Is mijn toegangs-controle systeem veilig?

ADI krijgt regelmatig de vraag: is mijn toegangscontrole systeem veilig? Hieronder beschrijven wij enkele punten die u kunt gebruiken om uw systeem nog veiliger te maken.

Kaarten en kaartlezers

Een kaart wordt gebruikt als codedrager waarmee een persoon zich identificeert bij een deur(kaartlezer) of apparaat. Er zijn veel verschillende kaartprotocollen in omloop, sommige hebben een zwakke of geen encryptie. Kaarten zonder of met een zwakke encryptie kunnen eenvoudig te kopiëren zijn waardoor kwaadwillende personen zichzelf toegang kunnen verschaffen.

Er zijn verschillende kaarten met verschillende encryptie niveaus te verkrijgen. Momenteel zijn MIFARE DESFire EV2 en HID SEOS de best beveiligde kaarten, beide met een 128 bits AES encryptie.

OSDP

OSDP is een communicatie protocol dat apparaten zoals kaartlezers en deurcontrollers met elkaar laat communiceren. Het voorziet de industrie van een oplossing die verder gaat dan het conventionele Wiegand protocol en voegt hoogwaardige toepassingen toe zoals bi-directionele communicatie. Het OSDP protocol maakt gebruik van de AES-128 encryptie over een RS-485 communicatielijn. Hierdoor is het haast onmogelijk geworden om via de bekabeling bruikbare data te kunnen onderscheppen.

Biometrie

U kunt voor extra veiligheid gebruik maken van biometrie. Een vingerafdruk is per persoon uniek en kan gebruikt worden voor toegangscontrole.

PIN codes

Voor extra veiligheid kunt u gebruik maken van 2 factor authenticatie. Een goed voorbeeld hiervan is een keypad met een ingebouwde kaartlezer. De persoon krijgt pas toegang na het aanbieden van een geldige kaart (iets wat ik heb) en het aanbieden van een PIN code (iets wat ik weet). De kaart is waardeloos zonder het weten van de bijbehorende PIN code. Deze werkingmode kunt u ook tijd gestuurd instellen, zo kunt u bijvoorbeeld 's nachts kaart + PIN gebruiken en overdag enkel kaart.

Sloten en deuren

Het volgende punt in de beveiliging is het kiezen van het juiste hang- en sluitwerk.

Controleer altijd of het type deur geschikt is voor de situatie waar het in gebruikt wordt, een boarddeur kan eenvoudig gesaboteerd worden en is bijvoorbeeld niet geschikt voor een laboratorium of wapenkamer.

Kies altijd voor een goede kwaliteit elektrische sluitplaat voor binnendeuren of een elektromechanische meerpuntssluiting voor buitendeuren.

Zorg ervoor dat het overige hang- en sluitwerk van goede kwaliteit is, denk hierbij aan scharnieren, cilinders,

en beslag en zorg ervoor dat dit SKG gekeurd is voor buitendeuren.

Let op dat vluchtdeuren bij een calamiteit eenvoudig te ontgrendelen zijn (Fail safe). Houdt u hierbij aan de in uw regio geldende wetten voor brandveiligheid.

Elektronische deurbeslagen

Hou er bij het gebruik van een elektronisch deurbeslag rekening mee dat dit geen high security oplossing is, het deurbeslag vergrendelt alleen de dagschoot. Daarnaast is er geen deurstand signalering aanwezig op een elektronisch deurbeslag waardoor een deurgeforceerd melding niet getoond wordt in de software.

Wanneer u elektronische deurbeslagen gebruikt adviseren wij slotkasten met een anti flipper beveiliging te gebruiken om te voorkomen dat de deur met een bankpas open gemaakt kan worden. Zo kunt u ook met een deurbeslag een veilige oplossing bieden.

Deurcontacten

Toegangscontrole is ervoor bedoeld om te bepalen wie er wanneer toegang heeft tot een deur, als de deur open blijft staan door een brandblusser tegen de deur te zetten heeft heel het toegangscontrole systeem geen nut.Een deurcontact is een magneet contact dat vaak op of in de deur gemonteerd wordt en geeft de mogelijkheid om te monitoren of de deur open of dicht is. Wanneer u deurcontacten plaatst kunt u gebruikmaken van de volgende functies:

- Deur te lang open alarmen
- Deur geforceerd alarmen
- Deurstand signalering
- Betrouwbare aanwezigheid rapporten
- Betrouwbare werking anti-bassback

Software opties

Wanneer de hardware en de opbouw van het systeem voldoet aan de veiligheidseisen is het belangrijk om de juiste software functies te gebruiken voor extra veiligheid.

Anti-passback

Anti-passback zorgt ervoor dat wanneer een gebruiker zijn kaart doorgeeft aan een ongeautoriseerde gebruiker de kaart geweigerd zal worden, de gebruiker is namelijk al binnen. Anti-passback zorgt voor een extra laag veiligheid, maar zal niet voorkomen dat ongeautoriseerde gebruikers mee kunnen lopen wanneer de deur open is.

Door gebruik van deurcontacten zorgt u ervoor dat de anti-passback altijd op de juiste manier functioneert. Wanneer u uw pas aanbiedt bij de deur maar de deur niet opent zal u nog in het buitengebied blijven waardoor u alsnog naar binnen kunt.

Procedures en audits

Wanneer het systeem geplaatst is bij de klant en voldoet aan zijn wens, is het belangrijk om ook de juiste procedures te gebruiken. Er kan veel tijd en energie in de bovenstaande oplossingen gestoken worden, maar als een verloren of gestolen kaart in het systeem blijft staan heeft zelfs de sterkst beveiligde kaart geen nut.

Autorisatie en rechten

Wees zorgvuldig bij het aanmaken van autorisaties en gebruikers, controleer goed of gebruikers toegang nodig hebben tot de ruimte in een autorisatie. Personeelszaken heeft bijvoorbeeld weinig te zoeken in een serverruimte.

Wat gebeurt er wanneer iemand uit dienst treedt? Of wanneer een gebruiker een andere functie krijgt binnen een bedrijf? Pas de autorisaties aan waar nodig of verwijder een gebruiker bij het uit dienst treden, om onrechtmatige toegang te voorkomen. Wanneer er veel tijdelijk personeel werkzaam is of er veel personeel wissel is, adviseer dan om een integratie met een personeelsdatabase of CRM systeem te gebruiken, hierdoor worden kaarten meteen geblokkeerd wanneer iemand het bedrijf verlaat.

Houdt bij wie rechten heeft tot de software en zorg ervoor dat ze ook de juiste systeembeheerder rechten hebben.

Audits en onderhoud

Adviseer de klant om maandelijkse security audits uit te voeren, hiermee controleert u maandelijks uw systeem en zorgt u ervoor dat het systeem ook in de toekomst veilig blijft.Controleer bijvoorbeeld de rechten van gebruikers, staan er nog kaarten in van gebruikers die het bedrijf hebben verlaten? Ziet u alarm meldingen in het systeem die kunnen duiden op misbruik of een storing in het systeem?

Laat uw systeem ook regelmatig onderhouden, sloten en deuren kunnen naar verloop van tijd misschien minder goed sluiten, regelmatig onderhoud kan dit voorkomen. Ook de noodstroomaccu's hebben onderhoud nodig.

Procedures

Schrijf goede procedures over hoe bepaalde handelingen in het systeem uitgevoerd dienen te worden of wat te doen bij een calamiteit. Informeer uw personeel over de verantwoordelijkheden en gebruik van het systeem. Spreek mensen erop aan als ze een brandblusser gebruiken om de deur open te laten staan.

Zoals u hierboven gelezen heeft zijn er een aantal punten waar u rekening mee dient te houden wanneer uw klant vragen heeft over de veiligheid. Eén van deze punten toepassen op uw toegangscontrole systeem maakt het nog niet veilig.