

Troll privatskole

Dokumentets formål

Dette dokumentets formål er å kartlegge og forbedre selskapets interne brukerstøtte, oppfølging av support, effektivisering av brukerstøtte. Det tar også for seg bedriftens overvåkningsløsninger ihht. Sikker drift – så vel som brukeres vern for uønsket innsyn og angrep.

Situasjonsrapport

Troll privatskole (heretter omtalt som Troll) er en mellomstor, selveid bedrift og fungerer som en ordinær privatskole. Skolen har 150 ansatte med 132 årsverk. Skolen består av totalt to bygg i Bergen kommune bydel Bergenhus med sykkelavstand mellom. IT- avdelingen på skolen leverer IKT drifts og supporttjenester til ansatte, elever (heretter omtalt som brukere) og til eventuelle tredjeparter som låner skolens bygg på kveldstid til arrangementer (evt. Lokale lag, foreninger og politiske parti). Bedriften mottar mange henvendelser fra ansatte på skolen, primært relatert til brukerstøtte, og programvare. Dette ved siden av generelle henvendelser som dokumentet ikke tar for seg.

Henvendelser fra tredjepart går via skoleledelsen til IT- avdelingen, men utgjør en svært liten del av driften og henvendelsene til IT- avdelingen.

IT- avdelingen består av fem ansatte, hvorav fire er fast ansatt for avdelingen, mens den øvrige (heretter referert som Ola) er ansatt som lærer og IKT arbeider hvor skolens ledelse avser tid til IKT arbeid utenfor fast og vikarierende undervisning.

Av økonomiske- og sikkerhetsmessige hensyn er all serverdrift skilt ut til ekstern tjenestetilbyder. Server med applikasjoner, systemer og lagring gjøres gjennom skolens internettforbindelse.

IT- avdelingen benytter seg av VNC for fjernstøtte til skolens elever og ansatte. Operativsysteminstallasjoner skjer ved hjelp av minnepinne og en egenkomponert installasjon av Windows 7 – skolens operativsystem for ansatte. Elever står selv ansvarlig for operativsystem og lisensiert programvare, men hvor IT- avdelingen er behjelpelig innenfor support og oppdateringer.

Ansatte i IT- avdelingen har alle hver sin smarttelefon.

Målsetning

Etter avdelingsmøte tirsdag 5. juni 2012 ble det ytret ønske om å revidere og gjennomgå avdelingens håndtering av innkommende henvendelser. Dette kommer i lys av flere tilbakemeldinger fra ansatte i bedriften hvor muntlige beskjeder, så vel som skriftlige ikke har blitt fulgt tilstrekkelig opp – og i mange tilfeller – ikke er registrert i saksbehandlingssystemet.

Det er samtidig ytret ønske fra skolens ledelse at generell saksbehandlingstid skal ned fra ti arbeidsdager til syv arbeidsdager i løpet av høstsemesteret 2012, og fra syv til fem dager i løpet av vårsemesteret 2013. Dette stiller større krav til den enkelte ansatte i avdelingen, avdelingens verktøy for håndtering av supporthenvendelser og avdelingens arbeidsstruktur. Det er i den forbindelse også sendt en forespørsel til skolens ledelse om å få frigjort mer tid til IKT- gjøremål for Ola og mulighet for fast ansettelse på IT- avdelingen, i den grad bruk av IKT utstyr stiger raskt i undervisningsøyemed.

Det er i dag mulig for samtlige klasseforstandere / klasseveiledere, kontorpersonell og IT- avdelingen for å resette passord for samtlige elever på skolen. For ansatte i skolen er det IT- avdelingen og rektor på skolen som kan tilbakestille passord og brukerkontoer.

Det er kommet en bekymringsmelding fra elevrådet hvor personvernet til den enkelte elev, og elevene som gruppe er i fokus. Frykt for at andre enn eleven selv skal få tilgang til en elevs data, E-post og hjemmeområde (hver elev har 50Mb til disposisjon på skolens nett) er årsak til henvendelse. Elevrådet har i sin henvendelse til skolens ledelse ytret at dette allerede har skjedd – men uten å kunne dokumentere hendelsen. Rektor har derfor bedt IT- avdelingen om å hindre slikt fra å skje igjen. Både ovenfor skolens elever så vel som skolens ansatte.

Det er også meldt at ansatte og elever føler seg usikre på om de blir overvåket gjennom VNC og/eller TeamViewer. Begge grupper ønsker tilbakemelding på teknologiens virkemåte. Rektor ønsker forsikringer om at tjenesten ivaretar de ansattes og elevenes personvern.

Oppgave 1

a og b.

Fokus på stadig effektivisering og lønnsomhet i IKT bransjen har gjort det nødvendig å automatisere flest mulig tjenester, effektivisere arbeidsstrukturen og redusere kostnader.

Eksaminand vil derfor vektlegge besvarelsen noe mer i oppgave 1, a og b.

Brukerorientert drift

IT- avdelingen hos Troll har som mål å sette brukeren i fokus – ikke systemet.

Derfor har det vært bred aksept og vanlig praksis at skolens ansatte, elever og tredjepart kan kontakte og sende henvendelser til IT- avdelingen på den måten som måtte falle dem naturlig i sin hverdags- og arbeidssituasjon.

Dette har til i dag medført at IT- avdelingen har kontaktpunkter pr. E-post, telefon (åpningstid 08.00 – 15.30 på skoledager), egen chat kanal gjennom skolens internkommunikasjonsprogram - Lync, SMS, internpost (skriftlige notater), skriftlig og muntlig ved oppmøte til avdelingens servicemottak.

Det har også vært normalt at henvendelser kommer fra brukere og tredjepart muntlig i skolens miljø utenfor servicemottaket.

Alle henvendelser som blir mottatt legges inn i IT- avdelingens ticketsystem (TrackIT fra Numara) og blir løst fortløpende eller etter avtale med bruker. Henvendelser på E-post blir automatisk generert som en henvendelse i TrackIT som enkelt kan flyttes og tildeles en av de ansatte i IT- avdelingen. Henvendelser pr. telefon, chat, muntlig, skriftlig og SMS føres inn manuelt som et supportoppdrag.

Enhver sak (saks ID i TrackIT) blir deretter fulgt opp av en tekniker fortløpende. Enten over telefon, E-post eller ved fysisk oppmøte. Internpost, Chat og SMS er også en mulighet for å gi bruker tilbakemelding.

Etter avdelingsmøte tirsdag 5. juni har undertegnede brukt onsdag 6. juni til å kartlegge ansatte i IT-avdelingens trender og statistikk. Det ble også levert ut et enkelt spørreskjema til de ansatte på skolen om hvilke punkter de følte fungerte best, hva som kunne forbedres og hva som ikke fungerte tilfredsstillende ut i fra de ansattes ståsted. De ansatte besvarte også på vegne av elever. Et

tilsvarende – men med andre spørsmål – spørreskjema ble utlevert til alle på IT- avdelingen for hvilke områder vi selv mener vi kan forbedre oss på. Ut i fra disse tilbakemeldingene vil funksjonelle krav bli satt for hvordan drift og support kan forbedres, og saksbehandlingstid kan reduseres.

Det har også utført en kartlegging på separate og tilfeldig utvalgte henvendelser til IT- avdelingen hvor det viser seg at henvendelser innsendt gjennom chat og direkte oppmøte løses på gjennomsnittlig to arbeidsdager. Det viser seg også under kartleggingen at elever er de brukerne som er flinkest til å sende forespørsler pr. chat, fysisk oppmøte og SMS.

Det viser seg samtidig at henvendelser gjort med pr. internpost, muntlig og E-post tar lengst tid for å løse. Undersøkelsen blant de ansatte på IT- avdelingen viser ønske om kompetanseheving, ønske om flere brukere til å kontakte pr. chat, færre henvendelser pr. notat og ingen muntlige henvendelser utenfor servicekontoret ved fysisk oppmøte. Undersøkelsen viser også at det får mye tid med til reinstallasjon av datamaskiner og programvare og bomturer (henvendelser sendes pr. internpost, mail eller lignende) og når IT- avdelingen kommer til bruker er vedkommende gått for dagen eller ikke tilgjengelig. Dette har skapt mye unødvendig merarbeid og er mange skjulte kostnader for IT-avdelingen og skolen. IT- avdelingens ansatte forteller i brukerundersøkelsen at bruk av chat funksjonen så vel som fjernstyringsapplikasjonen er svært effektive tiltak mot disse tingene.

For å bedre gjennomføre avdelingens arbeidsoppgaver er det ønsket bedre synkronisering mellom TrackIT og E-post systemet Outlook. Dette for å kunne synkronisere teknikers gjøremål, brukers kontaktinformasjon og nødvendig saksinformasjon direkte til teknikers smarttelefon. Dette i ønske sammen med de ansatte selv hvor oppdateringer og endringer kan bli utført mens teknikere er på oppdrag – uavhengig av bygg.

Fjernstyring / fjernassistanse

Det vil også bli oppfordret at ansatte i større grad benytter seg av chat- funksjonen slik at IT-avdelingen kan fjernstyre datamaskinen gjennom VNC. Sikkerheten for personvern opp mot bruk av VNC vil vi komme tilbake til senere i dokumentet. Her vil tilgangskontroll og rettigheter bli revidert. Tilstrekkelig informasjon og opplæring i chat funksjonen vil bli distribuert og formidlet på førstkommende personalmøte.

Undertegnede finner det også nødvendig for å utvide driftsstøtteapplikasjonene da ikke alle skolens ansatte og elever er tilgjengelig i skolenettet. IT- avdelingen vil derfor oppfordre skolens ledelse til å anskaffe nødvendig antall lisenser for bruk av TeamViewer – en supportapplikasjon som vil fungere etter de krav IT- avdelingen og skolens ledelse har bestilt. Teknologien og dens virkemåte, sammen med VNC vil bli presentert for skolens ledelse samt elevrådet.

Et felles dokument vil bli utarbeidet i fellesskap på engelsk for å kunne informere elever som behersker Norsk mindre godt.

Kompetanseheving

Det er på generelt grunnlag, også i spørreundersøkelsen, ønsket av de ansatte i IT- avdelingen å få økt sin egen kompetanse, spesielt med hensyn til personvern. Det er også et gjengående ønske om økt kompetanse i drift og vedlikehold av operativsystemer fra Microsoft (konfigurering og utrulling av Windows 7) og Apple (iOS). Det utarbeides derfor et eget dokument utenfor dette som vil ta for seg

mulighetene og tjenestetilbydere som kan gi økt kompetanse hos medarbeidere, noe som vil hjelpe skolen i sitt mål om å redusere tiden for å løse en supporthenvendelse og økt effektivitet gjennom mer tilfredse og beherskende ansatte.

Automatisk programinstallasjon og administrering.

Som en av de mest forespurte henvendelsene til IT- avdelingen er applikasjonsstøtte. Oppdateringer av Java, Flash og Adobe Reader samt nyinstallasjoner av standardprogrammer i undervisningen er blant gjengangere til IT- avdelingen.

Mange brukere føler ubehag ved å oppdatere programmer de selv ikke kjenner til og ber derfor IT-avdelingen om råd og assistanse når programmene varsler om nye versjoner og oppdatering.

Undertegnede finner det derfor gunstig å anskaffe en lisensiert utgave av Ninite.

Tjenesten kan man finne på Ninite.com. Dette er et program som håndterer automatisk utrulling, oppdatering og avinstallasjon av aktuelle programvarer som støttes av Ninite – og om IT- avdelingen kan bestille en egen skreddersydd installasjon for. Dokumentet går ikke teknisk i dybden på denne applikasjonen. Dette gjøres med minimal brukerinteraksjon fra IT- avdelingen målt opp mot dagens situasjon med manuell oppdatering.

Informasjonstavler i ganger og personalrom

Det er ikke vektlagt stort fokus på dette punktet i gjeldende dokument.

Det er derimot sendt forespørsel fra IT- avdelingen om å få kunne publisere aktuelle nyheter og viktige meldinger på de ansattes- og elevenes infotavler. Infotavlene opereres pr. i dag utelukkende for administrative og undervisningsformål til de ansatte og elever på dagtid, og eventuell informasjon til tredjepart på kveldstid. IT- avdelingen ønsker tilgang til dette mediet for å varsle om viktige og aktuelle program- og systemoppdateringer, trender og trusler (eksempelvis phishing angrep på mail, forsøk på sosial manipulering i skolens nettverk). Henvendelse meldt fra leder på IT- avdelingen til skolens ledelse. IT- avdelingen avventer svar.

Tilgang til gjestenett for tredjepart

For å imøtekomme henvendelsen fra tredjepart er det ønskelig for Troll å anskaffe en skriver for automatisk generering av kontoer med passord til det trådløse gjestenettet. På den måten vil også disse kunne få tilgang til internett i Troll sine lokaler. Rent teknisk vil kontoen ha en levetid (være gyldig) i seks timer fra generering.

Kostnaden for en slik tilgangsskriver flettes inn i totalbeløpet for utleie av lokalene og vil tjene seg selv inn i løpet av første halvår, for deretter å være en merinntekt for skolen. Beløpet er kalkulert av skoleledelsen basert på anskaffelsesprisen til IT- avdelingen.

Skriveren er allerede bestilt av rektor.

Oppgave 2

a og b.

Eksaminand vil fokusere på de etiske og personvernrelaterte, også innenfor områdene inbefattet overvåkning, men tar teknologisk overvåkning i betraktning.

Overvåkning av data og brukere

Troll har i dag automatisk overvåkning av datatrafikk inn- og ut av skolen. Både i form av båndbredde innhold og tjenester. Dette gjøres automatisk gjennom skolens brannmur.

Brannmuretjenesten er levert av Palo Alto som tillater systemadministrator, databehandler og

behandlingsansvarlig til å kontrollere mengde bruk, til hvilket formål basert på tjeneste, nettside og applikasjoner - samt hvem på innsiden av skolens nett som har utført dette.

Det er derfor opprettet separate roller og rutiner for hvordan og når data fra brannmuren skal behandles. Databehandler kan analysere mengden trafikk og eventuelle alarmer fra brannmuren ved varsler om angrep og/eller virus. Tilgang til å se hvem på innsiden som har aksessert hvilke nettsider, tjenester og utført handlinger på nettet ligger utelukkende hos behandlingsansvarlig. Behandlingsansvarlig kan kun lese ut informasjonen i samråd med rektor, politi og/eller på oppfordring fra datatilsynet under revisjon. Behandlingsansvarlig skal kun uthente informasjon mens rektor eller rektors stedfortreder (eller politi/datatilsynets) tilstedeværelse.

Overvåkning av nettverk

Skolen har over en periode hatt problemer med datanett om har periodvis falt ut.

Med konsulent fra Cisco har nødvendig overvåkningsverktøy blitt installert for trådløse nett så vel som kablede nett.

Brukere som benytter det trådløse nettet. Administrativt, elev og gjestenett blir logget i kontrollerens logg. Denne loggen kan kun uthentes av behandlingsansvarlig.

Vern av roller – vern om personvernet

Behandlingsansvarlig har to brukerkontoer til brannmuren – hvorav den med tilgang til sensitiv informasjon ikke blir benyttet i tilfeller annet enn beskrevet over.

Dokumentasjonen og prosessen for uthenting av denne data ligger tilgjengelig i servicekontoret til IT-avdelingen slik at skolens ansatte, elever og tredjepart kan innhente informasjon. Dette ihht. Bestemmelser om innsynsrett. Denne dokumentasjonen vil bli gjennomgått og signert lest av elevrådsleder og rektor sammen med undertegnede. Eventuelle korreksjoner i dokumentasjonen vil bli utført i samarbeid med partene, innenfor IT-avdelingens retningslinjer og med hensyn til personvernet og personopplysningsloven.

Når behandlingsansvarliges brukerkonto logger på brannmuren og/eller kontrolleren for det trådløse nettet, genereres det automatisk en E-post rapport til rektor – øverste ansvarlig for skolen for kontroll og validering. Det ligger i rektors arbeidsinstruks og rolle at slike varsler skal kontrolleres opp mot vedtak. Viser til intervju på ITpro.no publisert 6.11.2011 av Håvard Hatlevik om viktigheten for kontroll av sensitive data og for å hindre vikarierende motiv i å tre fremfor brukernes personvern i skolens hverdag.

Personvern og rutiner for fjernstøtte

I forbindelse med de tilbakemeldinger om er gitt fra elevrådet er det besluttet at VNC avinstalleres fra samtlige datamaskiner for elever. Denne brukergruppen vil heretter få installert TeamViewer for fjernassistanse. Dette med hensyn til at svært mange ønsker bedre sikkerhet og at elevene ofte er utenfor skolens nettverk.

TeamViewer installeres, og nytt passord genereres for hver sesjon.

Selv om ID forblir den samme, vil ingen ha tilgang til datamaskinen uten at bruker aktivt åpner programmet og oppgir det nye passordet. I samråd med elevrådet og rektor vil dette bli presentert og godkjent av begge parter som akseptabel måte for å hjelpe elevene i deres hverdag. Revidering og nødvendig dokumentasjon vil bli fremskaffet til alle parter er tilfreds med den nye løsningen.

Elevrådsleder har sammen med undertegnede gått over de grunnleggende teknologiene og funksjonene til TeamViewer samt en demonstrasjon på virkemåte på et tidligere tidspunkt og tilbakemeldingene fra elevrådsleder er positive.

Samtidig vil VNC bli oppdatert til å kun gi adgang til databehandlere i IT- avdelingen. Dette gjøres ved at lokale passord til VNC fjernes og at adgang kun gis til personer i IT- avdelingen. Microsoft Active Directory vil bli brukt som kilde for tilgangskontroll. Dette sikrer at kun personlige passord hos IT- avdelingen vil gi tilgang til ansattes datamaskiner i fjernsupports øyemed. (les begrepsforklaringer for utdypelse).

Resetting av eget passord

I henvendelsen fra elevrådsleder til rektor ble det påpekt svakheter i rutinene for passordresetting, med udokumenterbar påstand om at elev hadde fått tilgang til annen elevs brukerkonto. I og med det ikke kan dokumenteres – hverken i systemet eller av elevrådsleder kan ikke reaktive tiltak utføres. Som et preventivt tiltak vil IT- avdelingen anskaffe et verktøy som tillater brukere og elever å tilbakestille sine egne passord for egne brukerkontoer.

De tekniske detaljene vil ikke dette dokumentet innfatte, men kravspesifikasjonen er tofaktors brukeridentifisering – hvor nytt passord vil bli sendt pr. SMS til bruker (elev eller lærer)

Dette vil bedre sikkerheten for aktuelle personer, så vel som redusere antall brukerhenvendelser til IT- avdelingen. Spesielt etter ferier hvor det er større pågang for nye passord.

Målbare krav

Det settes en «nullvisjon» som mål for uønsket innsyn i andres personlige kontoer. Dette innbefatter at ingen skal få tilgang til data, eller brukerinformasjon som ikke er deres egne – eller for dem til å se.

Risikoanalyse

Risikoanalysen i sin helhet er kortfattet da dokumentet i så stor grad det lar seg gjøre vil besvare på eventuelle risikoelementer. Likevel er det satt fokus på følgende punkter som potensielle og reelle risikopunkt for IT- avdelingen hos Troll.

Utbrenthet

- Med den stadige teknologiske nyvinningen som gjøres stilles grunnleggende krav til læring og oppdatering hos de ansatte. Det vil derfor sammen med skolens ledelse bli vurdert sammen med den enkelte ansatte i neste medarbeidersamtale. Dette dokumentet presiserer dette, men går ikke i detalj på kartleggingsmetode og tiltak.

Psykisk press

- IT- avdelingen har fra skolens ledelse blitt forespeilet et målbart krav om forbedring ihht. Tid for å løse en suppoorthenvendelse. En reduksjon fra ti til fem arbeidsdager på to semestre (ett kalenderår) vil kunne føre til økt press og bekymring for mestringsevnen til gruppen så vel som den enkelte ansatt i IT- avdelingen. Det vil derfor bli kartlagt behov for kompetanseheving til de ansatte i deres ønskede – og trengte områder. Det vil også bli

vurdert arrangering av sosiale tilstelninger i - og utenfor arbeidstiden som med fordel også kan inkludere øvrige ansatte for bedre sosialisering. Dette vil bli vurdert fortløpende sammen med IT- leder og skolens ledelse. Eventuelle positive utfall vil også komme ut av økt sosialisering med andre IT- avdelinger i andre bedrifter og skoler. Her vil møteplasser som bla.a ATEA Community bli vurdert som passende tiltak.

- Det gjøres flere tiltak for å redusere arbeidsmengden mot dagens henvendelser med automatisering av installasjon, oppdatering og avinstallasjon av applikasjoner. Å være i forkant av slike oppdateringer og ta ting med en gang vil spare avdelingen for mange henvendelser – og brukerne for frustrasjon og usikkerhet.

Inntrenger i datasystemet / innsyn i vernet data

Brannmuren fra PaloAlto vil – så langt det lar seg gjøre, hindre uvedkommende i å nå resurser inne i skolens bygg. Når det gjelder serverne står disse hos en ekstern leverandør hvor sikkerhetsdokumentasjon er levert IT- avdelingen og skolens ledelse. Leverandøren har fått sin dokumentasjon godkjent av Datatilsynet og er godkjent av Det Norske Veritas. Denne dokumentasjonen ligger tilgjengelig elektronisk på skolens nett, og i papirkopi hos skolens ledelse, behandlingsansvarlig og i servicemottaket. Denne dokumentasjonen finnes også på engelsk for de av elevene som behersker dette bedre enn Norsk.

Øvrig risiko er i dag knyttet opp til u autentisert pålogging, sosial manipulering eller svikt hos databehandler. Det er derfor bedt om mer tid til å lære opp databehandlere til å identifisere sosial manipulering og phishing. Det vil samtidig anskaffes en systemløsning hvor brukere selv kan resette passord gjennom to faktors identifisering (mobil og elevnummer) og hvor nytt passord sendes på SMS.

Det vil bli reviderte rettigheter for lærere ovenfor hvem som vil ha tilgang til å administrere hvilke elevers brukerkontoer og passord. Det vil kun bli de nærmeste lærerne samt rektor som vil få tilgang til å tilbakestille en elevs passord. IT- avdelingen er automatisk systemadministrator, men rutinene vil tilsi at IT- avdelingen ikke skal resette passord til elever, med mindre annet er avtalt med lærer eller rektor på forhånd.

Oppsummering

I samråd med skolens ledelse og elevrådet vil tiltak for å bedre sikkerheten til de ansatte og elevene bli iverksatt som nevnt i dokumentet. IT- avdelingen vil i løpet av sommeren innføre nye systemer som gjør det mulig for brukere å selv resette passord til sine brukerkontoer og implementere ny løsning for fjernstyring av datamaskiner (fjernsupport).

IT- avdelingen har - i eget notat - vurdert kost/nytt ved å anskaffe TeamViewer og Ninite til skolen for fjernstøtte utenfor skolens nett og programutrulling, oppdatering og avinstallasjon.

Dokumentet vil bli fremvist rektor, elevrådsleder og IT- sjef for signering og godkjenning. IT- avdelingen vil med dette gi økt fokus på personvern til skolens brukere preventive tiltak som beskrevet i dokumentet

Kost/nytte for anskaffelse av Ninite og TeamViewer

Skolens ledelse ønsker å redigjøre for hvor mye tid som kan spares inn ved å anskaffe disse verktøyene til skolens bruk. IT- sjefen har i samarbeid med undertegnede gjort et estimat på hvor det går bort et halvt årsverk i transport av personell til og fra datamaskiner som kunne ha vært fjernstyrt med TeamViewer. Stor del av kostnaden her er den skjulte kostnaden hvor ansatte ikke er ved arbeidsplassen når teknikere ankommer – og må deretter returnere med uoppgjort oppdrag. Sammen med elever og ansatte som kan befinne seg hjemme eller på reise utgjør dette både en ren besparelse samt det vil være et verktøy som vil gi økt servicegrad for brukere på Troll skole. Anskaffelsen vil også være en faktor som vil hjelpe IT- avdelingen i å nå sine nye mål fra skoleledelsen.

Den samme statistikken er hentet ut og viser at det vil være minimum et kvart årsverk å spare på implementasjon av Ninite i skolen. Applikasjoner som Java og Adobe Flash krever regelmessige oppdateringer – både for sikkerheten og for funksjonaliteten. Nettsteder som YouTube krever Adobe Flash for å vise innhold, og det er derfor anbefalt at programvaren oppdateres regelmessig – helst så fort ny versjon foreligger. Anskaffelsen vil også være en faktor som vil hjelpe IT- avdelingen i å nå sine nye mål fra skoleledelsen.

Anskaffelseskostnadene for Troll er estimert til hhv.

- TeamViewer: 15.000,-
- Ninite Pro: 50.000,-

Begrepsforklaring

Oppetid

Tiden hvor IKT utstyr (servere, nettverk og øvrig IKT infrastruktur) fungerer og disponibel for tilregnet bruk.

Mellomstor bedrift

EUs definisjon av små og mellomstor bedrift

Forenklet gjelder følgende for å bli klassifisert som en SMB bedrift. Bedriften må:

1. Ha under 250 årsverk, og
2. Ha en årlig omsetning under 50 mill. EURO (ca NOK 400 mill.), eller årlig balanse under 43 mill. EURO (ca NOK 350 mill.), og
3. Være uavhengig - det vil si:
 - mindre enn 25 % av aksjer/stemmerettigheter eies av bedrifter utenfor SMB definisjonen.
 - bedriften eies av institusjonelle eiere
 - bedriften bekrefter uavhengighet der eierforhold er vanskelig å verifisere

Brukere

Omtalt som ansatte og elever ved skolen. Dette er primærbrukere av IT- avdelingen og IKT utstyret.

Tredjepart

I dokumentet er tredjepart referert til som, brukere av IKT utstyr og/eller infrastruktur på skolen som ikke er ansatte (i jobbsituasjon) eller elever (i undervisningsøyemed) på skolen.

Ansatte og elever i privat øyemed sidestilles med tredjepart.

Smarttelefon

Mobiltelefon med funksjoner utover ordinært virkeområde – tale og SMS.
Gjerne med støtte for kalender, bedriftsapplikasjoner og systemverktøy.

VNC og Teamviewer

Er to programmer som tillater IT- avdelingen å drive fjernsupport for datamaskinene i og utenfor nettverket.

- VNC er førstevalget for ansatte da datamaskinene er meldt inn i skolens domenenett og man dermed bruker datamaskinenes domenenavn for oppkopling. Kan brukes utenfor skolens nettverk men kan være begrenset.
- TeamViewer fungerer over alt i verden – også på elevers private datamaskiner. Dette krever derimot egen ID som IT- avdelingen ikke styrer og som må oppgis ved henvendelse.

Begge applikasjonene er lisensbelagt og er anskaffet av skolen til bruk av IT- avdelingen.

Ninite

Ninite er et system for utrulling, oppdatering og tilbakekalling (avinstallasjon) av aktuelle programvarer. Programmet finnes i både gratisutgave for gratisapplikasjoner (her kan man kun installere) og som lisensiert utgave hvor IT- avdelingen kan administrere datamaskinene i nettet. Her kan man enkelt installere, oppdatere og avinstallere applikasjoner ved behov.

Lync

Kommunikasjonsapplikasjon fra programvareleverandøren Microsoft.

Servicekontakt

IT- avdelingens kundemottak for support- og generelle henvendelser.
Bemannet fra 08.00 til 16.00 hver skoledag samt planleggingsdager.

Ticketsystem (TrackIT)

Applikasjon fra programleverandøren Numara som tildeler hver henvendelse et saksnummer for oppfølging av henvendelsen for IT- avdelingen og de ansatte. Programvaren gir tekniker(e) og bruker mulighet for å oppdatere saken og følge med de siste oppdateringene i sin forespørsel.
Innsyn for brukere skjer gjennom en nettside med webgrensesnitt.

Behandlingsansvarlig og databehandler

Forskjell på behandlingsansvarlig og databehandler ligger i oppgaver og ansvar rundt data som er innsamlet, behandles og vurderes:

- Behandlingsansvarlig er ansvarlig for sikkerheten til datasystemet (elektronisk eller fysisk), kontroll på databehandlere og hvem som skal ha tilgang til hvilke data for hvilket formål.
- Databehandler kan ikke alene stå for dokumentasjon av informasjonssystemet og sikkerhetstiltakene, såfremt ikke databehandleren også er systemansvarlig / behandlingsansvarlig. Databehandler kan derimot sammen med systemansvarlig være med på utforming av dokumentasjon og sikkerhetstiltak.
- Behandlingsansvarlig kan også være en databehandler.

Active Directory

En katalogtjeneste for brukere, datamaskiner, grupper og rettigheter.

Brukes til å definere brukeres rettigheter, datamaskiners rettigheter og grupperes rettigheter.

En datamaskin og person kan være medlem av en gruppe, og en gruppe kan være medlem av en annen gruppe. Dokumentet omtaler Active Directory som kilde for tilgangskontroll for VNC. Ved å gi ansatte i IT- avdelingen de nødvendige rettighetene, vil disse få rettigheter til nevnte oppgaver.

Phishing og sosial manipulering

- Phising er en et moderne ord, og brukt til formålet – fiske (fishing). Formålet med phishing er å samle inn data og informasjon som kan brukes til å utnytte en person, enten for kunskap, penger eller identitetstilgang.
- Sosial manipulering er å utgi seg for å være noe man ikke er. Her kan ansatte eksempelvis få henvendelser som tilsynelatende kommer fra mennesker, avdelinger eller selskaper som er falske – eller på vegne av. Dette for de samme formål som phishing.

Dette konkluderer rapporten

Sign:

Dato: