



Germany

Global Standards - Connecting Business

Presseinformation

Angst vor Viren bei RFID-Transpondern nach EPC-Standard unbegründet

Köln, 30. März 2006. Seit einigen Tagen verunsichern Schlagzeilen die Anwender von RFID-Systemen dahingehend, dass Computer-Viren auch RFID-Transponder befallen können. Ein Befall von EDV-Systemen durch EPCglobal-konforme Transponder kann jedoch nahezu ausgeschlossen werden.

Da prinzipiell jeder Datenträger ein schädliches Computerprogramm enthalten kann, ist eine Bedrohung grundsätzlich nicht auszuschließen. Entscheidend ist jedoch, ob es dem Virus gelingt, von dem RFID-Transponder in ein EDV-System einzudringen. Nach den Standards von EPCglobal wird lediglich ein Elektronischer Produkt-Code, der EPC, auf dem Transponder gespeichert. Der EPC ist eine eindeutig definierte Nummer, die ein Objekt weltweit überschneidungsfrei definiert. Um ein EDV-System vor Virenangriffen zu schützen, muss daher lediglich überprüft werden, ob ein korrekter EPC vom Transponder gelesen wurde oder nicht. Falls nein, werden die gelesenen Daten schon im Reader gelöscht und nicht an verarbeitende EDV-Systeme weitergegeben.

Prinzipiell wird zwischen zwei Arten von Virenangriffen unterschieden. Bei der ersten Art von Angriffen (buffer overflow) wird dem EDV-System eine Datenmenge angeboten, die die erwartete Datenmenge bei weitem überschreitet. Der Angreifer hofft nun, dass das verarbeitende EDV-System unprofessionell programmiert wurde und Probleme mit der Verarbeitung dieser größeren Datenmenge hat. Das Ergebnis ist in der Regel ein Systemabsturz. Da aber die Länge eines EPC bekannt ist, können Transponderinhalte, die länger als ein EPC sind, ohne Probleme identifiziert und gelöscht werden. Diese Identifikation kann schon

vom RFID-Reader vorgenommen werden, so dass verdächtige Daten das weiterverarbeitende EDV-System niemals erreichen.

Bei der zweiten Art von Angriffen (code insertion) ist auf dem Transponder ein schädliches Computerprogramm gespeichert, welches in ein EDV-System geschleust und ausgeführt werden soll. Gelingt dies, könnte das eingeschleuste Programm schädliche Aktionen ausführen. Aber auch hier vereitelt das Konzept von EPCglobal jegliche Möglichkeit der Infektion oder Ausbreitung. Durch die exakte Definition eines EPC mit Kopfdaten, Filterdaten und Nummernteil können korrekte und somit unschädliche Transponderinhalte zuverlässig erkannt werden. Alle anderen Inhalte können daher auch bei dieser Art von Angriffen vom Reader identifiziert und gelöscht werden.

Die Diskussion über RFID-Viren kommt nicht unerwartet. Jede populäre Technologie sieht sich früher oder später diversen Angriffen ausgesetzt. Bei Verwendung der RFID-Technologie nach den Standards von EPCglobal kann das Gefährdungspotenzial jedoch durch einfache Filterroutine nahezu ausgeschlossen werden.

Bei Rückfragen wenden Sie sich bitte an:

GS1 Germany GmbH

Monika Gabler, Leiterin Presse- und Öffentlichkeitsarbeit

Maarweg 133, 50825 Köln

Tel: 0221/94714-535, Fax 0221/94714-590

Mail: gabler@gs1-germany.de,

Homepage : www.gs1-germany.de