Article
Tio saker att tänka på när man väljer passersystem

DETEKTOR - NR 2 - 2021

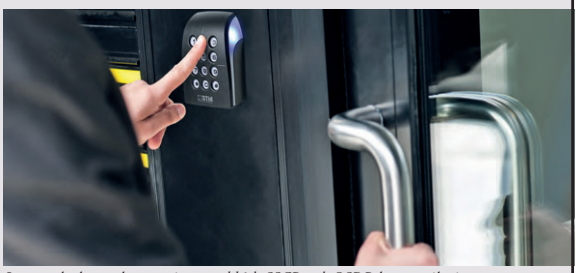
tema: id-hantering & passerkontroll

Robert Jansson, Stid Security:

Tio saker att tänka på när man väljer passersystem

Att välja passersystem är kanske inte alltid så lätt. Robert Jansson är med över 20 år i branschen en expert som gärna delar med sig av sin erfarenhet. Sedan 2019 är han försäljningsdirektör för Stid i Norden och i Österuropa.

I den här artikeln ger han tio råd om saker man tänka på när man väljer passersystem.



Läsaren ska kunna kommunicera med både SSCP- och OSDP-kommunikationsstandarderna.

1: Se passersystemet som ett säkerhetssystem.

Det kan verka självklart att man ska se passersystemet som ett säkerhetssystem, men det är idag lätt att avledas av en massa funktioner under processens gång. Så därför tycker jag man inititalt ska ställa sig följande frågor:

- Vilka behov har vi?
- Metodiken – hur ska vi nå målen?
- Vilkas resurser krävs för att nå målen?

Med svaren på dessa frågor som ledstjärna i upphandlingsprocessen reduceras risken för att lockas köpa fel lösning avsevärt. Då slipper du att hamna fel, exempelvis genom att låta installera ett proprietärt system eller en lösning med för låg säkerhet.

2: Välj tillverkare från den ”fria världen”

Undvik system från länder med ett autokratiskt styrelseskick. På senare år har vi sett exempel på hur sårbara säkerhetssystem kan vara när producenter från diktaturer direkt eller indirekt adderat bakdörrar till komponenter eller system. Statsunderstödda cyberattacker är vardag och inget hindrar den här typen av länder från att använda bakdörrar i exempelvis läsare i syfte att komma åt viktig information.

3: Tänk hållbarhet och etiska hänsyn.

Klimatfrågan är het och hållbarhet blir allt viktigare, inte minst i våra val av produkter. Men även etik när det gäller under vilka förhållanden produkterna har tillverkats bör finnas med i vågskålen.

4: Välj öppen teknologi

Systemet ska ha ett öppet API, helst utan massiva kostnader eller att det är gratis att ansluta till system som HR eller LDAP för att möjliggöra identitetshantering från ett överordnat system och länka fysisk tillträdeskontroll till ett digitalt passersystem.

5: Kompatibilitet

Systemet ska vara kompatibelt med fler än en extern leverantörs kontrollenheter och kunna anslutas med öppna standarder som TCP/IP eller öppen källkod, exempelvis RS485 och kryptering ska ske via öppna standarder som AES.

6: Säkra öppna kommunikationsprotokoll

Undercentralerna ska kunna använda olika kommunikationsprotokoll som den äldre amerikanska ”halvöppna” OSDP från SIA eller ännu hellre den nyare och totalt öppna europeiska SSCP från SPAC. Eftersom kryptering från kontrollenheten och ner till läsare är viktig rekommenderar jag starkt SSCP då den bara fungerar om krypteringen är påslagen. I OSDP kan det hända att den lämnas avstängd och det är lätt att missa att kontrollera som slutanvändare. Därför är ett kommunikationsprotokoll som inte kan fungera i okrypterat läge att föredra.

7: Läsarna och säkerheten

Läsaren ska kunna kommunicera med både SSCP- och OSDP-kommunikationsstandarderna för att se till att du som användare är fri att byta kontrollenhet över tid och inte begränsas av det faktum att din kontrollenhet endast kan stödja antingen OSDP eller SSCP. Läsarna ska också vara utrustade med funktionen ”transparent mode” som är den högsta säkerhetsstandarden där inga nycklar lagras i läsarna men där kontrollenheten kommunicerar transparent genom läsaren med crypto-token i användarens hand. Läsaren ska också kunna uppdateras för nya referensmodeller framöver. Som ett minimum idag ska den läsa både Desfire EV3 och mobil-ID från olika leverantörer med ”Desfire-liknande” säkerhet.

8: Välj framtidssäkert

När man väljer kort/identitetsbärare bör man eftersträva den senaste tekniken där endast öppna standarder används och där inter-operabilitet är en del av infrastrukturen. Ett riktigt öppet teknologikort är ett kort som kan erhållas av många leverantörer/tillverkare och där priset och tillgängligheten inte kontrolleras av en enda leverantör/tillverkare. Välj teknik som används av statliga myndigheter och stora företag världen över. Nyckeln till tillförlitlighet är att välja en kortteknik. En huvudregel är att välja en betrodd gemensam kriterienivå på EAL5 + eller ännu högre på en öppen plattform. Var skeptisk till patenterade kortteknologier som låser in dig i en lösning. Kom ihåg att du kommer att leva med ditt system under mycket lång tid med behov av nya funktioner. Enligt min personliga syn är det bästa alternativet idag att hålla öppet för framtiden med en pålitlig teknik och därför välja Desfire EV3.

9: Läsare för alla

Se till att läsarna är enkla att använda även för personer med nedsatt syn eller med annan funktionsnedsättning. Bakgrundsbelyst knappsats och möjligheter till avläsning på distans är fördelar då det underlättar för exempelvis rullstolsburna personer. Om möjligt välj en produkt som har ett godkännade från någon organsation för funktionsnedsatta inom EU, typ Unadev.

10: Vandalsäkra och vädertåliga läsare

Läsarna behöver tåla alla slags väder och andra förhållanden över tid. Kräv livstidsgaranti och se till att de har ett certifierat vandalskydd i nivå IK10. Läsare med knappsats ska ha IK8 på knappsatsläsare. Kräv också IP65-klassning för att säkerställa att läsaren fungerar under alla väderförhållanden och att de klarar temperaturer ner till -30 eller lägre.

Kontenta: Av alla punkter är den första den allra viktigaste. Det är den som övriga punkter styrs av. Se passersystemet som ett säkerhetssystem. Tänk säkerhet i alla lägen, både teknisk och drift, i såväl det korta som det långa perspektivet. Då skapar du förutsättningarna för ett bra val av passersystem.