



Skapat av: Tomas Eiksson Ägare: Decado AB

Datum: 2009-05-28 Sidan 1 av 5

Hur bygger man upp en upplysningsplan?

-Ett dokument från
Secure-IT.se

Vi innehar F-skattebevis

Momsregistrerings nr SE556650187901

Namn
Decado AB

Adress
Box 6111, 800 06 Gävle

Telefon
026-10 02 30

Fax
026-10 19 52

Org.nr
556650-1879

Säte
Gävleborg



Skapat av: Tomas Eiksson Ägare: Decado AB

Datum: 2009-05-28 Sidan 2 av 5

Upplysningsplan #1

Upplysningsplan

Att vara IT-ansvarig eller IT-säkerhetsansvarig på ett företag kan många gånger kännas som att jobba i ständig motvind. Vi som besitter dessa roller har nog så klart för oss de risker vår verksamhet står inför och vilka rent ekonomiska kostnader det kan bli om en incident råkar inträffa. Vi är också väl medvetna om hur vårt företags renommé kan skadas om det blir allmänt känt att vi inom organisationen brister i vårt sätt att jobba med säkerhet.

På Decado AB har vi sett otaliga fall av incidenter som har inträffat på grund av dålig eller total avsaknad av upplysning gällande IT- och informationssäkerhet. Att göra en plan för hur man upplyser och informerar personalen om kända hot och risker behöver inte vara så svårt. Vi skall nu titta närmare på hur en upplysningsstrategi kan se ut.

Först av allt vill vi dock poängtera att upplysning och utbildning i det här fallet inte är samma sak. Utbildning skall ske på ett djupare plan medan upplysning skall ske under mer allmänna former.

Här ger vi nu lite förslag på hur du på ett bättre sätt kan nå ut i din organisation med information gällande IT- och informationssäkerhet.

1. Skaffa dig bundsförvanter

Det bästa sättet för dig som IT-ansvarig att nå ut med säkerhetsrelaterade budskap är att få chefer samt mellanchefer med på noterna. Om företagets ledning får inblick i och förstår varför man bör lägga mer krut på att upplysa personalen om IT-säkerhetsrelaterade frågor kommer ditt arbete att bli mycket lättare.

Hur får man då chefen att lyssna?

Oavsett om du talar med ägare, VD, economichef, mellanchefer eller någon annan individ inom organisationen som har ett ansvar så förstår man dessa två ord:

Pengar och badwill

Att råka ut för incidenter kan kosta enorma belopp räknat i kronor och ören. Men det kostar kanske ännu mer i skadat renommé? Se till att du som säkerhetsansvarig får tillgång till kvalitetstid där du på ett väl förberett sätt får möjlighet att beskriva för VD och all övrig personal i ledande befattning varför företaget bör lägga energi på en väl genomarbetad strategi för IT- och informationssäkerhet. I denna strategi ingår även en plan för upplysning av personalen.

Om ledningsgruppen består av personer med sunt förnuft kommer de att köpa ditt resonemang och ställa sig bakom ditt arbete. Därefter kommer det att gå mycket enklare att fortsätta arbetet i den övriga organisationen. Det är inte du som IT-ansvarig som "tycker en massa" utan det är företagets ledning som har beslutat att organisationen skall jobba enligt en fastslagen plan vad gäller IT- och informationssäkerhet.

2. Låt VD vara först ut på banan

Nu när ledningsgruppen är med på noterna kan det vara lämpligt att VD för företaget går ut med ett inledande e-brev där man informerar samtliga i personal om de beslut som är tagna. Detta kommer att underlätta för dig som IT-ansvarig inom företaget. VD bör i detta brev också lägga tonvikt på att det är varje medarbetares skyldighet att jobba aktivt med säkerhetsrelaterade frågor.

Vi innehar F-skattebevis Momsregistrerings nr SE556650187901

Namn	Adress	Telefon	Fax	Org.nr	Säte
Decado AB	Box 6111, 800 06 Gävle	026-10 02 30	026-10 19 52	556650-1879	Gävleborg



Skapat av: Tomas Eiksson Ägare: Decado AB

Datum: 2009-05-28 Sidan 3 av 5

3. Köp en bok åt ledningsgruppen

Köp hem till exempel Predrag Mitrovic utmärkta bok Handbok i IT-säkerhet och distribuera den till individer i ledande befattning. Om din organisation består av väldigt många chefer och mellanchefer kanske du får rikta in dig på några få utvalda som ofta kommer i kontakt med ditt dagliga arbete.

Som IT-chef eller IT-ansvarig skall du vara experten inom området men en väl skriven bok med granskad och korrekt fakta belyser än mer vikten av att jobba med säkerhetsrelaterade frågor inom organisationen. Försök att få folk intresserade och framförallt få dem att förstå vidden av att INTE jobba med de säkerhetsrelaterade frågorna.

4. Hitta rätt forum för upplysning

Hur ser ditt företag ut? Har ni många avdelningskontor spridda över landet? Är ni många eller få anställda? Hur ser den digitala infrastrukturen ut?

Vi rekommenderar två bra sätt att sprida upplysning inom en organisation:

Via Intranet och/eller företagets webbsida

Bygg upp en avdelning på det lokala Intranätet eller företagets webbsida (om en publik webbsida används bör denna del ligga bakom en inloggning (en personaldel)). Denna avdelning kan t.ex. inkludera information, upplysningar, tips, hotbilder samt åtgärder och rekommendationer som gör att alla inom organisationen gradvis höjer sin medvetenhet och kompetens gällande säkerhetsrelaterade frågor. Detta kan också vara en utmärkt plats att inkludera företagets IT-policy på.

5. Jobba även med ett e-brev

Skapa en mall för ett e-brev som behandlar upplysning och information gällande IT- och informationssäkerhetsrelaterade frågor. Detta brev kan till exempel distribueras två gånger per månad och innehållet bör hållas kort och naturligtvis uppdaterat. Hänvisa till ovanstående valt forum för bredare och fördjupad information.

6. Ge ditt forum och e-brev lite tyngd

Denna punkt kanske kommer i fel ordning men hur som haver bör du fundera på ett samlingsnamn för dina upplysningsansträngningar. Lägg lite tid och energi på att skapa en fungerande mall (designmässigt) som går igen både gällande det forum du väljer samt i ditt e-brev. Visa att du tar detta både viktiga och absolut nödvändiga arbete på största allvar.

Här finns inget utrymme för ett ursäktande upplägg som dina medarbetare kastar i den digitala soptunnan ihop med önskad reklam. Ge ditt e-brev samt ditt säkerhetsforum ett bra och relevant namn innan du presenterar dessa för första gången. Sanktionera ditt namnval med ledningen så att de är med på ditt upplägg.

7. Jobba med tips

Att ge korta och enkla tips som höjer säkerheten kring företagets information är ett bra sätt att utbilda medarbetarna. Distribuera dessa tips på din forum plats och i ditt e-brev. Dessa tips skall naturligtvis vara kopplade till hur din organisation jobbar. Det är ingen idé att skriva om Linuxsäkerhet om inte företaget använder Linux som OS. Det är inte

Vi innehar F-skattebevis Momsregistrerings nr SE556650187901

Namn	Adress	Telefon	Fax	Org.nr	Säte
Decado AB	Box 6111, 800 06 Gävle	026-10 02 30	026-10 19 52	556650-1879	Gävleborg



Skapat av: Tomas Eiksson Ägare: Decado AB

Datum: 2009-05-28 Sidan 4 av 5

heller någon idé att skriva och skriva flera A4-sidor eftersom dina medarbetare med all säkerhet har mycket att göra om dagarna och inte heller har den kompetens som du besitter inom området.

Ett utmärkt sätt att ta död på ett intresse innan det knappt har börjat är att lägga i femmans växel direkt. Ingen vill känna sig som en idiot och få har tiden att gå igenom sida upp och sida ner med material under arbetstid (om det inte ligger inom deras ansvarsområde förstås). Börja med små enkla steg och när du får gehör bland dina medarbetare kan du gradvis växla upp informationsmängd och svårighetsgrad.

Hur märker jag då att folk läser det jag skriver?

Det märker du på ett ökat engagemang gällande ditt ansvarsområde. När du har distribuerat ditt forum och ditt e-brev under en tid kommer du med all säkerhet att få ett ökat antal frågor gällande säkerhet. Du kommer också att få en större mängd feedback och information om hot och risker samt annat intressant som dina medarbetare har läst eller hört om.

Lämpligen kan du också utföra tester. Utarbeta tester med säkerhetsrelaterade frågor som du distribuerar digitalt eller på hederligt papper. Har ditt företag flera avdelningar eller satellitkontor kan du redovisa testerna som "lagtävlingar". Undertonen skall naturligtvis vara alvarlig men detta kan vara ett sätt att göra säkerhetsarbetet lite mera lustfyllt.

Lokalkontor Gävle hade 10 rätt och lokalkontor Uppsala hade 15 rätt, vill Gävle ha revansch till nästa gång tro?

Gör till exempel en intern tävling där ett frågeformulär distribueras varje månad. Summera och redovisa ställningen under året och kora en vinnare vid julfesten. Titeln "Bäst på informationssäkerhet inom Företaget AB" borde vara en merit för vem som helst.

8. Marknadsför ditt område

Hitta ett lämpligt sätt att marknadsföra området säkerhet. Ett exempel kan vara att göra en version av tio guds ord där vi istället pratar om tio bevingade ord från IT-ansvarig. T.ex. e-post, nedladdning, lösenord, sekretess osv. Knyt dessa tio ord till företagets IT-verksamhet och beskriv under varje ord hur man arbetar säkert med respektive. Förpacka sedan dessa tio budord snyggt bakom glas och ram och se till att varje avdelning får sitt exemplar.

Dock är det mycket viktigt att vi aldrig inbjuder till att skapa ett löjes skimmer över vårt arbete med säkerhetsrelaterade frågor. Dessa frågor är några av de viktigaste på dagordningen men vi pratar om en komplex verklighet som många har svårt att ta till sig. Då måste man finna lämpliga vägar att nå ut med sitt budskap.

9. Utbilda, för alltid

Arbeta fram en plan för intern utbildning inom områdena IT- och informationssäkerhet. Se till att all nyanställd personal omgående får ta del av detta utbildningsprogram. Se också till att all övrig personal får genomgå detta program, denna utbildningsplan finns det inget sista datum för då teknik likväl som hotbilder hela tiden förändras i rask takt.

10. Håll dig uppdaterad

Det ligger under ditt ansvar som IT-chef eller IT-ansvarig att vara uppdaterad inom ditt ansvarsområde. Om du inte vet hur landet ligger gällande IT- och informationssäkerhet kan du knappast kräva att övrig personal skall veta det heller. Inget teknikområde går framåt i sån takt som det informationstekniska vilket gör att du som ansvarig hela tiden måste söka nya vägar att införskaffa information och förkovra dig. Implementerar ni ny teknik inom företaget så förändras också säkerhetsläget (i många fall drastiskt).

Vi innehar F-skattebevis Momsregistrerings nr SE556650187901

Namn	Adress	Telefon	Fax	Org.nr	Säte
Decado AB	Box 6111, 800 06 Gävle	026-10 02 30	026-10 19 52	556650-1879	Gävleborg



Skapat av: Tomas Eiksson Ägare: Decado AB

Datum: 2009-05-28 Sidan 5 av 5

11. Budgetera

Se till att arbete med IT- och informationssäkerhet finns med i din budget. Det kostar pengar att jobba aktivt med säkerhet men de pengarna är ändå bara en bråkdel av mot vad det i förlängningen kostar att ignorera dessa viktiga områden.

Vi hoppas att du nu har fått lite mer grepp om hur du kan lägga upp en plan för upplysning inom ditt företag.

Vi innehar F-skattebevis

Momsregistrerings nr SE556650187901

Namn	Adress	Telefon	Fax	Org.nr	Säte
Decado AB	Box 6111, 800 06 Gävle	026-10 02 30	026-10 19 52	556650-1879	Gävleborg