



Amsterdam Zuid Oost, 11 januari '08

Geachte relatie,

Als een van de toonaangevende fabrikanten in de toegangscontrole- en beveiligingsindustrie neemt Keyprocessor haar verantwoordelijkheid richting haar klanten zeer serieus. Keyprocessor staat dan ook volledig achter haar producten en oplossingen.

In recente berichtgeving op internet, televisie en in dagbladen wordt gesproken over het kraken van de zogenaamde Mifare chip. Deze wordt onder andere toegepast in het openbaar vervoer en als betalingskaart maar ook in toegangscontrole kaarten. Volgens deze berichtgeving is het, onder bepaalde omstandigheden, mogelijk de gegevens te manipuleren en/of te kopiëren.

De beschreven methode en benodigde apparatuur om de beveiliging te kraken is behoorlijk kostbaar en zal dus alleen interessant zijn in situaties waarin een hoog niveau van beveiliging nodig is, omdat er grote bedragen of belangen mee gemoeid zijn.

Het is daarom van groot belang dat de beveiliging berust op een samenhangend geheel van maatregelen en procedures en niet uitsluitend op het aanbieden van een kaart.

Aanvullende identificatie voorzieningen zijn bijvoorbeeld pincodes, vingerafdruklezers en bewakingscamera's. Ook door het gebruik van Anti-pass Back is het mogelijk om dubbele kaarten te signaleren. Als een kaart al binnen is en hij wordt nogmaals aangeboden, wordt dit gesignaleerd. Deze voorzieningen zijn reeds binnen ons security management systeem iProtect geïntegreerd (pincode bij inbraak, SmartTouch, video bij transactie).

Behalve technologische oplossingen zijn ook de organisatorische maatregelen een belangrijk onderdeel binnen het Risico Management. Om te voorkomen dat Mifare kaarten met kwaadaardige bedoelingen worden uitgelezen adviseert Keyprocessor de volgende procedures te implementeren:

- Verlies of diefstal van kaarten dient onmiddellijk gemeld te worden, zodat zij worden verwijderd uit het systeem
- Voorkom het delen of uitlenen van kaarten
- Kaarthouders dienen, wanneer zij niet op het werk zijn, hun kaarten niet voor derden zichtbaar te dragen
- Verdachte activiteiten in de nabijheid van kaartlezers dienen gemeld te worden
- Voorkomen van 'meelopen' door toegangsdeuren van medewerkers zonder dat zij de eigen kaart gebruiken

Concluderend kunnen wij stellen dat bij juist gebruik van de kaart gevoegd bij een geavanceerd systeem zoals iProtect, de klant zich geen zorgen hoeft te maken dat er ongeoorloofd toegang wordt verleend.

Indien u nog vragen heeft over bovenstaande informatie dan verzoeken wij u contact op te nemen met het customer care center. Telefoon: 020- 462 07 00 of e-mail:

ccc@keyprocessor.com