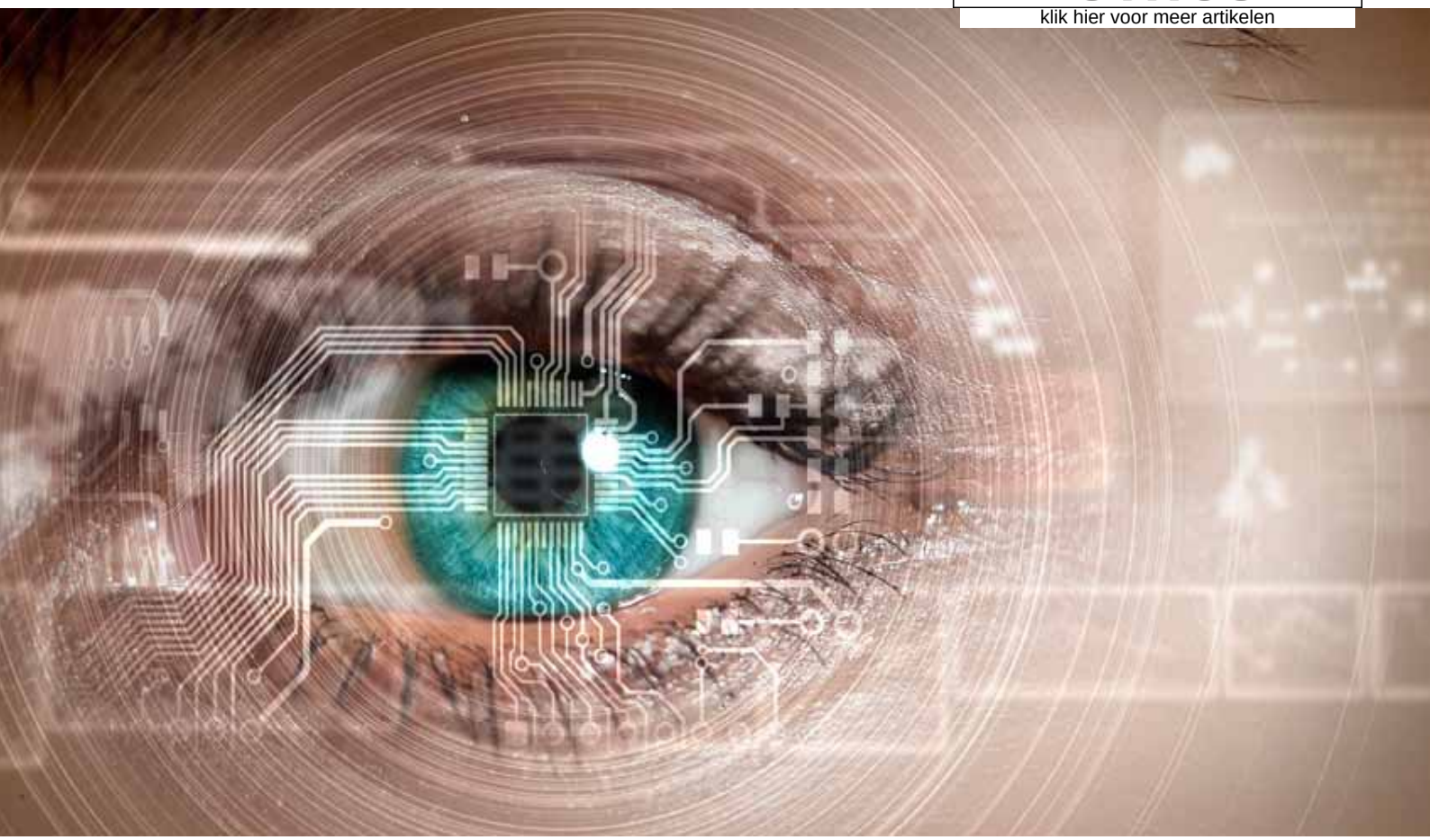

Beveilig de beveiliging

Bij het betrekken van een pand wordt gewoonlijk ook gekeken naar de beveiliging ervan. In de praktijk blijkt dat als een beveiligingssysteem eenmaal is geïnstalleerd, er niet meer naar wordt omgekeken. Maar de technologie ontwikkelt zich verder, en op een gegeven moment is het huidige beveiligingssysteem niet meer effectief, want verouderd. Daarom is een periodiek onderzoek van het systeem en de daarbij behorende processen (zoals het beleid) niet alleen geen overbodige luxe, maar zelfs noodzaak.

Een jaarlijks onderzoek van het beveiligingssysteem moet bijvoorbeeld controleren of de diverse lagen van het systeem (inbraakalarm en bewegingssensors, bijvoorbeeld) nog goed op elkaar aansluiten. Bij het onderzoek moeten alle belanghebbenden worden betrokken: de eigenaar van het pand, de systeemleverancier, de installateur en de eindgebruiker.

Veilige communicatie

De individuele componenten van een toegangscontrolesysteem moeten met elkaar communiceren. Standaard onderdelen van die communicatie zijn onder meer card-gebruiksgegevens, gegevens met betrekking tot het ontsluiten van deuren, gegevens met betrekking tot het controleren van het procespad, veranderingen in de privileges van de cardhouder, enzovoort. Het is daarom van groot belang dat deze uitwisseling van informatie van de communicatie-media op twee manieren wordt beveiligd: zowel het feitelijke communicatie-medium (bedraad of draadloos) als de gegevens moeten worden beveiligd.

Als de communicatie plaatsvindt via draden, kan uit diverse methoden, interfaces en protocollen worden gekozen. Het meest bekende (en feitelijk de industrie standaard) is het Wiegand-protocol. Reden waarom dit zo populair is, is dat het algemeen

wordt ondersteund door vrijwel alle producenten van readers en bedieningspanelen. Meer moderne communicatiemethodes zoals RS485 en TCP/IP bieden meer veiligheid en zijn daarom te prefereren.

Bedrading

Als een kwaadwillende toegang kan krijgen tot de bedrading die wordt gebruikt voor de communicatie tussen de reader en het invoeritem, kunnen berichten worden onderschept. Dit zou kunnen leiden tot een verlies aan privacy, maar ook dat een onderschept bericht kan worden herhaald en een deur kan worden geopend. Het zou tevens mogelijk zijn om ook gewoon een 'ontsluit' bericht te sturen. Daarom is een beveiligd protocol belangrijk, waarbij in het ideale geval gebruik wordt gemaakt van a/ tweezijdige authenticatie om ervoor te zorgen dat elk apparaat het andere apparaat vertrouwt, b/ encryptie, en c/ bescherming tegen het herhalen van onderschepte berichten.
Het kan een open deur lijken, maar zorg er ook voor dat de bedrading van het beveiligingssysteem afgeschermd is tegen ongeoorloofde praktijken: leg ze in speciale goten en zorg dat ze moeilijk te identificeren zijn. Dus bundel ze samen met andere kabels die ook door die goten lopen. Let wel op dat, in sommige gevallen, het plaatsen van de voedingskabels (stroom) bij de kabels van de communicatie van gegevens niet wenselijk is vanwege storingen. Logisch is dat met name de cardreaders aan de randen van het bedrijfsterrein of bij de ingang van het bedrijfspand extra beschermd moeten zijn. Tevens dienen de aansluitingen zodanig te zijn beveiligd dat het niet mogelijk is om stekers los te trekken of klemmen te verwijderen. Hiervoor zijn speciale voorzieningen op de markt, zoals krimpfolie die over de aansluitingen kan worden aangebracht.
Daarnaast kunnen cardreaders en andere componenten extra worden beveiligd door toepassing op de panelen van speciale schroeven/bouten, die alleen met speciaal gereedschap kunnen worden verwijderd. Het kan overigens geen kwaad om bij een inspectie van het gehele beveiligingssysteem ook de panelen te controleren op beschadigingen die kunnen duiden op poging tot inbraak.

Antipassback

Een andere manier om de beveiliging naar een hoger plan te trekken is het zodanig programmeren van de software van de toegangscontrolesystemen dat er geen toegang wordt verleend aan een persoon (cardhouder) die volgens het systeem al in het gebouw aanwezig is. Deze functie, ook wel 'antipassback' genoemd, is geïntegreerd in veel toegangscontrolesystemen. Let wel op dat als deze functie aanwezig is, er twee readers nodig zijn bij de deur: een 'in' reader en een 'uit' reader. Een bijkomend voordeel van het 'antipassback' systeem is dat het voorkomt dat gebruikers hun card gebruiken om meerdere personen in één keer binnen te laten, het zogenoemde 'tailgating'.

Gebruik meerdere identificatie-systemen

Het gebruik van meerdere identificatiemiddelen is een verdere garantie dat degene die de card bij een reader aanbiedt ook de rechtmatige gebruiker is van die card. De authenticatie vindt dan in het ideale geval plaats via iets dat je hebt (bijvoorbeeld een card), iets dat je weet (zoals een wachtwoord) en iets dat je bent (een biometrisch item zoals vingerafdruk of irisherkenning). Dit ideale geval kan voor sommige organisaties wat teveel zijn, maar een combinatie van twee componenten zoals een card en een wachtwoord kan al voldoende effectief zijn. Hiervoor is een reader benodigd die zowel de card kan lezen als waarop het wachtwoord kan worden ingetypt. Deze zogeheten keypad readers zijn ideale oplossingen voor situaties waar aanvullende lagen van beveiliging nodig zijn, zoals een laboratorium binnen een pand: de card geeft dan toegang tot het gebouw, maar alleen de combinatie card-wachtwoord geeft toegang tot het laboratorium.
Een keypad reader zorgt er ook voor dat een card die iemand kwijt is geraakt, niet door een ander kan worden misbruikt om toegang te krijgen tot een 'restricted area'. Dat wachtwoord moet wel regelmatig worden gewisseld, om te voorkomen dat het na verloop van tijd om een of andere reden bekend raakt bij kwaadwillenden. Let wel op dat bij sommige systemen het wachtwoord in de card zelf wordt opgeslagen. Dat werkt wel wanneer de card-technologie veilig is, maar het is beter om het wachtwoord in het systeem zelf op te slaan.

Het gebruik van biometrische readers om ervoor te zorgen dat de persoon die de card aanbiedt dezelfde persoon is aan wie de card is verstrekt, kan worden toegepast in omgevingen waar een nog hoger niveau van beveiliging noodzakelijk is. Nog veiliger is het om een biometrische authenticatie vooraf te laten gaan aan een mechanische (card), eventueel weer in combinatie met een wachtwoord/code. Toegegeven, dit wordt wel erg gecompliceerd en kan tot opstoppingen leiden bij de ingang van een complex. Een alternatief is dan om deze 'triple combination' alleen te gebruiken voor de meest bedrijfskritische afdelingen, of alleen buiten de gewone kantooruren waar het risico van ongeoorloofde toegang het hoogst is, of wanneer er een verhoogd risico is op inbraak (denk aan bedrijfsspionage).

Tips voor het gebruik van cards

Voor een veilig gebruik van identificatie-cards gelden de volgende tips:
- verloren cards dienen direct te worden gedeactiveerd in het systeem.
- op de zwarte markt zijn cards te koop: zorg voor een systeem dat alleen de 'eigen' cards valideert.
- als een illegale card wordt aangeboden, moet het systeem direct alarm slaan.
- elk alarm moet worden opgevolgd en elke onregelmatigheid onderzocht.

- trap niet in het verkooppraatje van alternatieve aanbieders dat hun cards goedkoper zijn en net zo goed werken als de (waarschijnlijk) duurdere van de systeemproducent.
- gebruik geen contactloze cardreaders die alleen werken op het serienummer op de smartcard (CSN-readers). De techniek is er niet voor niets in geïntegreerd. Het gebruik van een CSN-reader voor een smartcard is hetzelfde als het plaatsen van een hoogwaardige reader op een glazen deur.
- de gebruiker moet zijn card niet prominent dragen als hij of zij zich buiten het complex bevindt.
- let op als mensen zogenaamd per ongeluk tegen je aan botsen: er bestaan elektronische apparaatjes die de gegevens van je smartcard kunnen lezen en kopiëren (het zogeheten 'bump and clone'). Denk aan het skimmen van bankpasjes, dat werkt op dezelfde manier. Er bestaan RFID-beschermende hoesjes die om de card kunnen worden gezet.
- zet geen gegevens op de card waaruit kan worden afgeleid waar deze van toepasing is. Dit maakt het moeilijker voor de 'vinder' om de card te misbruiken. Denk aan logo's of zelfs afdelingen op de card.
- organisaties die meerdere locaties hebben, moeten voor elke locatie een andere code gebruiken. Hiermee wordt voorkomen dat een verloren card in alle locaties kan worden misbruikt.
- als een gebruiker zijn card verliest, moet hij dat direct melden. Zo niet, dan volgt een forse boete. Zorg er ook voor dat een vervangende card zo duur is, dat de legale gebruiker er wel voor zorgt dat hij zijn card niet kwijtraakt.

Tweedelijns beveiliging

Na de card is natuurlijk de reader het tweede doelwit van kwaadwillenden. Zorg dus dat er niet met de readers kan worden geknoeid, en dat er een alarm wordt gegeven wanneer er op wat voor manier dan ook misbruik van wordt gemaakt. Er zijn veel technieken die pogingen tot misbruik detecteren. Een effectieve methode, bijvoorbeeld, is dat wanneer inbreuk met een zogeheten stil alarm wordt gemeld, de betreffende deur of poort met een CCTV-systeem wordt gemonitord zodat de misbruiker op heterdaad kan worden betrapt. Een dergelijk detectiesysteem is ook nuttig om eventuele storingen tijdig te signaleren.
Wanneer een organisatie bijvoorbeeld meerdere locaties heeft kunnen zogenoemde convergerende systemen effectief zijn. Zo kan iemand die is ingelogd in Utrecht logischerwijze niet zijn computer opstarten die in Nijmegen staat. Of dichterbij: iemand die niet 'bij de poort' is ingelogd, kan zijn pc op zijn werkplek niet opstarten.
Uiteraard dienen de gegevens (beveiligingslogs) zeer goed te worden beveiligd. Deze bevatten namelijk gevoelige data, zoals wie is door welke deur gegaan, hoe laat, waar heeft hij gezeten, welk card nummer heeft hij, enzovoort. Als deze gegevens elektronisch worden opgeslagen, moeten ze versleuteld zijn en extra beveiligd, liefst door een derde, daarin gespecialiseerde partij.
Deze logs moeten regelmatig worden bekeken om eventuele patronen te kunnen signaleren die afwijken van de standaard gang van zaken. Voorbeeld: als iemand abnormaal veel tijd nodig heeft om van het ene naar het andere controlepunt te komen, en als de card binnen zeer korte tijd op twee ver uit elkaar liggende punten wordt aangeboden, dan is er waarschijnlijk een gekloonde card in omloop.

We geven hier slechts enkele voorbeelden en tips voor het veilig gebruik van middelen voor toegangscontrole. Sommige kunnen een mate van 'overkill' hebben, andere te weinig bescherming bieden. Neem een expert in de arm om een adequate beveiliging te installeren. Ook al denkt u geen beveiliging nodig te hebben. ■