, men den tilbyderen en benytter privat. Skulle denne tilbyderens server være svartelistet vil all e-post fra denne stanses, uavhengig av hva avsenderadressen i e-posten måtte være.

Har du spørsmål rundt savnet e-post, kan du ta kontakt med brukerstøtte. Vi trenger avsenders e-post eller e-post-domenet og omtrentlig tidspunkt for å ta saken videre.

AKTUELLE TJENESTER

IT-avdelingen tilbyr noen tjenester rundt e-post som kan være interessante:

OVERSIKT OVER STOPPET E-POST

Du kan få tilsendt en ukentlig oversikt over all e-post som er stanset for levering til din konto. Gå inn på følgene webside for å abonnere på denne tjenesten: **https://tjinfo.uib.no/wantspamrep**

GJØR MIN E-POSTADRESSE UBLOKKERBAR

Her kan du ta forbehold mot at IT-avdelingen avviser e-post til deg. E-post som normalt ville bli stoppet av spam-filtrene vil da leveres til din konto. Merk at du her også kan reaktivere spamfilteret hvis og når du ønsker det. Webadresse: **https://tjinfo.uib.no/wantspam**

MIDLERTIDIG E-POSTADRESSE UTEN SPAMFILTRERING

I noen tilfeller må man oppgi sin e-postadresse på web for å motta en tilbakemelding fra et sted på nettet. Det kan for eksempel være bestilling på hoteller eller nettsider som krever at det oppgis en e-postadresse for å få tilsendt et passord eller lignende. Dessverre kan en slik melding ofte *ligne på spam* og vil kunne bli avvist.

Dette kan du omgå ved å lage en midlertidig mottakeradresse som ikke spamsjekkes. Mer om dette på webadressen: **https://tjinfo.uib.no/safemail**

VI SNAKKER MED: POSTMASTER

Forvaltning av vårt e-postsystem ligger under den litt flyktige tittelen postmaster. Som i andre tilfeller er ikke dette en person, men en rolle som deles mellom flere.

Siden temaet denne gang er e-post, har vi snakket med senioringeniør Hans Morten Kind og overingeniør Trond Davidsen ved IT-avdelingen, halvparten av teamet **postmaster@uib.no**. Resten heter Kjell Rune Abbedissen og Ivan Vågenes.

Er e-post et sikkert kommunikasjonsmedium?

Trond: Nei – e-post er ikke pålitelig. SMTP-protokollen (fremføringsmotoren for e-post) har ingen leveringsgaranti. Heller ingen garanti mot endring av innholdet underveis i forsendelsen, eller garantier rundt avsenders autentisitet (at avsender virkelig er den en utgir seg for å være).

Hans Morten: Enhver bedrift eller organisasjon står fritt til å gjøre en lokal vurdering av om innholdet er spam, og derfor har en ikke noen garanti for levering.

Trond: Eneste reelle alternativ for å kunne garantere en e-post mot endring er å kryptere e-posten.

Hans Morten: Det finnes dog ikke etablerte internasjonale nettverk for nøkkelutveksling, så kryptering må avtales mellom de enkelte brukere.

Leveringsgaranti – hva ligger det i dette?

Trond: Med leveringsgaranti tenker vi bl.a. på om vi kan garantere at en e-post kommer frem til mottaker. Vet avsender om e-posten virkelig når mottaker eller blir stoppet i et spamfilter på veien? Eller om e-posten ble levert til mottaker? Adresseforfalsket e-post kjenner vi jo alle til. E-post garanterer ikke avsender eller innhold, noe som gjør at det f.eks. kan sendes spam i andres navn. Folk tror nok gjerne at e-post er mer pålitelig enn det protokollen kan garantere.

Hans Morten: Det er i prinsippet like enkelt å forfalske en e-post som det er å forfalske et postkort.

Vedlegg i e-post er skumle ting. Hvordan bør vi forholde oss til det?

Trond: Vedlegg til e-post skannes når e-posten ankommer UiB. Men tradisjonelt anbefales det ikke å åpne vedlegg hvis ikke dette er et vedlegg du forventer fra avsender. Dette er jo noe av det som ligger i begrepet "social engineering" - å lure folk til å gjøre noe de ikke vil gjøre.

Hans Morten: Rutinene rundt skanning av vedlegg i e-post som kommer til UiB er gode. Problemet er "zero-day", altså før skannerprogramvaren er oppdatert med en spesifikk virusdefinisjon.

Noen råd til brukerne?

Trond: E-post som er sendt til deg bør du ikke videresende (forward) til andre uten videre. Dette er enkelt og greit dårlig folkeskikk. Vurder hva som er sendt til deg og husk på at den som sendte dette ikke nødvendigvis ønsker at dette skal videre. Kanskje avsender ser på dette som fortrolig. Sjekk i det minste med avsender og spør om det er OK at du sender e-posten videre.

Hans Morten: Begynn på en ny e-post og unngå lange e-poster – ikke reply, reply, reply i det uendelige. Behold bare den delen du svarer på og ikke hele e-posten med hele historien. Vi har også tilfeller der folk kjører "reply" på e-post med sensitiv informasjon.

Trond: Dobbeltsjekk hvem du sender e-posten til. Det finnes nok tragiske historier her, og det kan få vanvittige konsekvenser hvis feil informasjon går til feil mottaker eller på felles lister.

Hans Morten: Det er ingen angreknapp etter at du har sendt en e-post! I praksis er det liten og ingen mulighet for å stanse eller hente tilbake en sendt e-post.

Begge har et inderlig ønske om at studenter og ansatte ikke automatisk videresender e-post fra sine private e-postkontoer til sin UiB-adresse. Gratis e-post tilbydere har gjerne liten, dårlig eller ingen spamfiltrering, noe som er med å øke belastningen på systemene våre.

Ivan Vågenes og Hans Morten Kind er to av UiBs postmastere, som sørger for at e-posten havner der den skal. »

Grafisk utforming: Formidlingsavdelingen, UiB

© 2009 Universitetet i Bergen | IT-avdelingen
Adresse: Postboks 7800 5020 Bergen
Besøksadresse: Nygårdsgaten 5
Telefon: (+47) 55584700 Faks: 55584299
Kontakt: post@it.uib.no
Ansvarlig redaktør: IT-direktøren
http://it.uib.no