ergonomic solutions

Sicherung von Geräten, Daten und Netzwerken

Was PCI DSS 3.0 Compliance für Sie bedeutet

Ein Ergonomic Solutions White Paper
Vorwort von Chris Field, Fieldworks Connections

TECHNOLOGY MOUNTING SOLUTIONS

Zahlungssicherheit im Laden bedeutet mehr als nur gute Schlösser und Schlüssel

Obwohl europaweit Vorschriften und bewährte Verfahren zur Verbesserung der Zahlungssicherheit eingeführt werden, gibt es in den unterschiedlichen Bereichen immer noch sehr viel Unsicherheit darüber, wie Ladenbesitzer am besten reagieren sollten.

Bei einigen wurde ihre Unsicherheit von Anbietern ausgenutzt, die gezielt Angst schüren, um Lösungen zu verkaufen, die manchmal übertrieben sind und unnötige Investitionen, schlechte Ergonomie am Checkout und Schwierigkeiten für die Kunden beim Zahlungsmitteleinsatz nach sich ziehen.

Manchmal gehen die getroffenen Maßnahmen auch in die falsche Richtung – wenn sie z. B. die PCI Council Richtlinien zu erfüllen scheinen, sich in der Praxis jedoch nicht unter allen Umständen bewähren.

Es bleibt die einfache Tatsache, dass die Anbieter von Terminals zwar die meisten Aspekte der PCI Sicherheitsstandards umgesetzt haben, sich der Einzelhändler aber um die letzte Verteidigungslinie gegenüber potenziellen Kriminellen kümmern muss. Diese Kriminellen werden ständig cleverer und entschlossener: Tagtäglich sind auf Online-Auktionen über 5000 Terminals verfügbar, während die legitimen Terminals im Einzelhandel unter ständiger Bedrohung stehen.

Als Ergebnis werden Einzelhändler von Unternehmen aus dem Terminal-Sicherheitssektor bestürmt, dies z. T. aufgrund der an sie gestellten PCI Anforderungen, aber auch, weil das Problem der Datensicherheit immer wieder Schlagzeilen macht und den Kunden Sorgen bereitet.

Hierbei handelt es sich um begründete Bedenken, wie die möglichen Konsequenzen nachlässiger Datensicherheitsstrategien auf Einzelhändler jeder Größe zeigen. Nur kommt für die Ladenbesitzer der Druck, reagieren zu müssen, genau zu einem Zeitpunkt, an dem sie sich jede einzelne Investition sehr genau überlegen müssen. Sie befinden sich bereits in einem schwierigen Umfeld und müssen deshalb noch stärker auf das Kundenerlebnis achten. Unter nach wie vor schwierigen Geschäftsbedingungen muss der Einzelhandel noch stärker auf das Kundenerlebnis achten, in mobile Terminals mit Drahtlos-Netzanbindung neu investieren und hierbei die PCI DSS 3.0 Datenschutzanforderungen einhalten.

Wir haben uns zur Zusammenarbeit mit dem Marktführer Ergonomic Solutions entschlossen, weil uns unsere Mitglieder aus dem Einzelhandel gebeten hatten, etwas Licht ins Dunkel mit einem Praxisleitfaden zur Sicherheit von Zahlungsdaten zu bringen, der nicht nur die physische Sicherheit von Terminals und anderen Zahlungsgeräten, sondern auch die Auswirkungen der PCI Compliance auf Gerätesicherheit, Management, Registrierung und Wartung sowie auf die

Zahlungsumgebung beschreibt.
Wir möchten das Problem nüchterner angehen und es Einzelhändlern erleichtern, ihre Optionen zu verstehen, damit sie Entscheidungen auf der Grundlage ihrer speziellen Anforderungen treffen können.

Dieser Leitfaden macht es Händlern einfacher, die PCI DSS 3.0 Empfehlungen vollständig umzusetzen:

- Physische Sicherheit von Zahlungsterminals
- Zahlungsumgebung
- Skimming-Vorbeugung
- Risikobewertungen

Dieses Verfahren wird von führenden Unternehmen im Zahlungssektor, von VeriFone bis Visa, befürwortet und entspricht den Richtlinien und Anforderungen des PCI DSS 3.0 Council.

Chris Field
Fieldworks Connections

Die Gefahren

Im Zahlungssektor haben einige auf den Angstfaktor gesetzt, um Einzelhändler auf den Weg manchmal übermäßiger, manchmal falscher oder auch unnötiger Sicherheitsmaßnahmen für feste und mobile Checkout-Terminals und weitere Ergänzungen zu zwingen.

In Zahlungsterminals wurde bereits erheblich investiert. Viele Einzelhändler wollen deshalb ganz sicher nicht hören, dass sie noch mehr Geld für die Gerätesicherung ausgeben müssen. Eine ehrliche Vorgehensweise ist es, ihnen beim Verständnis der Risiken und beim Erstellen eines eigenen Risikoprofils zu helfen, das dann auf spätere Investitionen angewandt werden kann. Das unterscheidet sich stark vom Vorgehen der Verunsicherer, die nur am Verkauf eigener Lösungen interessiert sind.

Es geht deshalb um einen Mittelweg zwischen Untätigkeit und Überreaktion.

Die PCI DSS 3.0, 9.9 gibt an, dass ein Händler die POS-Geräte, die Zahlungskartendaten über direkte physische Interaktion mit der Karte erfassen, vor Manipulation und Austausch schützen muss. ***Dies wird für Händler nach dem 30. Juni 2015 zur Bedingung****.*

Zu Mobilgeräten gibt das Dokument an: Wenn ein Händler ein Mobilgerät, das Teil einer Zahlungslösung ist, entweder besitzt oder anderweitig dafür verantwortlich ist, ist der Händler dafür verantwortlich, Maßnahmen zur Durchsetzung und Einhaltung der Sicherheit dieses Geräts zu ergreifen. Die in diesem Abschnitt beschriebenen Maßnahmen müssen auch für jegliche zusätzlichen Hardwarekomponenten getroffen werden, die Bestandteile der mobilen Zahlungslösung sind (z. B. Kartenlesegeräte).

5.1. Verhinderung des unbefugten Gerätezugriffs
5.1.1. Der Händler ist verantwortlich für die Gewährleistung der Integrität und Sicherheit des mobilen Geräts und seine sichere Aufbewahrung bei Nichtgebrauch (z. B. Verschließen in einem Schrank, Anbinden an der Kasse bzw. ununterbrochene Beaufsichtigung).

Die Gefahren sind real, und es ist dringend nötig, sie gemäß den Sicherheitsanforderungen der Payment Council Industry Data Security Standards (PCI: DSS) zu bekämpfen, wenn Einzelhändler Strafzahlungen und den Verlust von Kundenvertrauen bei Datendiebstahl vermeiden wollen.

Jegliche Sicherheitsverletzung bei Zahlungskartendaten hat für die betroffenen Unternehmen weitreichende Konsequenzen, darunter:

- Verpflichtungen zur Benachrichtigung der Behörden
- Rufschädigung
- Verlust von Kunden
- Potenzielle finanzielle Haftung
- Rechtsstreitigkeiten

Viele Anbieter physischer Sicherheitsvorkehrungen ignorieren PCI aber schlicht und konzentrieren sich nur auf das Gerät.

Die Ergebnisse sind:

- Fehlinvestition
- Fehlende langfristige Rendite (ROI)
- Fehlende PCI Compliance
- Gewählte Lösung lange vor dem ROI obsolet
- Gewählte Lösung schreckt Betrüger ab, aber auch Kunden

Angst kann auch den natürlichen Instinkt des Einzelhändlers ausschalten, der ihm sagt, dass alle Technologie- und Ausrüstungsinvestitionen von einem soliden ROI- und TCO-Modell gestützt werden. Das ist falsch: Einzelhändler möchten nicht nur die harten finanziellen ROI-Fakten verstehen, sondern auch die so genannten weicheren und trotzdem so entscheidenden Vorteile hinsichtlich der Kundenerfahrung, die sich in Kaufbereitschaft niederschlägt.

Wichtig ist ein Ausgleich zwischen Sicherheit, Zugänglichkeit und Design. Die Lösung muss berücksichtigen, was morgen sein wird, und nicht nur kurzfristige Abhilfe bei einem Problem schaffen, um anschließend die Investition abschreiben zu müssen.

Es geht nicht nur um die Geräte

Weil es bei PCI um den Schutz von Daten geht, ist es wichtig, nicht nur das Gerät zu sichern, sondern die gesamte Verkabelung, die es mit dem Netzwerk verbindet, das Netzwerk, in dem es arbeitet, und die gesamte Umgebung, in die das Netzwerk und die Geräte eingebunden sind. Wenn die Ausrüstung unabhängig vom Netzwerk behandelt wird, besteht das Risiko inkompatibler Mehrfachlösungen, übersehener Bereiche, möglicher Doppelarbeit und eines ROI-Modells, das schwierig einschätzbar sein kann.

Die Konzentration allein auf die Geräte kann erhebliche Kosten verursachen:

- Wenn das Gerät nicht befestigt wird, wird es im Umgang zwischen Mitarbeitern und Kunden fallen gelassen
- Die Verkabelung verschleißt im Gebrauch, wodurch das Gerät in den Manipulationsschutz modus umschaltet und unbrauchbar wird
- Die Sicherung allein des Geräts verhindert nicht notwendigerweise Betrug in anderen Bereichen des Netzwerks wie über die Kabel

Wir müssen uns deshalb um zwei Hauptbereiche kümmern:

- Sicherung fester wie mobiler Geräte
- Sicherung der Umgebung

Anforderungen der PCI DSS 3.0 ab 30. Juni 2015

Sicherung von Terminals oder mobiler Geräte

Laut Visa müssen Einzelhändler alle Zahlungsterminals überwachen und überprüfen, die ihre Karten akzeptieren. Hierzu gehört die Untersuchung der Geräte auf jegliche Auffälligkeiten, wie fehlende oder geänderte Dichtungen bzw. Schrauben, nicht originale Verkabelung, Öffnungen im Gerät oder neu hinzugefügte Aufkleber bzw. anderes Material, das Beschädigungen durch Manipulationen am Gerät verbergen könnte. Die Einzelhändler müssen mindestens Folgendes überprüfen:

- Befindet sich das Terminal am vorgesehenen Platz?
- Stimmt der Herstellername?
- Stimmt die Modellnummer?
- Ist die Seriennummer auf dem Aufkleber aufgedruckt und wird sie korrekt auf dem Bildschirm angezeigt?
- Sind Farbe und allgemeiner Zustand des Terminals so wie beschrieben und ohne zusätzliche Auffälligkeiten oder Kratzer (besonders an Gehäusenähten)?
- Sind die Sicherheitssiegel und -aufkleber des Herstellers ohne Spuren von Entfernungs- oder Manipulationsversuchen vorhanden?
- Entsprechen die Sicherheitsmerkmale und Referenznummern des Herstellers der Beschreibung?
- Sind die vorgesehenen UV-Markierungen vorhanden und wie beschrieben?
- Entsprechen alle Terminalverbindungen der Beschreibung, haben die Kabel denselben Typ und dieselbe Farbe, gibt es lose Drähte oder zerstörte Anschlüsse?
- Ist die Zahl der Verbindungen am Terminal so wie erwartet?
- Entspricht die Gesamtzahl der benutzten Terminals der Zahl der offiziell installierten Terminals?

Bei der Sicherung von Terminals geht es um:

» Vorbeugung von Diebstahl bzw. Austausch gegen nicht autorisierte Terminals
» Vorbeugung von Datendiebstahl in der Zahlungsinfrastruktur
» Verhinderung, dass Skimming-Ausrüstung zum Terminal bzw. Netzwerk hinzugefügt wird
» Sicherung von PIN-Daten vor Ausspähen („Schulter-Surfen“)
» Sicherung unbeaufsichtigter Terminals vor physischer Entfernung
» Sicherung nicht nur des Terminals, sondern auch der Kabel

Das obige Diagramm beschreibt das Gesamtsystem von Zahlungsgeräten, Anwendungen, Infrastrukturen und Benutzerstrukturen, das von den PCI Sicherheitsstandards strukturiert wird.

Wir sind der Ansicht, dass die richtige Vorgehensweise ein Mittelweg zwischen der Gerätesicherung und der Einschränkung der Gebrauchsfähigkeit (und damit der Kundenfreundlichkeit) ist. Ein Gerät kann so gesichert werden, dass es fast unmöglich ist, es zu stehlen; das schreckt kriminelle Ingenieure aber ebenso wenig ab wie untreue Mitarbeiter. Im PCI Dokument Skimming-Vorbeugung, bewährte Praktiken für Kaufleute, wird Einzelhändlern als bewährte Vorgehensweise dringend empfohlen, Sicherheitsanbindungen mit Schlüsselmanagementdiensten sowie Geräteregistrierung und -verfolgung einzusetzen, um die Gefährdung von Terminals und Kabeln zu verhindern.

Beachtet werden müssen aber auch der physische Standort des Geräts und die Sicherheit der Komponenten. Kann das Gerät leicht entfernt werden; sind die Komponenten fest miteinander verkabelt oder physisch geschützt, um einfache Manipulation bzw. Diebstahl zu verhindern? Terminals müssen stets so platziert werden, dass die PIN-Eingabe von Kunden vor Blicken anderer Kunden geschützt ist; wenn möglich, sollte dies einen PIN-Ausspähschutz („Shielding“) einschließen.

Bei der Gebrauchsfähigkeit geht es nicht nur um Bequemlichkeit, sondern auch um die Einhaltung der europäischen Vorschriften zur Barrierefreiheit und Zugänglichkeit. Wenn die Anforderungen der Vorschriften mit einem Terminal in einer Halterung erfüllt werden können, sollte überlegt werden, die Halterung von einer reinen „Ablage“ in eine Befestigung abzuändern, die das Terminal physisch festhält und das Risiko von Blitzdiebstählen mindert.

Wenn das Absperren des Terminals nicht mit den Vorschriften zur Barrierefreiheit und Zugänglichkeit vereinbar ist, sollte erwogen werden, eine Sicherheitsanbindung am Gerät und der Halterung anzubringen, um so eine gewisse Beweglichkeit bei gleichzeitigem Schutz vor Blitzdiebstahl sicherzustellen.

Die zunehmende Verwendung von Technologie mit Kundenschnittstelle in der Einzelhandelsumgebung mit Geräten wie Chip- & PIN-Terminals, iPads und zahlreichen anderen tragbaren Geräten verschafft vielen Kunden ein neues Shoppingerlebnis, dies geht aber auf Kosten von mehr Diebstahl- und Betrugsfällen. Der Laden im Allgemeinen und der Checkout im Besonderen sind immer raffinierterer Formen von Kriminalität ausgesetzt. Das höchste Risiko besteht bei Karten- und PIN-Daten. Untersuchungen haben gezeigt, dass es nur etwa 30 Sekunden dauert, ein komplettes Kartenterminal gegen ein identisches mit elektronischen Skimmern versehenes auszutauschen.

Kriminelle haben eine hohe Kompetenz hinsichtlich der Funktionalität und Schwachstellen vieler Terminals entwickelt. Wenn einmal die Sicherheitsausstattung eines bestimmten Terminals erfolgreich geknackt ist, ist es einfacher, die entsprechenden Erkenntnisse für Angriffe auf ähnliche Terminals zu benutzen, was die Sicherheit am Checkout umso wichtiger macht.

Das iPad und andere Tablet-Anwendungen haben die Art verändert, in der wir Mobiltechnologie nutzen und zu einer Neubewertung der herkömmlichen kommerziellen Technologieintegration besonders im Einzelhandel geführt. Allerdings sind diese Geräte hochwertig und heiß begehrt.

Zum Schutz digitaler Daten, zur Verhinderung von Datendiebstahl und weiteren Sicherung der Hardware hat Ergonomic Solutions verschiedene Sicherheitsschlösser für Zahlungsterminals, mobile Geräte und POS-Hardware entwickelt.

Sicherung der Umgebung

Hier geht es um die Sicherung des Geräts als Ausrüstung mit IP-Verbindung. Mit Datenverschlüsselung zwischen den einzelnen Punkten im gesamten Netzwerk müssen alle potenziellen Angriffspunkte analysiert und gesichert sowie Prozesse und Verfahren für ihre Überwachung eingesetzt werden.

- Geräteregistrierung und -verfolgung
- Compliance durch Prozesse und Verfahren
- Dokumentation bewährter Verfahren
- Risikobewertung
- Wirkungsanalyse und Reaktionsverfahren

Geräteregistrierung und -verfolgung

Die Sicherung von Geräten ist die eine Sache; es ist aber ohne Weiteres möglich, dass ein gesichertes Gerät manipuliert worden ist und es keine Verfahren gibt, dies herauszufinden. Mit der Zunahme von Skimmingfällen, bei denen Betrüger Teminals manipulieren, um Kartendaten sowohl über das Gerät als auch über das Netzwerk stehlen zu können, ist es entscheidend wichtig geworden, alle Geräte zu registrieren, was auch den PCI Council Empfehlungen entspricht.

Bei der Registrierung müssen die folgenden Schlüsseleigenschaften erfasst werden:

- Serien- und Modellnummer des Geräts
- Hersteller
- Vorhandene Merkmale (durch Gebrauch verursacht)
- Bild des Geräts
- Anschlusstyp
- Farbe der Anschlussleitung
- Zahl der Anschlüsse
- Displayständer, Sammelbüchsen und andere Verkaufshilfen in der Nähe des Terminals
- Platzierung von Sicherheitssiegeln (Hersteller- bzw. zusätzliche Siegel)
- Standort, z. B. Checkout Nr. 1

Manipulierte Terminals können so erkannt werden, weil ihre ursprünglichen eindeutigen Eigenschaften aufgezeichnet wurden. Wenn ein vorhandenes Terminal in irgendeiner Weise abweicht, kann es in betrügerischer Absicht verändert worden sein.

Dies ist auch sicherer für die Benutzer, weil sie einen eigenen und eindeutigen Account erhalten, und eine gute Lösung für Unternehmen, die sicherstellen möchten, dass ihre Ausrüstungen erfasst werden und nach Personalwechseln weiter verfügbar sind.

Die Registrierung ermöglicht es auch Administratoren, ihre Sperrprogramme über ein einziges Webportal zu verwalten und Zugriffsberechtigungen und Schlüssel an die individuelle Umgebung anzupassen. Schlüssel können bei Bedarf einer Person, einem Checkout oder einer Region zugeordnet werden.

Administratoren können

- Registrieren und sperren individuell oder insgesamt für Individuen oder Gruppen (Läden/Bereiche usw.)
- Master-keyed-, Like-keyed oder Shared-keyed-Programme verwalten
- Benutzeraccounts für ihre Endnutzer erstellen, über die Ersatzschlüssel bestellt oder Kombinationscodes gespeichert werden können
- Benutzer auffordern, Schulungsvideos aufzurufen und Accountdaten zu überprüfen

» Aufzeichnen, wer Eigentümer einer Sperre ist, und Berichte herunterladen
» Eigentümer verlorener Schlüssel finden
» Sperren wieder neuen Benutzern zuordnen

Einzelne Benutzer können:

» Ersatzschlüssel bestellen
» Gespeicherte Kombinationscodes abrufen (evtl. für zukünftige Benutzung?)
» Account- und Schlüsselcodedaten überprüfen
» Ihre persönlichen Daten aktualisieren

Wir empfehlen auch ein eindeutiges Gerätekennzeichnungssystem als zusätzliche Manipulationssicherung, wie ein UV-Hologramm-Siegel, das nur unter UV-Licht sichtbar ist und weder ersetz- noch wiederherstellbar ist. Ein derartiges Siegel ist nicht nur manipulationssicher, sondern es signalisiert dem Personal auch, dass das Zahlungsterminal am Checkout mit besonderer Umsicht und speziellen Verfahren zu behandeln ist, um die Sicherheitsstandards zu erfüllen.

Abgleich

Das in diesem Bericht beschriebene Verfahren ist mit dem PCI DSS 3.0 Council Dokument abgeglichen: Punkt-zu-Punkt-Verschlüsselung. Anforderungen an Lösungen und Testverfahren: Verschlüsselung, Entschlüsselung und Schlüsselmanagement in sichere Verschlüsselungsgeräte, Version 1.1.1.

3A-1.1 Einhaltung von Inventarkontrolle und Überwachungsverfahren, um alle Checkout-Geräte zu identifizieren und zu lokalisieren, einschließlich ihrer Standorte:

- Im Einsatz
- Einsatzbereit
- In Reparatur oder anderweitig nicht in Gebrauch
- In Überstellung

Lösung: Register & Retrieve-Datenbank und -Checklisten

3A-1.2 Mindestens einmal jährliche Inventur der Checkout-Geräte, um Entfernung bzw. Ersatz von Geräten zu erkennen.

Lösung: Register & Retrieve-Checkliste

3A-1.3 Pflege eines dokumentierten Inventars aller Checkout-Geräte mit mindestens folgenden Angaben:

- Gerätemarke und -modell
- Standort (Ort/Einrichtung und/oder Identität des Ladeninhabers)
- Seriennummer
- Allgemeine Beschreibung
- Foto des Geräts, das deutlich Gerätetyp/-modell zeigt (zur Unterstützung bei der identifizierung unterschiedlicher Geräte)
- Sicherheitssiegel, Aufkleber, verborgene Markierungen usw.
- Zahl und Art der physischen Geräteanschlüsse
- Datum der zuletzt durchgeführten Inventur
- Firmwareversion
- Hardwareversion
- Anwendungen (einschl. Versionsnummern)

Lösung: Register & Retrieve-Datenbank

3A-1.4 Implementierung von Verfahren zum Erkennen von Abweichungen bei der jährlichen Inventur, einschließlich fehlender oder ersetzter Checkout-Geräte und zur Reaktion darauf. Die Reaktionsverfahren müssen den Einschluss jeglicher Verfahren vorsehen, die von allen zutreffenden PCI Zahlungsorganisationen definiert wurden, einschließlich Zeitrahmen für Berichte über Vorfälle, und die Einrichtung einer Kontaktstelle für Einzelhändler, bei der fehlende/ersetzte Terminals gemeldet werden können.

Lösung: Register & Retrieve-Datenbank

3A-4.1 Bereitstellung von Anleitungen für den Einzelhändler im P2PE Handbuch zur Auswahl geeigneter Standorte für den Einsatz von Terminals, wie z. B.:

- Regelung des öffentlichen Zugangs zu Geräten in einer Weise, dass er nur auf die Teile des Geräts beschränkt wird, die eine Person zur Ausführung einer Transaktion bedienen muss (z. B. PIN-Pad und Kartenlesegerät)
- Aufstellung von Terminals in einer Weise, dass sie von autorisiertem Personal beaufsichtigt/überwacht werden können (z. B. im Rahmen täglicher Terminalprüfungen durch Verkaufs-/Sicherheitspersonal)
- Aufstellung von Terminals in einer Umgebung, die vor Manipulationsversuchen abschreckt (z. B. mit geeigneter Beleuchtung, Zugangswegen, deutlich sichtbaren Sicherheitsvorkehrungen usw.)

Lösung: Register & Retrieve-Checkliste

3A-4.2 Bereitstellung von Anleitungen für den Einzelhändler im P2PE Handbuch zur physischen Sicherung eingesetzter Terminals, um unbefugtes Entfernen/Ersetzen zu verhindern, einschließlich Beispielen dafür, wie Terminals physisch gesichert werden können.

Lösung: Register & Retrieve
Sicherheitsanbindungen

3B-8 Der Lösungsanbieter implementiert Manipulationserkennungen für Terminals in seinem Besitz und gibt dem Einzelhändler die entsprechenden Informationen.

Lösung: StealthSafe

3B-8.1.1 Bereitstellung von Anleitungen für den Einzelhändler im P2PE Handbuch zur Durchführung regelmäßiger physischer Prüfungen von Terminals, um Manipulationen bzw. Modifikationen daran erkennen zu können. Die detaillierten Verfahren für die Durchführung regelmäßiger physischer Prüfungen müssen einschließen:

- Beschreibung der Manipulationserkennungen
- Anleitung für physische Untersuchungen, einschließlich Fotos oder Zeichnungen

des Terminals, die zeigen, was untersucht werden muss, so z. B.:

- Fehlende oder geänderte Dichtungen bzw. Schrauben, nicht originale Verkabelung, Öffnungen im Gerät oder hinzugefügte Aufkleber bzw. anderes Abdeckungsmaterial, das zum Verdecken von Beschädigungen durch Manipulationen benutzt werden könnte.
- Anleitungen zum Wiegen von POI Terminals beim Neueingang und anschließend regelmäßig zum Vergleich mit den Spezifikationen des Herstellers, um so potenziell in die Terminals eingesetzte Ausspähmechanismen erkennen zu können.

» Empfehlungen für die Häufigkeit der Prüfungen

Lösung: Register & Retrieve-Datenbank und -Checklisten
Sicherheitsanbindungen

3B-8.2 Implementierung von Manipulationserkennungen und/oder Prozessen für Terminals an entlegenen bzw. unbeaufsichtigten Stellen — z. B. Einsatz von Kameras oder anderen physikalischen Vorrichtungen, um das Personal bei physischen Eingriffen zu warnen.

Lösung: Sicherheitsanbindungen

Über Ergonomic Solutions

Ergonomic Solutions ist seit der Gründung 1996 rasch gewachsen und nun weltweit führend bei Design, Herstellung und Lieferung ergonomisch optimaler, fortschrittlicher Montage- und Sicherheitslösungen für eine Vielzahl von Kassen- und mobiler Technologie im Einzelhandel, in Banken, öffentlichen Verkehrsmitteln und im Gastgewerbe. Ergonomic Solutions ist seit langem führend bei der Planung und Optimierung von Arbeitsplätzen und unsere anerkannte Ergonomieberatung hat viele große europäische Einzelhändler bei der Gestaltung von Arbeitsplätzen unterstützt, die die Zugänglichkeit, Bedienbarkeit, Sicherheit und den Komfort für ihr Personal und ihre Kunden optimieren.

Unsere Produktvielfalt an technologischen Halterlösungen bietet ergonomische Lösungen für eine breite Anwendung. Von der Einzelhandelsfläche bis hin zur Vorstandsetage können wir Lösungen anbieten, die garantieren, dass Ihre IT-Investitionen den verfügbaren Arbeitsplatz optimal nutzen und dabei vor Beschädigung und Diebstahl geschützt sind.

Über Fieldworks Connections

Fieldworks Connections bringt Einzelhändler, Marken und Entscheider zusammen, um die Zukunft des Multi-Channel-Trading zu entwickeln.

Wir gehören heute zu einer Gemeinschaft, die in Europa, Asien und den USA traditionelle ebenso wie neue Kanäle umfasst. Mit unserem Einfluss können wir Unternehmen unterstützen, die auf ihren gewählten Märkten wachsen möchten und Risiken durch Anwendung bewährter Verfahren mindern.

Fieldworks Connections wird von einem Team erfahrener Journalisten, Marketingexperten, Analysten und Consultants geleitet, dem ein Beirat führender Einzelhändler, Consultants und Akademiker zur Seite steht.

www.fieldworksconnections.co.uk