KANDIDATUPPSATS

Säkerhetsanalys av Olofströms kommuns IT-verksamhet - En utvärdering av informationssäkerhet

Linus Göransson

Datateknik
15 högskolepoäng

Halmstad, 2013-09-26

Säkerhetsanalys av Olofströms kommuns IT-verksamhet

En utvärdering av informationssäkerhet

Kandidatuppsats

September 2013

Författare: Linus Göransson

Handledare: Philip Heimer

Examinator: Urban Bilstrup

Sektionen för informationsvetenskap, data- och elektroteknik
Högskolan i Halmstad
Box 823, 301 18 HALMSTAD

© Copyright Linus Göransson, 2013. All rights reserved.
Kandidatuppsats
Sektionen för informationsvetenskap, data- och elektroteknik
Högskolan i Halmstad

Förord

Jag vill rikta ett stort tack till min handledare, Philip Heimer, som har bistått mig med betydelsefull information och rådgivning under arbetets gång.

Jag vill speciellt rikta ett stort tack till Olofströms kommuns IT-chef, Ronny Haglund, som lät mig utföra en säkerhetsanalys av Olofströms kommuns IT-verksamhet.

Tack!

Sammanfattning

Uppsatsen syftar till att utvärdera informationssäkerheten i Olofströms kommuns IT-verksamhet för att jämföra resultatet med BITS. Vidare syfte med uppsatsen är att se över de övriga Blekingska kommunernas syn på informationssäkerhet samt hur de arbetar med det. Uppsatsen klarlägger även Olofströms kommuns anställdas syn på informationssäkerhet samt ger en sammanfattning hur deras dator-, lösenords- och e-posthantering ser ut. En tillsyn av Olofströms kommuns dokument "Säkerhetsinstruktion IT, för användare" genomförs för att utvärdera huruvida dokumentet uppnår en acceptabel säkerhetsnivå för informationshantering.

Sammanfattningsvis visar resultaten att Olofströms kommun genomför ett aktivt arbete med informationssäkerhet. Resultaten visar även att de övriga Blekingska kommunerna anser att informationssäkerhet är viktigt och de jobbar någorlunda likvärdigt med det. Angående Olofströms kommuns dokument "Säkerhetsinstruktion IT, för användare" föreslås ett antal åtgärder som bör vidtas för att dokumentet ska vara à jour. Slutligen rekommenderas ett eventuellt samarbete mellan de Blekingska kommunerna för att ta fram ett gemensamt styrdokument för användarna.

Nyckelord: *datasäkerhet, informationssäkerhet, BITS, säkerhetsintruktion, IT, säkerhetsnivå, informationshantering*

Innehållsförteckning

1. Introduktion **1**
1.1 Bakgrund 1
1.2 Syfte och frågeställningar 2
1.3 Avgränsning 2
2. Begreppet informationssäkerhet **4**
2.1 BITS (Basnivå för informationssäkerhet) 5
3. Metod **7**
3.1 Datainsamling 7
3.1.1 Intervjuer 7
3.1.2 Enkätundersökning 8
3.1.3 Platsinspektion 9
4. Resultat **11**
4.1 Intervjuer 11
4.1.1 Olofströms kommun 11
4.1.2 Övriga kommuner i Blekinge 12
4.2 Enkätundersökning 13
4.2.1 Enkätfrågor 14
4.3 Platsinspektion 23
5. Diskussion **25**
5.1 Metoddiskussion 25
5.2 Resultatdiskussion 25
6. Slutsats **28**
Referenser **30**
Bilaga 1: Säkerhetsinstruktion IT, för användare **32**
Bilaga 2: Missivbrev till enkätundersökningen **40**
Bilaga 3: Enkätundersökningen **41**

Figurförteckning

Figur 1: Områdena i informationssäkerhet 5

Tabellförteckning

Tabell 1: Sammanställning av enkäten 14

Tabell 2: Exempel på olika kombinationer 18

Tabell 3: Sammanställning av platsinspektionen 23

Diagramförteckning

Diagram 1: Resultat från första frågan i enkätundersökningen 14

Diagram 2: Resultat från andra frågan i enkätundersökningen 15

Diagram 3: Resultat från tredje frågan i enkätundersökningen 15

Diagram 4: Resultat från fjärde frågan i enkätundersökningen 16

Diagram 5: Resultat från femte frågan i enkätundersökningen 17

Diagram 6: Resultat från sjätte frågan i enkätundersökningen 17

Diagram 7: Resultat från sjunde frågan i enkätundersökningen 18

Diagram 8: Resultat från åttonde frågan i enkätundersökningen 19

Diagram 9: Resultat från nionde frågan i enkätundersökningen 19

Diagram 10: Resultat från tionde frågan i enkätundersökningen 20

Diagram 11: Resultat från elfte frågan i enkätundersökningen 21

Diagram 12: Resultat från tolfte frågan i enkätundersökningen 21

Diagram 13: Resultat från trettonde frågan i enkätundersökningen 21

1. Introduktion

1.1 Bakgrund

Whitman & Mattord (2012) nämner att informationssäkerhetens historia började med datasäkerhet. Under andra världskriget användes de första stordatorerna som var utvecklade för att knäcka olika koder. Det var främst då säkerhetsbehovet av fysiska platser samt hård- och mjukvara var stort eftersom man var tvungen att skydda sig från utomstående hot. De främsta utomstående hoten var under denna tid bland annat fysisk stöld av utrustning eller vandalisering.

Under 1960-talet togs allt fler stordatorer i bruk för att uträtta mer avancerade uppgifter. Samtidigt blev det allt mer viktigt att dessa stordatorer kunde kommunicera med varandra på ett smidigare sätt istället för att skicka informationen, som fanns på magnetband, mellan olika datacentraler via post. Tack vare dessa behov började en amerikansk federal myndighet vid namn Advanced Research Project Agency (ARPA) att undersöka möjligheten till att utveckla ett nätverksbaserat kommunikationssystem som skulle användas till informationsutbyte för militära ändamål. Projektet fick namnet ARPANET efter sin finansiär och utvecklades av bland annat Lawrence Roberts, även känd som grundaren av Internet. ARPANET är med andra ord föregångaren till det vi idag kallar för Internet (Whitman & Mattord, 2012).

I början av 1970-talet togs ARPANET i bruk och blev sedan populärt och började användas i allt större utsträckning, vilket i sin tur ledde till att de tänkbara missbruken ökade. I samband med detta upptäckte Robert Metcalfe, en av grundarna till det populära nätverksprotokollet Ethernet, väsentliga problem med säkerheten kring ARPANET. Problemen bestod bland annat av att det inte fanns tillräckligt med skydd mot obehöriga användare. Det fanns inte heller någon kontroll av identifiering eller befogenhet till systemen. Till följd av detta släppte det amerikanska försvarsdepartementet ett dokument, Rand Report R-609, som var ett försök att fastställa flera olika kontroller som ansågs nödvändiga för att skydda ett system. Detta dokument blev en viktig milstolpe i datasäkerhetens historia eftersom den bara inte innehöll skydd av fysiska platser samt hård- och mjukvara, utan den innehöll även hur data skulle säkras för att förhindra obehörig åtkomst till dessa data. Rand Report R-609 är det dokument som startade studien av datasäkerhet (Whitman & Mattord, 2012).

Persondatorerna började etablera sig under 1980-talet. Dessa persondatorer innehöll mikroprocessorer vilket betydde att datorerna inte längre behövde vara stora maskiner i speciella rum, utan de fick plats på ett vanligt skrivbord. Under 1980-talet hade mindre företag och organisationer råd med att köpa persondatorer och till följd av detta ändrades därför fokus inom datasäkerhet. Det blev även viktigare under 1980-talet att koppla samman dessa maskiner för att de skulle kunna arbeta ihop, men det var först under 1990-talet som detta etablerade sig eftersom nätverk av persondatorer blev allt vanligare, till synes behovet av att koppla samman dessa nätverk. Behovet gav grunden

till det vi idag kallar för Internet, ett globalt nätverk av nätverk (Whitman & Mattord, 2012; Gollmann, 2011).

Jesan (2006) nämner i sin artikel att information räknas idag som en av de viktigaste resurserna i de flesta företag. Så fort företagens interna nätverk ansluts till Internet blir nätverken ett tänkbart mål för cyberattack. De senaste åren har allt fler företag fått en ökad medvetenhet om behovet att förbättra informationssäkerheten, men även en insikt att en eventuell förbättring av informationssäkerheten är viktig för det nationella skyddet (Whitman & Mattord, 2012).

1.2 Syfte och frågeställningar

Syftet med uppsatsen är att utvärdera informationssäkerheten i Olofströms kommuns IT-verksamhet, men även utvärdera hur viktigt informationssäkerheten anses vara i de övriga kommunerna i Blekinge samt hur de jobbar med informationssäkerheten i dessa kommuner. Uppsatsen kommer även att klarlägga hur Olofströms kommuns anställda ser på informationssäkerheten, om de ser den som en för- eller nackdel i deras dagliga arbete samt hur dator-, lösenords- och e-posthanteringen ser ut bland dem. Resultatet kommer sedan att jämföras med skriften Basnivå för informationssäkerhet (BITS) för att klarlägga vilka delar som är godkända enligt skriften och vilka eventuella brister som behöver åtgärdas. Utöver detta kommer även Olofströms kommuns dokument "Säkerhetsinstruktion IT, för användare" (bilaga 1) att utvärderas för att undersöka om dokumentet uppnår en acceptabel säkerhetsnivå för informationshantering.

För att uppfylla ovanstående syfte kommer uppsatsen att grunda sig på följande tre frågeställningar:

- Hur viktigt anses informationssäkerhet vara i de Blekingska kommunerna i allmänhet och i Olofströms kommun i synnerhet och hur jobbar man med informationssäkerhet i kommunerna?
- Hur ser Olofströms kommuns anställda på informationssäkerhet? För- eller nackdelar med informationssäkerhet?
- Hur ser dator-, lösenords- och e-posthanteringen ut bland Olofströms kommuns anställda?

1.3 Avgränsning

Efter diskussion med Olofströms kommuns IT-chef, Ronny Haglund, kom vi fram till att kommunen var mest intresserad av vilka hot och risker som kan tänkas uppstå inifrån, det vill säga kunskapen och eventuella brister om informationssäkerhet bland Olofströms kommuns anställda. Eftersom BITS är en omfattande skrift samt att jag inte hade tillräckligt med tid kommer uppsatsen enbart fokusera sig på specifika delar från skriften. De delar som uppsatsen kommer att fokusera sig på är dator-, lösenord- och e-posthantering samt den fysiska säkerheten i kommunens serverhall.

2. Begreppet informationssäkerhet

Säkerhet definieras enligt Nationalencyklopedin (2013) som:

> *"**säkerhet**, i allmän betydelse resultatet av åtgärder eller egenskaper som minskar sannolikheten för att olyckor eller andra oönskade händelser skall inträffa."*

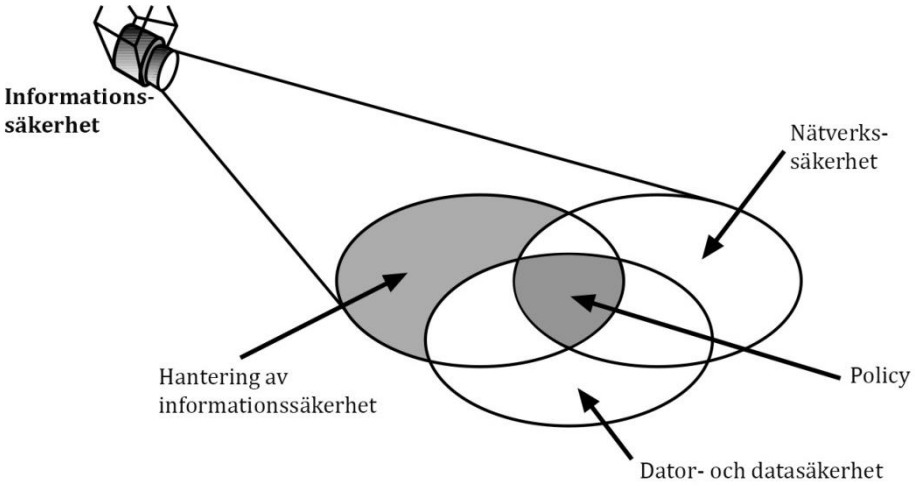
Vad är säkerhet? Enligt Syrén (2005) betyder säkerhet att vara och att känna sig säker från eventuella hot. Carlsson & Jacobsson (2012) nämner att idag finns säkerhet i olika former och i olika omgivningar, till exempel fysisk säkerhet eller brandsäkerhet. Vad är då informationssäkerhet? Först och främst nämner Syrén (2005) att information kan förekomma på olika sätt hos ett företag och att information inte längre är en ogripbar tillgång och därför måste den skyddas mot hot, till exempel otillåten åtkomst. Hon nämner även att om vissa skyddsåtgärder vidtas minskas risken att hoten utlöses.

CIA-begreppet består av tre centrala begrepp för informationssäkerhet. Begreppen beskrivs som de tre målen med informationssäkerhet. Med andra ord används dessa begrepp om man vill skydda informationen mot de hot den kan utsättas för. De tre målen är (Whitman & Mattord, 2012; Gollmann, 2011):

- Konfidentiellt (eng. confidentiality) – informationen ska vara skyddad mot otillåten åtkomst.
- Integritet (eng. integrity) – informationen är och förblir fullständig, det vill säga att informationen inte har förändrats på ett icke-godkänt sätt.
- Tillgängligt (eng. availability) – informationen ska vara tillgänglig när den behövs.

Carlsson & Jacobsson (2012) nämner att om ett system ska kunna anses som säkert behöver man tänka på alla tre begreppen eftersom de går in i varandra och på så sätt kompletterar varandra. Ovanstående begrepp kan vara en bra början för implementering av skydd för informationen mot diverse hot. Panko (2010) menar att det oftast är den tekniska delen som ligger i fokus och att många köper och implementerar brandväggar eller liknande för att skydda informationen, men utan ledning, riktlinjer och kunskap är den tekniska delen inte till någon nytta.

The Committee on National Security Systems (CNSS) definierar att informationssäkerhet är ett skydd av information och dess viktiga delar, till exempel mjuk- eller hårdvaran som tillhandahåller informationen. Deras modell är baserat på CIA-begreppet och i figur 2.1 visar deras modell att informationssäkerhet innehåller tre breda områden. Dessa är hantering av informationssäkerhet, dator- och datasäkerhet samt nätverkssäkerhet. Informationssäkerheten finns till för att skydda de olika begreppen och för att göra detta kan man använda sig av policydokument eller utbildningar (Whitman & Mattord, 2012).



Figur 1: Områdena i informationssäkerhet

På senare tid har säkerhetsexperter ansett att fokusen på de tre målen inte reflekterar kravet för att skydda konfidentiell information. Därför har man valt att utöka CIA-begreppet med fyra mer begrepp och dessa är riktighet (eng. accuracy), tillförlitlighet (eng. authenticity), användbarhet (eng. utility) och ägande (eng. possession) och nedan följer en kort förklaring om varje begrepp:

- Riktighet (eng. accuracy) – informationen ska inte innehålla felaktig information, utan innehålla det värdet som slutanvändaren förväntar sig.
- Tillförlitlighet (eng. authenticity) – informationen ska vara sanningsenlig i sitt ursprung.
- Användbarhet (eng. utility) – informationen ska vara användbart för särskilda ändamål.
- Ägande (eng. possession) – kontroll över informationen som sägs vara i ägande, om man får det, oberoende av format eller andra egenskaper.

Dessa fyra begrepp togs fram för att skapa en bättre möjlighet att hålla informationen säker (Whitman & Mattord, 2012).

2.1 BITS (Basnivå för informationssäkerhet)

MSB, även kallad Myndigheten för samhällsskydd och beredskap, har en skrift vid namn BITS (Basnivå för informationssäkerhet). I skriften står följande (MSB, Myndigheten för samhällsskydd och beredskap, 2006):

"I denna skrift, BITS (Basnivå för informationssäkerhet), redovisas ett antal rekommenderade administrativa säkerhetsåtgärder som minst bör vidtas för att uppnå en acceptabel säkerhetsnivå för informationshanteringen i en organisation."

3. Metod

Det finns olika metoder som kan användas när en säkerhetsanalys ska utföras mot en verksamhet för att se om de följer de rekommendationer som anges i BITS. I detta kapitel redogörs vilken metod som kommer att användas när säkerhetsanalysen ska genomföras.

Först och främst finns det två sorters undersökningar, kvalitativa och kvantitativa, som kan användas beroende på vilket sätt undersökningen ska genomföras. Exempel på en kvalitativ, även kallad intensiv, undersökning kan vara intervjuer, observationer eller fältstudier. Exempel på en kvantitativ, även kallad extensiv, undersökning kan vara enkäter. Med andra ord handlar en kvalitativ undersökning om att skapa en ökad förståelse inom ett specifikt område genom djupgående frågor medan en kvantitativ undersökning används för att ange frekvenser i olika frågor genom att göra olika beräkningar. En kvantitativ undersökning innehåller oftast frågor om "hur ofta", "hur många" eller "hur vanligt" någonting är (Jacobsen, 2012; Trost, 2012).

Enligt Jacobsen (2012) bör metodvalet avgöras av problemställningen som den aktuella undersökningen innehåller och enligt Trost (2012) ska metodvalet inte avgöras av tradition eller socialt tryck. Dock anses en kvantitativ undersökning vara mer riktig och tillförlitlig enligt det sociala trycket och därmed ett självklart val när metodvalet ska göras.

Jag har valt att utesluta en litteraturundersökning eftersom arbetet går ut på att utvärdera informationssäkerhet i Olofströms kommuns IT-verksamhet, det vill säga att förstå och ta reda på hur de anställda ställer sig till de rekommendationer som anges i BITS samt hur de ställer sig till informationssäkerhet överlag.

3.1 Datainsamling

3.1.1 Intervjuer

Intervjuer, även kallad den öppna intervjun, är en metod som kan användas som en datainsamlingsmetod. I en intervju pratar undersökaren och den som blir undersökt om ett specifikt ämne. Vanligtvis görs intervjuerna genom ett personligt möte eller genom telefon. Det är också vanligt att undersökaren antecknar det som sägs i en intervju för att kunna analysera resultatet vid ett senare tillfälle. Intervjuer är användbart om man är intresserad av att veta vad den enskilda individen tycker och tänker i olika frågeställningar (Jacobsen, 2012).

Enligt Jacobsen (2012) är det även bra att begränsa sig till vissa individer eftersom det är tidskrävande och kräver mycket för- och efterarbete om man ska välja intervju som en datainsamlingsmetod. Intervjuer genererar även mycket data från anteckningar eller ljudupptagningar. Intervjuar man då för många individer finns det en risk att inte kunna skapa någon helhetsyn på grund av för mycket data.

Jag kommer att intervjua Olofströms kommuns IT-chef, Ronny Haglund, för att få en överblick av hur Olofströms kommuns IT-miljö ser ut och är uppbyggd. För att besvara frågeställningarna om hur viktig informationssäkerhet anses vara i de Blekingska kommunerna samt hur man jobbar med informationssäkerhet i kommunerna kommer jag även, utöver Ronny Haglund, att intervjua IT-cheferna i de andra kommunerna i Blekinge.

Intervjun med Ronny Haglund kommer att ske genom ett personligt möte medan intervjuerna med IT-cheferna i de andra kommunerna i Blekinge kommer att ske genom e-post. Under intervjun med Ronny Haglund kommer jag att använda mig av ljudupptagning för att sedan transkribera hela intervjun och plocka ut det relevanta för uppsatsen. De övriga intervjuerna kommer att ske genom e-post och svar förväntas ges på samma sätt.

3.1.2 Enkätundersökning

Enkätundersökning är en annan metod som kan användas som en datainsamlingsmetod. En enkät består av ett par frågor med tillhörande svar som den besvarande ska besvara och kan därför ta olika lång tid att besvara (Trost, 2012).

Enligt Trost (2012) kan en enkätundersökning ha öppna och icke öppna frågor. Det betyder att frågorna i enkätundersökningen har redan definierade svarsalternativ eller inga alls. Det är till en fördel att använda icke öppna frågor, med redan definierade svarsalternativ, eftersom det kan vara tidskrävande att behandla de skrivna svaren från en enkätundersökning med öppna frågor. Detta för att handstilen hos en del människor kan uppfattas oläslig, en del skriver långa och ingående svar medan andra skriver korta svar som kan vara svåra att förstå innebörden av. Något som är vanligt bland svaren i en enkätundersökning med öppna frågor är att en del människor inte skriver något alls. En annan fördel med icke öppna frågor, som Trost (2012) tar upp, är att en del människor kan känna sig osäker på att svara på vissa frågor och därmed struntar i att svara. En del människor tycker också det kan vara jobbigt att uttrycka sig skriftligt.

Till en enkätundersökning är det bra att skriva med ett följebrev, även kallad missivbrev, till dem som ska besvara frågorna. Detta för att en enkätundersökning ska se mer inbjudande ut och chansen att fler svarar ökar. Det är också viktigt att göra ett urval vid en enkätundersökning. Vissa verksamheter kan ha flera tusen anställda och det medför att det blir komplicerat och kostar för mycket att försöka samla in data från alla (Trost, 2012).

Jag kommer att genomföra en enkätundersökning bland Olofströms kommuns anställda för att besvara frågeställningen om de ser informationssäkerhet som en för- eller nackdel i deras dagliga arbete samt hur dator-, lösenords- och e-posthanteringen ser ut bland dem. Enkätundersökningen kommer att ske genom en webbenkät och inbjudan kommer att skickas ut till respondenterna med hjälp av IT-avdelningens e-postlistor.

När jag ska utforma webbenkäten kommer jag att använda mig av enkätverktyget SurveyMonkey. Detta verktyg kommer att ge mig en sammanställning av resultaten som jag sedan kommer att infoga som diagram i Microsoft Word. Som jag nämnde tidigare under kapitlet "Syfte och frågeställningar" kommer jag sedan att jämföra resultatet med BITS.

Efter diskussion med Olofströms kommuns IT-chef, Ronny Haglund, kommer jag att välja att skicka ut enkätundersökningen till samtliga anställda i Olofströms kommun. Enligt Ejlertsson (2010) är en webbaserad enkätundersökning delvis bättre än en enkätundersökning på papper eftersom urvalet blir mycket större samt att det blir en mindre kostnad och är inte lika tidskrävande. Därför väljer jag att göra en webbaserad enkätundersökning. Inbjudan kommer att skickas ut genom e-post och kommer att innehålla ett följebrev, även kallad missivbrev (bilaga 2), tillsammans med en länk till enkätundersökningen. Missivbrevet kommer att beskriva undersökningens syfte. Undersökningen kommer att utföras anonymt och det kommer inte gå att härleda vem som har besvarar enkäten. Detta är ett självklart val dels för att få en bra pålitlighet och trovärdighet, men också för att ingen förvaltning ska behöva visa sig sämre än de andra förvaltningarna.

En nackdel med en webbaserad enkätundersökning är att man kan få en väldigt låg svarsprocent. Detta kan bero på många olika faktorer. En av faktorerna kan vara att det inte finns tid till att svara eller att ämnet inte är intressant. Idag tar också de flesta emot mycket e-post och risken att bli drabbad av något virus eller liknande är stor. Många blir därför misstänksamma och vägrar därför att öppna bilagor från en okänd avsändare (Jacobsen, 2012).

Enligt Jacobsen (2012) hade intervjuer gett en högre svarsprocent, men det är en tidskrävande process samt en högre kostnadsfråga.

3.1.3 Platsinspektion

Jag kommer att genomföra en platsinspektion i Olofströms kommuns serverhall för att undersöka den fysiska säkerheten. BITS tar upp om den fysiska säkerheten och vilka åtgärder som krävs för att exempelvis förhindra förlust, skada eller stöld av organisationens resurser. Dessa åtgärder kommer jag att använda mig av när jag ska göra platsinspektionen i kommunens serverhall.

4. Resultat

4.1 Intervjuer

Intervjuer har skett med samtliga kommuner. Eftersom uppsatsen handlar om de Blekingska kommunerna i allmänhet och Olofströms kommun i synnerhet samt att jag ville ta reda på hur Olofströms kommuns IT-miljö ser ut och är uppbyggd kommer resultatet av Olofströms kommun vara lite mer utförligare än resterande kommuner.

Intervjun med Olofströms kommuns IT-chef, Ronny Haglund, ägde rum den 25 februari 2013, klockan 13:00 i en av IT-avdelningens lokaler.

4.1.1 Olofströms kommun

Olofströms kommun är en av Blekinges fem kommuner och har runt 1400 anställda. Dessa anställda är fördelade på fem olika förvaltningar; Kommunlednings-, Utbildnings-, Social-, Kultur och Fritids- samt Samhällsbyggnadsförvaltningen.

IT-avdelningen i Olofströms kommun går under Kommunledningsförvaltningen och de ansvarar för allt IT-relaterat i kommunen. IT-avdelningen består av en IT-chef, en IT-administratör, en systemtekniker och fyra IT-tekniker. Det finns en befattningsbeskrivning som dock inte är fastställd av kommunfullmäktige eftersom de inte längre förordar att kommunen ska ha dessa kvar. IT-avdelningen har dock valt att ajourhålla sina befattningsbeskrivningar eftersom de anser att det är en bra dokumentation för verksamheten. I skrivande stund lever Olofströms kommun i dubbla världar eftersom de är mitt uppe i en migrering där de ska byta från en Novell-miljö till en renodlad Microsoft-miljö. Idag finns det runt 750 arbetsstationer fördelat på administration (400 stycken) och förskolorna samt låg- och mellanstadieskolorna (350 stycken). På högstadie- och gymnasieskolan får varje elev en egen bärbar dator (även kallad en-till-en-konceptet). Bland högstadie- och gymnasieskolan finns det runt 1000 arbetsstationer och IT-avdelningen lägger ungefär två heldagar i veckan på ren platssupport för att hjälpa eleverna med diverse datorproblem. Allt från trasiga skärmar till hårddiskar som havererar.

Eftersom Olofströms kommun i skrivande stund byter från en Novell-miljö till en renodlad Microsoft-miljö har IT-avdelningen legat lite lågt med att ha en introduktionsdag för de nyanställda. IT-avdelningens uppgift är inte att utbilda, utan att informera. Tanken är att introduktionsdagen ska komma igång igen när migreringen är klar. Då är det tänkt att man ska gå igenom bland annat IT-säkerhetspolicyn, allmänt om hur kommunens nät är uppbyggt och hur man jobbar i miljön (till exempel vart man ska lagra dokument och liknande). I övrigt ligger all utbildning på respektive chef samt att de nyanställda blir tilldelade relevanta dokument. Olofströms kommun har en interaktiv utbildning på deras intranät som baseras på IT-säkerhetspolicyn samt dokumentet "Säkerhetsinstruktion IT, för användare". Den interaktiva utbildningen avslutas med ett diplom som kan skrivas under att man har utfört utbildningen.

I Olofströms kommun anses informationssäkerhet vara viktigt. Det är betydelsefullt att de har gjort allt de kan för att säkra informationen. För närvarande finns det ingen antagen IT-säkerhetspolicy i Olofströms kommun. Det finns dock en IT-säkerhetspolicy som arbetades fram 2004 tillsammans med Sölvesborgs kommun och Karlshamns kommun och som Olofströms kommun lever efter idag. Tillsammans med denna policy finns det ett kompletterande dokument som heter "Säkerhetsinstruktion IT, för användare" som förklarar de regler som gäller för de anställda i deras arbete i Olofströms kommuns IT-miljö.

4.1.2 Övriga kommuner i Blekinge

Nedan redogörs frågorna och svaren från intervjun med varje kommun. Samma frågor ställdes till samtliga kommuner. I en av kommunerna intervjuade jag IT-chefen och i de resterande kommunerna intervjuade jag (efter vidarebefordring) en person som jobbar specifikt med frågor som berör informationssäkerhet.

Följande frågor ställdes till kommunerna:

1. Hur viktigt anses informationssäkerhet vara i er kommun?
2. Hur jobbar man med informationssäkerhet i er kommun (Exempel: IT-policy, utbildningar)?

Jag valde intervjufrågorna för att de kunde besvara mina frågeställningar. På första frågan var svaren förväntade eftersom jag antog att informationssäkerhet anses viktigt i de olika kommunerna.

4.1.2.1 Sölvesborgs kommun

Från Sölvesborgs kommun intervjuade jag kommunens IT-chef, Thomas Hallberg.

1. Informationssäkerhet anses viktigt i Sölvesborgs kommun, men enligt Thomas borde kommunen jobba mer med detta.
2. Kommunen jobbar med informationssäkerhet genom en IT-policy och en IT-säkerhetsinstruktion. Dock anser Thomas att kommunen borde jobba mer aktivt med deras sätt att tänka när de exempelvis pratar i telefon på tåg eller bussar eftersom detta även ingår i informationssäkerhet.

4.1.2.2 Karlshamns kommun

Från Karlshamns kommun intervjuade jag kommunens informationssäkerhetsansvarige, Jens Odevall.

1. Jens anser att informationssäkerhet är viktigt i Karlshamns kommun. Dock anser han att det alltid finns behov av att göra mer för att förebygga, som i så många andra områden.

2. Karlshamns kommun har tagit fram såväl informationssäkerhetspolicy som säkerhetsinstruktioner för användare. Dessa dokument ska alla nyanställda läsa igenom innan de får tillgång till kommunens system.

4.1.2.3 Ronneby kommun

Från Ronneby kommun intervjuade jag kommunens GIS- och IT-säkerhetssamordnare, Yvonne Stranne. GIS är en förkortning av geografiskt informationssystem.

1. Eftersom en kommun är en offentlig organisation är det viktigt med informationssäkerhet och därmed anses det viktigt att jobba med just denna fråga i Ronneby kommun.
2. I Ronneby kommun jobbar man främst med styrdokument (IT-policy, Policy för IT-säkerhet, Regler och riktlinjer för IT-säkerheten samt IT-säkerhetsinformation för användare).

4.1.2.4 Karlskrona kommun

Från Karlskrona kommun intervjuade jag kommunens informationssäkerhetschef, Anders Danielsson.

1. Informationssäkerhet anses vara mycket viktigt i Karlskrona kommun. Invånarna ska kunna känna en tillit till kommunen att man vet att informationen hanteras på ett säkert sätt.
2. Karlskrona kommun har en informationssäkerhetspolicy som följer de rekommendationer som finns enligt BITS samt Svensk Standard ISO 17799 (som är en standard som ingår i ISO 27000-serien). Denna policy är från 2007 och beslutades av kommunfullmäktige. Karlskrona kommun använder även DISA (Datorstödd informationssäkerhetsutbildning för användare) som grundutbildning. Utöver detta har förvaltningarna ytterligare utbildning beroende på verksamhet.

4.2 Enkätundersökning

En enkätundersökning (bilaga 3) har genomförts som de anställda i Olofströms kommun getts möjlighet att svara på. Detta för att dels ta reda på hur de ser på informationssäkerhet, hur dator-, lösenords- och e-posthanteringen ser ut bland de anställda i Olofströms kommun och om informationssäkerhet är en för- eller nackdel i deras arbete.

Enkätundersökningen var uppdelad i fem delar och bestod av 13 frågor. Den första delen behandlade allmänt om datoranvändning, eventuell utbildning om informationssäkerhet samt om de anställda i Olofströms kommun känner till kommunens IT-säkerhetspolicy. Den andra delen behandlade datorhantering för att undersöka hur datorerna används. Vidare behandlade den tredje delen lösenordshantering. Den här delen innefattade struktur av lösenordet, användning av

samma lösenord i externa sammanhang samt hur ofta lösenordet byts. Den fjärde delen behandlade e-posthantering för att undersöka om de anställda öppnar all e-post och bifogade filer de får till sin e-postadress samt om de använder sin e-postadress för att skicka och ta emot privata e-post. Den femte och sista delen behandlade om de anställda anser att informationssäkerhet är en för- eller nackdel i deras arbete. Jag använde mig av enkätverktyget SurveyMonkey till utformningen av enkäten och sammanställning av svaren. Tabell 4.1 visar en sammanställning av enkäten.

Startdatum:	2013-03-04
Slutdatum:	2013-03-28
Antal inbjudningar:	1338
Antal svar:	237
Svarsprocent:	18 %

Tabell 1: Sammanställning av enkäten

4.2.1 Enkätfrågor

De resultat som redogörs nedan är uppdelad i två delar. Den första delen innehåller vad som står i BITS (MSB, Myndigheten för samhällsskydd och beredskap, 2006), alternativt från dokumentet "Säkerhetsinstruktion IT, för användare", och den andra delen innehåller hur det ser ut bland kommunens anställda med en jämförelse mellan BITS, alternativt från dokumentet "Säkerhetsinstruktion IT, för användare", och resultatet för varje fråga. Vid vissa frågor finns det inget att jämföra, men jag valde att ta med dessa frågor ändå eftersom de är viktiga i arbetet med informationssäkerhet. Likadant här valde jag frågorna till enkätundersökningen för att de kunde besvara resterande frågeställningar.

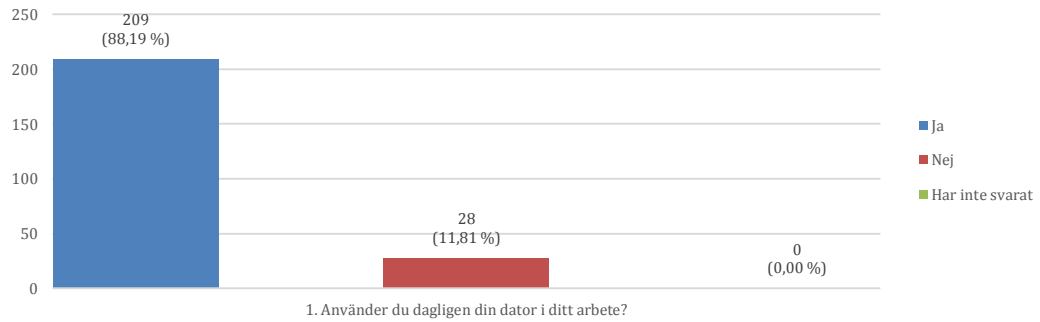


Diagram 1: Resultat från första frågan i enkätundersökningen

Olofströms kommun

Första frågan finns inget att jämföra från BITS. Tanken med frågan var att jag främst ville veta hur många av Olofströms kommuns anställda som använder sin dator dagligen i sitt arbete och resultatet visar att majoriteten gör det. Detta är inget förvånande resultat eftersom idag använder de flesta en dator på sin arbetsplats.

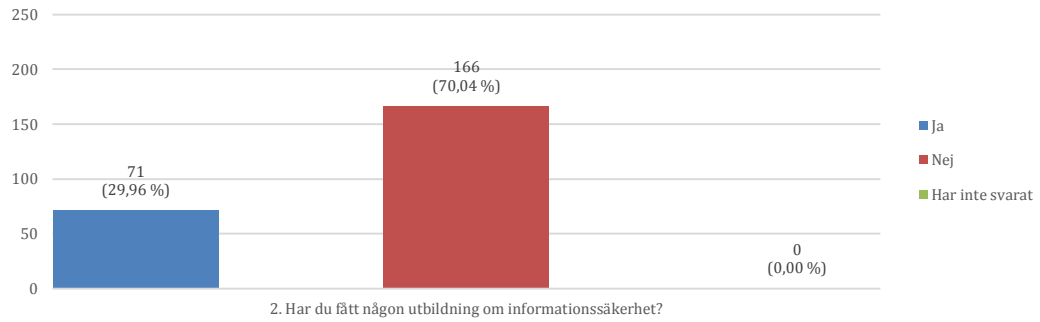


Diagram 2: Resultat från andra frågan i enkätundersökningen

Basnivå för informationssäkerhet

- *Utbildningsinsatser inom informationssäkerhet ska genomföras regelbundet*

Det är viktigt att genomföra utbildningar kontinuerligt, både för att kunskapen om informationssäkerhet ska vara tillräcklig, men även för att bibehålla säkerhetsmedvetandet och motivationen för att upprätthålla säkerheten.

Olofströms kommun

Som resultatet visar har majoriteten av kommunens anställda inte fått någon utbildning om informationssäkerhet. Detta kan innebära en säkerhetsrisk för Olofströms kommun eftersom vissa av de anställda troligtvis inte har tillräcklig kunskap om informationssäkerhet och därmed kan det vara svårt att bibehålla ett säkerhetstänk som anställd.

Som tidigare nämnt är IT-avdelningens uppgift inte att utbilda, utan att informera. De har dock legat lågt med att ha introduktionsdag för de nyanställda eftersom de är mitt uppe i ett miljöbyte. Eventuella utbildningar ligger på respektive chef.

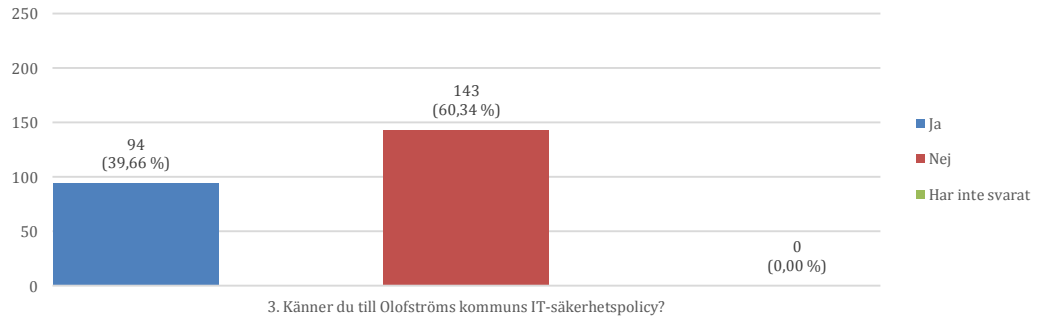


Diagram 3: Resultat från tredje frågan i enkätundersökningen

Basnivå för informationssäkerhet

- *Det ska finnas dokumenterade, av ledningen beslutade, säkerhetsinstruktioner för användare (Säkerhetsinstruktion, användare)*

Säkerhetsinstruktion för användare redovisar de generella informationssäkerhetsregler som gäller för personalens hantering av organisationens informationssystem och IT-resurser. Den kan exempelvis klargöra vad som gäller för framtagning, bearbetning, klassning och sparande av dokument, för den egna arbetsstationen, restriktioner för elektronisk post och användning av Internet m.m.

Olofströms kommun
Som resultatet visar känner majoriteten av Olofströms kommuns anställda inte till kommunens IT-säkerhetspolicy. Detta är också en säkerhetsrisk eftersom vissa av de anställda inte vet vilka riktlinjer det är som gäller för till exempel hantering av information, inloggning eller lösenord.

Även här är det upp till respektive chef att ansvara för att varje anställd blir tilldelad relevanta dokument, i det här fallet IT-säkerhetspolicyn, eller att den interaktiva utbildningen genomförs.

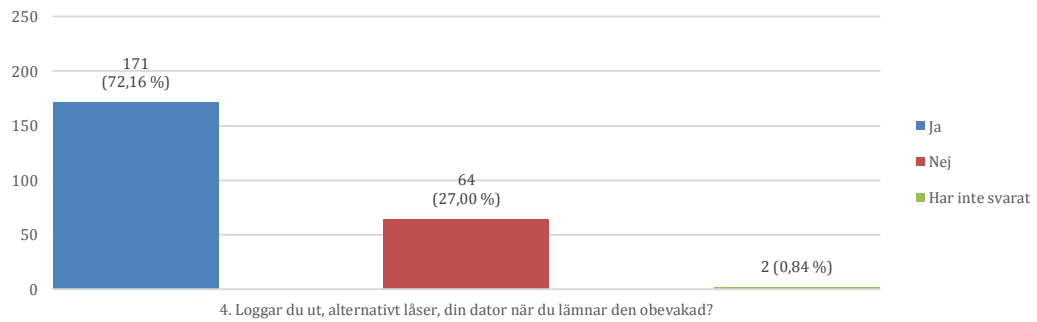


Diagram 4: Resultat från fjärde frågan i enkätundersökningen

Basnivå för informationssäkerhet

- *För arbetsstation ska gälla att:*
  - *användare som lämnar den obevakad ska aktivera skärmsläckare med automatisk låsning*
  - *upplåsning ska ske med lösenord*

Säkerhetsinstruktion IT, för användare

- *När Du tillfälligt lämnar arbetsplatsen skall lösenordsskyddad skärmsläckare användas. Vid längre frånvaro, ex rast, lunch, skall arbetsstationen loggas ur.*

Olofströms kommun
Resultatet här visar att majoriteten loggar ut, alternativt låser, sin dator när man lämnar den obevakad. Då man inte vet vilka det är som har svarat är det svårt att veta vilka det är som inte loggar ut, alternativt låser, sin dator. Det kan vara anställda som endast använder en dator för att bara exempelvis tidsrapportera och därmed inte behöver logga ut, alternativt låser, sin dator eftersom det oftast går snabbt att tidsrapportera. Det finns heller ingen tidsbegränsning för inloggning.

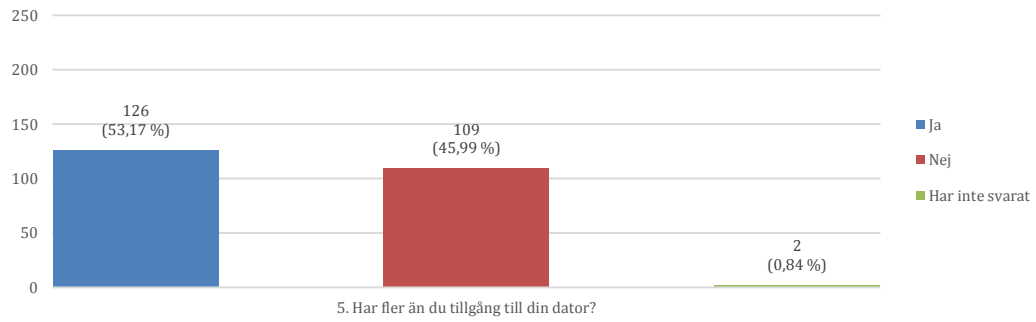


Diagram 5: Resultat från femte frågan i enkätundersökningen

Olofströms kommun

Här visar resultatet att vissa delar dator med varandra. Det kan bero på att de anställda som jobbar inom äldreomsorgen inte har en egen dator, utan delar på en eller två datorer. Dock måste man logga in med sitt användarnamn och lösenord för att kunna använda datorn, men att det finns flera användare på samma dator kan vara en säkerhetsrisk om de anställda inte har kunskap om informationssäkerhet eller följer de riktlinjer som gäller.

Varje användare har en egen hemkatalog som endast användaren själv kan nå. Lagrar man information på den lokala disken finns den tillgänglig för alla som kan starta datorn och man behöver oftast inte använda något lösenord för att komma åt dessa diskar.

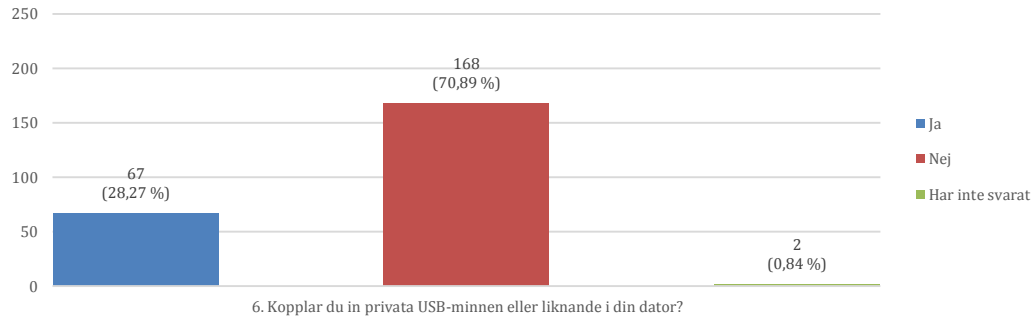


Diagram 6: Resultat från sjätte frågan i enkätundersökningen

Säkerhetsinstruktion IT, för användare

- *Lagringsmedia som Du använder i hemdatormiljö skall viruskontrolleras innan de får användas i kommunens nätverk.*

Olofströms kommun

Som resultatet visar kopplar majoriteten inte in privata USB-minnen eller liknande i sin dator. Detta är ett positivt resultat eftersom detta kan innebära en stor säkerhetsrisk om man lyckas få in ett virus i sitt lagringsmedium. Dock skyddas vissa av arbetsstationerna med hjälp av klientskyddet Microsoft Forefront och eftersom kommunen är mitt uppe i ett miljöbyte skyddas de arbetsstationer som ännu inte fått den nya klienten med Trend Micro:s virusskydd.

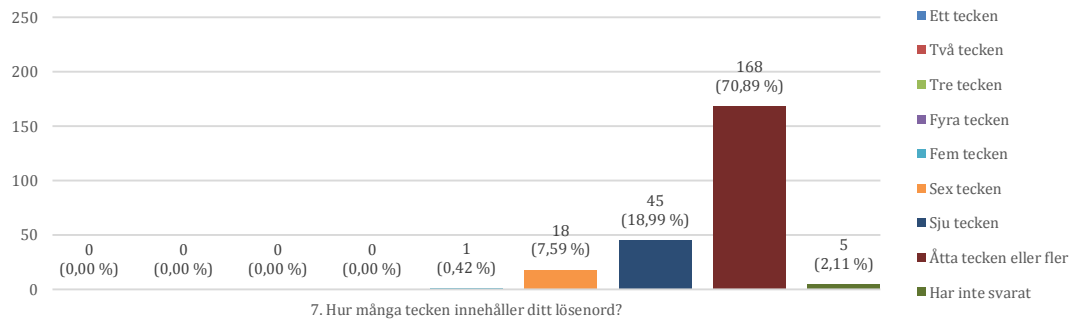


Diagram 7: Resultat från sjunde frågan i enkätundersökningen

Basnivå för informationssäkerhet

- *För lösenord ska gälla att:*
  - *de ska bestå av minst 8 tecken för såväl användare som systemadministratörer/-tekniker och vara konstruerade så att de inte lätt går att pröva sig fram till eller gissa*

Varför är det bra med åtta tecken eller fler? Ju fler tecken, ju fler olika sorters lösenordskombinationer blir det. Nedanför följer ett exempel:

Om ett lösenord innehåller...	
...tre tecken och enbart siffror ger det:	10^3 = 10 * 10 * 10 = 1000 olika kombinationer
...fyra tecken och enbart siffror ger det:	104 = 10 * 10 * 10 * 10 = 10000 olika kombinationer

Tabell 2: Exempel på olika kombinationer

Om man förlänger lösenordet med åtta tecken och låter lösenordet innehålla små bokstäver (inte å, ä, ö) och siffror ger det totalt 2 251 875 390 625 olika kombinationer. Om man låter lösenordet innehålla stora bokstäver, små bokstäver och siffror ger det totalt 167 961 600 000 000 olika kombinationer.

Som man kan se ökar antalet kombinationer ju längre och ju fler tecken ett lösenord innehåller. Genast blir det mer tidskrävande att testa alla kombinationer från exempelvis en dator.

Säkerhetsinstruktion IT, för användare

- *Lösenordet skall bestå av minst 6 tecken och skall konstrueras så att det inte lätt kan kopplas till dig som person. Tecknen å, ä och ö får inte användas i lösenord.*

Olofströms kommun

Varje användare som har ett aktivt konto har också ett tillhörande lösenord. Resultatet visar att de flesta som har svarat har ett lösenord med åtta tecken eller fler. Detta är ett positivt resultat eftersom Olofströms kommuns IT-säkerhetspolicy uppmanar att

lösenordet ska bestå av minst sex tecken. Första gången en anställd loggar in fås det ett tillfälligt lösenord av IT-avdelningen. Den anställde blir då uppmanad av systemet att byta till ett personligt lösenord. Om man inte byter lösenordet blir användarkontot låst.

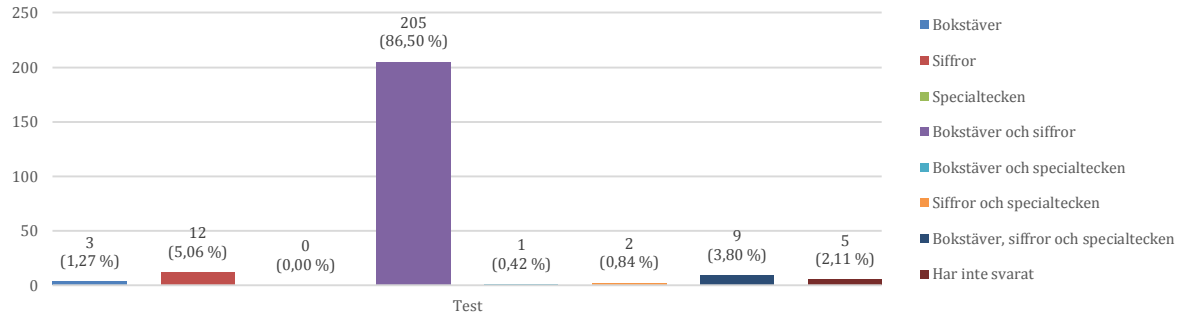


Diagram 8: Resultat från åttonde frågan i enkätundersökningen

Säkerhetsinstruktion IT, för användare

- *Undvik enkla repetitiva mönster såsom t ex "ABC1234", "AAA1111" får inte användas. Använd inte heller andra lättforcerade lösenord, såsom eget eller familjemedlems namn eller enkla tangentkombinationer av typen "QWERTYU". För att väsentligt försvåra lösenordsknäckning bör bokstäver, siffror och specialtecken (#&+) blandas i lösenordet.*

Olofströms kommun

Som resultatet visar har en klar majoritet ett lösenord som innehåller bokstäver och siffror. Detta är ett mycket positivt resultat eftersom majoriteten även hade åtta tecken eller fler i sitt lösenord. Resultatet visar också att tolv stycken av de svarande har enbart siffror i sitt lösenord.

Detta kan vara en allvarlig säkerhetsrisk eftersom det är vanligt att man tar sitt födelsedatum eller sitt personnummer som lösenord.

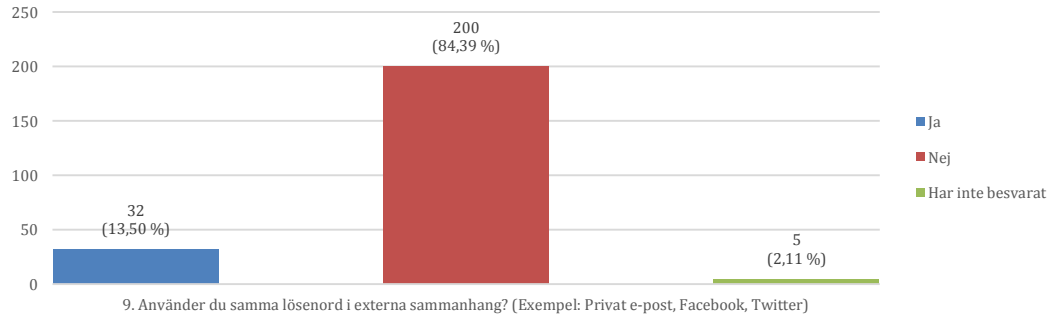


Diagram 9: Resultat från nionde frågan i enkätundersökningen

Basnivå för informationssäkerhet

- *Användare ansvarar för att:*
    - *ej använda samma lösenord externt*

Olofströms kommun

Som resultatet visar använder majoriteten inte samma lösenord i externa sammanhang. Detta är ett positivt resultat med tanke på social ingenjörskonst. Om en användare försöker logga in i ett system med felaktigt lösenord kommer användarkontot att spärras efter tre misslyckade försök. Om detta händer behöver man kontakta IT-avdelningen och då får man ett nytt tillfälligt lösenord.

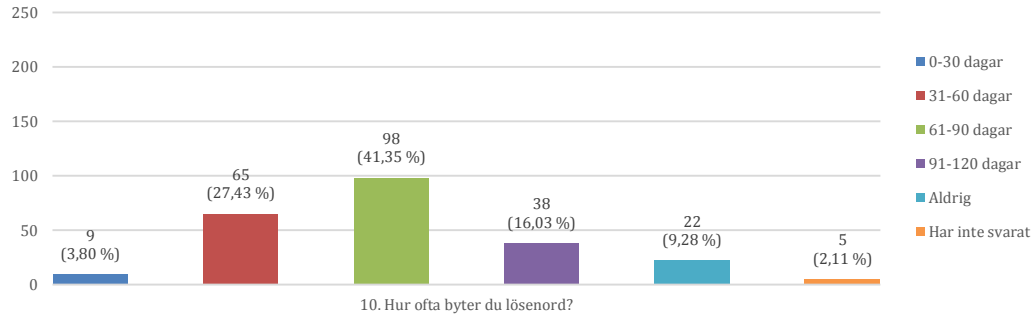


Diagram 10: Resultat från tionde frågan i enkätundersökningen

Basnivå för informationssäkerhet

- *För lösenord ska gälla att:*
  - *användarna ska tvingas byta lösenord enligt tidsintervall som systemägaren beslutar*

Säkerhetsinstruktion IT, för användare

- *Du skall därför:*
  - *Byta lösenordet var 90:e dag. Du får en påminnelse på skärmen när det är dags att byta.*

Olofströms kommun

Resultatet blev som förväntat med att de flesta, som har svarat, byter sitt lösenord efter 61-90 dagar. Detta resultat kändes förväntat eftersom de får en påminnelse på skärmen när det är dags att byta.

Något som var förvånande är att det är en del som byter sitt lösenord varje eller varannan månad. De som byter sitt lösenord oftare sitter troligtvis och arbetar med konfidentiell information där hög säkerhet erfordras. Som resultatet visar är det även några som aldrig byter sitt lösenord. Det kan ses som en säkerhetsrisk och bör inte förekomma.

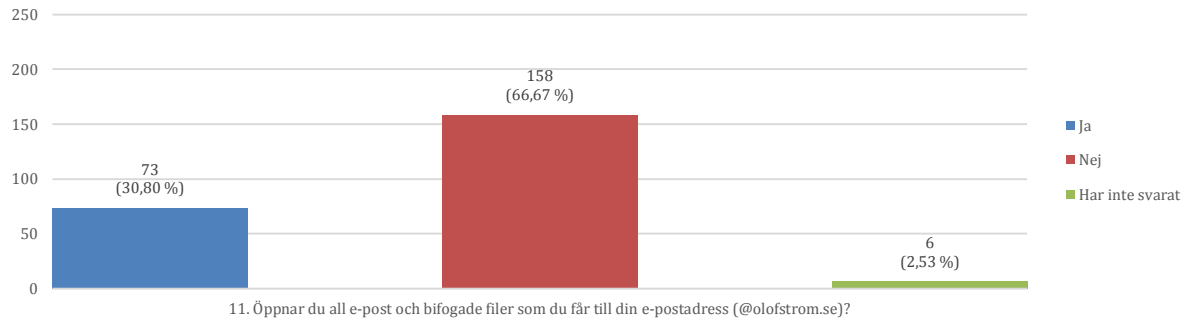


Diagram 11: Resultat från elfte frågan i enkätundersökningen

Olofströms kommun

Av de som har svarat öppnar vissa av dem all e-post och bifogade filer som de får till sin e-postadress. Att vissa öppnar all e-post och bifogade filer kan ses som en säkerhetsrisk eftersom virus kan sprida sig lätt bland användare om man inte är uppmärksam. Dock skannas all e-post med hjälp av Trend Micro:s virusskydd för att sedan varna för eventuella virus.

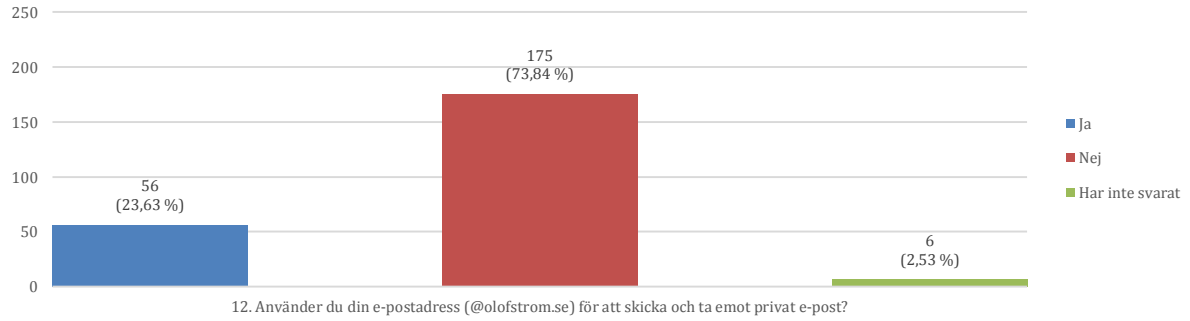


Diagram 12: Resultat från tolfte frågan i enkätundersökningen

Olofströms kommun

Det är inte förbjudet, enligt IT-säkerhetspolicyn, att skicka och ta emot privat e-post. Dock uppmanar policyn att den privata e-posten snarast tas bort från användarens inkorg, men resultatet visar att det bara är en minoritet som skickar och ta emot privat e-post med sin e-postadress. Det finns en risk att virus kan spridas även här om man inte är uppmärksam.

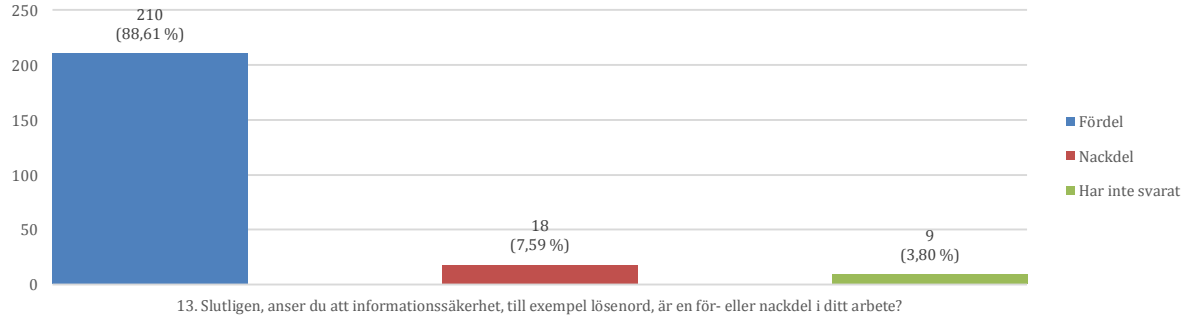


Diagram 13: Resultat från trettonde frågan i enkätundersökningen

Olofströms kommun

Till sist frågades om informationssäkerhet anses som en för- eller nackdel i arbetet. Flertalet av de svarande anser att informationssäkerhet är en fördel i deras arbete och därmed ett mycket positivt resultat. Endast 18 stycken tycker att informationssäkerhet är en nackdel i deras arbete. Till denna fråga fick varje deltagare en möjlighet att skriva varför informationssäkerhet är en för- eller nackdel i deras arbete. 96 stycken av de svarande valde att kommentera.

Svaren varierade, men de som tyckte att informationssäkerhet är en fördel i deras arbete syftade på att det är viktigt att inte alla ska ha tillgång till sekretessbelagd information, att man känner sig trygg och säker samt att det är viktigt att enbart behöriga använder systemen. De som tyckte att informationssäkerhet är en nackdel i deras arbete syftade på att det är jobbigt att komma ihåg alla lösenord och det medför att man måste skriva ner dem på lappar.

4.3 Platsinspektion

En platsinspektion av Olofströms kommuns serverhall har skett. Den gick till på följande sätt att jag bad om en rundtur i huset som serverhallen befinner sig i, samtidigt ställde jag frågor som berörde den fysiska säkerheten. Frågorna är framtagna utifrån åtgärderna som tas upp i BITS om den fysiska säkerheten.

Nedanför finns en sammanställning av platsinspektionen i form av en tabell innehållande fråga, kommentar och en utvärdering:

Finns funktioner för att förhindra obehörig fysisk tillträde till organisationens lokaler och information?	Ja. Det finns i form av passagesystem med taggar och tillhörande kod. Behörigheterna är begränsade under kväll och natt.	Ja
Har IT-utrustning som kräver avbrottsfri kraft identifierats?	Ja. Reservkraft finns till serverhallen i form av dieselaggregat och UPS.	Ja
Finns larm kopplat till larmmottagare för: - brand, temperatur, fukt? - sker test till larmmottagare?	Ja. Dessa testas regelbundet.	Ja
Finns i direkt anslutning till viktig datorkommunikationsutrustning kolsyresläckare?	Ja.	Ja
Regleras tillträde till utrymmen med känslig information eller informationssystem utifrån informationens skyddsbehov? Tillträdesrättigheter, rutiner för upprättande?	Ja. Tillgång till serverhallen är begränsad till IT-avdelningen, fastighetsavdelningen och Securitas.	Ja
Är korskopplingsskåp låsta?	Ja. Dessa är låsta och förvaras inte i samma rum.	Ja
Raderas känslig information på ett säkert sätt från utrustning som tas ur bruk eller återanvänds?	Ja. Ett särskilt program används för att radera känslig information från utrustning som tas ur bruk.	Ja
Finns möjlighet att reglera och mäta temperatur och fuktighet?	Ja. Detta sköts av leverantör.	Ja

Tabell 3: Sammanställning av platsinspektionen

5. Diskussion

I detta kapitel framför jag mina tankar och reflektioner om metodvalet och resultatet.

5.1 Metoddiskussion

Jag använde mig av en kvalitativ och kvantitativ metod för att få fram mitt resultat. Den kvalitativa metoden innefattade intervjuerna och platsinspektionen, medan den kvantitativa metoden innefattade enkätundersökningen. Jag valde att göra en personlig intervju med Ronny Haglund eftersom jag bland annat kunde vidareutveckla frågor som kunde misstolkas, för att jag kunde få utförligare svar av honom och med hjälp av transkribering efter inspelningen fick jag utförligare information om Olofströms kommuns IT-miljö.

Gällande de andra kommunerna i Blekinge valde jag att skicka ut intervjufrågorna genom e-post. Anledningen till varför jag gjorde det var på grund av tidsbrist och därför kände jag att det var ett bra val. Nackdelen med att jag skickade ut frågorna genom e-post var att de dels var enkla frågor, men även att de svarade på ett sätt för att de inte vill verka dåligt insatta. De kunde misstolka frågorna och skrev endast korta svar.

Gällande enkätundersökningen fanns det fördelar med att jag skickade ut den som en webbenkät, förutom de som nämnts under kapitlet "Metod". Frågorna som utgjorde enkäten testades på folk i min närhet för att jag skulle veta om man förstod frågorna. En annan fördel var enkätverktyget SurveyMonkey som användes till utformningen av enkäten och sammanställning av svaren. SurveyMonkey var ett bra strukturerat verktyg, användarvänligt och det skapade en användarvänlig enkät. Som tidigare nämnts, och som Jacobsen (2012) nämner, finns det en risk att en webbaserad enkätundersökning ger en väldigt låg svarsprocent och det stämde överens med denna undersökning.

Personliga intervjuer hade gett mig en högre svarsprocent, men eftersom det hade blivit en tidskrävande process, samt en högra kostnadsfråga, valde jag att göra en webbaserad enkätundersökning eftersom urvalet blev större (Jacobsen, 2012).

Platsinspektionen i Olofströms kommuns serverhall anses vara välgjord eftersom de punkter som undersöktes gav ett givande resultat. Det var viktigt att vara väl förberedd och det var bra att utgå från BITS.

5.2 Resultatdiskussion

Som tidigare presenterats under kapitlet "Begreppet informationssäkerhet" är de sju begreppen (konfidentiellt, integritet, tillgängligt, riktighet, tillförlitlighet, användbarhet och ägande) viktiga i dagens arbete med informationssäkerhet. Dessa begrepp är relevanta både nationellt som internationellt och är bra att utgå ifrån när man jobbar med informationssäkerhet i de Blekingska kommunerna. Resultatet som jag fick genom intervjuerna, enkätundersökningen och platsinspektionen var någorlunda förväntade –

på ett positivt sätt. Först och främst visste jag sedan innan att Olofströms kommun jobbar aktivt med informationssäkerhet. Dock kan det vara bra för organisationer att det kommer in en eller flera personer som ser verksamheten med helt andra ögon än vad de ansvariga gör. Det kan vara väldigt lätt att köra på sitt spår eftersom det i stort sett aldrig har hänt någon allvarlig incident inom organisationen.

Resultatet från enkätundersökningen visar också på att de som har svarat har koll på informationssäkerhet och varför det är viktigt, trots att majoriteten inte har fått någon utbildning om det samt att majoriteten av de svarande inte känner till Olofströms kommuns IT-säkerhetspolicy. Gällande frågan "Hur ofta byter du lösenord?" byter de flesta sitt lösenord efter 61-90 dagar. Detta är ett positivt resultat eftersom kommunens IT-säkerhetspolicy säger att lösenordet ska bytas var 90:e dag. Användarna får en påminnelse om att det är dags att byta lösenord och resultatet visar att de flesta byter sitt lösenord vid det tillfället. Viktigt att nämna är att tidigare använda lösenord inte kan återanvändas. Resultatet visar också att 22 stycken aldrig byter sitt lösenord och detta kan innebära en säkerhetsrisk för kommunen.

Resultatet visar också på att Olofströms kommuns IT-säkerhetspolicy inte är antagen samt att den är daterad 2004. Med andra ord har det inte gjorts någon revidering sedan dokumentet arbetades fram. Eftersom det har hänt mycket sedan 2004, främst inom informationssäkerhetsområdet, och av resultatet att döma, behöver kommunen arbeta mer med sin IT-säkerhetspolicy samt med utbildningar om informationssäkerhet. Det är känt sedan tidigare att kommunen är mitt uppe i en migrering och planerar, när migreringen är klar, att ha en introduktionsdag för de anställda. Detta är positivt för de anställda eftersom det blir lättare att bibehålla ett säkerhetstänk som anställd och därmed kan kommunen motverka att de har anställda som exempelvis aldrig byter sitt lösenord.

6. Slutsats

Enligt SOU 2005:42 finns det ingen direkt lösning till att förhindra problem som uppstår inom informationssäkerhet. Detta för att informationssäkerhet är under ständig utveckling och inte direkt greppbar. Som tidigare nämnt och som Panko (2010) nämner är det viktigt att ha en ledning, riktlinjer, kunskap och utbildningar för att bevara en acceptabel säkerhetsnivå. Utan detta kan det vara svårt som anställd att bibehålla ett säkerhetstänk och därmed finns det en risk att allvarliga incidenter inträffar.

Slutresultatet av uppsatsen visar på att Olofströms kommun arbetar aktivt med informationssäkerhet. Däremot finns det alltid utrymme för nya idéer till möjliga förbättringar. En av dessa förbättringar är förslagsvis att uppdatera dokumentet "Säkerhetsinstruktion IT, för användare" eftersom den dels är framtagen 2004 och det har hänt mycket inom informationssäkerheten sedan dess.

Några förslag till framtida förbättringar i dokumentet är att:

1. Det är en fördel om dokumentet är antagen av kommunfullmäktige eftersom det då finns ett dokument som måste efterföljas och som alla är införstådda med.
2. Uppdatera vissa begrepp som idag har ett annat namn. Exempelvis KBM som idag benämns som MSB.
3. Ändra antalet tecken i användarnas lösenord från sex tecken till åtta tecken. Det kommer inte göra en större skillnad eftersom majoriteten av de svarande i enkätundersökningen redan har åtta tecken eller fler i sitt lösenord och BITS rekommenderar att ett lösenord ska ha minst åtta tecken.
4. Ändra begrepp angående enheter exempelvis diskett, modem och liknande. Idag används USB-minnen och externa hårddiskar mer frekvent.

Angående de Blekingska kommunerna har resultatet givit sådan information att ett förslag angående samverkan gällande styrdokument är på sin plats. Detta är till en fördel eftersom det dels är positivt ur ett kostnadsperspektiv och det är även mer tidseffektivt. Ett gemensamt styrdokument för IT-säkerhetsinstruktioner för alla kommuner i Blekinge skulle underlätta för respektive IT-avdelning då de olika kompetenserna kan komplettera varandra. Kommunerna jobbar ungefär likadant med informationssäkerhet och strävar efter att hela tiden utveckla arbetet kring det. Kommunerna tillhör trots allt samma län, varför inte samarbeta?

Referenser

Carlsson, B. & Jacobsson, A. (2012). *Om säkerhet i digitala ekosystem*. Lund: Studentlitteratur

Ejlertsson, G. (2010). *Enkäten i praktiken. En handbok i enkätmetodik*. Lund: Studentlitteratur

Gollmann, D. (2011). *Computer Security*. West Sussex: John Wiley & Sons Ltd

Jacobsen, D. I. (2012). *Förståelse, beskrivning och förklaring: introduktion till samhällsvetenskaplig metod för hälsovård och socialt arbete*. Lund: Studentlitteratur

Jesan, J. P. (2006). *Information security*. >http://ubiquity.acm.org/article.cfm?id=1117695< Hämtad: 2013-04-08

Myndigheten för samhällsskydd och beredskap (2006). *Basnivå för informationssäkerhet (BITS)*. >https://msb.se/RibData/Filer/pdf/24855.pdf< Hämtad: 2013-04-08

Nationalencyklopedin (2013). *Säkerhet*. >http://www.ne.se/säkerhet/322447< Hämtad: 2013-04-08

Panko, R. R. (2010). *Corporate Computer and Network Security*. Boston: Prentice Hall

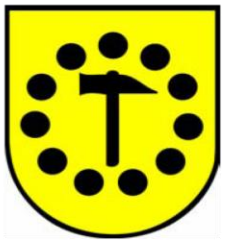
SOU 2005:42. *Säker information. Förslag till informationssäkerhetspolitik*. Delbetänkande från InfoSäkutredningen

Syrén, A. (2005). *På egen risk. En handbok om informationssäkerhet*. Stockholm: SIS Förlag

Trost, J. (2012). *Enkätboken*. Lund: Studentlitteratur

Whitman, M. E. & Mattord, H. J. (2012). *Principles of Information Security*. Boston: Course Technology

Bilaga 1: Säkerhetsinstruktion IT, för användare



Säkerhetsinstruktion IT, för användare

1 INLEDNING **2**

2 HANTERING AV INFORMATION **2**

3 BEHÖRIGHET **3**

FÖR ATT FÅ BEHÖRIGHET KRÄVS ATT 3

4 INLOGGNING **3**

5 EN SÄKER ARBETSPLATS **4**

ARBETSSTATION 4
KRINGUTRUSTNING MED MELLANLAGRINGSMÖJLIGHET 5
VÅRT LOKALA NÄTVERK (LAN) 5

6 INTERNET **6**

7 E-POST **6**

8 INCIDENTER, VIRUS MM **7**

TECKEN PÅ DATAVIRUS KAN VARA ATT 8
OM DU MISSTÄNKER VIRUS I DATORN SKALL DU 8

9 STÖD OCH HJÄLP **8**

10 NÄR EN ANSTÄLLNING UPPHÖR **8**

1 INLEDNING

Kommunernas Säkerhetspolicy IT beskriver närmare hur vi arbetar med IT-säkerheten och hur ansvaret för säkerheten fördelas. Vår Säkerhetspolicy IT följer Krisberedskapsmyndighetens (KBM´s) rekommendation ”Basnivå för IT-säkerhet (BITS)”. I detta dokument, ”Säkerhetsinstruktion IT, för användare”, klargörs de regler som gäller för personalens arbete i Blekinge Väst IT-miljö.

Mål
Denna instruktion syftar till att ge dig kunskaper och riktlinjer om hur Du hanterar

- olika former av information
- den teknik vi använder
- e-post, internet,
- incidenter mm

Instruktionen syftar också till att skydda de värden som informationen representerar och att förebygga att uppgifter och information som omfattas av sekretess röjs, ändras eller förstörs.

Instruktionen skall ge alla medarbetare kunskap och kännedom om hur information, kommunikationsnät, datasystem och arbetsplatser skall hanteras för att felaktigheter och störningar skall undvikas.

2 HANTERING AV INFORMATION

Den information Du lagrar på nätverket säkerhetskopieras automatiskt. Du skall därför lagra din information i egen, alternativt verksamhetsgemensam hemkatalog.

- Egen hemkatalog är ditt personliga arkiv, som Du skall använda för lagring av personlig information. De filer Du sparar i din hemkatalog kan endast Du nå.
- Gemensam katalog är ett arkiv för lagring av gemensam information för en förvaltning, avdelning eller ett arbetslag.

Om Du lagrar information på din lokala hårddisk (ex C:\) är Du personligen ansvarig för att säkerhetskopiering sker, t ex på diskett. När Du lagrar information på din lokala hårddisk (ex C:\) riskerar Du att förlora information, som inte kan återskapas till rimliga kostnader. Du försvårar också möjligheten att dela information med Dina medarbetare.

Tänk också på att den information Du lagrat på lokal disk är tillgänglig för alla som kan starta din dator. Man behöver ofta inte använda något lösenord för att komma åt dessa diskar.

Med stöd av ovanstående gäller att:

⇨ **Ingen lagring på lokala diskar skall förekomma.**

3 BEHÖRIGHET

Våra datasystem (nätverk, servrar och program) är utrustade med behörighetskontrollsystem för att säkerställa att endast behöriga användare kommer åt information. Vilken behörighet Du får till lagrad information och till våra datasystem beror helt på dina arbetsuppgifter och avgörs av din chef. (Din chef lämnar skriftlig beställning till IT-enheten för tilldelning av behörigheter.)

För att få behörighet krävs att

- Du informerats om innehållet i denna säkerhetsinstruktion och om kommunens Säkerhetspolicy IT
- att Du fått utbildning på de datasystem Du kommer att använda.

När IT-enheten registrerat dig som användare får Du en **användaridentitet** uppbyggd på delar av ditt förnamn och efternamn. I undantagsfall kan gruppidentitet användas för tillgång till basinformation.

4 INLOGGNING

Primärt skall inloggning ske med personlig användaridentitet. Sker inloggning med gruppidentitet får ingen personlig information lagras på gemensam enhet. Första gången Du loggar in får Du ett **tillfälligt lösenord** av IT-enheten. Du blir uppmanad av systemet att byta till ett personligt lösenord. Om Du inte byter lösenord blir Ditt användarid låst.

Lösenordet är strängt personligt och skall hanteras därefter. Tänk på att Du själv kan bli misstänkt om någon använder ditt lösenord för olämpliga ändamål.

Du skall därför:

- inte avslöja ditt lösenord för andra eller låna ut din behörighet.
- skydda lösenordet väl.
- omedelbart byta lösenord om Du misstänker att någon känner till det.
- byta lösenordet var 90:e dag. Du får en påminnelse på skärmen när det är dags att byta.

Även i andra datasystem än nätverket bör Du byta lösenord var 90:e dag. I dessa datasystem ges dock oftast ingen påminnelse.

Lösenordet skall bestå av minst 6 tecken och skall konstrueras så att det inte lätt kan kopplas till dig som person. Tecknen å, ä och ö får inte användas i lösenord.

Undvik enkla repetitiva mönster såsom t ex ”ABC1234”, ”AAA1111” får inte användas. Använd inte heller andra lättforcerade lösenord, såsom eget eller familjemedlems namn eller enkla tangentkombinationer av typen ”QWERTYU”. För att väsentligt försvåra lösenordsknäckning bör bokstäver, siffror och specialtecken (#&+) blandas i lösenordet.

⇨ **Viktigast av allt är att Du väljer ett lösenord som Du kommer ihåg.**

Tidigare använda lösenord kan inte återanvändas. När Du byter till ett nytt lösenord kontrollerar systemet att Du inte använder något av de senaste 13 lösenorden.

Om Du glömmer ditt lösenord och försöker logga in i nätverket eller i ett verksamhetssystem med felaktigt lösen, kommer ditt användarid att spärras efter tre felaktiga försök. Om detta inträffar vänder Du dig till IT-enheten, samt i vissa verksamhetssystem till systemansvarig. Du kommer då att få ett nytt tillfälligt lösenord.

5 EN SÄKER ARBETSPLATS

Kommunen eftersträvar att alla skall ha en säker arbetsplats, inte bara avseende IT-säkerheten. Med arbetsplats avses de personliga utrymmen och material som Du har tillgång till och förfogar över i ditt arbete, som t ex ditt tilldelade tjänsterum, de utrymmen vi gemensamt använder och de utrymmen Du använder vid distansarbete.

Utöver de regler som finns under kapitel 2, 3 och 4 gäller följande regler:

Arbetsstation

Följande gäller för samtliga datorarbetsplatser:

- När Du tillfälligt lämnar arbetsplatsen skall lösenordsskyddad skärmsläckare användas. Vid längre frånvaro, ex rast, lunch, skall arbetsstationen loggas ur.
- Du är ansvarig för den arbetsstation med tillhörande hårdvara som Du förfogar över.
- Fysiska ingrepp i din arbetsstation med tillhörande hårdvara får endast utföras av IT-enheten.
- Vid fel på arbetsstation med tillhörande hårdvara skall Du omgående anmäla detta till IT-enheten.
- Arbetsstationen med tillhörande hårdvara får inte bytas ut, förändras eller medtagas utan IT-enhetens medgivande.
- Installation och konfiguration av hårdvara får endast utföras av IT-enheten eller av IT-enheten anvisad/godkänd person.
- Mjukvara (program) skall godkännas och installeras av IT-enheten eller av IT-enheten anvisad/godkänd person.

Dator, som Du använder **utanför** din ordinarie arbetsplats kan utgöra en säkerhetsrisk. Därför skall:

- Du hålla utrustningen och datamedia under ständig uppsikt om Du inte kan låsa in den.
- Du tänka på att Du inte får lagra sekretessbelagd eller för verksamheten känslig information på datorn.
- Du förvarar en säkerhetskopia av all information i din hemmakatalog på nätverket.
- datorn vara utrustade med system för behörighetskontroll, virusskydd och brandvägg.

Lagringsmedia som Du använder i hemdatormiljö skall viruskontrolleras innan de får användas i kommunens nätverk.

Anm Med dator avses alla enheter som kan behandla och/eller lagra information, ex handdatorer (sk PDA), mobiltelefoner, bärbara datorer etc

Se även fastställda policys

Kringutrustning med mellanlagringsmöjlighet

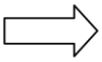
Handdatorer, digitala kameror, mobiltelefoner mm kan lätt bli virusbärare då Du kan mellanlagra information för transport mellan olika datorer i dessa. Därför skall Du inte ansluta denna typ av kringutrustning mot en dator som Du inte med säkerhet vet har ett uppdaterat virusprogram.

Vårt lokala nätverk (LAN)

Vårt nätverk är en mycket viktig gemensam resurs som ger oss alla möjlighet att lagra information, dela på skrivare och program, upprätta kommunikation mm.

Följande regler gäller för nätverket:

- Information, oavsett media, som enligt lagar, förordningar och interna regler bedöms som sekretessklassad med hänsyn till rikets säkerhet får ej lagras i vårt lokala nätverk (LAN).
- Inloggning på nätverket skall primärt ske med din personliga användaridentitet (se kap 3 och 4).
- All inloggning eller försök till inloggning under annan, eller med annans identitet är absolut förbjuden.
- Destruktivt arbete på det lokala nätverket med t ex avsikt att skada lagrad information, ses som mycket allvarligt och är absolut förbjudet och kommer att beivras.
- När Du arbetar i kommunens nätverk förekommer loggning och registrering av dina transaktioner.
- Utskrifter av dokument på gemensam skrivare skall snarast hämtas.
- Information som sparas på det lokala nätverket skall lagras på anvisad plats (Se kap 2)
- Det är förbjudet att ansluta sig till externt nätverk via egen icke godkänd uppkoppling t e x modem.
- För att få tillgång till resurser i vårt interna nätverk med extern uppkoppling, för att t ex arbeta från hemmet, skall ett avtal tecknas mellan verksamhetsansvarig och den anställde som reglerar teknik och datasäkerhet mm.
- Det är förbjudet att utnyttja felkonfigureringar och programfel eller att med andra metoder skaffa sig utökade systemrättigheter eller annan personlig rättighet än den som tilldelats av systemägaren.



Kom ihåg att Du ansvarar för allt som registrerats med din användaridentitet.

6 INTERNET

När Du använder Internet kan säkerheten påverkas i mycket hög grad beroende på Ditt beteende.

Inga program får utan särskilt tillstånd laddas ner från Internet (ex spelprogram, skärmsläckare, gratisprogram eller andra program).

Det är inte tillåtet att via Internet titta eller lyssna på material av pornografisk, rasistisk eller nazistisk karaktär. Förbudet gäller också material som är diskriminerande (religion, kön, sexuell läggning, nationalitet, etc.) eller har anknytning till kriminell verksamhet eller satanism. Undantag får göras när materialet är viktigt för planering och genomförande av undervisning.

För att få ett effektivt resursutnyttjande av Internet-kapaciteten och förhindra att skadlig kod kommer in i nätverket filtreras datatrafiken.

När Du surfar på Internet representerar Du kommunen. Gör det med gott omdöme så att ditt agerande på nätet inte skadar kommunens anseende. Agera i enlighet med våra värderingar så att det Du förmedlar på nätet inte skadar kommunen.

Du bör tänka på att Du lämnar spår i loggfiler som lagrar information om Internettrafiken till och från kommunen. Loggfilerna är offentliga handlingar och visar vilka webbplatser Du har besökt.

Allmänt gäller att den som laddar ner filer från Internet har gott omdöme och endast hämtar sådan information som är relevant för arbetet, är tillåten och kommer från välrenommerade webb- eller ftp-platser.

Se vidare aktuell Internetpolicy

7 E-POST

E-post är ett redskap som primärt skall användas i tjänsten. E-post ska behandlas på samma sätt som övrig post. Brevlådan bör tömmas varje dag. Den som av någon anledning inte kan göra det bör se till att någon annan sköter tömningen.

Det är inte förbjudet att ta emot och skicka personlig post. Den personliga posten bör dock snarast tas bort från användarens brevlåda.

⇨ **Skicka aldrig sekretesshandlingar eller integritetskänsliga uppgifter som e-post.**

Tänk på upphovsrätten när filer bifogas så att Du inte gör dig skyldig till upphovsrättsintrång.

Informationsinnehåll får inte kränka en eventuell upphovsmans eller annans lagliga rättigheter. Om Du har tillstånd att använda bild eller text skall Du alltid ange källa.

För att undvika risk för virusspridning via e-post och onödig belastning av systemresurser:

- bör Du endast öppna bifogade filer från avsändare Du känner till. Kontrollring avsändaren om Du är osäker på innehållet.
- skall Du följa de råd om inställningar i och hantering av e-postsystemet som Du får av din IT-funktion.
- bör Du vara selektiv med att använda stora gruppadresser (massutskick) och med att skicka eller vidarebefordra meddelanden som innehåller stora filer.
- skall Du inte sprida din e-postadress till mindre seriösa ställen varifrån Du t ex kan förvänta dig reklam.
- tillåts inte bifogade filer som är större än 10 mb.

Använd inte heller din vanliga användaridentitet och ditt lösenord när Du registrerar dig i konferenser eller publika e-postservrar.

Om Du misstänker att det kommit in virus via e-postsystemet skall Du agera som beskrivs i avsnittet om ”Incidenter, virus mm”. (Se 8)

Filtrering av e-post, se under avsnitt ”Incidenter, virus mm”. (Se 8)

Se vidare aktuell E-postpolicy.

8 INCIDENTER, VIRUS MM

Om Du misstänker att någon obehörig använt din användaridentitet och varit inne i systemet skall Du:

- notera när Du senast var inne i systemet själv.
- notera när Du upptäckte intrånget.
- omedelbart anmäla händelsen till IT-enheten eller din chef.
- dokumentera alla iakttagelser i samband med upptäckten och försöka att fastställa om kvaliteten på din information har påverkats.

Kort om datavirus
Datavirus kan beskrivas som ett program eller en programsekvens vars uppgift är att kopiera sig själv och tränga in i andra program för att utföra något otillbörligt. I värsta fall kan datorns hårddisk raderas eller kan viruset kopiera sig självt i det oändliga tills hela systemet bryter samman.

Datavirus är ofta ytterst smittsamma och ”smittkällan” kan vara svår att identifiera. Gratisprogram, spelprogram och filer som laddas ner från Internet eller medföljande filer till e-post är de vanligaste smittbärarna.

Kommunen har programvaror för viruskontroll som kontinuerligt kontrollerar nätverket. Även disketter och filer som Du hämtar från Internet kontrolleras av antivirusprogram i nätverket.

Tecken på datavirus kan vara att
- datorn utför operationer/arbete utan att Du själv startat det, t ex förändringar sker på skärmen (tecken flyttas, försvinner etc.)
- pip eller hälsningar på skärmen
- datorn uppträder på ett onormalt sätt, t ex arbetar mycket långsamt.

Om Du misstänker virus i datorn skall Du
- avbryta allt arbete på det ställe i programmet där Du gjorde upptäckten.
- se till att ingen använder datorn/programmet.
- omedelbart anmäla förhållandet till IT-enheten, systemansvarig. OBS att anmälan skall ske per telefon eller personligt, EJ per e-post.
- skriva ner alla iakttagelser som Du tror kan ha samband med händelsen.

Om Du får brev med virusvarning där man talar om att ett virus är på gång skall Du inte skicka meddelande om detta till alla inom kommunen utan kontakta IT-enheten som kan avgöra om det är en seriös varning eller bara ett skämt. Skicka inte heller någon varning externt innan Du kontrollerat med IT-enheten.

För att förhindra att virus kommer in i det interna nätverket sker filtrering av datatrafiken. IT-enheten svarar för att filtrering sker utifrån aktuella virusvarningar.

9 STÖD OCH HJÄLP

Genom IT-enheten kan Du få stöd och support avseende Garanti-/funktionsarbetsplatsen. För verksamhetsspecifika program kan Du kontakta respektive systemansvarig. Är Du osäker kan Du dock alltid vända dig till IT-enheten för råd. Synpunkter och förslag till förändring av ”Säkerhetsinstruktion IT, för användare” anmäler Du till respektive kommuns IT-säkerhetsråd.

10 NÄR EN ANSTÄLLNING UPPHÖR

När en anställning upphör skall:
- det material Du har sparat rensas och tas bort. Arbetsmaterial skall överlämnas till anvisade medarbetare.
- ansvarig chef avsluta den anställdes behörigheter i nätverket och i verksamhetssystemen genom anmälan till IT-enheten respektive systemansvarig.
- ansvarig chef anmäla till systemansvarig för e-post-systemet hur kontot skall hanteras.

Bilaga 2: Missivbrev till enkätundersökningen

Hej!

Jag heter Linus Göransson och studerar IT-forensik och informationssäkerhet vid Högskolan i Halmstad. I mitt examensarbete håller jag på att göra en säkerhetsanalys av Olofströms kommuns IT-verksamhet.

Analysen utförs i samarbete med IT-avdelningen och görs för att se om IT-verksamheten uppnår en acceptabel säkerhetsnivå för informationshantering. Analysen består bland annat av en enkätundersökning och du är härmed inbjuden att delta i undersökningen. Undersökningen utförs anonymt och det kommer inte gå att härleda vem som har besvarat enkäten.

Med hjälp av ditt deltagande i undersökningen hjälper du inte enbart mig i mitt examensarbete, utan du hjälper även IT-avdelningen att få en överblick över hur informationssäkerheten upplevs bland er anställda. Det i sin tur är viktigt i deras fortsatta arbete med informationssäkerhet för att skapa en bättre och säkrare arbetsmiljö.

Enkäten, som du når genom att klicka på länken nedan, består av 13 frågor och den beräknas ta cirka 3-7 minuter av din tid att besvara. Har du några frågor om enkäten eller om det är något annat du funderar på, kan du kontakta mig på telefonnummer 0760-12 22 21 eller via e-post gorlin10@student.hh.se.

Enkäten är öppen för besvarande till och med 2013-03-28.

Tack för din hjälp!

Med vänlig hälsning,
Linus Göransson

Länk till enkäten: https://www.surveymonkey.com/s/SBLHFYR

Bilaga 3: Enkätundersökningen

Allmänt

* 1. Använder du dagligen din dator i ditt arbete?

- Ja
- Nej

* 2. Har du fått någon utbildning om informationssäkerhet?

- Ja
- Nej

* 3. Känner du till Olofströms kommuns IT-säkerhetspolicy

- Ja
- Nej

Datorhantering

* 4. Loggar du ut, alternativt låser, din dator när du lämnar den obevakad?

- Ja
- Nej

* 5. Har fler än du tillgång till din dator?

- Ja
- Nej

* 6. Kopplar du in privata USB-minnen eller liknande i din dator?

- Ja
- Nej

Lösenordshantering

* 7. Hur många tecken innehåller ditt lösenord?

- Ett tecken
- Två tecken
- Tre tecken
- Fyra tecken
- Fem tecken
- Sex tecken
- Sju tecken
- Åtta tecken eller fler

* 8. Innehåller ditt lösenord bokstäver, siffror och/eller specialtecken? (Exempel: !, @, $, &)

- Bokstäver
- Siffror
- Specialtecken

- Bokstäver och siffror
- Bokstäver och specialtecken
- Siffror och specialtecken
- Bokstäver, siffror och specialtecken

* 9. Använder du samma lösenord i externa sammanhang? (Exempel: Privat e-post, Facebook, Twitter)

- Ja
- Nej

* 10. Hur ofta byter du ditt lösenord?

- 0-30 dagar
- 31-60 dagar
- 61-90 dagar
- 91-120 dagar
- Aldrig

E-posthantering

* 11. Öppnar du all e-post och bifogade filer som du får till din e-postadress (@olofstrom.se)

- Ja
- Nej

* 12. Använder du din e-postadress (@olofstrom.se) för att skicka och ta emot privat e-post?

- Ja
- Nej

Övrigt

* 13. Slutligen, anser du att informationssäkerhet, till exempel lösenord, är en för- eller nackdel i ditt arbete?

- Fördel
- Nackdel

Varför?

HÖGSKOLAN
HALMSTAD