Jämtlands Gymnasieförbund

Revisorerna

2013-11-26

Direktionen

Revisionsrapport: Granskning av IT-säkerhetspolicy

Revisionen har genom KPMG genomfört en granskning av IT-säkerhetspolicy.

Revisionen önskar att direktionen lämnar synpunkter på de slutsatser som finns redovisade i sammanfattningen senast den 28 februari 2014. Av svaret bör det framgå vilka eventuella åtgärder som ska vidtas och när de beräknas vara genomförda.

För revisorerna i Jämtlands Gymnasieförbund

Staffan Ekström
Ordförande

Jämtlands gymnasieförbund

Granskning av IT-säkerhetspolicy
Revisionsrapport

Offentlig sektor
KPMG AB
26 november 2013
Antal sidor: 10

Granskning IT-säkerhet.docx

Innehåll

1.	Sammanfattning	1
2.	Bakgrund	2
3.	Syfte	2
4.	Avgränsning	2
5.	Revisionskriterier	2
6.	Ansvarig nämnd/styrelse	2
7.	Metod	3
8.	Projektorganisation	3
9.	Jämtlands Gymnasieförbunds IT-säkerhetspolicy	3
10.	Tillgängligheten till IT-systemen	4
11.	Utbildning i IT-säkerhet	5
12.	Ansvarsfördelning	6
13.	Rutiner för säkerhetsincidenter	6
14.	Övrig säkerhet	7
14.1	Lösenordshantering	7
14.2	Fysisk säkerhet	7
14.3	IT-säkerhetshöjande åtgärder och resursbehov	8

1. Sammanfattning

Vi har av revisorerna för Jämtlands Gymnasieförbund fått i uppdrag att följa upp om IT-säkerhetspolicyn efterlevs.

Revisorerna har bedömt att det finns en risk för att policyn inte efterlevs, och att riskerna för störningar i verksamheten uppstår.

Syftet med granskningen har varit att bedöma efterlevnaden av IT-säkerhetspolicyn[1].

Vi har därför granskat *om förbundet har rutiner* för att klara ett urval av de mål som anges i policyn och om förbundet:

- följer upp tillgängligheten till IT-systemen
- säkerställer att alla anställa som berörs av IT får utbildning i IT-säkerhet samt att riktlinjer för användning av IT-resurserna är kända av såväl elever som personal.
- säkerställer att ansvarsfördelningen avseende samtliga IT-system är aktuell, kartlagd och dokumenterad.
- har rutiner för att säkerställa att samliga säkerhetsincidenter rapporteras och utreds av IT-samordnare eller liknande.

Generellt kan sägas att det gjorts ett gediget arbete med att ta fram rutiner, riktlinjer och policies. Dokumenten börjar dock bli gamla och behöver uppdateras. Vi rekommenderar att IT-säkerhetspolicyn uppdateras och kompletteras med en policy för informationssäkerhet.

Vi rekommenderar också att hela IT-avdelningens organisation ses över då det är helt uppenbart att mycket av det som IT-säkerhetspolicyn stadgar, inte görs.

Vid granskningstillfället saknades en komplett och aktuell systemförteckning inkluderande ansvarsfördelning, dokumenterad riskbedömning och åtgärder samt loggar som kan identifiera t.ex. intrångsförsök. Systemförteckningen håller på att uppdateras och vi rekommenderar att system för loggning införskaffas. Loggning är en förutsättning för att kunna upptäcka säkerhetsincidenter.

Förbundet har relativt gammal IT-infrastruktur som troligen kräver mer arbete av IT-tekniker än om infrastrukturen varit nyare. I genomsnitt har varje IT-tekniker över 500 användare att supporta, vilket i alla jämförelser är en hög kvot.

Tillgängligheten kan inte garanteras. Det sker ingen kontinuerlig övervakning av hur systemen mår. Backup görs bara varannan till var tredje vecka. Vår rekommendation är att detta åtgärdas snarast möjligt och att backup körs en gång per dygn.

[1] Fastställd av direktionen 2007-05-21, § 34

Rutiner för varje viktig server måste tillskapas för att få igång ett alternativ vid ett eventuellt totalhaveri.

Utbildning i IT-säkerhet behöver förbättras. Det sker ingen kontroll över att användare har förstått och tillämpar uppställda krav i enlighet med IT-säkerhetspolicyn.

2. Bakgrund

Vi har av revisorerna för Jämtlands Gymnasieförbund fått i uppdrag att följa upp om IT-säkerhetspolicyn efterlevs.

Revisorerna har bedömt att det finns en risk för att policyn inte efterlevs, och att riskerna för störningar i verksamheten uppstår.

3. Syfte

Syftet med granskningen har varit att bedöma efterlevnaden av IT-säkerhetspolicyn[2].

Vi har därför granskat *om förbundet har rutiner* för att klara ett urval av de mål som anges i policyn och om förbundet:

- följer upp tillgängligheten till IT-systemen
- säkerställer att alla anställa som berörs av IT får utbildning i IT-säkerhet samt att riktlinjer för användning av IT-resurserna är kända av såväl elever som personal.
- säkerställer att ansvarsfördelningen avseende samtliga IT-system är aktuell, kartlagd och dokumenterad.
- har rutiner för att säkerställa att samliga säkerhetsincidenter rapporteras och utreds av IT-samordnare eller liknande.

4. Avgränsning

Vår granskning är översiktlig och avser som framgår under syftet förbundets rutiner avseende ett urval av målen.

5. Revisionskriterier

Vi har bedömt om rutinerna/verksamheten uppfyller IT-säkerhetspolicy.

6. Ansvarig nämnd/styrelse

Granskningen avser förbundsdirektionen, som är ansvarig för förbundets verksamhet.

Rapporten har saklighetsgranskats av Linda Lignell, Mattias Ramstedt och Christer Jakobsson.

[2] Fastställd av direktionen 2007-05-21, § 34

7. Metod

Granskningen har genomförts genom:

- Dokumentstudie av relevanta dokument
- Intervjuer med berörda tjänstemän

8. Projektorganisation

Granskningen har genomförts av Göran Andersson, seniorkonsult.

9. Jämtlands Gymnasieförbunds IT-säkerhetspolicy

Utdrag från förbundets IT-säkerhetspolicy

”IT-säkerhetspolicyn gäller system och information som behandlas med hjälp av informationsteknik. Såväl organisatoriska åtgärder som fysiska och logiska skyddsåtgärder inbegrips, såsom en fastställd IT-säkerhetspolicy, ansvarsfördelning, utbildning, riskanalys, behörighetsregler, säkrad driftsmiljö, åtkomstskydd i datorer, säkerhetskopiering, etc.”

”Det övergripande målet med IT-säkerhetsarbete är att minimera riskerna för störningar i skolornas och enheternas verksamheter, på grund av fel i eller felaktig användning av ett eller flera IT-system. Vårt IT-säkerhetsarbete innebär att:

- tillgängligheten till IT-systemen ska säkerställas
- data- och telekommunikation ska vara säker
- IT-systemen ska skyddas mot obehörig åtkomst
- driftsstörningar och intrång ska kunna följas upp med hjälp av dokumenterad historik (loggar)
- användare får endast tillgång till den information som behövs för att kunna utföra sina arbetsuppgifter
- det som anställd inte är tillåtet att besöka sidor på Internet som enligt svensk lag är förbjudna eller kan anses som oförenliga med förbundets policys och planer
- leva upp till gällande lagar och externa krav på förbundetst informationssystem
- alla anställda inom förbundet som i sina arbetsuppgifter berörs av IT ska få utbildning i IT-säkerhet
- användandet av förbundetts IT-system granskas systematiskt

- arbetet med IT-säkerhet ska bedrivas systematiskt och omfatta all verksamhet
- IT-säkerhetsfrågorna ska beaktas redan vid upprättandet av kravspecifikation och anskaffning av informationssystem
- ansvarsfördelningen för samtliga IT-system inom förbundets verksameht ska vara aktuell, klarlagd och dokumenterad
- alla säkerhetsincidenter, konstaterade eller misstänkta ska rapporteras till och utredas av IT-samordnare eller motsvarande som förbundet utser
- förbundet ska ha IT-personal med rätt kompetens som fortlöpande utbildas i takt med att datorsystemen utökas och förändras”

Kommentar

Vi bedömer att IT-policyn är på en rimlig nivå. Dock, vilket framgår av följande kapitel, är efterlevnaden låg. Policyn fastställdes 2007 och utvecklingen inom IT går snabbt. Vi rekommenderar att policyn uppdateras för att säkerställa att den täcker in den utveckling som varit sedan den upprättades och beslutades.

I samband med detta kan med fördel även en informationssäkerhetspolicy utvecklas och beslutas om. Den relaterar till IT-säkerhetspolicy men täcker in så mycket mer. Mer om detta finns att läsa på www.informationssakerhet.se , en sida som Myndigheten för Säkerhet och Beredskap (MSB) ligger bakom.

10. Tillgängligheten till IT-systemen

För att överhuvudtaget få tillgång till IT-systemen krävs att användaren, oavsett elev eller personal, skriver under en försäkran om att användaren tagit del av och förstått förbundets IT-säkerhetspolicy. Det finns väl beskrivet i dokument hur distributionen och påskrift av IT-riktlinjerna för användare ska ske.

Användare får tillgång till systemen hemifrån via särskild inloggning. Vid lokal inloggning utanför skolan har användaren endast tillgång till sin egen dator.

Förbundet följer inte systematiskt upp tillgängligheten till de olika IT-systemen. Om en användare av någon anledning inte har tillgång till något system får denne signalera till IT-avdelningen som då utreder anledningen till detta.

Tillgången till information över internet är ej begränsad. Det är fullt möjligt att besöka vilken hemsida användaren vill.

Backup av viktiga servrar görs med 2 - 3 veckors mellanrum. Det innebär att om någon användare blir av med data riskerar användaren 2 - 3 veckors arbete. Det finns dock en funktion inbyggd i Novellnätet som gör att upp till 90 procent av datat kan återskapas.

Vid ett totalhaveri av en server finns det i princip inga säkerhetsfunktioner. För ett par av servrarna finns dedicerade reservservrar men det har inte gjorts något skarpt test på återställning. En bedömning är att det kan ta upp till tre veckor innan en ny server kan vara igång.

Kommentar

Av IT-säkerhetspolicyn framgår ”användandet av förbundets IT-system granskas systematiskt”. Det finns system som kontinuerligt övervakar de system som används och signalerar om det är risk för överbelastning eller liknande. Jämtlands Gymnasieförbund har inte ett sådant system.

Förbundet bör överväga att begränsa tillgången till viss typ av information via internet.

Anledningen till att backup inte görs t.ex. varje natt beror på att med den utrustning som förbundet förfogar över skulle det alldeles för lång tid att köra backup. Det skulle helt enkelt inte hinnas med. Vi rekommenderar att undersöka möjligheterna och kostnaderna för att förbättra rutinerna. Tills detta är gjort rekommenderar vi att användarna informeras om detta förhållande så att de ges tillfälle att göra egna backuper på viktiga dokument om de så önskar. Troligen behövs någon form av bandrobotar i kombination med inkrementell backup. Att köra backup var tredje vecka är inte acceptabelt.

Vad gäller säkring av servrar vid totalhaveri måste det finnas rutiner för varje server. I samband med vår granskning har nu ett sådant arbete påbörjats, vilket är nödvändigt och glädjande.

11. Utbildning i IT-säkerhet

Det finns mycket bra information framtagen i form av riktlinjer för användning av förbundets IT-resurser. Dessa riktlinjer har alla användare tillgång till. Någon direkt utbildning hålls däremot inte. Det sker heller inga aktiviteter som gör att förbundet kan veta huruvida riktlinjerna är kända av vare sig elever eller personal.

Kommentar

Bristen kan enkelt åtgärdas genom att t.ex. årligen låta användarna svara på en webb-enkät eller liknande, där ett antal frågor rörande IT-säkerheten ställs. De som inte svarar, eller de som inte har tillräckligt många rätt på frågorna kan stängas av och inte längre få tillgång till IT-resurserna.

Av IT-säkerhetspolicyn framgår att ”alla anställda inom förbundet som i sina arbetsuppgifter berörs av IT ska få utbildning i IT-säkerhet”.

12. Ansvarsfördelning

En förteckning över vilka system som finns är framtagen och innehåller;

1) Namn på systemet
2) Typ av system
3) Vem som är systemägare
4) Vem som är systemförvaltare
5) Vem som är systemadministratör
6) Ven som driftar systemet

Dessutom framgår av dokumentet vad som förväntas av respektive systemägare, systemförvaltare, systemadministratör och den som driftar systemet.

Dokumentet är dock inte helt aktuellt och det saknas uppgifter i flera av ”rutorna”.

Kommentar

Dokumentet behöver uppdateras och kompletteras. Gärna med så detaljerad information som möjligt, t.ex. istället för att ange Jämtlands Gymnasieförbund som systemägare bör en person anges. Vi kan konstatera att i samband med vår granskning uppdateras nu systemförteckningen. Initiativet i sig är gott och hade varit berömvärt om uppdateringen varit ett resultat av en planlagd och återkommande revidering av alla styrdokument. Det framgår tydligt i IT-säkerhetspolicyn att ”ansvarsfördelningen för samtliga IT-system inom förbundets verksamhet ska vara aktuell, klarlagd och dokumenterad”.

13. Rutiner för säkerhetsincidenter

Det finns inga rutiner för att säkerställa att samtliga säkerhetsincidenter rapporteras och utreds av IT-samordnare eller liknande. Det finns inga loggar över t.ex. intrångsförsök eller liknande.

Kommentar

Det bör finnas någon form av system som signalerar om det görs intrångsförsök. Skolan hanterar delvis känsliga uppgifter om elever, däribland betyg. Det framgår också av IT-säkerhetspolicyn att ”driftsstörning och intrång ska kunna följas upp med hjälp av dokumenterad historik (loggar)”.

14. Övrig säkerhet

14.1 Lösenordshantering

Gymnasieförbundet använder ett FirstClass-system tillsammans med alla övriga skolor i länet som kallas Zonline. Det ägs och driftas av Regionförbundet i Jämtlands Län, tidigare Kommunförbundet.

Från deras användardatabas (som heter Zorro) finns en MIIS-koppling som provisionerar ut användarkonton till kommunernas AD/eD. Därmed är det samma användarnamn och lösenord som används i FirstClass som också används för inloggning i Novell. Därmed är det också reglerna för lösenord i FirstClass som styr hur ofta det uppdateras.

Jämtlands Gymnasieförbund har regler som säger att lösenord ska bytas var 60:e dag. Detta fungerade vid granskningstillfället inte. I praktiken behövde användaren inte ändra lösenord.

Vad gäller konstruktionen av lösenord krävs sex tecken varav en ska vara en siffra.

Kommentar

Efter vårt besök har IT-samordnaren påpekat bristerna till Regionförbundet och har fått svar från dem att alla gruppers policy har blivit ställd till Standard efter senaste server-uppgraderingen. Men det ska korrigeras så att JGY:s policyregel återställs, vilken är 60 dagar.

Konstruktionen med sex tecken varav en siffra anses idag vara alldeles för enkel. Det finns hundratals olika program på internet idag som en ”hackare” kan använda för att knäcka ett sådant lösenord på några få sekunder.

Systemet tillåter hårdare krav på lösenordskonstruktion och vi rekommenderar att kravnivån höjs. Det går t.ex. att ställa krav på;

- Minsta antalet tecken i lösenordet
- Blandat bokstäver och siffror samt specialtecken
- Uppmaning att byta lösenord med valda intervaller
- Blockning av tidigare använda lösenord

14.2 Fysisk säkerhet

Alla servrar som driftas av förbundet står i ett särskilt rum med luftkonditionering. Utrustning för backup står i ett annat rum. Serverrummet har väggar av betong och en dörr av trä. Backup-rummet har väggar av betong och dörr av stål.

Vid ett eventuellt strömavbrott finns en UPS[3] som försörjer servrarna med elektricitet under 2 -3 timmar.

Datorer som står i datasalar är fysiskt fastlåsta.

Kommentar

Den fysiska säkerheten är god förutom att dörren till serverrummet bör bytas till en dörr som står emot brand. 2 - 3 timmar UPS är tillräckligt för att vid längre strömavbrott göra en kontrollerad avstängning av systemen.

14.3 IT-säkerhetshöjande åtgärder och resursbehov

För att arbeta med IT-säkerhetshöjande åtgärder krävs en riskbedömning. Denna skall dokumenteras och ligga som underlag till åtgärder. Någon strukturerad riskbedömning görs inte, vilket inte innebär att tekniker och IT-samordnare inte vet vilka system som är mest kritiska.

Det finns heller ingen medveten satsning på IT-säkerhetshöjande åtgärder.

Förbundet har i nuläget 5,5 IT-tekniker och ca 3 150 användare. Teknikerna känner att de kan få den utbildning som de behöver, men att det inte finns tid att vidareutbilda sig.

Förbundet håller just nu på med att bygga om lokaler och delvis dra nytt nät. I samband med detta kommer nätdragningen att dokumenteras, något som inte skett i större omfattning tidigare.

Förbundets IT-samordnare är numera även ansvarig för marknadsföring av gymnasieförbundet.

Kommentar

5,5 IT-tekniker på 3 150 användare innebär över 570 användare per tekniker. Vi anser att det är mycket. Det är omöjligt att på ett objektivt sätt säga hur många användare varje tekniker bör kunna hinna med. Det beror väldigt mycket på hur systemen är uppsatta, hur många automatiserade processer som finns, vad som kan göras i systemen, användarnas datormognad och mycket mer. På olika diskussionsforum för IT-tekniker på internet talas det om antal användare som ligger långt under 570 per användare.

Vi rekommenderar att en genomlysning av IT-teknikernas arbetssituation görs.

KPMG, dag som ovan

Göran Andersson
Seniorkonsult

[3] Uninterruptible power supply