När driftstoppet inträffar

- Ett whitepaper om hantering av extrema incidenter i IT-miljöer

Varje organisation bör ha en medvetenhet om att det är en fråga om när, inte om, en incident i ett IT-system inträffar. Hur förbereder man sig för att hantera ett driftstopp och minimera konsekvenserna?

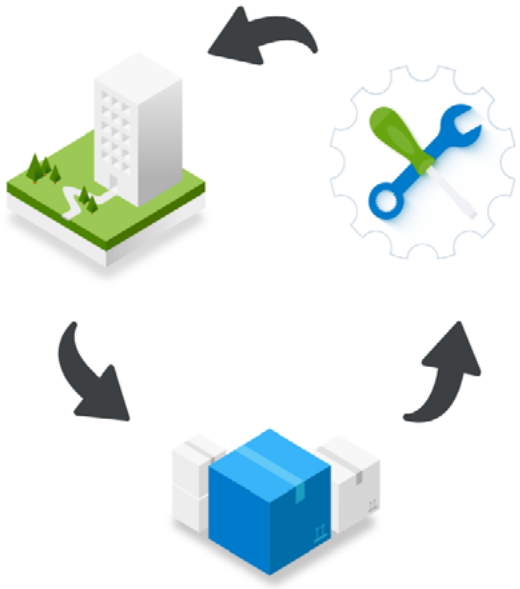
Nya tekniska lösningar implementeras i vitt skilda sammanhang för att underlätta komplicerade arbetsprocesser. De har en sak gemensamt: de fungerar inte felfritt för evigt. Att förbereda sig för det oväntade kan låta som en logisk motsägelse, men på samma sätt som de flesta av oss har hemförsäkring som ett skydd mot brand och andra händelser som vi hoppas aldrig ska inträffa, bör en organisation ha en medvetenhet om att det är en fråga om när, inte om, en incident i ett IT-system inträffar.

Incidenterna kan komma i olika skepnader. Vissa är bara irriterande medan andra kan lamslå hela organisationen eller orsaka stor ekonomisk skada. De går inte att helt skydda sig mot, men med rätt förberedelser och kunskap kan riskerna ofta minimeras och konsekvenserna mildras.

I detta whitepaper kommer vi att se närmare på tre verkliga incidenter, hur de hanterades och vilka insikter de kan ge oss.

Incident 1: Självbetjäningstekniken som slutade fungera

Så kallad self-service technology, själv-betjäningsteknik på svenska, har de senaste åren skapat möjligheter för kunder att betjäna sig själva inom olika verksamheter, som banker, butiker eller flygplatser. En av de vanligaste tillämpningarna är självscanningen i dagligvaruhandeln - en teknik som gör att kunden själv scannar och betalar sina varor utan att behöva passera det traditionella kassabandet. Självscanning gör att kunden kan packa sina varor redan i butiken och slipper lägga tid på att stå i kö till kassan, medan det för butikens del innebär att personal frigörs och att kundupplevelsen kan förbättras. Förutsatt att allting fungerar.



Stilleståndet på ett hundratal butiker

En tisdag i februari slutade självscannings-tekniken på en av Sveriges största butiks-kedjor att fungera. Stilleståndet kom plötsligt och oväntat, och inom kort var hundratals missnöjda kunder på väg ut från butikerna utan att ha kunnat köpa sina varor.

– Vi monitorerar servrarna och övervakar inköpen, och såg plötsligt att omsättningen gick ner till noll i hela Sverige, minns Anders Holm, chef för teknisk service på Visma EssCom. Strax därefter blev samtliga våra telefonlinjer nerringda av butikspersonal och det blev snabbt uppenbart att vi hade med en allvarlig incident att göra.

Stilleståndet visade sig beröra cirka 200 butiker och ett tusental enheter. Butiksägaren hade varit beredd på centrala problem och hade investerat i säkerhetssystem mot hackerattacker, men snart stod det klart att detta inte var någon attack utifrån. Enheterna hade dödats av något så oskyldigt som ett fel i en firmwareuppgradering. Problemet var att det inte gick att lösa på distans: samtliga enheter behövde hämtas in för att uppgraderas och därefter köras ut till butikerna igen.

> Vi är vana att hantera incidenter av den här kalibern, men det är sällan något inträffar av denna volym, säger Anders Holm.

Att nollställa och uppdatera en enhet är okomplicerat, men flera tusen enheter från ett par hundra butiker gör att det plötsligt behövs en enorm logistikkedja. Lösningen blev att skapa en sambandscentral, ett "war room" varifrån arbetet kunde koordineras.

Incident 1: Självbetjäningstekniken som slutade fungera

– Vi satte ihop ett team som mer eller mindre låste in sig och började lägga upp en plan för hur vi skulle gå till väga, berättar Anders Holm. Vi kontaktade leverantören av enheterna för att få tag på alla delar vi behövde: jiggar, sladdar, mjukvara, kontakter. Vi kallade in all personal vi hade tillgång till och började fördela uppgifter.

För att kunna göra en uppdatering behövs en liten kabel. Det fanns två sådana att tillgå. I hela Sverige.

– Det var ju lite i underkant, säger Anders Holm. Men vi lät en tekniker obducera den ena, så att vi kunde skapa fler kablar. Samtidigt skickade vi ut folk till butikerna för att hämta in samtliga enheter på alla sätt vi kunde: med bil, bud och tåg. Vi arbetade dygnet runt - sorterade, märkte upp och installerade uppdateringar och nästa morgon började arbetet med att köra ut dem till butikerna.

Närmare hundra personer arbetade i skift dygnet runt i flera dagar, och framåt fredagen var samtliga enheter återlämnade till butikerna och i drift.

> Incidenten var förstås oväntad, men det är just för oförutsedda händelser det är viktigt att ha färdiga rutiner, säger Anders Holm.

Vi har en checklista för så kallade major incidents, vilken vi snabbt kunde anpassa till den aktuella situationen.

Arbetstoppen var visserligen extrem även med våra mått mätt, men rutinerna gjorde att vi snabbt hade en logistikkedja på plats och kunde arbeta systematiskt för att lösa problemet så snabbt som möjligt.

Planera för det värsta

- Lita aldrig på att systemen alltid kommer att fungera. Ta fram krishanterings-planer i förväg
- Var proaktiv: inventera system och håll hård- och mjukvara i gott skick
- Tänk på hela livscykeln, var medveten om att problemen oftast kommer mot slutet av livslängden
- Investera i övervakning

Incident 2: Virusvarningen som störde ut kassafunktionen

På ett varuhus går det en morgon plötsligt inte att göra dagsavslut. Samtliga transaktioner i kassasystemet avstannar och omsättningen upphör därmed totalt. Ingen vet varför.

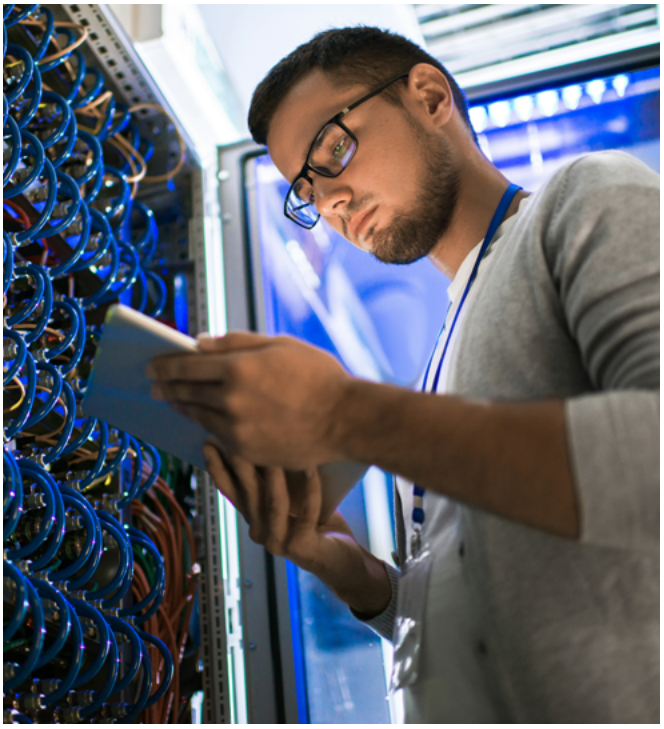
– I vanliga fall fungerar det så att kassan läser till servern, som sorterar och skickar data vidare, berättar Fabian Mogren, VD på Visma EssCom. Men nu stod pengarna still i butiksledet och kom inte vidare.

Virusskydd räcker inte alltid

Vid en närmare undersökning visade det sig att virusskyddet slagit till, vilket orsakade stor oro hos kunden som ville att servern skulle patchas snarast möjligt.

– Vi följde dock vår checklista och drog i handbromsen, säger Fabian Mogren. Vi reagerade på att kundens mjukvarupark var osund. De hade ett gammalt system som drivits med konstgjord andning på ett osupporterat operativsystem.

Kunden hade vid upprepade tillfällen haft problem med virus eftersom utrustningen även användes som arbetsstationer – servrarna hade såväl skärm som tangentbord inkopplade och förmodligen hade fler än en anställd använt datorerna för att kolla sin privata mail. Säkerheten höjdes heller inte av bristfälliga lösenord.



Vid en genomgång av systemet visade det sig att virusskyddet var ett falsklarm: filen med dagsavslutet saknade hashinfo och sattes därför (i och för sig helt korrekt) i karantän.

– Det var ett relativt enkelt problem att åtgärda, säger Fabian Mogren.

> Det farliga i situationen var oron som denna incident skapade hos kunden. Om vi hade förhastat oss och patchat systemet så hade vi dödat hela kedjan med dagsavslut och orsakat stor ekonomisk skada.

Incident 3: Kassasystemen som alltid kraschade punktligt

En rikstäckande butikskedja har ett välfungerande IT-system, där allt fungerar hyggligt. Utom i Jönköping, där något krånglar varje dag. Prisuppdateringar fungerar inte ena dagen, kampanjer uppdateras inte andra dagen. Dagsavslut släpar, hårddiskar skär ihop och belastnings-peakar och dataförluster drabbar ortens butiker mycket oftare än kedjans övriga butiker i resten av landet. Problemen är ett mysterium, eftersom IT-systemen är identiska i samtliga butiker.

– En märklig sak som butiksägaren reagerade på var att all trafik gick igång på morgonen efter att ha stått still hela natten, berättar Anders Holm. I vanliga fall ska kassasystemet uppdateras under natten, men i Jönköping stod det still.

Samtliga kassor gick ner exakt samtidigt

En analys av övervakningsloggarna gav en ledtråd: samtliga kassor i en butik gick ner på sekunden samtidigt. Exakt samma scenario i nästa butik. En tekniker skickades därför ner för att gå igenom sladd efter sladd, och upptäckte snart felet: den lokala elfirman hade kopplat en timer på strömmen till kassorna för att spara energi under natten.

– I en installation av den här komplexiteten är det viktigt att förstå var tidur får eller inte får sitta, säger Anders Holm. Vi har den erfarenheten, men uppenbarligen inte den lokala firman som förstås bara ville väl, men orsakade betydande skador.

> Här visade sig övervakning av systemet vara extremt värdefull eftersom den gav oss de avgörande ledtrådarna som gjorde det möjligt att identifiera felet.

Sammanfattning

Incidenter i IT-miljöer inträffar och ibland kan även relativt enkla orsaker leda till extrema situationer. Det går aldrig att helt skydda sig, men genom att vara medveten om riskerna och planera för oväntade situationer är det möjligt att bygga upp rutiner som kommer att vara till stor hjälp den dag en incident inträffar.

Att kritiskt gå igenom sin IT-miljö och sina rutiner kan dessutom ge värdefull kunskap om potentiella riskområden, och därmed även hjälpa din organisation att avvärja vissa incidenter innan de hunnit inträffa.

Att tänka på

- Resonera tidigt kring hur produkter väntas fungera mot slutet av sin livslängd
- Underskatta inte komplexiteten – att köpa in erfarenhet utifrån kan löna sig många gånger om
- Tänk på utbytesmodeller, reservdelar och alla adaptrar och sladdar som kan behövas och att de finns i tillräckligt antal
- Sätt av pengar för ett nytt projekt när utrustningen kommer att behöva bytas eller uppgraderas
- Fundera på hur övergången ska ske – inte bara tekniskt utan även logistiskt
- Förbered för riskscenarion så beredskapen står i proportion till hur allvarlig en kris skulle bli, inte i proportion till förväntad felfrekvens
- Låt processen ta tid och börja i tid, att behöva göra saker i panik är inte kostnadseffektivt
- Är du på väg att göra en förändring? Köp know-how och spara pengar på sikt. Jämför aktörer på marknaden och se till helheten av lösningen och hur den ska prestera under hela sin livscykel.

Visma hjälper dig hela vägen

Digitaliseringen har medfört att så gott som alla system idag är uppkopplade, och när uppkopplingen inte fungerar blir det ofta en kedjereaktion som orsakar allvarliga problem på flera ställen i kedjan.

– Alla större system idag lider dessutom av ”lapptäckesjukan”, säger Fabian Mogren.

> ”Marknadens krav ökar ständigt och tvingar företag att bygga på med funktioner och till slut har man byggt sig ett plockepinn där ingen vågar röra gamla delar av rädsla för att råka förstöra något.

– I ett sådant läge är det ibland lockande att blunda för riskerna, så länge allt fungerar bra, säger Anders Holm. Problemet är bara att man då är totalt oförberedd på en större incident, och när den väl inträffar blir konsekvenserna onödigt stora.

Större incidenter går aldrig att undvika helt, men övervakning och proaktivt arbete kan leda till snabb och korrekt respons och kapacitet att lösa problemen.

– En inte försumbar del av beredskapen är medvetenheten om att det kan hända något, säger Fabian Mogren. Vår erfarenhet är att utrustning med en livslängd på tre till fem år bjuder på minst två rejäla överraskningar. Har man då inga rutiner eller en färdig checklista kan det ta stopp ordentligt.

– Vår styrka är att vi har lång erfarenhet av krisande system, säger Anders Holm. Vi tar det alltid på allvar men gör inget förhastat, och är duktiga på att lokalisera felen. Vi har färdiga rutiner som vi kan anpassa för den aktuella situationen som låter oss arbeta metodiskt och snabbt.

Vill du veta mer om hur Visma EssCom kan hjälpa din organisation – kontakta oss på 010 - 141 16 00 eller info.esscom@visma.se

Visma EssCom ingår i Vismas CIS-division och är en rikstäckande totalleverantör av teknisk service, support och IT-drift. Vi installerar, driftar och supporterar IT-system för att minimera driftstopp och intäktsbortfall.