28 SIDOR OM ENKLARE OCH SÄKRARE IT

Inuit forum

EN KUNDTIDNING FRÅN INUIT 2017

SAMI LAIHO – KRÖNIKA
Whitelisting as an option

DEREK MELBER
Säker IT-miljö

RAKESH JAYAPRAKASH
Business Intelligence i fyra steg

ANDREAS RIDDERSTEDT
Värdet av ditt IT-system

inuit

Inuit forum

Inuit forum är Inuits kundtidning som har som ambition att inspirera och ge nya insikter med kunder och andra intressanta personer som delar med sig av sina erfarenheter och belyser och ger kunskap om aktuella ämnen.

Redaktör Markus Arvidson
08-753 05 10
markus.arvidsson@inuit.se

Design Jaform

Foto Jonas Alvsten

Text Susanne Hägwall
Sami Laiho
Markus Arvidsson

Om Inuit

Inuit är en värdeadderande distributör som jobbar exklusivt med utvalda tillverkare inom IT-säkerhet och IT-administration. Vårt mål är att våra produkter och lösningar ska skapa kundnytta genom ökad produktivitet och säkra IT-plattformar. Tillsammans med våra partners hjälper vi dagligen över 3000 kunder att uppnå högre effektivitet och säkerhet.

INUIT AB
Enebybergsv. 10A
182 36 Danderyd · Sweden
08-753 05 10
inuit.se

Enklare^{X}

Känner du att saker och ting kunde göras enklare? Blir du frustrerad över komplexa processer? Då är du i gott sällskap. I en färsk undersökning* uppger 74 procent att besvärliga och komplexa processer hindrar deras förmåga att nå sina mål.

Det framgår även att 60 procent av de tillfrågade tycker att den tekniska utvecklingen hindrar dem från att nå affärsmålen. Alltså inte sina egna mål utan verksamhetens mål, som i de flesta fall har en direkt koppling till det ekonomiska resultatet.

För att driva en framgångsrik verksamhet behöver fokus läggas på att förenkla processer och arbetssätt och inte minst dra nytta av teknikens möjligheter. Teknik kan idag hjälpa till att effektivisera vardagen för personalen samt automatisera processer och rutinuppgifter. Och med analysverktyg kan verksamheten fatta datadrivna beslut som bygger på fakta istället för på gissningar. Här har IT möjlighet att vara drivande och ta på sig ledartröjan genom att visa hur teknik kan göra vardagen enklare.

Något vi alla kan ta till oss är att ständigt fråga sig ”hur kan detta göras enklare?” vilket gör att gamla arbetssätt ifrågasätts och ersätts när enklare metoder finns.

Simple & smarter

Vårt ledord på Inuit är ”simple & smarter” vilket är utgångspunkten i de lösningar vi vill erbjuda. Vi vill att våra smarta lösningar gör våra kunders vardag enklare, effektivare och säkrare.

I detta nummer av Inuit forum möter du intressanta personer med stor passion för sina respektive specialistområden. Du får ta del av djupgående artiklar, konkreta tips, intressanta fakta samt möta några av våra fantastiska kunder.

Jag vill rikta ett stort tack till alla som läser vår blogg, laddar ned vårt content, deltar på våra webinar och event, följer oss på sociala medier och inte minst använder våra produkter. Tillsammans med våra partners vill vi göra er vardag lite enklare.

Markus Arvidsson
Marknadsansvarig, Inuit AB

** Business Simplification 2015: The Unmet Strategic Imperative*

INNEHÅLL

ANDREAS KARLSSON – CHANGE MANAGER

Förändringsarbete med ökad kvalitet

Idag råder mer eller mindre ständig förändring i alla organisationer. Det gäller inte minst inom IT. Ändå genomförs förändringsarbetet ofta på ett ostrukturerat och ineffektivt sätt. En vanlig orsak är att man saknar eller inte prioriterar problem management. Med en bättre förståelse för sambandet mellan incident, problem och change ökar kvaliteten i de tjänster IT levererar.

EN FENA PÅ CHANGE
Andreas Karlsson är konsult inom IT Service Management på Sogeti och har bred erfarenhet som Change Manager.

Som regel finns en inbyggd tröghet och oro för förändring som kräver ett tydligt ledarskap och kommunikation. Många inser att något måste göras för att skapa bättre leveranser, eller en mer hållbar arbetssituation. IT jobbar till bristningsgränsen med att hantera återkommande incidenter, agera brandkår och leverera god support. Mitt i leveransstressen är det ofta svårt att förstå vad det skulle innebära och vad värdet skulle vara av ett mer strukturerat arbetssätt.

En okunskap hos IT-ledning och personal om hur man kan skapa ett effektivt förändringsarbete leder till att man lägger tid på fel saker, istället för att stanna upp och ta tag i orsakerna.

Ökade krav på struktur och att alla talar samma språk

Andreas Karlsson arbetar som konsult inom IT Service Management på Sogeti och har bred erfarenhet som Change Manager:

– Det är vanligast att initiativet till change management tas i de organisationer som levererar IT till en extern part, trots att incitamenten i form av effektivitetsvinster är lika stora i företagsinterna IT-leveranser. Leveranskraven till kund är högre, ofta direkt kopplade till leveransansvaret via olika SLA:er. Dessutom kommer det ständigt nya krav på säkerhet, inte minst när det gäller till exempel finansiella transaktioner och hantering av annan känslig information.

Ett exempel på en sådan IT-säkerhetsstandard är ISO29100:2011, som ställer krav utifrån en rad säkerhetsaspekter samt att man har ordning, reda och struktur på sin IT. Detta hjälper ITIL dig med. Som regel är det i de allra flesta fall just krav utifrån som sätter tryck på företag att agera. Allt fler organisationer vill visa upp att de har kontroll för att kunna mäta sig i konkurrensen.

– När kunderna blir mer medvetna och kraven i upphandlingar tydligare, gäller det att vi som levererar IT-tjänster har rätt kunskap, både på lednings-, konsult- och verksamhetsnivå. Kunderna ska kunna lita på att alla talar samma språk.

IT är en fabrik – så får du till en fungerande leveransprocess

Ett sätt att beskriva vikten av bättre struktur i IT-arbetet är att likna det vid en fabrik. Ingen tillverkande industri klarar sig utan tydligt strukturerade rutiner och processer. Det handlar om allt från tillverkning till försäljning:

- Hur ska leveransprocessen formaliseras?
- Hur hanterar vi om produkten går sönder
- Varför går den sönder och hur rättar vi till det?
- Vad gäller för garantiärenden? osv.

– Inom IT är inställningen en helt annan, trots att IT är en central del av leveransen! Här behöver fler företag tänka om och börja i rätt ände med ett tydligt commitment från företagsledningen.

För att lyckas måste ledningen ha kunskap och förmåga att tydliggöra vad man vill åstadkomma: sätta mål, avsätta rätt resurser och ställa krav på projektet. Genom att utbilda IT-personalen, låta dem

rent praktiskt prova på att arbeta på ett annat sätt, till exempel producera rapporter, ta fram underlag, blir förändringen mer verklig. Det är viktigt att förstå att syftet är ”att göra det bättre för mig och mitt bidrag till IT-leveransen”.

Hoppa inte över kvalitetssteget – problem management

Första steget är att analysera processen för incident management. Börja titta på rutinerna inom servicedesken, där finns ofta en känsla för vad som orsakar vad. Ta ut trendrapporter, följ hur olika incidenter hanteras, om de är enstaka eller återkommande. Gå sedan till botten genom att hitta samband och ställ frågan: varför uppstår problemet gång på gång?

Många projekt fokuseras på incident management och change management, men missar det viktiga mellansteget problem management. Det är ofta en bortglömd process, som inte formaliseras och därmed utgör ett glapp.

– En väl fungerande problem management är ett bevis på bra kvalitet! Går vi inte till botten med problemet som orsakar alla incidenter är det svårt att välja rätt väg i förändringsarbetet. Orsaken behöver inte vara IT-störningar, det som du från början ser som systemproblem kan istället handla om kompetensbrist och behov av utbildning.

Genom att prioritera problemanalysen kopplat till IT-avdelningens incidenthantering får du ut mer av ditt change managementarbete.

I'm too lazy to be an admin on my machine

Trust me, Whitelisting is the easy option.

To prove to everyone that removing admin rights from end users is the best choice you can make, I thought I would share my personal story on how I got into this business. I haven't been using admin rights on my own computer since 2002 even if I could. I run my own environment and company so nothing prevents me from doing it – except wisdom and a bit of laziness I would say. On the other hand, it would be very hypocritical of me not to practice what I preach to the security community

As I said, it all started in 2002 when I had my family computer infiltrated by Smiley-figures one morning. I went to our computer that I shared with the person I was living with at that time and opened my Outlook only to be faced with these yellow Smiley's jumping all over my desktop. I asked my roommate what they were and she said it was such fun to start the morning with a few smiles. I instantly took measures to prevent it by removing admin rights from both of us and told her that from now on she installs stuff only to her profile not to all users. In a way, you could say that the first driving force for me to ditch admin rights was security based.

The other reason that kept me away from admin rights was totally unrelated to security. At that time, I was a normal Windows user who believed that Windows ran a lot better if you just reinstall it every now and again. For me that was once every 6 to 12 months. Now what totally amazed me was the fact that this machine that we used the most but didn't have admin rights, it just kept running and running. In fact, I reinstalled it, while still being happy with the performance, in January 2007 because of a physical hard disk failure. Therefore, I say that the decision to keep away from admin rights has never been security based for me but based solely on the fact that I'm just way too lazy to be an admin. I skipped 5-10 reinstalls on that machine and I don't like reinstalling or any other sort of extra work. Nowadays I do like the fact that I am security aware and that I can block more than 85% of all threats out there in my environments but just as important is the fact that running as a non-admin prevents you from writing trash on your own computer and its registry. Without admin rights you have better performing computers with a longer lifetime.

In 2005 I went to a security conference in Orlando. Someone speaking there asked the 1200 people in the audience if there was really anyone who didn't use admin rights for end users – I was the only one who raised my hand. Trust me I've had my downs on being the only believer, along with Aaron Margosis from Microsoft of course. Luckily in the past decade things have changed and now I have more people who share my opinions. Though even today when you create a new user in Windows it is an admin by default. In Windows 10 there is a small win for us as the new "Child accounts" are now limited users – not perfect but an advancement I would say!

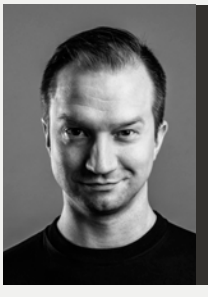
The place we were at was called Buena Vista to be exact. I was sure we were lured into the place just to hear the news during the conference that the name of the new Windows had just been finalized – it would be called Vista. At that time, I of course had really no idea how "Buena" Vista would be. Vista did however bring one feature that has made my life so much easier – UAC (User Account Control). That is probably one of the only few things I still thank Vista for. With UAC, I could now easily use a limited account and just be asked for elevation to another user when needed. This is why I always called UAC the "Automatic RunAs". UAC is very important for security for admins on servers for example but for limited users it's just handy – not a security feature really as they have no admin rights to protect from.

In 2002 something else happened that had made my life a lot easier. That year I deployed the first whitelisting solution to a customer environment with around 35000 computers. Deploying whitelisting is the best idea for any company but it is "easy" only after removing admin rights. When you don't have admin rights you can create whitelists of containers rather than items. So instead of 200 lines listing apps that are allowed you list just "C:\Program Files\" and prevent anyone from adding apps to the folder. The environment is still using whitelisting as are most of my other customers nowadays as well. When people ask me how horrible it is to add every new app to the whitelist I tell them about the containers and explain the other option – Black-Listing or catching the bad guys instead – around 300000 of them, every day. Trust me, Whitelisting is the easy option.

My previous boss once gave me the best credit I've had. He was showing the new CTO around the company and asked me to come along as I had developed most of their systems. When he mentioned that they were using whitelisting the future CTO panicked and said: "That's so much extra work that I believe we should remove it!". My boss asked him to follow and took him to the room that had the monitor that showed all active and previous alerts from our Anti-Virus. He then asked: "What do think about the Anti-virus of our company?". The future CTO replied: "What do you mean? There's nothing on the screen". My boss smiled and replied: "Exactly! All the minutes we lose on administering whitelisting we save as hours and days on not taking care of the Anti-Virus alerts".

Stay limited – stay secure

Sami Laiho



SAMI LAIHO

Sami Laiho är MVP Windows Expert. Han har varit Microsoft Certified Trainer i över 15 år och är en populär talare på bl.a. Microsoft TechEd runtom i världen.

Derek Melber, Technical Evangelist hos ManageEngine

Är din IT-miljö tillräckligt säker?

Visste du att det tar i snitt hela 146 dagar att upptäcka en nätverksattack? Och att 1 av 5 små och medelstora företag drabbas av nätverksattacker? För att skapa ett bättre proaktivt skydd är mer ordning i Active Directory och en behörighetsstruktur enligt "Least Privilege-principen" två nycklar till framgång.

Med en allt mer komplex IT-miljö bestående av både centrala serverenheter, egna system och molntjänster ökar behovet av att ha kontroll på säkerheten. Trots det saknar många företag idag ett bra proaktivt skydd när det gäller centrala och verksamhetskritiska delar som Active Directory, domän- och serverenheter.

Risken för intrång eskalerar i och med den digitala transformationen och hoten består av en rad olika typer av attacker. Många är lösenordsattacker där målet är att söka reda på ingångar via administratörslogin. Det kan till exempel handla om att testa de vanligaste användarlösenorden inom IT. En annan mer avancerad attackteknik är *brute force*, som skannar av en stor mängd möjliga teckenkombinationer och längder på lösenord för att lyckas med ett dataintrång. *"Pass-the-hash attacker"* har i sin tur siktet inställt på att via en specifik dator komma åt nyckeln till administratörsrättigheterna och därigenom "ta kontroll" över nätverket. Oavsett vilken form av attack det handlar om, så kan vi vara säkra på att de som ligger bakom attackerna alltid är minst ett steg före, ofta flera.

Vad kan ett företag då egentligen göra för att skydda sig mot de säkerhetshot, illvilliga program, kodknäckartekniker och hackare som jobbar i det dolda för att ta sig in i hjärtat av ditt företags IT-miljö?

En klassisk vanföreställning – "det händer inte oss!"

Derek Melber är Technical Evangelist hos ManageEngine och ägnar sedan ett antal år tillbaka det mesta av sin tid att resa runt i världen och berätta om hur företagen kan öka säkerheten och samtidigt bli bättre på att utnyttja möjligheterna i Active Directory.

– Det finns mycket företag kan göra för att med ganska små medel förbättra sin IT-säkerhet avsevärt. Då handlar det inte om att spendera dyra pengar på olika verktyg utan först och främst se över den grundläggande säkerheten och rutinerna kring lösenordshantering på IT-avdelningen, menar Derek Melber.

Att säkerhetsriskerna i de flesta företag ändå fortfarande är så höga, beror enligt Derek många gånger på en klassisk vanföreställning: "Det är inget problem för oss, vi har ju inte blivit attackerade!" Denna inställning grundar sig ofta i en brist på kunskap, pengar eller ren ovetskap om de faktiska riskerna. Men dataintrång är idag ett i högsta grad verkligt och allvarligt hot för organisationer över hela världen.

En vanlig missriktning är också att företag fokuserar på multipla virusskydd och brandväggar för att skydda sig mot externa hot, utan att först ha full kontroll på den interna säkerhetsstrukturen. Genom att rikta mer fokus mot administratörsrättigheterna kan företag skapa ett bättre proaktivt skydd och därigenom begränsa effekterna av dataintrång.

Starkare proaktivt skydd med rätt behörighet

Att begränsa rättigheterna för enskilda användare minskar sårbarheten för organisationen avsevärt. En allt mer spretig IT-miljö bestående av egna system och servrar, molntjänster, applikationer och både interna och externa användare påverkar övervakningen av Active Directory. Ett "ostädat" AD utgör en stor säkerhetsrisk på många företag, men med ett proaktivt skydd i form av bättre planering och kontroll av vem som gör vad går det att skapa en mycket säkrare IT-miljö.

– För att nå dit måste du börja från grunden och förenkla. Städa upp bland administratörsrättigheterna, strukturera och ta reda på vad som är enskilda behörigheter och prioritera enligt principen "Least Privileged". De mest säkra IT-miljöerna idag följer Least Privilege-principen. Faktum är att du genom att sätta rätt begränsningar i adminrättigheterna kan minska sårbarheten med uppemot 90 procent, menar Derek Melber.

Least Privileged bygger på att användare enbart ska ha priviligierad åtkomst till den information och de IT-resurser som krävs för att kunna utföra en specifik åtgärd för en viss

Att begränsa rättigheterna för enskilda användare minskar sårbarheten för organisationen avsevärt.

avgränsad nivå, som en process, en användare, en modul eller ett program. Denna åtkomst styrs vanligtvis via behörigheter. För att få en realistisk bild av vad Least Privileged-principen innebär på just ditt företag behöver du först skapa en bättre förståelse för hur rättigheter beviljas: Vilka behörigheter gäller för vilka grupper? Hur definieras administratörsbehörigheter utifrån vissa roller och förutsättningar eller arbetsuppgifter? Hur ges behörighet till enskilda filer, kataloger, applikationer etc? Och vad bestämmer vem som får göra vad? Därutöver behöver även delegeringsrättigheter definieras. När kartan är ritad behöver säkerheten upprätthållas med rutiner och system för hur rättigheter löpande kontrolleras utifrån dessa olika nivåer.

– Med ADManager Plus vill vi göra det enklare för IT att skapa en bättre kontroll och löpande uppföljning av sitt AD. På ManageEngine har vi fokuserat på att fylla de gap vi upplever finns i Microsofts program. Med hjälp av rapportering och analys, monitorering och tydliga varningssignaler vill vi hjälpa organisationen att härda sina system och på så sätt stärka upp sin IT-säkerhet.

VAD ÄR
LEAST PRIVILEGED?

Least Privileged bygger på att användare enbart ska ha priviligierad åtkomst till den information och de IT-resurser som krävs för att kunna utföra en specifik åtgärd för en viss avgränsad nivå, som en process, en användare, en modul eller ett program. Denna åtkomst styrs vanligtvis via behörigheter.

IT som funktion skapar större värde för verksamheten

Behoven och utmaningarna när det gäller IT har ändrats radikalt de senaste åren. I takt med att nya programalternativ och leveransmodeller har växt fram, samtidigt som slutanvändarnas krav ökar, har ITs roll förändrats. Idag ser alltfler organisationer på IT som en funktion som bidrar till ett ökat värde för verksamheten, snarare än olika system i sin IT-miljö. Fokus på mjuka värden snarare än hårda tenderar att öka.

Andreas Ridderstedt, systemspecialist ITSM på Tele2.

Här hittar du en videointervju med Andreas Ridderstedt.

Idag är det mycket sällan bara IT som behöver få tillgång till och förstå den information som skapas i organisationens IT-system. Olika slutanvändare och beslutsfattare ställer olika krav på information, vilket också påverkar allt ifrån insamling och bearbetning av data till gränssnitt och automatisering av processer. Fler modeller och alternativ för att sätta upp sin IT-miljö innebär nya möjligheter, men också svåra avvägningar för att hitta den "optimala" setupen av system och kompetens.

Andreas Ridderstedt, systemspecialist ITSM på Tele2, ser en trend i att fler organisationer går mot att köpa tjänster istället för specialistkonsulter som tidigare:

- Ansvarsfrågan är mycket viktig för organisationerna, som hellre vill köpa en funktion som kan garantera ett specifikt värde av IT-leveransen.

Tre vanliga utmaningsområden är ärendehantering, övervakning och supportproblem som teknikbekymmer och fel som inte kan hittas. Bristande incidenthantering och låg grad av automatisering är ofta ett problem inom ärendehantering. Ett annat är att många organisationer har ett bristfälligt, eller helt saknar, ärendehanteringssystem och istället använder mail eller rent av postit-lappar.

- Ofta grundar sig problemställningen i att man saknar en eller flera processer, eller att spårbarheten är dålig. En vanlig utmaning är till exempel Helpdeskens arbete med att hantera beställningar, planera och följa upp ärenden. "Hur ska vi göra och vad ska vi ha för system?" är vanliga frågor vi får från kunder. Många upplever att de inte nyttjar IT optimalt, berättar Andreas.

Detsamma gäller övervakning. Där upplever IT ofta att de inte får någon mer vägledning av nuvarande övervakning än att en röd varningslampa indikerar att en felsökning måste göras någonstans i systemen. Det kan också handla om områden där ingen övervakning sker idag, som med bättre kontroll eller åtgärd skulle öka kvaliteten på IT-leveransen och skapa effektivare arbetsprocesser i organisationen.

Ett ekosystem av tjänster

För att hjälpa organisationer som står inför dessa utmaningar och inte själva har den tid, resurser eller energi som krävs har Tele2 valt att skapa ett ekosystem av tjänster baserat på ManageEngines produktportfölj.

- Med ManageEngines lösningar får våra kunder en enkel, dynamisk och skalbar lösning som ligger i molnet, tillgänglig via Azure. Det innebär att kunden kan anpassa lösningen utifrån sitt eget utnyttjande och varierande behov. Genom att vi på Tele2 även själva an-

Andreas Ridderstedt ser en trend i att fler organisationer går mot att köpa tjänster istället för specialistkonsulter som tidigare.

vänder ManageEngines lösningar i vår egen IT-miljö och använder systemen i praktiken, bygger vi också kontinuerligt vår kunskap ur ett användarperspektiv. Det är en viktig policy för oss att leva som vi lär och att hela tiden testa och utvärdera de olika delarna i ManageEngines ekosystem.

För att få en tydligare bild av behov och kravställning behöver organisationen först rita kartan. Det är ett viktigt första steg för att kunna hitta sin förbättringspotential. Förståelsen för värdet av vad organisationens IT-system levererar, för vem och i vilket sammanhang är central för att kunna optimera processerna.

Organisationer vill ha enkla verktyg och effektiva processer

Om bristen på information och effektiva processer är ena sidan av myntet, så är svårigheterna att räkna på en investering den andra. För att kunna göra rätt bedömning är det viktigt att se till hela den totala kostnaden. Direktkostnaden för investeringen är den enkla posten att räkna på, men att till exempel utvärdera en lösning on-premise mot en molntjänst eller ett ärendehanteringssystem mot ett annat, kräver så mycket mer. Hur många incidenter hanteras? Hur ofta sker felsökning? Hur mycket tid lägger vi ner på att hitta fel? Vad är direkt mätbart? Och vilka blir effektivitetsvinsterna på kort och lång sikt? Vad tjänar vi på att automatisera vissa av de arbetsuppgifter som görs idag?

IT är en förutsättning för att verksamheter idag över huvud taget ska kunna fungera. Ändå saknar många organisationer riktlinjer för hur IT-arbetet och relaterade kostnader ska mätas och utvärderas.

- Många vill ha enkla verktyg och effektiva processer, där repetitiva moment så långt det är möjligt kan automatiseras. Samtidigt har de svårt att se vad de kan bli bättre på och vad som är viktigt och inte viktigt. Många gånger skulle de problem som finns kunna åtgärdas relativt enkelt genom bättre kontroll, menar Andreas Ridderstedt.

Förståelsen för hur IT som en funktion kan skapa värde för hela verksamheten kommer att bli avgörande för hur väl organisationer lyckas i framtiden och till vilken kostnad.

Snabbväxande ManageEngine

En stark utmanare till de stora spelarna

> *Komplexa IT-system leder många gånger till att företagen måste anlita konsulthjälp, vilket blir kostsamt både direkt och i längden,*
>
> **ERIK TJÄRNQVIST** · INUITS PRODUKTCHEF FÖR MANAGEENGINE

Hur kan vi erbjuda samma lösningar som de stora IT-jättarna, men till en tiondel av priset? Frågan la grunden för affärsidén som ManageEngine senare skulle bygga hela sin verksamhet på. Idag förser ManageEngine över 120 000 kunder världen över med prisvärda programvaror. Det gör företaget till det snabbt växande alternativet till de största leverantörerna av IT-infrastruktur.

Från småskalig till utmanare

ManageEngine är ZOHO Corporations division för IT-lösningar till företag och grundades 1996, då under namnet Adventnet. Initialt utvecklades enbart produkter för nätverksövervakning, men så småningom utvidgades produktportföljen till att inkludera allt fler företagslösningar. År 2003 bytte Adventnet namn till ManageEngine.

Ungefär sju år senare gav sig ManageEngine in på riktigt i matchen med de stora jättarna. De befintliga alternativen var dyra, komplexa programvaror från de traditionella IT-leverantörerna, eller osäkra gratislösningar utan garantier. Däremellan saknades alternativ – något som bolaget tog fasta på när de lanserade ManageEngine 90:10 promise. Affärsidén var att kunna erbjuda 90 procent av de funktioner som "The Big 4": Hewlett Packard, IBM, BMC och CA Technologies gjorde, men till 10 procent av priset.

ManageEngine 90:10 promise. ManageEngines framgångsrika affärsidé byggde på att kunna erbjuda 90 procent av de funktioner som "The Big 4": Hewlett Packard, IBM, BMC och CA Technologies gjorde, men till 10 procent av priset.

Fokus på utveckling bäddar för framgång

Idag använder fler än 120 000 företag världen över ManageEngines produkter för IT-infrastruktur och affärsapplikationer. Det prisvärda ekosystemet av enkelt förpackade produkter resulterar i att bolaget får en ny svensk kund varje vecka.

– Användarvänligheten tillsammans med priset gör att ManageEngines produkter passar svenska företag väldigt bra. Sverige har få företag med över tusen anställda och IT-avdelningarna är oftast små. Komplexa IT-system leder många gånger till att företagen måste anlita konsulthjälp, vilket blir kostsamt både direkt och i längden, menar Erik Tjärnqvist, produktchef ManageEngine på Inuit.

Utöver de prisvärda systemen tror Erik Tjärnqvist att framgången bottnar i företagets innovationsförmåga. Till

skillnad från många andra IT-företag har ManageEngine alltid fokuserat på produktutveckling framför traditionell försäljning. I kombination med bra marknadsföring genom Google har företaget lyckats göra sajten till sin marknadsplats där du enkelt både kan hitta information och köpa produkterna.

– Istället för att ha säljare på fälten har de kunnat anställa fler människor som utvecklar nya och befintliga produkter. Det har resulterat i att företaget har lyckats bygga över 90 funktionella IT-lösningar – det är unikt inom IT-branschen.

Integration – en allt viktigare fråga

De senaste årens stora utmaning inom IT är integration. Med en allt mer komplex och omfattande IT-miljö ökar också behovet av sömlösa integrationer mellan olika system. ManageEngine har valt att samla sina lösningar i en enhetlig produktportfölj. Att ManageEngines lösningar dessutom via olika APIer kan integreras med i princip vilka produkter som helst, öppnar upp helt nya möjligheter.

– I framtiden kommer vi se fler samarbeten mellan olika systemaktörer: SaaS-lösningar från ZOHO kommer att kunna integreras ännu bättre med ManageEngines on premise-lösningar. Redan idag kan du köpa ManageEngines applikationer i Microsofts molntjänst Azure. Det är ett stort genomslag i sig och något vi kommer se allt mer av framöver.

Även behovet av Business Intelligence kommer fortsätta att växa i takt med att mängden data ökar. BI-system som ManageEngines Analytics Plus blir allt viktigare för att sammanställa, sortera och analysera data som annars ligger utspridd över olika system. Till skillnad från många traditionella BI-verktyg fokuserar ManageEngines Analytics Plus på IT-avdelningens arbete och behov. Precis som resten av företagets produkter är mjukvaran utvecklad av tekniker, för tekniker.

– Det är så ManageEngine alltid har tänkt och kommer fortsätta att utveckla sina produkter i framtiden – för sina faktiska användare, avslutar Erik Tjärnqvist.

Privileged accounts en av de största säkerhetsriskerna

De flesta företag är medvetna om vikten av en bra brandvägg och antivirus. Idag är det dock det som händer på insidan som utgör det största hotet. Det är också en av anledningarna till att hackers siktar in sig på just dessa användarkonton. Med en tydligare strategi för hantering av administratörsrättigheter kan du öka säkerhetsnivån avsevärt och samtidigt säkerställa att företaget kan leva upp till de nya regelverk som ställer allt högre krav på IT-avdelningens kontrollansvar.

Oavsett om du har manuella rutiner eller system för att hantera privileged accounts, konton med administratörsrättigheter, är hanteringen ofta minst sagt bristfällig. Det är lätt att man skapar sig lokala, ofta personberoende, rutiner för att underlätta i det dagliga adminarbetet. Det är inte heller ovanligt att systemlösenord till servrar, databaser och olika applikationskonton sparas i lokala xls-filer eller på post-it-lappar på ett "säkert ställe". Systemadministratörerna ges ofta höga behörigheter, samtidigt som det är svårt att följa upp vad någon har gjort.

Nycklarna till effektiv och säker kontohantering

Genom att rikta mer fokus mot administratörsrättigheterna skapas ett bättre proaktivt skydd. Att ge rätt access till de som verkligen behöver det när de behöver det är nyckeln till en väl fungerande privileged password management.

För att bemöta säkerhetsproblematiken med administratörskonton finns framförallt tre områden som du behöver ta kontroll över:

- **Tydlig och enhetlig lösenordshantering** – undvik manuella rutiner, arbeta mer med dolda, automatgenererade lösenord där det är möjligt för att undvika att ge ut rotlösenord.
- **Systematiserade accessrutiner** – arbeta utifrån ett tydligt ownership concept för att veta vem som har privileged access till vad, vem som äger resurserna. Sträva efter central styrning av åtkomst kopplat till automatisk uppdatering av register över administratörsrättigheterna. Skapa en rutin för tidsbegränsade accesser.
- **Process för kontroll och uppföljning** – definiera tydliga policys och uppföljningsrutiner för att säkerställa att ni följer regelverk som till exempel PCI och GDPR samt för att kunna genomföra regelbundna user audits med full spårbarhet.

WEBINAR
ON DEMAND

Vill du veta mer hur du kan säkra upp din IT-miljö med privileged password management? Kolla in vårt inspelade webinar där du även får se exempel på hur hantering av administratörsrättigheter kan fungera i verktyget Password Manager Pro.

Ta det lugnt – ligg steget före

Många IT-avdelningar brottas fortfarande med hygienfaktorer avseende IT operations management. Arbetet präglas ofta av brandsläckningar när problem väl uppstår. Många gånger är framförhållningen dålig och det uppstår flaskhalsar i hanteringen. Genom att arbeta mer proaktivt och ta kontroll över resurserna kan IT arbeta mer effektivt och metodiskt med bättre resultat.

Jonas Åström berättar hur. →

Ta det lugnt – ligg steget före

> *Data och historik är företagets guldgruva som enligt min mening inte utnyttjas till sin fulla potential. Genom att lära sig av sin egen data är det möjligt att förutspå problem och vidta åtgärder proaktivt.*
>
> JONAS ÅSTRÖM

Ett nätverk ligger nere, en säkerhetslucka uppdagas, en server kraschar, plötsligt uppstår behov av extra lagringsutrymme och så vidare. Denna typ av reaktivt arbetssätt leder ofta till ineffektivitet, oplanerade kostnadsposter och en allmänt stressig vardag på IT-avdelningen.

Övervaka och få kontroll

Antalet enheter i form av servrar, routrar, nätverk, brandväggar, skrivare, tjänster och applikationer ökar och sambanden dem emellan blir alltmer komplexa. Om IT-avdelningen saknar överblick kommer brandsläckningarna att fortsätta och situationen blir ohållbar i längden. Med rätt verktyg kan du övervaka och ta tillbaka kontrollen över företagets IT-infrastruktur och IT operations.

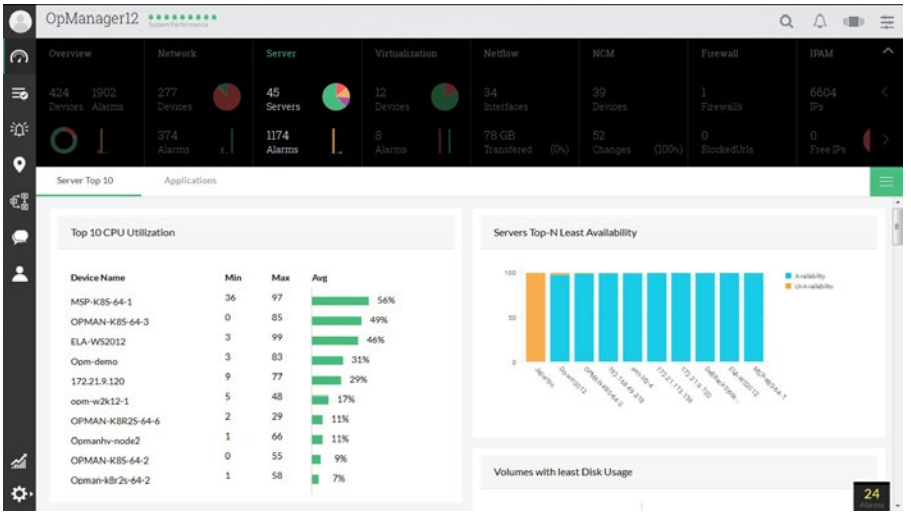
Jonas Åström, delägare och konsult på Layer 8 IT-Services AB med ett långt förflutet inom IT-branschen, brinner för smartare datacenternätverk och nätverkssäkerhet. Jonas har hjälpt flera företag att implementera ManageEngine OpManager, en plattform för server- och nätverksövervakning.

– Jag ser som min största uppgift att få IT-avdelningar att arbeta mer proaktivt. En grundförutsättning är att få överblick och kontroll på resurserna och infrastrukturen. Då är chansen större att det finns tid över för analys, som kan ge ett mer effektivt och metodiskt arbetssätt med automatiserade workflows, larm, notifieringar och mallar, säger Jonas.

Att ha koll är en säkerhetsfråga

Med ett övervakningsverktyg som ManageEngine OpManager kan IT-avdelningen centralt övervaka och visualisera samtliga resurser. Det är enkelt att se status i realtid över vad som fungerar, vad som behöver åtgärdas samt eventuella säkerhetsbrister eller intrång. På så sätt blir det lätt att få en bild av hur nätverket, servrar och applikationer mår just nu – men också i det långa loppet.

– Du vill i största möjliga mån undvika paniksamtal från medarbetare och chefer om brister i IT-infrastrukturen. IT ska istället vara först med att upptäcka och åtgärda problem som uppstår, säger Jonas.



ManageEngine OpManager v.12.2 tar nätverks-, server- och datacenterövervakning till nästa nivå.

Automatisering och rapporter

Vid server- och nätverksövervakning samlas mängder av data in och historiken är enligt Jonas en många gånger underutnyttjad källa till information.

– Data och historik är företagets guldgruva som enligt min mening inte utnyttjas till sin fulla potential. Genom att lära sig av sin egen data är det möjligt att förutspå problem och vidta åtgärder proaktivt.

Du ska direkt kunna se när diskutrymmet börjar ta slut, eller när en server tappar kontakt med nätverket, för att kunna agera. Du kommer också att börja se mönster, trender och därmed kunna kapacitetsplanera, menar Jonas. Utifrån analysen är det också möjligt att skapa regler med larm och notifieringar, bygga workflows som genererar automatiserade moment samt ta fram en väl fungerande rapportfunktion.

Configuration management och driftsäkerhet

För att säkra upp IT-driften är det viktigt att du är medveten om hur enheterna är konfigurerade och vem som gör ändringar. En felaktig eller obehörig konfigurationsförändring kan medföra långtgående effekter på säkerhet och tillförlitlighet.

Med configuration management kan du automatisera policybaserade förändringar och konfiguration för hela ditt IT-system. Det skapar en tillförlitlig drift och täpper till eventuella säkerhetsrisker.

Förutspå IT-investeringar och sätt en realistisk IT-budget

IT behöver också förstå och kunna förutspå behov på ett tidigt skede inför till exempel kommande företagsförvärv, massiva rekryteringssatsningar eller avyttringar. Att i ett tidigt skede få notifiering om att till exempel nätverkskapaciteten är på bristningsgränsen gör att du bättre kan planera och stötta affärsverksamhetens tillväxt.

Att få detaljerad insikt och information om fabrikat, tillverkare, när enheten slutade säljas och när supporten upphör, ger bra underlag för att planera och budgetera för framtida IT-investeringar.

OpManager framtidssäkrar och effektiviserar IT operation management

ManageEngine OpManager är en komplett plattform för server- och nätverksövervakning med ett webbaserat gränssnitt. I systemet kan du hantera hela företagets IT-infrastruktur centralt, med automatiserade workflows, intelligenta larm och notifieringsmöjligheter samt konfigurerbara regler och mallar. Installationen är enkel och det går snabbt att sätta upp ett fungerande 24/7 övervakningssystem. OpManager går lätt att integrera med andra ManageEngine-produkter vilket förenklar hanteringen av hela flödet – från ax till limpa.

– Jag rekommenderar att du börjar med att scanna av och göra översyn för att se hur många devices du vill övervaka och konfigurera. Sätt ramarna, men börja smått och växa in i OpManager. Alla delar är separat licensierade och huvudlicensieringen är per enhet. Du behöver inte köra allt på en gång, avslutar Jonas Åström.

LÄS MER

Läs om hur OpManager stödjer organisationers ITOM satsningar

VAD ÄR ITOM?

IT operations management (ITOM) innefattar hela den tekniska infrastrukturen inom en organisation inklusive enskilda applikationer, tjänster, lagring, nätverk och anslutningar.

Därmed inkluderar det den dagliga driften och alla processer och tjänster som förvaltas av en organisations IT-avdelning. En effektiv IT operations management säkerställer tillgänglighet, effektivitet och prestanda av organisationens processer och tjänster.

Den digitala revolutionen gör att det finns teknik i varje steg av en organisations värdekedja och denna mycket komplexa och snabbt föränderliga tekniska miljö består av nya digitala system som är starkt beroende av IT-infrastruktur och andra tekniska tjänster. Det är därför allt fler organisationer känner ett behov av att ha en lösning (som OpManager) som kan ge dem den överblick och kontroll som behövs för att IT skall kunna leverera vad som förväntas av dem för att verksamheten skall fungera.

Jonas Åström, delägare och konsult på Layer 8 IT-Services AB med ett långt förflutet inom IT-branschen, brinner för smartare datacenternätverk och nätverkssäkerhet.

— RAKESH JAYAPRAKASH —

Så optimerar du IT-verksamheten med Business Intelligence

Mängden data inte bara ökar, ökningen går också allt snabbare!

Big data är idag ett vedertaget begrepp och åsikterna är flera om hur vi bör förhålla oss till att vi endast drar nytta av en bråkdel av all data som produceras. Utmaningen är att data i sig inte har något värde alls om den inte kan tolkas, eller ens hittas, och förädlas till användbar information för vår verksamhet – Business Intelligence.

Vi fattar idag alltfler datadrivna beslut och många verksamheter är helt beroende av att kunna följa och analysera den data som skapas för att kunna säkerställa sina leveranser och upprätthålla sin konkurrenskraft. Ändå saknar många företag en strategi för att analysera data. Något som bör utgöra en självklar del i företagets IT-strategi. Att kunna ställa rätt frågor, identifiera rätt data och skapa ett ramverk för analysen kommer bli avgörande för att nå framgång.

Utmaningen är inte bara mängden oidentifierad data, utan kanske framförallt alla de olika applikationer, system och databaser, anpassade för olika saker och olika syften, där all data registreras. Ofta fungerar dessa som isolerade öar i IT-miljön och är generellt sett svåra att få en överblick över. Ju fler system företaget har desto större är också utmaningen och behovet av att veta. Men även på det mindre IT-intensiva företaget leder utmaningen med en växande mängd data många gånger till bristande kontroll och ineffektivitet.

Olika mål, drivkrafter och behov

Med hjälp av intelligenta IT-verktyg och anpassad analys finns idag stora möjligheter att arbeta mer aktivt för att ta kontroll och fatta rätt beslut baserat på data som tidigare varit dold och ostrukturerad.

Rakesh Jayaprakash arbetar som Technical Support Engineer på ManageEngine och menar att mycket handlar om att sträva efter att normalisera, analysera och sortera företagets data. "Make it easy" blir ett mantra genom att tillgängliggöra och anpassa informationen utifrån organisationens olika roller:

– Vi går mer och mer mot ett självservicebeteende. Tidigare var det framförallt systemanalytiker som hade ansvaret för att tolka och analysera företagets data för att sedan rapportera det till verksamheten. I dagens organisationer ser vi istället att ansvaret för att analysera och agera flyttas mer och mer över från analytikern till den som har direkt behov av informationen, den vanliga teknikern, IT-chefen eller VD:n för den delen. Det handlar om att ta ägarskap om informationen och addera värde utifrån vad olika data kan berätta för mig utifrån min roll

Det viktigaste i en sådan förändring är att inse att olika roller och aktörer har olika behov. Då gäller det att skapa rätt förutsättningar baserat på vilken typ av

> – För oss på ManageEngine har det varit viktigt att ge makten till användare att bestämma! Det ska vara enkelt.
>
> RAKESH JAYAPRAKASH, MANAGEENGINE

Make it easy!
Rakesh Jayaprakash arbetar som Technical Support Engineer på ManageEngine och menar att mycket handlar om att sträva efter att normalisera, analysera och sortera företagets data. "Make it easy" blir ett mantra genom att tillgängliggöra och anpassa informationen utifrån organisationens olika roller.

Webinar med Rakesh:
Self-service analytics for enterprise IT and beyond.

data som är relevant för vem och på hur behovet ser ut utifrån vad informationen ska användas till. Olika roller och individer har också ofta helt olika mål med vad de vill få ut och använda informationen till.

Vikten av analys utifrån användarens behov
Rakesh ger exempel på tre vanliga roller som har helt olika förutsättningar:

1 – Systemteknikern har behov av att gå in i detalj på systemtekniska och utvecklingsmässiga flöden för att till exempel kunna prioritera, mäta och utvärdera IT-avdelningens arbete, automatisera och dra lärdom av tidigare arbete. Det kan till exempel handla om att identifiera mönster när det gäller nätverksfel.

2 – Chefen för servicedesken behöver i sin tur få en överblick över hur det dagliga arbetet fungerar eller hur olika arbetsflöden kan effektiviseras och planeras bättre. Informationen kan till exempel användas till att fånga upp missnöjda kunder och hitta områden där servicen kan förbättras.

3 – Den verksamhetsansvarige, t ex IT-chefen eller VDn som fattar besluten, är istället mer intresserade av att ha en övergripande kontroll och få information som kan ligga till grund för framtida affärs- och verksamhetsbeslut eller att bestämma rätt bemanning.

– Det viktiga här är att förstå att det inte finns en rapport som passar alla. Traditionella, statiska rapporter som med jämna mellanrum som regel mailas ut fungerar inte, utan skapar snarare fler följdfrågor än ger relevanta svar.

När ansvaret och handhavandet för analysen flyttar "närmare verksamheten" behövs system och processer som kan göra det enkelt och skapa rätt förutsättningar för Business Intelligence när det gäller både relevans och flexibilitet.

– För oss på ManageEngine har det varit viktigt att ge makten till användare att bestämma! Det ska vara enkelt. Det är också bakgrunden till att vi utvecklat analysverktyget Analytics Plus, som du inte ska behöva vara databasexpert för att jobba i. Genom att använda våra standard dashboards anpassade för olika roller och behov, eller skapa egna, vill vi bidra till bättre Business Intelligence för både dig i din roll på IT och din organisation.

BUSINESS INTELLIGENCE I FYRA STEG

1. Se till att inkludera en analysstrategi som en del i din IT-strategi.
2. Skapa rätt förutsättningar och underlag för uppföljning baserat på olika roller och behov.
3. Dra nytta av företagets data genom att ställa rätt frågor, identifiera rätt mätetal och skapa rätt dashboards.
4. Välj ett flexibelt och enkelt analysverktyg som var och en kan förstå och anpassa utifrån sina egna behov. På så sätt kan fler i organisationen förvandla data till användbar information som bygger företagets Business Intelligence.

MEA
STOCKHOLM
2016

ManageEngine Användarkonferens

I oktober anordnade Inuit den mycket uppskattade ManageEngine Användarkonferens för sjätte gången. Intresset för enkla och användarvänliga verktyg för säker och förenklad IT-administration (IT Management) är större än någonsin. Deltagarna lärde sig mycket nytt, lyssnade på inspirerande föreläsningar och det fanns dessutom gott om tillfällen för nätverkande och erfarenhetsutbyte. Majoriteten av de vi talade med använde idag en eller flera av ManageEngines produkter, och såg stor potential i att addera fler produkter från ManageEngines produktportfölj som komplement eller utökad funktionalitet.

Läs mer på nästa uppslag om några av deltagarnas erfarenheter från konferensen.


Overvakning
Applications Manager
OpManager
MEA
STOCKHOLM
2016

MEA STOCKHOLM 2016

Åtta kundinsikter från ManageEngine Användarkonferens

Anna Nilsson t.v. här tillsammans med sin kollega Charlotte Klingström, också från Örebro Universitet.

ANNA NILSSON, SYSTEMANSVARIG, ÖREBRO UNIVERSITET

Anna Nilsson från Örebro Universitet uppskattar ManageEngines användarkonferens för att agendan innehåller aktuella ämnen som berör henne, men också för att stort fokus ligger på nätverkande.

– Jag passar på att prata med andra som arbetar med IT på olika lärosäten. Vi har mycket att vinna på att dela erfarenheter då vi arbetar på liknande sätt och dessutom har ungefär samma stödsystem och processer. Det finns många saker för oss att ta tag i och det första jag ska göra på måndag är att formalisera arbetet genom att sätta ihop en förvaltningsgrupp så att vi kan bli bättre på att sätta rätt prioriteringar, säger Anna Nilsson.

TIM HUHTALA, SERVICE DESK TEAMLEDARE, MEKONOMEN GROUP

Tim är på användarkonferensen för att nätverka och få tips om hur Mekonomen kan dra ännu mer nytta av ServiceDesk Plus genom till exempel ManageEngine Plugins. Mekonomen Group har sedan helt nyligen en ny servicedeskfunktion, och är mycket nöjda med ServiceDesk Plus.

– Ärendehanteringssystemet har på riktigt överträffat våra förväntningar och då har jag sett en hel del system i mina dagar. Jag har pratat med många intressanta personer här och fått bra information som jag kommer ha konkret nytta av framöver, säger Tim Huhtala.

OLA AXÉN, DRIFTSTEKNIKER, TEKNISKA VERKEN I LINKÖPING

Tekniska Verken i Linköping har varit ManageEngine-användare i nästan 10 år. ServiceDesk Plus körs på 30 anläggningar och företaget använder också Recovery-Manager Plus. Ola har Active Directory som sitt primära intresseområde, men inspirerades av dragningen om IT-säkerhet som hölls av Derek Melber, Technical Evangelist på ManageEngine.

– Derek fångade mig verkligen när han berättade om IT-säkerhet. Hans bakgrund och erfarenheter gör att det känns som han förstår mig och min vardag. När jag är tillbaka på kontoret kommer jag att ladda hem och utvärdera ADAudit Plus, säger Ola Axén.

MARTIN ÖLANDER, UTVECKLINGSCHEF, KINNARPS AB

Kinnarps AB ska byta ut det gamla servicedesksystemet och utvärderar just nu ServiceDesk Plus samt 2-3 andra system på marknaden. För Martin är det viktigt att få en bättre bild av produkten och också veta vad som är på gång framöver när det gäller produktutveckling och användargränssnitt.

– Styrkan i ManageEngine är ju verkligen helheten, alltså att inte bara plocka en modul utan samverkan mellan de olika delarna skapar möjligheten att dra nytta av ett helt ekosystem. Jag ser fram emot att borra djupare i ServiceDesk Plus för att se om de lever upp till våra krav, säger Martin Ölander.

ALEXANDER NORDIN, SUPPORTTEKNIKER SPECIALISERAD PÅ SERVICEDESK PLUS, REGION HALLAND

Alexander Nordin har varit specialist på ServiceDesk Plus i snart ett halvår inom Region Halland och börjar nu snegla på de ytterligare möjligheter som ManageEngine erbjuder.

– Jag har börjat titta närmare på integrationerna och alla plug-ins. Jag ser även ett behov av att utveckla rapporteringen och kan tänka mig att komplettera med Analytics, säger Alexander Nordin.

MARIA EDBLOM TAUSON, SENIOR INFRASTRUCTURE SUPPORT SPECIALIST, UMEÅ UNIVERSITET

Maria från Umeå Universitet deltar på användarkonferensen för andra gången och uppskattar att fylla på med djupgående kunskaper som är relevanta för henne.

– Under dessa dagar ligger fokus på utbildning och inte på sälj, vilket jag uppskattar. Analytics och ManageEngine Plugins verkar spännande, men för att köra accesshantering krävs en del förarbete. Jag är nu jätteivrig på att gå hem och testa, säger Maria Edblom Tauson.

FREDRIK ELGH, IT-TEKNIKER MED ANSVAR FÖR SUPPORT, VBG GROUP TRUCK EQUIPMENT

VBG Group använder ServiceDesk Plus för sin kundsupport och Fredrik deltar på användarkonferensen för att lära sig mer om ManageEngines övriga produkter och möjligheter. Genom konferensen får han god insikt i vad som händer framgent och passar på att ställa detaljerade frågor direkt till utvecklarna.

– Vi har höga krav på rapporter och jag vill titta närmare på Analytics Plus som på ett kraftfullt sätt visualiserar data i dashboards. Jag har fått prata med många tekniker och efter konferensen vet jag på vad, och hur, vi ska satsa framöver, säger Fredrik Elgh.

KRIS SMITH, SUPPORTTEKNIKER, EITECH AB

Elteknikbolaget Eitech är mitt uppe i att sätta upp en ny AD-infrastruktur helt baserat på ADManager Plus. Kris har fått bra insikt och kunskap om vad som är best practice och vet nu bättre hur han ska gå vidare.

– Vi vill göra rätt från början och undvika eventuella misstag och då är denna användarkonferens oerhört bra. Utöver ADManager Plus som vi har idag, tittar vi också närmare på om ADAudit är något för oss. Jag lärde mig mycket under Rakesh Jayaprakash pass om Analytics och har aldrig tidigare sett data från så många olika källor presenteras i den typen av interaktiva grafer. Tillbaka på kontoret kommer vi att följa de steg som Derek rekommenderade kring IT-säkerhet. Återigen, vi vill göra rätt från början och har nu bra verktyg för att fortsätta resan framåt, säger Kris Smith.

MEA
STOCKHOLM
2016


TDC
inuit
ManageEngine


inuit

— CHECKLISTA FÖR GDPR —

GDPR innebär nya utmaningar och risker för IT

EU har sedan 2012 utarbetat ett nytt regelverk, GDPR (General Data Protection Regulation), för att skydda personuppgifter som registreras och behandlas. De nya, striktare reglerna innebär att organisationer nu måste revidera sina befintliga dataflödesförfaranden och säkerhetsstrategier så att de överensstämmer med de krav som GDPR ställer.

Och tiden är knapp – regelverket träder i kraft i maj 2018.

Sju steg till en konkret handlingsplan för din IT-avdelning
I praktiken innebär de skärpta kraven i GDPR, som ersätter dagens PUL, flera förändringar för din organisation för att kunna säkerställa att det nya regelverket följs. Ett stort ansvar faller per automatik på IT-avdelningen när det gäller att skapa rätt förutsättningar. Ändå saknar många organisationer fortfarande en konkret handlingsplan.

Vi har skapat en checklista för att underlätta förberedelserna inför GDPR:

1. ***Ta ett tydligt ägarskap*** genom att fastslå processer, roller och ansvar när det gäller hur och varför personuppgifter hanteras och lagras i din organisation. Tydliggör och balansera ansvaret mellan personuppgiftsansvarig och personuppgiftsbiträde, som till exempel kan vara en driftsleverantör där behandling av personuppgifter ingår i uppdraget.
2. ***Kartlägg och revidera*** befintliga granskningsmodeller, säkerhetssystem och intrångspolicys samt definiera ansvarsområden så att de möter GDPR:s krav på ansvarsskyldighet.
3. ***Etablera och förankra*** ett riskbaserat förhållningssätt i organisationen när det gäller hantering av särskilt känsliga personuppgifter.
5. ***Gör konsekvensanalyser*** för att fastslå vilka eventuella risker som finns redan innan vissa data behandlas. På så sätt kan åtgärder för att begränsa riskerna sättas in i ett tidigt skede och minska eventuella skadekostnader.
6. ***Dokumentera*** all information relaterad till behandling av personuppgifter. Vilken typ av data samlas in? Hur samlas den in, överförs och lagras? Hur skyddas dessa data från att röjas?
7. ***Se över vem som har tillgång*** till personuppgifterna och till vem de delas, samt protokollför hur länge uppgifterna ska lagras. Så länge de lagras måste din organisation kunna säkerställa att de är krypterade och skyddade mot skada och intrång.
8. ***Fastställ rutiner*** för att övervaka filer och mappar som innehåller personuppgifter så att alla intrångsförsök kan identifieras omedelbart och rapporteras.

Anpassningen till GDPR är en investering i bättre informationssäkerhet.

THORIR EGGERTSSON, VD INUIT

LADDA NER

I ManageEngines GDPR-handbok kan du läsa mer om vad som krävs för att följa kraven och hur du kan förbereda din organisation.