

DECERNO WHITEPAPER

Legacy och säkerhet



DECERNO

PART OF ADDNODE GROUP

Legacyssystem slutar sällan att fungera. De slutar att vara säkra.

Så här tar du reda på var ni står
innan ni väljer väg framåt.

Inledning: När skyddet inte hänger med

Det börjar sällan med något dramatiskt. Förr eller senare dyker det upp något i säkerhetsloggen som inte riktigt stämmer. Inloggningsförsök som sticker ut, trafik vid fel tidpunkt, ett mönster som någon reagerar på.

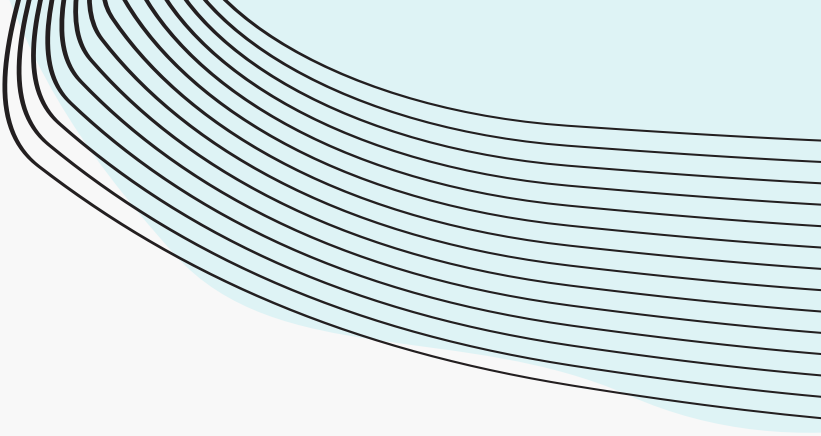
Många organisationer har system som varit i drift länge. De används varje dag och gör fortfarande sitt jobb. Men de får allt glesare med säkerhetsuppdateringar, och ibland inga alls. Ofta handlar det inte ens om ett enda system, utan om flera som åldrats parallellt under samma år.

Ofta går det bra ändå. En händelse reds ut, några personer får lägga annat åt sidan och konsulter kopplas in. Men efteråt finns frågan kvar: vad händer nästa gång? De flesta organisationer känner igen sig i det här. Nästan alla har minst ett system som beskrivningen passar in på.

Legacysystem har blivit enklare att angripa

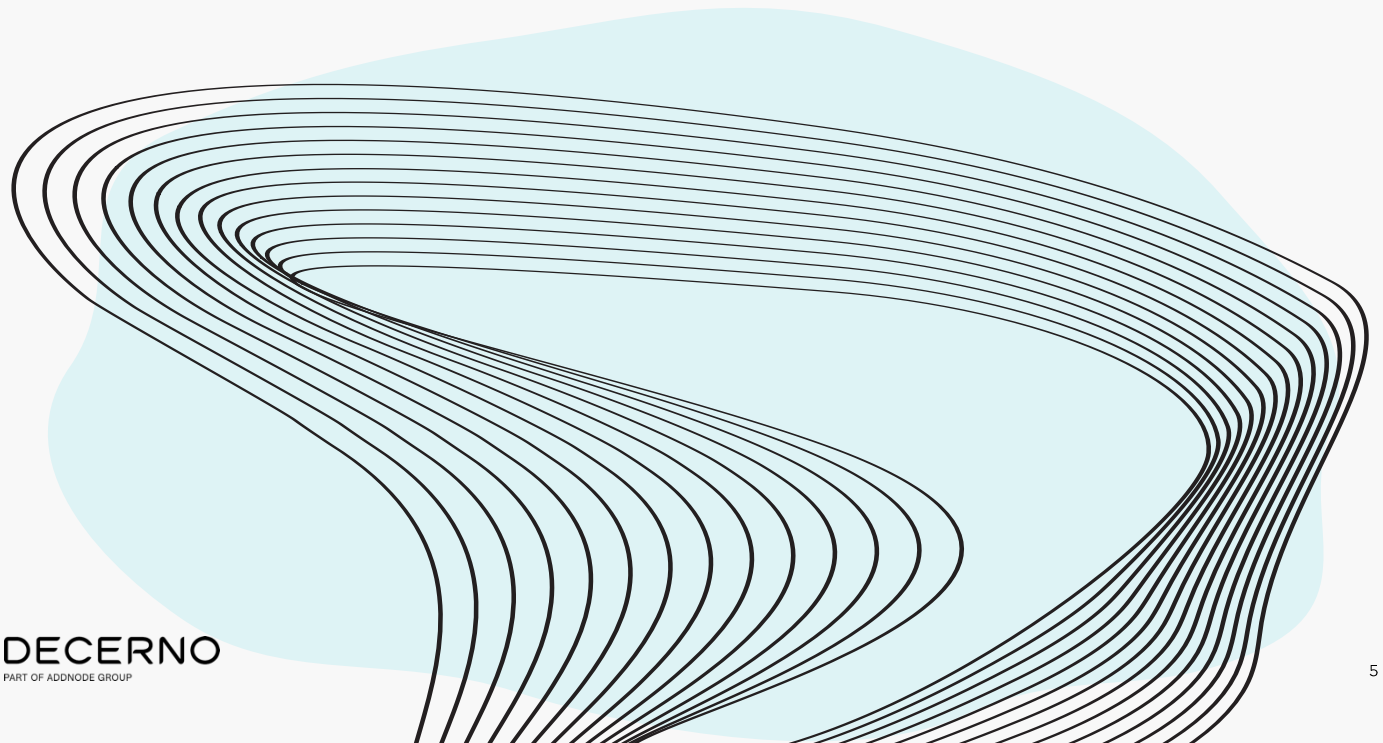
Många legacysystem är inte dåliga system. Tvärtom kan de vara stabila, välkända och djupt anpassade efter verksamheten. Problemet är att omvärlden runt dem har förändrats.

Tekniken är känd, sårbarheterna dokumenterade och ofta finns färdiga angreppsverktyg. När en komponent passerat end-of-life står en känd brist kvar öppen utan utsikt att patchas. Samtidigt är dagens angrepp i hög grad automatiserade och letar brett efter just den sortens exponering. Attackytan behöver alltså inte vara prominent för att hittas, den behöver bara vara igenkännbar.



Till det kommer att många angrepp idag är automatiserade och storskaliga. De letar brett efter system med just den sortens kända brister, oavsett hur känt eller okänt systemet är i övrigt. Ett system behöver alltså inte vara en uppenbar måltavla för att bli hittat. Det räcker att det går att känna igen.

Samtidigt är det sällan enkelt att uppdatera ett legacysystem. En patch kan påverka integrationer, speciallösningar och arbetsflöden som vuxit fram under många år. Därför skjuts uppdateringar ibland på framtiden. Inte för att någon struntar i säkerheten, utan för att varje förändring riskerar att störa något verksamheten är beroende av. I vissa fall finns det inte längre någon patch alls. Det vet angriparna också.



Nya krav gör det svårare att skjuta upp beslutet

Med NIS2 och den svenska cybersäkerhetslagen ökar kraven på många organisationer att arbeta mer systematiskt med risker, incidenter och skydd av verksamhetskritiska system.

Systematiskt betyder i praktiken att man ska ha koll på vilka system som är kritiska, vilka risker som finns kopplade till dem och hur incidenter ska upptäckas och hanteras. Det handlar inte om enstaka insatser, utan om ett arbetssätt som går att följa upp och visa upp.

Det betyder inte att alla legacysystem måste bytas ut direkt. Men det blir svårare att luta sig mot att ”det har ju fungerat hittills”. Skillnaden mot tidigare är att man numera behöver kunna visa att risken är under kontroll, inte bara utgå från att den är det.

För ett system som inte kan patchas, övervakas eller isoleras på ett rimligt sätt behöver det därför finnas en genomtänkt plan för hur risken ska hanteras över tid. Annars blir det svårt att visa att risken är under kontroll, både för den egna ledningen och vid en eventuell granskning.

Fler skyddslager hjälper, men löser inte grundproblemet

Det går att göra mycket runt ett legacysystem. Man kan segmentera nätverket så att systemet ligger mer avskilt, strama åt vem som har åtkomst, förbättra loggningen så att avvikelser syns, sätta upp övervakning och se över integrationerna mot andra system. Ofta är det precis rätt sak att göra, och det sänker risken påtagligt.

Men skyddslager runt systemet ändrar inte hur systemet fungerar inuti. Om systemet i grunden är svårt att uppdatera, om åtkomsten är svår att begränsa eller om varje liten förändring kräver veckor av testning, då finns grundproblemet kvar. Lagren köper tid och minskar risk, men de tar inte bort orsaken.

Då handlar modernisering inte längre bara om teknikskuld, prestanda eller användarupplevelse. Det handlar om säkerhet. Och då behöver man veta tillräckligt om systemet för att kunna avgöra var den gränsen går.

Tre frågor som visar var ni står

Innan ni bestämmer er för en väg framåt är det värt att ställa tre enkla frågor om varje verksamhetskritiskt system.

1

Går det att uppdatera?

Om svaret är nej, eller ”bara med stor möda”, är det i sig en risk värd att notera. Ett system som inte kan föras framåt i kontrollerade steg samlar på sig brister som inte går att täppa till.

2

Vet ni vad som händer om det slås ut?

Beroenden, integrationer och manuella reservrutiner avgör hur allvarligt ett avbrott blir. Ett system som många andra hänger ihop med ger större konsekvenser än ett som står för sig självt.

3

Går det att uppdatera?

Om svaret är nej, eller ”bara med stor möda”, är det i sig en risk värd att notera. Ett system som inte kan föras framåt i kontrollerade steg samlar på sig brister som inte går att täppa till.

Svaren ger en första bild av var de största sårbarheterna finns, och var det brådskar mest. De flesta organisationer upptäcker att riskerna inte är jämnt fördelade, några få system står för största delen av exponeringen.

Tre vägar framåt - och de utesluter inte varandra

När läget är klarlagt finns det sällan bara en möjlig väg. Tre alternativ återkommer ofta, och de utesluter inte varandra. Olika delar av samma system kan hanteras på olika sätt.

Kapsla in. Systemet får leva vidare, men isoleras och skyddas bättre. Passar när systemet fortfarande gör sitt jobb väl och ett byte vore dyrt eller riskabelt, men exponeringen behöver minska.

Byta ut. Den del som bär störst risk eller kostnad ersätts. Passar när grundproblemet inte går att skydda sig ur, eller när underhållet ändå blivit så tungt att det bär kostnaden av en modernisering.

Integrera bättre. Kopplingarna mot andra system byggs om så att de blir säkrare och enklare att underhålla. Passar när själva systemet kan behållas men dess sätt att prata med omvärlden är en del av problemet.

Vilken väg som passar avgörs av hur kritiskt systemet är, hur stor risken är och vad en förändring kostar i tid och störning. Därför kommer valet först, efter att läget är förstått.

Börja med att förstå läget

Alla system behöver inte bytas ut. Första steget behöver därför inte vara ett stort moderniseringsprojekt. Det kan vara att förstå läget: vad är mest sårbart, vilka beroenden finns och vad går att förändra utan onödig risk?

En tydlig lägesbild gör det lättare att prioritera. Den visar vad som kan vänta, vad som bör åtgärdas snart och vad som faktiskt kräver en större insats. Och den gör det möjligt att fatta beslut på fakta i stället för magkänsla, vilket både sänker risken och gör det lättare att försvara prioriteringarna inför ledning och vid granskning.

Kort sammanfattning

Legacysystem är ofta stabila och välfungerande, men har blivit svårare att skydda i takt med att omvärlden förändrats.

Det viktigaste att ta med sig:

- Kända sårbarheter och uteblivna patchar gör legacysystem till en växande säkerhetsrisk.
- NIS2 och cybersäkerhetslagen gör det svårare att skjuta moderniseringen på framtiden.
- Skyddslager runt systemet hjälper, men löser inte ett grundproblem i själva systemet.
- Det finns flera vägar framåt: kapsla in, byta ut eller integrera bättre.
- Rätt första steg är oftast att förstå läget, inte att starta ett stort projekt.

Nästa steg - vi hjälper er att förstå säkerhetsläget

Decerno hjälper organisationer att modernisera legacysystem på ett kontrollerat sätt, med säkerheten i fokus. Med erfarenhet från offentliga och privata verksamheter skapar vi tydliga planer som omsätter risk till handling.

Vill ni veta om ert system går att modernisera på ett kontrollerat sätt? Vi erbjuder ett kostnadsfritt migrerbarhetstest under NDA, där vi tittar på systemets tekniska förutsättningar, beroenden och möjliga vägar framåt.

Läs mer om hur vi arbetar med legacy-modernisering, boka en genomgång på decerno.se, eller hör av er direkt till Viktor.

Viktor Hellman
viktor.hellman@decerno.se
076 - 506 35 09
www.decerno.se

