Safety first!

In der heutigen Zeit gehört es schon fast zur Normalität, beim Kauf, egal ob online, mobile oder am POS, sich keine grossen Gedanken zu machen und seine Karte zu zücken. Aber gerade in der Payment Branche ist es wichtig, Sicherheit zu priorisieren und so einen möglichen Kartenmissbrauch zu verhindern. Auch in der Entwicklung hat sich einiges getan und mit der EMV Chip Technologie (Chip & Pin) wurde das Risiko vom Kartenmissbrauch in den vergangenen Jahren erheblich reduziert.

Doch bevor es weiter in die Tiefe geht, sollten einige Begrifflichkeiten geklärt werden:

PCI DSS

PCI DSS (kurz: PCI) steht für Compliance Payment Card Industry Data Security Standard und wurde von grossen Kartenmarken entwickelt, um sensible Daten annehmen und die Sicherheit in der Zahlungskartenbranche entwickeln und verwalten zu können. Der PCI bietet einen Pool von Sicherheitsstandards für Unternehmen, die Kreditkartendaten von Kunden annehmen. Diese Standards sollen den Verbrauchern und Händlern eine sichere Umgebung und Schutz gewährleisten.

Skimming

"Skimming (Deutsch: „Abschöpfen“) bezeichnet eine Reihe an Angriffsformen, die auf Kreditkarten oder Bankkarten abzielen. Hierbei werden Geldautomaten, Kassensysteme oder vergleichbare Terminals gehackt, infiziert oder auf eine andere Form, so beispielsweise durch den Einbau von zusätzlichen Geräten, manipuliert." (Zitat: IT-Service.network)

Wie genau können eigentlich Terminals manipuliert werden?

Um dies zu veranschaulichen, beleuchten wir das Skimming einmal näher:

Bei dieser Manipulation arbeiten die Betrüger mit Overlay-Skimmern. Dies bedeutet, dass eine Plastikhülle, die eine täuschend ähnliche Nachahmung der tatsächlichen Eingabeoberfläche mit Tastenfeld und Kartenschlitz darstellt, benutzt wird.

Wenn ein Terminal in so einer Hülle ist, können die Betrüger in wenigen Sekunden ohne grösseren Aufwand an alle wichtigen Daten der bezahlenden Kunden gelangen.

Im praktischen sieht das ganze so aus:

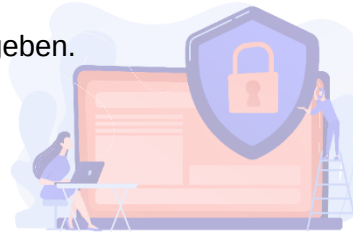
Der Kunde zieht nichts ahnend seine Karte durch den manipulierten Kartenschlitz und gibt über das ebenfalls manipulierte Tastenfeld den PIN ein. Jetzt sind die Kartendaten und der PIN vom Skimmer eingelesen und werden direkt via Bluetooth an ein Smartphone der Betrüger vermittelt.

Worauf kann man als Kunde in einem ersten Schritt selbst achten?

Bei einer Manipulation mit einem Skimmer wirken die Terminals klobiger. Die Tastatur kann ebenfalls ein wichtiges Indiz sein, da bei diesem Betrug die Tasten sehr schwer zu drücken sind. Wenn Ihnen dies auffallen sollte, sollten Sie umgehend das Personal informieren.

Und wie schützen Sie sich jetzt am besten?

Achten Sie darauf, dass Sie Ihr Terminal nicht an fremde Personen geben, denn im Normalfall sollten Sie von Ihrem Provider Bescheid bekommen, wenn ein Technikerbesuch ansteht. Falls dennoch unangekündigter Besuch vor der Türe steht, halten Sie sicherheitshalber nochmals Rücksprache, bevor Sie Ihr Terminal aus der Hand geben.



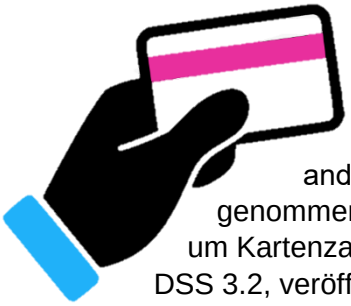
Wie sagt man so schön "vertrauen ist gut, aber Kontrolle ist besser". Dies trifft vollkommen auf die Terminal Sicherheit zu. Sie können Ihr Terminal täglich auf Manipulationen oder andere Auffälligkeiten untersuchen. Ein weiterer wertvoller Hinweis ist es, die Mitarbeitenden auf dieses Thema aufmerksam zu machen und die entsprechenden Massnahmen durchzugehen.

Pflichten für stationäre Geschäfte

Ein wichtiger Sicherheitsstandard für die Terminals ist der PCI. Seit dem 1. Juli 2015 ist es Pflicht, dass die POS-Devices geschützt sein müssen. Wenn dies nicht der Fall ist, läuft der Händler Gefahr, keine Kartenzahlungen mehr anbieten zu dürfen.

Die PayTec AG ist sich dessen bewusst und bietet ihre Terminals für Kunden und Partnern daher nur mit den höchsten zugelassenen Sicherheitsstandards an.

Neueste PCI DSS Regulierungen



Die PCI DSS Regulierung beschäftigt sich nicht nur mit der physischen Sicherheit der Karteninhaberdaten durch kriminelle Angriffe, sondern auch mit dem physischen Diebstahl von Hardware, welche dieselben Daten beinhalten. In dieser Regulierung, „Protect card-readig devices and terminals, used to capture cardholder data“, wird darauf Bezug genommen, dass alle Händler, die POS-Devices und POS-Terminals verwenden, um Kartenzahlungen zu akzeptieren, die neuesten PCI DSS Regulierungen (z.Z. PCI DSS 3.2, veröffentlicht im April 2016) beachten müssen.

Zusammengefasst in 3 Schritten:

1. Bestandshaltung von Terminals/Devices

Von der Erstverwendung an ist es wichtig, die physische Sicherheit der Kartenlesegeräte kontinuierlich zu kontrollieren. Besitzt man ein einzelnes Gerät, stellt dies keinen grossen Aufwand dar. Jedoch bei einer Vielzahl von Geräten sind eine geeignete Erfassung und das laufende Monitoring unabdingbar. Nur so kann die Sicherheit effizient gewährleistet werden. Erfasst werden sollte der genaue Standort des Terminals und alle wichtigen Angaben über das Gerät (z.B. Modell, Seriennummer und weitere gerätespezifischen Details). Falls es zu einer Änderung kommt, zum Beispiel ein Standortwechsel, sollte dies sofort notiert werden.

2. Regelmäßige Kontrolle der Terminals/Devices auf Manipulationen und Substitutionen

Durch die regelmässige Kontrolle können Manipulationen verhindert werden. Die PCI DSS Regulierung legt hier keine Häufigkeit der Überprüfung fest. Dies können die Händler für sich selbst bestimmen und sollte in Abhängigkeit vom Risikoprofil des jeweiligen Devices festgelegt werden. Das Risikoprofil setzt sich aus der Art des Gerätes, dem Standort sowie der Überwachung zusammen. Der Händler ist für die Prüffrequenz verantwortlich.

3. Schulung des Personals

Der letzte wichtige Schritt, um Manipulationen zu verhindern, liegt in der richtigen Schulung des Personals. Betrüger können manipulierte Devices an die Unternehmen senden oder sogar sich als autorisiertes Wartungspersonal ausgeben. Dadurch können sie zu sensiblen Daten gelangen. Um dem vorzubeugen, gilt es durch regelmässige Schulungen des Personals ein starkes Sicherheitsbewusstsein aufzubauen und ihr Gespür und Wissen in diesem Bereich zu stärken und zu vertiefen.

Natürlich ist es trotz aller Tipps und Tricks wichtig die POS-Geräte regelmässig zu überprüfen und somit den Kunden ein einwandfreies Bezahlerlebnis bieten zu können.

Bei weiteren Fragen können Sie sich gerne an die folgende E-Mail-Adresse wenden: info@paytec.ch.