ELK IMPLEMENTATIETRAJECT HEEFT ZIJN SECURITY ASPECTEN IN ZICH!

Of het nu gaat om de verbouwing van een woning of, zakelijk gezien, het implementeren van een kritische verandering in een bedrijf, zoals een nieuw softwaresysteem, je zult het eerst moeten plannen en organiseren om het tijdens de verandering te controleren, zodat alle risico's vooraf geëlimineerd worden.

Plannen en organiseren gaat vaak op 'gevoel', er gaat tijdens de verandering gegarandeerd veel mis, bijvoorbeeld door communicatie over meerdere onveilige kanalen (mail, telefoon, chat), en het afbreukrisico is groot. Er zijn veel risico's mee gemoeid. Het levert veel stress op en kost uiteindelijk veel geld. En hoe zorg je er nu voor dat het veilig is wat je gaat doen?

Of het nu gaat om het upgraden van programmatuur, de migratie van data of het installeren van technische componenten, het zijn tijdrovende processen waarin vele groepen mensen acties moeten leveren en waarbij we regelmatig worden geconfronteerd met onverwachte en onaangename verrassingen, ook op securitygebied. Liever zouden we 'in controle blijven' en de situatie volledig in de hand hebben.

Een terugblik op de werkwijze; wat werkte niet?

Veel bedrijven kozen er in de jaren 90 voor om planning en organisatie van veranderingen vast te leggen in tekstverwerking of spreadsheetpakketten, waarbij beveiliging een groot gemis is! In een tekstverwerking pakket zag je vaak een geheel van verschillende hoofdstukken. Activiteiten, betrokkenen, het communicatieprotocol en vele andere onderdelen werden in hoofdstukken ondergebracht. Dit bleek niet werkbaar, omdat het totale overzicht ontbrak en sturing op verandering daardoor niet mogelijk was.

Ook in een spreadsheetpakket liepen we tegen de grenzen van het pakket aan, omdat de hoeveelheid taken, afhankelijkheden en betrokkenen al snel te groot werd. Inzicht en overzicht ontbraken. Niet verwonderlijk, want de genoemde programma's zijn perfect als tekstverwerker of spreadsheet, maar zijn geen implementatie softwarepakketten die specifiek gericht zijn op het gecontroleerd implementeren en het elimineren van risico's.

De grootste gevaren bij het gebruik van spreadsheets en tekstverwerkers zijn:

- qua beveiliging is er weinig tot niets te regelen, wat zeker met de nieuwe GDPR wetgeving grote gevolgen kan hebben;
- geen logging, je kan niet aantonen waar het mis gaat of beter kan;
- bij hergebruik kan je niet snel starten en moet je hopen dat de template niet corrupt is;
- mensen worden niet aangestuurd en communicatie gaat over verschillende kanalen met als gevolg:
    - projecten lopen uit vanwege het missen van een stap in het stappenplan: de afbakening van taken is onduidelijk;
    - geen alarmering;
    - Toewijzing van menselijke resources door planning, elk bedrijf heeft met ad hoc zaken te maken, die zijn niet te vangen in een spreadsheet of tekstverwerker. Dit heeft zijn weerslag op de doorloop van projecten.

De oplossing, wat werkt wel!

Dit wetende is het verstandig om je te oriënteren op een geautomatiseerd stappenplan, dat je daadwerkelijk werk uit handen neemt. En dat ervoor zorgt dat je bij implementaties volledig veilig en secure in regie bent.

Werken in een afgeschermde omgeving is daarom belangrijk en naast de betere beveiliging zijn de voordelen die je dan voor jezelf creëert:

- Dat je daarna een stappenplan hebt dat altijd consistent en overzichtelijk is. Je ziet meteen wat de totale doorlooptijd is en wat de impact is voor de business, want alles kan dan automatisch doorgerekend worden. Je kan hierdoor gaan sturen en begeleiden in plaats van brandjes blussen.
- Noodzaak is wel dat de programmatuur zodanig beveiligd is, dat alleen de mensen die geautoriseerd zijn toegang hebben. Er zijn te veel voorbeelden van documenten die onbedoeld zijn gaan zwerven of waarin per ongeluk ongezien een wijziging heeft plaatsgevonden. Dit kan desastreuze gevolgen hebben in een project en risico's van datalekken liggen hier op de loer.

Denk hierbij aan https://www.noordhollandsdagblad.nl/-zaanstreek/burgemeester-zaanstad-doet-aangifte-van-lekken-documenten-cultuurcluster en dat is maar een simpel voorbeeld. De keren dat dit heden nog voorkomt, is onvoorstelbaar.

Bij elk implementatietraject is een goede communicatie het hart van de implementatie. Het is de bedoeling dat het hart gecontroleerd en veilig alle processtappen van een implementatietraject aanstuurt. Tijdens het traject is het cruciaal dat communicatie actueel inzicht en overzicht blijft geven van activiteiten, verantwoordelijkheden, afhankelijkheden, tijden, afdelingen en medewerkers.

Daar liggen de uitdagingen in het implementatieproces dat je moet stroomlijnen wil je `in controle' zijn. Als manager wil je je bezighouden met je eigenlijke werk, en meer aandacht geven aan de mens zelf. Security issues mogen je niet afleiden van de normale implementatie problematiek. Mobile toegang geeft veel voordelen, maar brengt wel security vraagstukken met zich mee.

De laatste stap, mobiele toegang

Vroeger was het alleen maar mogelijk om medewerkers een terugkoppeling te geven omtrent hun activiteiten en de voortgang te volgen door middel van de desktop of laptop.

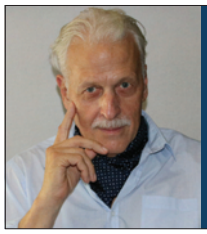
Tegenwoordig wil je ongeacht waar je bent, dus ook vanaf huis of een andere locatie, de voortgang kunnen volgen en niet direct gebonden zijn aan een desktop of laptop. Je wilt je eigen activiteiten te kunnen afmelden via elk mobiel device zonder gebruik te hoeven te maken van e-mail of sms, maar wel beveiligd!

Alleen, hoe ga je om met de beveiligingsaspecten? Want alles wat zich extern bevindt, draagt een groter risico met zich mee. Medewerkers moeten de mogelijkheid krijgen om eigen activiteiten kunnen afmelden, maar niet die van een ander. Het is dus noodzakelijk om strikt persoonsgebonden te werken. En ervoor te zorgen dat de informatie die wordt gedeeld, beperkt is en wordt afgeschermd van ongewenste ogen. Ook persoonsgebonden informatie, zoals een mobiel nummer en e-mailadressen, mogen niet gedeeld kunnen worden via het internet.

Een implementatie is een serieuze business. Er mag niets fout gaan, want er is veel geld mee gemoeid. Dreigende datalekken en security vraagstukken moeten goed geregeld worden, omdat het grote imagoschade kan veroorzaken.

Het is dus werkelijk van groot belang dat de beveiliging op alle fronten goed is geregeld, want uiteindelijk verzamelen we activiteiten die van belang zijn voor een organisatie en haar business. Dit mag simpelweg niet op straat terecht komen.

Het is belangrijk om stap voor stap te bouwen aan een succesvolle en veilige implementatie, waarbij vooraf alle risico's worden geëlimineerd.



Peter van Deutekom is Implementatiespecialist bij Mirada BV. Peter is bereikbaar via info@time-it.org.