Article

Öppna passersystem – en nödvändighet för ett säkrare skydd...

DETEKTOR - NR 1 - 2021

Robert Jansson, Stid Security:

Öppna passersystem – en nöd

Kan något annat än öppna passerkontrollsystem verkligen säkra det du försöker skydda? Frågan kommer från Robert Jansson, försäljningschef för Nordics och Österuropa på Stid Security. I den här artikeln förklarar han varför han tycker det är så viktigt att använda säkerhetssystem baserat på öppna plattformar och hur man skyddar systemen.

Artikelförfattaren Robert Jansson ser det som en nödvändig säkerhetsåtgärd att välja passersystem som baseras på öppen teknik.

Företag och organisationer runt om i världen spenderar miljoner varje år på passerkontrollsystem. De flesta av dessa köpare köper ett eller kanske två stora passerskontrollsystem under hela sin yrkeskarriär. Så när kunder är redo att spendera pengarna för att säkra sina lokaler är de kravspecifikationer som de använder i sina upphandlingsdokument ofta de som rekommenderas av konsultföretag.

Mitt arbete handlar om att uppmärksamma människor om vikten av ett tätt kontrollerat passersystem och hur man kan se till att systemet gör vad det byggdes för att göra. Det vill säga att låta rätt personer komma in och hålla bort fel personer. Enligt min erfarenhet är många av misstagen som görs faktiskt inbyggda i systemen, och det gör dem extremt svåra att fixa när de identifieras senare.

I de flesta fall har ett passersystem en fyra-nivåers arkitektur:

• En programvara med en databas, lokalt och eller i molnet, för att hantera människor med kalendrar, tidscheman och behörigheter.

• En kontrollernivå där ett autonomt liv utan koppling till överordnad programvara säkras och dit underliggande nivå av läsare kopplas.

• En läsarnivå som ansluts till överordnad kontrollernivå och i vilken personer som skall passera identifierar sig med kort, bricka eller i moderna system en mobiltelefon.

• En identitietsbärare i form av ett kort, tagg eller virtuellt kort i vilken personligt knuten information matchas i systemet med kalender, tid och behörigheter.

Properitära system – fortfarande ett problem

För 20–30 år sedan var marknaden extremt fragmenterad och i princip byggdes alla system från en enda leverantör på alla eller de flesta nivåer nämnda ovan. Så när du väl hade installerat systemet var du låst för den leverantören för systemets livslängd, och livet var, och är fortfarande mycket längre än systemets förväntade säkra livslängd. Problemet med properitära system kvarstår trots att det finns en stark trend mot öppna plattformar. Omvandlingen sker långsamt och kunderna betalar priset. Tänk dig att du köper en bil och att du är tvungen att köpa alla däck och bensin från en leverantör som kontrollerar pris och kvalitet så länge du äger bilen. Vem skulle göra det? Det är faktiskt vad du gör när du köper ett properitärt system där du inte kan uppdatera någon, eller för den delen, någon av de ovan nämnda nivåerna av arkitektur individuellt. Du bör till exempel kunna välja läsare eller kortteknologier från en rad olika leverantörer över tid. Detta är helt nödvändigt för att man skall kunna möta de risker och hot som man vet kommer att komma men inte exakt hur de kommer att se ut.

> ***”Mitt arbete handlar om att uppmärksamma människor om vikten av ett tätt kontrollerat passersystem och hur man kan se till att systemet gör vad det byggdes för att göra.”***

Uppgraderingsbar säkerhet nödvändig

Den som vill åt vad du skyddar bakom passersystemet kommer alltid att försöka komma åt det på enklaste sätt. Varför bryta upp dörren om man bara kan gå rätt igenom utan detektion?

Du skulle inte ha ett kostsamt passersystem om det inte fanns något att skydda så dina tillgångar är det värde som tjuven är intresserad av. Generellt sett är inkräktaren idag inte beväpnad med en kofot, utan med mycket sofistikerade verktyg för att digitalt bryta sig in i ditt system,

Article
Öppna passersystem – en nödvändighet för ett säkrare skydd...

DETEKTOR - NR 1 - 2021

ändighet för ett säkrare skydd

eventuellt utan att lämna spår. Denna verktygslåda växer varje dag och ett passerkontrollsystem måste kunna möta dessa nya hot och denna verktygslåda i samma takt.

Grundläggande säkerhet – överge lösenordskydd

De flesta läsare av den här artikeln vet att det är osäkert att använda ett användarnamn och lösenord för att logga in på ett säkerhetssystem. Men de gör det fortfarande. Därför är det första steget att stänga den öppna dörren ordentligt i säkerhetssystemet genom att använda sig av tvåfaktorsinlogging. Detta är utan tvekan den enklaste delen att ta itu med och kan göras med öppna standarder tillsammans med din IT-avdelning.

Kontroller – kompatibilitetskrav

På den andra nivån finns kontrollerheterna, och jag skulle se till att de överliggande mjukvarusystemen kan fungera med minst tre olika kontrollertillverkare och helst samtidigt. Utvecklingen och konkurrensen för att hålla, transportera och hantera dina identitetsdata säkert utvecklas ständigt, så vid varje given tidpunkt bör du kunna använda det senaste och säkraste produktvalet.

> ***”Tänk dig att du köper en bil och att du är tvungen att köpa alla däck och bensin från en leverantör som kontrollerar pris och kvalitet så länge du äger bilen. Vem skulle göra det?”***

Säkert protokoll med öppen källkod

Kortläsarna som ansluter till din kontrollernivå bör också vara öppna men säkra. Av denna anledning finns det en uppsättning säkra protokoll med öppen källkod att använda. De flesta tillverkare av kontroller och läsare använder dem som standard idag. Amerikanska OSDP (Open Supervised Device Protocol) listat av SIA och Europeiska SSCP (Smart Secure Communication Protocol) är två av de vanligaste säkra protokollen mellan styrenhet och läsare som också tillhandahåller fjärruppdateringar både med öppen, standard, AES-kryptering, för att skydda dataflödet från läsarna till styrenheterna.

GDPR-kompabilitet

Idag lägger regeringar, särskilt sedan GDPR blev lag i EU, allt mer tryck på att hålla flödet av personuppgifter, ofta i kringutrustning som kortläsare, säkra. Säkerhet på alla nivåer upprätthålls med hjälp av kryptering och nyckelhantering. Men hur säkert och var ska du lagra nycklarna för att vara GDPR-kompatibel? Jag rekommenderar starkt att du aldrig går under de vanliga kriterierna EAL5 + i nyckellagring av kringutrustning, till exempel i kortläsare som normalt är installerade åtminstone delvis i perimeterskyddet utanför det du vill skydda.

Inga nycklar lagras i läsarna

Jag skulle också titta på att använda så kallat “transparent mode” där inga nycklar lagras i läsarna alls utan passerkortet kommunicerar transparent genom läsaren med kontrollenheten. Se till att du som slutanvändare har full kontroll över säkerheten på alla nivåer och att du kan få tag i kortläsarprodukter för att passa dina styrenheter ovan i systemet, liksom passerkorten nedan, från många olika leverantörer.

Läsaren bör vara utformad på så sätt att den inte på något sätt låser dig i properitära teknologier. Och de bör alltid vara redo att uppdateras för att använda den senaste tillgängliga teknologin. Ett säkert val av en ”defacto” -standard på kort bör vara NXP Desfire-familjen nu vid evolution 3.

Använd Desfire

Desfire används i stor utsträckning över hela världen och är betrott på grund av det faktum att den bygger på öppna standarder. Utöver detta ser vi fördelar av många anledningar som säkerhet, flexibilitet men också enorma kostnadsbesparingar med en rörelse mot virtuella kort. De flesta anställda är idag utrustade med smarta telefoner med antingen ett PIN-kodlås eller i de flesta fall biometriska lås – så om du kan – gör så att det virtuella högsäkerhetskortet bara kommer att kännas igen i kortläsaren om du har låst upp det med en PIN-kod eller en biometrisk mall. Dessa kort kan normalt återkallas från användarnas telefoner antingen av offline-lösningar och/eller mer flexibla online-lösningar.

Virtuella kort kan i de flesta fall fungera parallellt med vanliga högsäkerhetskort i läsarna och detta är en viktig faktor eftersom övergången från kort till mobila ID:s kan ta tid.

> ***”Låt dig aldrig kidnappas av föråldrad, properietär eller patenterad teknik. ”***

Slutsatserna i korthet

För att avsluta detta, använd två- eller trefaktorautentisering för att både logga in som användare till säkerhetssystemet som styr från en till tusentals dörrar. Använd aldrig användarnamn och lösenord i några säkerhetssystem.

Använd öppen källkod och försök om möjligt att göra detta med kvalificerade certifikat för att säkerställa användarnas integritet och giltigheten hos loggfilerna. Slå på kryptering mellan systemet och systemenheterna och lita aldrig på en properitär kryptering. Använd en läsare som är öppen och säker både uppåt mot systemet och nedåt mot de säkra kodbärarna i form av kort, taggar eller virtuella kort i telefoner och låt den senaste tekniken i varje tid och tillfälle skydda dig och dina tillgångar över tid. Och slutligen, låt dig aldrig kidnappas av föråldrad, properitär eller patenterad teknik. Öppna passersystem är en nödvändighet för ett säkrare skydd.

Robert Jansson,
Försäljningschef för Nordics och Österuropa på Stid Security.