

## Kapitel 11 – Styrning av åtkomst

Information representerar kunskap och kunskap är en av de viktigaste resurserna i varje organisation. Skydd av information är därför av vital betydelse för överlevnad och framgång. IT-system i moderna organisationer tillhandahåller en nödvändig infrastruktur för verksamheten. Störningar i dessa system kan få allvarliga, i värsta fall fatala, konsekvenser för organisationen i sin helhet.

Åtkomstskydd av information är datorvärldens motsvarighet till tillträdes- och användningsskydd av fysiska tillgångar i den fysiska världen. Det finns många kopplingar mellan informationssäkerhet och fysisk säkerhet, bland annat kräver IT-resurser fysiska skydd. Men det finns också betydande skillnader såväl när det gäller hot och risker som skyddsmetoder. I dagens samhälle har såväl informationssäkerhet som fysisk säkerhet sin givna och nödvändiga plats i framgångsrika verksamheter.

### 11.1 Verksamhetskrav på styrning av åtkomst

**Mål: Att styra åtkomst till information.**

Åtkomst till information, informationsbehandlingsresurser och verksamhetsprocesser bör styras på grundval av verksamhets- och säkerhetskrav.

Regler för styrning av åtkomst bör ta hänsyn till policies för spridning och behörighet till information.

#### 11.1.1 Åtkomstpolicy

En organisations informationssäkerhetspolicy ska klart och tydligt ange de riktlinjer som gäller för tilldelning/fråntagning av åtkomsträttigheter till information, men också hur dessa rättigheters operativa användning ska kontrolleras.

Styrande för riktlinjerna är de krav som verksamheten ställer på organisationens samlade IT-resurser. Dessa krav kan vara av olika slag: funktionella, effektivitet, säkerhet, legala och avtalsmässiga. Informationssäkerhetspolicyn måste klarlägga de övergripande principer som ska gälla för informationsanvändning. En ofta tillämpad princip är ”behov-att-veta”-principen, som säger att varje medarbetare ska ha tillgång till exakt den information som krävs för att han eller hon ska kunna utföra sina arbetsuppgifter. En annan vanlig princip – som också styr utformningen av ”regler för styrning av åtkomst” – säger att ”det som inte är explicit tillåtet är förbjudet”.

Riktlinjerna och principerna ovan utgör grunden för det regelverk som ska styra åtkomst till IT-resurser i den operativa verksamheten

Operativ styrning av åtkomst kan ske på två olika sätt: obligatorisk- och frivillig åtkomststyrning. Vid obligatorisk åtkomststyrning måste åtkomsträttigheter definieras för samtliga användare till varje informationsresurs. Detta sker centralt som en systemadministrativ funktion. Vid frivillig åtkomststyrning definieras åtkomsträttigheter decentraliserat av ägaren till respektive informationsresurs. Obligatorisk åtkomststyrning är resurskrävande men att föredra ur säkerhetssynpunkt.

### 11.2 Styrning av användares åtkomst

**Mål: Att säkerställa behörig användares åtkomst och förhindra obehörig åtkomst till informationssystem.**

Formella rutiner bör finnas för styrning av åtkomsträttigheter till informationssystem och tjänster.

Rutinerna bör täcka alla stadier i användaråtkomstens livscykel, från registrering av nya användare till slutlig avregistrering av användare som inte längre behöver åtkomst till informationssystem och tjänster.

Särskild försiktighet bör iaktas, där det är lämpligt, ifråga om behovet av att styra fördelning av privilegierade åtkomsträttigheter som tillåter användare att förbigå normala systemspärrar.

#### 11.2.1 Användarregistrering

Systemet för användarregistrering ska omfatta samtliga användares ”livscykel som systemobjekt”, det vill säga sträcka sig från nyregistrering till slutlig avregistrering. En unik användaridentitet (tillsammans med lämplig loggning av användaraktiviteter) är en förutsättning för spårbarhet varigenom en användare kan göras ansvarig för sina handlingar. En rutin bör finnas och ett register upprättas vilket visar de åtkomsträttigheter varje individ tilldelats.

## Styrning av åtkomst

Viktigt är att alltid beakta de krav som finns för att skydda individers personliga integritet.

### 11.2.2 Styrning av särskilda rättigheter

Privilegierad behörighet – en åtkomsträtt som överträder normal åtkomstkontroll – ska tillämpas ytterst restriktivt. Det är väsentligt att tilldelning och användning av privilegierad behörighet sker så att spårbarheten upprätthålls. Olämplig tilldelning av privilegierad behörighet kan resultera i oönskade intrång i system.

### 11.2.3 Styrning av lösenord för användare

Tilldelning av lösenord bör ske genom en formell och sekretesskyddad rutin. Det är av vikt att

- utgivning av lösenord föregås av en säker användaridentifikation,
- regler för hur lösenord bör hanteras är fastställda,
- användaren har förstått och accepterat dessa regler.

Temporära lösenord bör användas sparsamt och utdelas endast efter positiv identifikation av användaren. De bör alltid tidsbegränsas. Används tillfälliga lösenord bör dessa vara av bra kvalitet och endast gälla för den första inlogningen.

### 11.2.4 Granskning av användares åtkomsträttigheter

Tilldelade behörigheter bör granskas efter varje förändring i arbetsuppgifter, men också med regelbundna intervall.

## 11.3 Användares ansvar

**Mål: Att förhindra obehörig användaråtkomst och åverkan eller stöld av information och informationsbehandlingsresurser.**

De behöriga användarnas medverkan är väsentlig för en effektiv säkerhet.

Användarna bör göras medvetna om sitt ansvar för att upprätthålla en effektiv styrning av åtkomst särskilt när det gäller användning av lösenord och säkerheten hos användarutrustning.

En policy som kräver ”renstädat skrivbord och tom bildskärm” bör införas för att minska risken för otillåten åtkomst till eller skada på pappersdokument, media och informationsbehandlingsresurser.

### 11.3.1 Användning av lösenord

Självalda lösenord bör vara av bra kvalitet, genom att exempelvis bestå av minst sex tecken (varav minst två ska vara numeriska eller specialtecken) samt inte vara associerbara till användaren på ett enkelt sätt. Lösenorden bör hållas hemliga. Lagras de på pappers- eller datamedia bör detta ske på ett säkert sätt. Lösenord bör aldrig lagras oskyddat i det IT-system det används.

### 11.3.2 Obemannad användarutrustning

Användarutrustning utan tillsyn måste skyddas på ett tillfredställande sätt. Ett bra hjälpmedel är lösenordsskyddade skärmsläckare. Lämnas persondatorer eller terminaler obemannade under en längre tid bör användaren logga ut. Arbetsstationer eller terminaler ska normalt aldrig slås av utan utloggning.

### 11.3.3 Policy för renstädat skrivbord och tom bildskärm

Ett sunt och vaket säkerhetsmedvetande är en naturlig komponent i varje säkerhetssystem. Som en allmän grundregel gäller att känslig information aldrig lämnas oskyddad när den inte används. Det är bland annat viktigt att

- påloggade men obevakade persondatorer eller terminaler är lösenordsskyddade (eller skyddade på annat sätt) och har skärmar som slocknar när de inte används,
- känsliga elektroniska dokument eller pappersdokument inte lämnas obevakade på en öppen plats (inte enbart på grund av risk för sekretessbrott utan också på grund av risk för brand, vattenskada, etc.).

## 11.4 Styrning av åtkomst till nätverk

**Mål: Att förhindra obehörig åtkomst till nätverkstjänster.**

Åtkomst till både interna och externa nätverkstjänster bör styras.

Användaråtkomst till nätverk och nätverkstjänster bör inte äventyra nätverkstjänsternas säkerhet, genom att säkerställa:

- (a) att det finns lämpliga gränssnitt mellan organisationens nätverk och nätverk som ägs av andra organisationer och publika nät;
- (b) att lämpliga autentiseringsmetoder används för användare och utrustningar;
- (c) att styrningen av användares åtkomst till informationstjänster fungerar.

### 11.4.1 Policy för användning av nätverkstjänster

Policyn för utnyttjande av nätverk och nätverkstjänster bör reglera tillgång och behörighet till just dessa. Policyn är av särskild betydelse om (delar av) organisationens IT-resurser är sammankopplade med andra interna eller externa nätverk eller nätverkstjänster.

### 11.4.2 Autentisering av användare för extern anslutning

Externa anslutningar kan innebära stora risker för obehörig åtkomst. Därför är det viktigt att rätt säkerhetsåtgärder vidtas. Exempel på sådana säkerhetsåtgärder är stark autentisering, dedikerad utrustning, privata linjer, motringning, etc. Vid automatisk uppkoppling till externa datorer bör även dessa autentiseras (autentisering av nod).

### 11.4.3 Identifiering av utrustning i nätverk

Automatisk identifiering av utrustning kan vara en bra lösning om speciell utrustning används eller anslutning sker från definierade anslutningspunkter. En riskanalys av aktuella hot kan innebära att automatisk identifiering bör kompletteras med annan teknik för autentisering.

### 11.4.4 Skydd av extern diagnos- och konfigurationsport

Diagnosportar för distansunderhåll bör vara avstängda och fysiskt skyddade när de inte används. När diagnosporten behöver användas bör uppkopplingen var styrd från organisationen.

### 11.4.5 Uppdelning i nätverk

Modern informationsteknik har introducerat nya samarbetsformer och nya former att interagera organisationer emellan, men också nya sätt att utföra traditionella arbetsuppgifter. Det har medfört många nya frågor och problem när det gäller informationssäkerhet med krav på radikalt nya lösningar.

Logiskt sektionerade nätverk med säkrad kommunikation mellan sektionerna är ett generellt försök att besvara och lösa flera av dessa frågor och problem. Ansatsen har introducerat en del nya säkerhetskoncept och -mekanismer, till exempel intranät, extranät, filtrerande router, brandvägg, DMZ (demilitarized zone) och VPN (virtual private network).

### 11.4.6 Skydd av nätverksanslutning

Användarnas möjligheter att ansluta till nätverket bör utgå från att det finns klart definierat vilken information som krävs för att utföra de arbetsuppgifter som innefattas i befattningen. Då behoven omfattar tillgång till delade nätverk och nätverk vilka går utanför organisationens avgränsningar kan särskilda restriktioner behövas.

### 11.4.7 Styrning av vägval

Regler för styrning av vägval kan vara nödvändigt för att inte överträda krav på åtkomstkontroll. Vid användning av delade nätverk och nätverk vilka går utanför organisationens avgränsningar kan detta vara extra viktigt.

## 11.5 Styrning av åtkomst till operativsystem

### Mål: Att förhindra obehörig åtkomst till operativsystem.

Säkerhetsanordningar bör användas för att begränsa åtkomsten till operativsystem till endast behöriga användare. Dessa anordningar bör möjliggöra följande:

- (a) autentisera behöriga användare i enlighet med en definierad åtkomstpolicy;
- (b) registrera lyckade och misslyckade försök till autentisering av system;
- (c) registrera användningen av särskilda systemprivilegier;
- (d) slå larm när systemsäkerhetspolicys bryts;
- (e) tillhandahålla lämpliga medel för autentisering;
- (f) i tillämpliga fall begränsa användarens uppkopplingstid.

### 11.5.1 Säker påloggningsrutin

En påloggningsrutin bör dels tillåta effektiv och enkel påloggning av legitima användare, dels minimera möjligheten till obehörig åtkomst. Systeminformation, hjälprutiner, etc. ska inte visas förrän fullständig påloggning har skett. Antalet tillåtna inloggningsförsök ska begränsas och misslyckade försök ska loggas. Det är lämpligt att påloggningsrutinen varnar för obehörig användning av systemet.

### 11.5.2 Identifiering och autentisering av användare

Samtliga legitima systemanvändare ska tilldelas en unik användaridentitet. I speciella fall är det lämpligt att en användare, exempelvis en systemadministratör, tilldelas flera identiteter.

Autentisering innebär att en påstådd identitet verifieras. En användare kan styrka sin identitet genom att

- veta något (till exempel "lösenord"),
- äga något (till exempel "aktivt kort"),
- "vara" något (till exempel "fingeravtryck").

### 11.5.3 Lösenordsrutin

Användning av lösenord är den vanligaste metoden för autentisering utom i särskilt känsliga tillämpningar, som till exempel elektronisk handel, där starkare metoder krävs. I vissa fall tilldelas permanenta lösenord men i normalfallet väljs lösenordet av användaren själv. Det är önskvärt att lösenordsrutinen

- kontrollerar att det valda lösenordet är av tillräckligt god kvalitet,
- tvingar användaren till lösenordsbyte med jämna tidsintervall,
- hindrar återanvändning av tidigare lösenord.

Lösenord bör aldrig visas eller lagras i klartext eller annan oskyddad form. Fabriksinställda lösenord i programvaror bör ändras i samband med installation.

### 11.5.4 Användning av systemhjälpmedel

Systemhjälpmedel bör användas mycket restriktivt och ej vara tillgängliga för vanliga användare. Särskilt gäller detta program vilka kan sätta system och tillämpningsspärrar ur spel. All användning av systemhjälpmedel bör loggas.

### 11.5.5 Tidsfördröjd nedkoppling

Automatisk utloggning och nedkoppling av terminaler efter en viss tid av inaktivitet kan vara lämplig för att hindra obehörig åtkomst. Tillämpningen av detta bör följas upp.

### 11.5.6 Begränsning av uppkopplingstid

Restriktioner i uppkopplingstid kan användas för att öka säkerheten. Det kan ske genom att det exempelvis bara är möjligt att vara uppkopplad till IT-systemen under normal kontorstid. En förutsättning är naturligtvis att verksamheten tillåter att man endast har tillgång till resurserna under normaltid.

## 11.6 Styrning av åtkomst till information och tillämpningar

**Mål: Att förhindra obehörig åtkomst av information i tillämpningar.**

Säkerhetsåtgärder bör utnyttjas för att begränsa åtkomst till och inom tillämpningssystem.

Logisk åtkomst till program och data bör begränsas till behöriga användare. Tillämpningssystem bör:

- (a) styra användares åtkomst till data och tillämpningssystem enligt definierad åtkomstpolicy;
- (b) ge skydd mot obehörig åtkomst via systemhjälpmedel och operativsystemprogram och mot skadliga program som har funktioner för att åsidosätta eller gå förbi systemets eller tillämpningssystemets styrning;
- (c) inte äventyra säkerheten i andra system med vilka informationsresurser delas.

### 11.6.1 Begränsning av åtkomst till information

Tillämpningssystem bör utformas så att differentierad åtkomst till systemdata och systemfunktioner kan tillämpas. Enskilda användare bör tilldelas åtkomsträtt i enlighet med gällande policy och regler för åtkomst samt de specifika krav tillämpningssystemet ställer.

### 11.6.2 Isolering av känsliga system

Speciellt känsliga eller kritiska system kan kräva helt eller delvis dedikerade tekniska plattformar. Systemet bör ha en utsedd ägare och vara väl dokumenterat. Dedikering kan ske genom användning av logiska och/eller fysiska metoder.

## 11.7 Mobil datoranvändning och distansarbete

**Mål: Att säkerställa informationssäkerheten vid användning av mobilutrustning och utrustning för distansarbete.**

Det skydd som krävs bör stå i proportion till de risker dessa särskilda arbetsmetoder orsakar. Vid mobil bearbetning bör risker med att arbeta i en oskyddad miljö beaktas och lämpligt skydd användas. Vid distansarbete bör organisationen använda skydd för arbetsplatsen och säkerställa att lämpliga anordningar är installerade för detta arbetssätt.

### 11.7.1 Mobil datoranvändning och kommunikation

Användning av bärbar IT-utrustning (bärbar pc, handdator, mobiltelefon, etc.) innebär särskilda risker, i synnerhet om de används på oskyddade platser som konferenslokal, flygplats och hotellrum. Speciella skyddsåtgärder kan bli nödvändiga mot stöld obehörig insyn eller avlyssning. Vidare kan det krävas speciella maskin- och programvaror för till exempel säkerhetskopiering, kryptering och viruskydd.

Det viktigaste säkerhetsskyddet vid mobil datoranvändning är dock användaren själv. Ett högt säkerhetsmedvetande parat med goda kunskaper i olika säkerhetsprocedurer är en grundförutsättning för effektivt säkerhetsskydd. Detta gäller naturligtvis för all IT-användning, men är speciellt viktigt vid mobilt bruk. En klart uttalad policy för mobil databehandling samt klara och heltäckande säkerhetsprocedurer och en relevant utbildning är därför tre hörnstenar för en säker mobil datoranvändning.

### 11.7.2 Distansarbete

Vid regelbundet och omfattande distansarbete, dvs. arbete från en fast plats utanför organisationen exempelvis i hemmet, är det viktigt att legala-, försäkrings- och arbetsmiljöaspekter har utretts och beaktats ordentligt.

Säkerhetsaspekter som bör beaktas särskilt är bland annat

- fysiskt skydd och förvaring (stöld, brand etc.),
- kommunikationsskydd,
- skydd mot obehörig insyn (familjemedlemmar, vänner, grannar, med flera),
- skydd mot obehörig användning,
- säkerhetskopiering och kontinuitetsplanering,
- revision och övervakning av säkerhet,
- stöd och underhåll av IT-utrustning.

Ett speciellt problem är personaldatorer som vanemässigt eller endast tillfälligtvis används för arbetsändamål. Dessa datorer är vanligen bristfälligt skyddade men ofta uppkopplade mot publika nät. Organisationen måste ha en klar policy och klara regler för om, hur och när personaldatorer kan användas i arbetet.

## Exempel



### 1 – Slarv med lösenord

Kvällstidningarna var en dag fyllda av ”sensationella avslöjanden” om de ”omänskliga” djurförsök Medytekk utfört under de senaste åren. Kvällspressen uppehöll sig speciellt vid sådana försök som fick göras om på grund av slarv. Djurförsöken var noggrant beskrivna med antalet försök och djur av olika slag per försök noggrant angivna. Det var uppenbart att journalisterna på något sätt hade fått tillgång till all forskningsdata för de senaste åren.

Den efterföljande undersökningen visade att Ida, laboratorieassistent Kalle Larssons sambo, har lämnat Kalles användaridentitet och lösenord till Bengt ”CyberBee” Olsson, en av de ”datorvana” ungdomarna i föreningen ”Stopp av djurförsök nu”. CyberBee hade tidigare frågat henne om hon kunde komma åt information om Medytekk djurförsök. Bengt ”CyberBee” Olsson har sedan loggat in som Kalle, kopierat olika filer samt sammanställt det underlag som kvällspressen använde sig av.

Ida råkade se Kalles invändaridentitet och lösenord i Kalles almanacka av en tillfällighet. Kalles hade skrivit upp dessa uppgifter på en gul ”kom-i-håg”-lapp som han sedan klistrade på insidan av almanacksbindningen.

#### Vad borde Medytekk ha tänkt på?



### 2 – Internt virusangrepp

Medytekks IT-chef Lennart Jakobsson och hans medarbetare var förtvivlade när man drabbades av ett tredje virusangrepp på två veckor. Viruset spred sig snabbt även denna gång och både forskningen och administrationen befann sig i något som bäst liknar kaos. Man var tvungen att ta ner systemet under två dagar för ”städning” varje gång vilket stört arbetsrutinerna kraftigt. IT-enheten fick arbeta nästan dygnet runt under dessa dagar eftersom användarna inte fått tillräckligt mycket utbildning för att kunna städa själva. Till råga på allt var stämningen något otrevlig och många har ifrågasatt IT-enhetens kompetens. Lennart visste att Göran Rubens övervägde att anlita externa experter.

Efter det andra virusangreppet har Jakobsson låtit installera ett ytterligare viruskydd. Det verkar inte ha hjälp och speciellt förbryllande var att ingen annan tycks ha drabbats. Dessutom verkade de aktuella virusen vara okända för båda leverantörerna av antivirusprogram.

Mitt under det brinnande arbetet ringer VD:s sekreterare Berit Qvick och vill träffa Lennart omgående. Hon berättar att man har sett en av medarbetarna på ekonomienheten, Barbro Sällström, använda en diskett på ett misstänkt sätt under morgonen. Barbro Sällström tittade runt om kring som för att kolla att ingen ser henne innan hon satte disketten i diskettläsaren. Efteråt la hon disketten i sin handväska som om hon ville gömma den. Under den efterföljande intern- och polisutredningen erkände Barbro Sällström att det var hon som initierade virusangreppen på uppmaning av sin pojkvän.

Barbro Sällström var kär i en utländsk forskare, James G. Watson, som arbetade för Medytekk för ett år sedan. Hon och Watson fattade tidigt tycke för varandra och var sambor medan Watson var i Sverige. Watson var en mycket begåvad kemist men missköte sitt jobb på grund av sitt stora intresse för datorer och internet. Efter flera månaders strul i det projekt han var engagerad i fick han lämna Medytekk och lämnade Sverige. Han var mycket bitter och tanken på hämnd gnagde i hans bakhuvud hela tiden. Idén att hämnas genom interna virusattacker fick han från en av sina hackerkontakter som också försåg honom med några nya, okända virus.

#### Vad borde Medytekk ha tänkt på?



### 3 – Hackerintrång

Sven Holgersson ersatte under en period Lennart Jakobsson. Holgersson kom till arbetet sent en fredagskväll för att göra en del systemuppdateringar. Han började med att se om någon var inloggad som skulle behöva varnas om det kommande systemavbrottet. Holgersson trodde för all del inte att någon skulle vara det men märkte

## Styrning av åtkomst

till sin förvåning att Stefan Eriksson var inloggad på distans. Han stirrade misstroget på sin skärm; Stefan Eriksson var ju på Bahamas på semester!

Efter samråd på telefon med Lennart Jakobsson kontaktade Holgersson IT-brottsenheten på Rikskriminalen. Man lyckades snabbt identifiera förbindelsens andra ändpunkt och kunde gripa en ung hacker på bar gärning. Den unge mannen höll på att experimentera med olika hackerverktyg och lyckades av en tillfällighet ta sig in på Medytekk system. Han var mycket förvånad över hur lätt det var att knäcka de flesta lösenorden med hjälp av en ordboksattack. Någon egentlig skada för Medytekk uppstod inte. Samtliga lösenord fick dock ändras för säkerhets skull. Vid den efterföljande rättegången hävdade den unge hackern att han borde få ersättning från Medytekk i stället för böter och det villkorliga straffet. Genom hackerattacken har Medytekk blivit medveten om en stor svaghet i säkerhetssystemet.

### Vad borde Medytekk ha tänkt på?



#### 4 – ”Fejkade” löner

Göran Rubens var förbryllad. Flera av projektledarna har klagat över felaktiga lönekostnader i samband med de månatliga uppföljningsmötena. Det var inte fråga om några stora summor, men i alla fall. Han misstänkte först att en eller annan månadslön har blivit felkonterad och bad för några veckor sedan Helene Petterson, en av trotjänarna på ekonomienheten, att kontrollera löneredovisningen. Hon har dock inte hittat något av intresse.

Rubens bestämde sig för att själv gå igenom samtliga lönelistor för året. Till sin förvåning noterade han att flera utländska forskare

– vilka har anlitats tidigare men, så långt han visste, inte under året – har fått lön för en eller två månader under året. Han bestämde sig att kontrollera saken med B-G Sjöström och respektive projektledare. Den fortsatta undersökningen visade att ingen av dessa forskare anlitats av Medytekk under året. En utskrift av deras personaldata avslöjade dessutom att de hade ett och samma bankkonto – ett konto som tillhörde Helene Petterson!

Helene Petterson erkände gråtande och berättade om en svårt alkoholiserad make, trasigt hemliv med förestående skilsmässa samt dålig ekonomi. Hon kom på sättet att ”skaffa extra pengar” när hon märkte att hon kunde ändra personaluppgifter på eget bevåg samt kände till användar-id och lösenord som tillhörde arbetskamrater med behörighet att skapa lönetransaktioner. När hon blev ombedd av Göran Rubens att granska löneredovisningen förstod hon att hon skulle bli avslöjad men kunde inte komma på något sätt att sopa igen spåren efter sig.

### Vad borde Medytekk ha tänkt på?

---

## Vad kan vi lära oss av dessa exempel?

### Exempel 1 – ”Social engineering”

Medytekk borde ha tänkt på att

- informera och utbilda alla datoranvändare om hur lösenord ska hanteras, bland annat förvaring, samt den enskildes ansvar för att det hanteras säkert,
- periodiskt följa upp hur lösenord hanteras,
- klassificera forskningsinformation mera finkornigt och begränsa åtkomsträttigheter på ett bra sätt,
- tillåta extern åtkomst endast för anställda som behöver det för sitt arbete, exempelvis med hjälp av stark autentisering av användare och/eller utrustning.

Medytekk borde också ha övervägt att

- informera personalen om olika hot i företagets omgivning och klargöra för de anställda hur de förväntas agera (se även kapitel 6 – Personal och säkerhet).

### Exempel 2 – Internt virusangrepp

Medytekk borde ha tänkt på att

- införa ett system för uppföljning och övervakning av driften som registrerar och varnar för avvikelser från normalt användarbeteende, exempelvis när en normalanvändare initierar exekvering av ett främmande program,
- införa en genomtänkt rutin för incidenthantering, genom att bland annat utbilda användarna i konsten att ”städa” efter ett virusangrepp.

### Exempel 3 – Hackerintrång

Medytekk borde ha tänkt på att

- införa ett system för uppföljning och övervakning av driften som registrerar och varnar för avvikelser från normalt användarbeteende, exempelvis när en användare börjar använda datasystemet på för honom/henne ovanliga tidpunkter,
- använda lösenord av bra kvalitet, genom att kräva att alla lösenord är minst sex tecken långa och innehåller minst två siffror eller specialtecken.

### Exempel 4 – Fejkade löner

Medytekk borde ha tänkt på att

- informera och utbilda alla datoranvändare om en lämplig hantering av lösenord – de måste hållas hemliga och det är den enskildes ansvar att de förvaras säkert,
- agera snabbt när det blev känt att personalen på ekonomienheten har ”lånat ut” sina personliga lösenord till varandra.

Medytekk borde också ha övervägt att

- föra en mera aktiv personalpolitik, bland annat för att stödja sina anställda vid eventuella personliga problem (se även SS-ISO/IEC 17799, Kapitel 6 Personal och säkerhet).

## Styrning av åtkomst

### Checklista – Styrning av åtkomst

Fråga	Ja	Delvis	Nej
Finns det riktlinjer för tilldelning respektive framtagna av åtkomsträttigheter till information?			
Har man fastställt övergripande principer för informationsanvändning?			
Finns det ett regelverk som styr den operativa åtkomsten till it-resurserna?			
Täcker regelverket rättsregler och avtalsmässiga skyldigheter?			
Finns det ett system för användarregistrering?			
Omfattar systemet hela livscykeln från nyregistrering till slutlig avregistrering?			
Behöver användning av särskilda rättigheter auktoriseras och kan den spåras?			
Sker tilldelning av lösenord genom en formell och sekretesskyddad rutin?			
Finns det klara regler för temporära och tillfälliga lösenord?			
Granskas tilldelade åtkomsträttigheter periodiskt?			
Finns det regler för utformning, användning och förvaring av lösenord?			
Känner användarna till dessa regler och har de accepterat dem?			
Finns det tekniska skydd och operativa procedurer för obemannad utrustning?			
Finns det riktlinjer för utnyttjande av nätverkstjänster?			
Finns det regler och teknisk utrustning för autentisering av externanslutningar inklusive extern anslutning av datorer?			
Är externa diagnosportar fysiskt skyddade när de inte används?			
Är kommunikationen säkrad i logiskt sektionerade nätverk?			
Finns det avtal/överenskommelse med leverantörer av nätverkstjänster för samarbete avseende säkerhet?			
Är metoden för identifiering och autentisering av användare tillfredställande med hänsyn till genomförd riskanalys?			
Finns det regler för användning av överfalls- och nödfallslarm?			
Finns det tillämpningar med begränsad uppkopplingstid?			
Hindrar begränsningen effektivt arbete enligt systemanvändarna?			
Är differentierad åtkomst till data och funktioner möjlig i de tillämpningssystem detta är önskvärt?			
Finns det revisionsloggar (avvikelseloggar) för användaraktiviteter?			
Finns det lämpliga system för driftsuppföljning och -övervakning?			
Sker loggning och loggranskning på ett säkert sätt?			
Finns det IT-verktyg för manipulering och sammanställning av loggar från olika utrustningar?			
Finns det en överenskommen standardtid för datorlockor i nätverket?			
Har det skett en särskild riskanalys för mobil datoranvändning?			
Har alla, enligt riskanalysen relevanta, skyddsåtgärder vidtagits?			
Har användarna av mobil utrustning fått en genomgripande utbildning i nödvändiga säkerhetsprocedurer?			
Finns det en policy och klara regler för distansarbete?			
Sker det en lämplighetsbedömning och en riskanalys i varje enskilt fall?			
Är användning av utrustning för distansarbete för privata ändamål reglerad?			
Regleras användning av personaldatorer i hemmiljö för arbetsändamål?			