Einfach, aber effektiv

Neben der elektronischen Artikelsicherung ist die Videoüberwachung die wichtigste Sicherheitsmaßnahme im Einzelhandel

Von Nora Burchardt

Der junge Mann schaut sich nervös um. Sein Blick streift durch den kleinen Laden. Er fühlt sich unbeobachtet, die Mitarbeiter sind abgelenkt. In diesem Moment greift er zu, direkt in die Warenauslage, und ist schon wenige Minuten später mit seiner Beute verschwunden. Viel zu häufig wird Ware nicht offiziell verkauft und durch Kassenscanner erfasst, sondern „läuft" auf anderen Wegen aus dem Unternehmen heraus. Nach aktuellen Studien bedeutet dies: Statistisch gesehen stiehlt jeder Haushalt pro Jahr Waren im Wert von über 50 Euro, insgesamt liegt laut EHI die Höhe der Inventurverluste im Einzelhandel bei 3,9 Milliarden Euro.

Die Videoüberwachungskameras von Samsung Electronics, wie sie hier zu Lande die Aasset Security GmbH vertreibt, sind im deutschen Einzelhandel weit verbreitet.

Dabei sind die technischen Möglichkeiten, sich gegen Diebstahl zu sichern, so vielfältig wie nie zuvor. Besonders die Videoüberwachung macht den Schutz des Eigentums bei gleichzeitiger Wahrung der Privatsphäre des Kunden möglich. Der Einsatz von Kameras ist freilich nicht nur gegen Diebe gerichtet; er ist vor allem ein Einsatz für die vielen ehrlichen Kunden, damit sich Diebstähle nicht auf den Verkaufspreis niederschlagen oder Mitarbeiter und Kunden unter Generalverdacht gestellt werden.

Um dies zu verhindern, gibt es zum Beispiel von Aasset Security und Samsung Electronics simple, aber äußerst effektive Möglichkeiten für den Einzelhandel. Sichtbare Videoüberwachung per Kamera ist wohl die bekannteste und beliebteste Methode, Diebe abzuschrecken oder zu überführen. Kameras und Geräte, die in Ein- und Ausgängen, in Verkaufs- und Lagerbereichen oder auch in Anlieferzonen installiert sind, verringern die illegale Entnahme von Waren. Unerlässlich ist bei der Planung einer Überwachungsanlage die Einbeziehung von Datenschutzbeauftragten und Betriebsräten, um die Rechte der Mitarbeiter und Kunden zu wahren.

Trotz des zunehmenden Kameraeinsatzes ist jedoch vielen Beteiligten nicht immer klar, welche Möglichkeiten die Technik bietet. Beispielsweise lassen sich direkt in Videokameras Privatzonen bilden, um ganze Kassenbereiche oder einzelne PIN-Code-Eingabegeräte auszublenden – der Datenschutz bleibt gewährleistet. Per Vorschaumonitor im Eingangsbereich können Kunden schon beim Betreten des Geschäfts erkennen, dass Kameras installiert sind. Dem Kunden wird auf diese Weise ein Sicherheitsgefühl vermittelt und mögliche Diebe direkt abgeschreckt.

Für viele Unternehmen sind Kameras unerlässlich und besonders für Hausdetektive die Unterstützung ihrer täglichen Arbeit. Mit der passenden Technologie lässt sich jeder noch so kleine Winkel einer Filiale überblicken, Verdächtige können herangezoomt und identifiziert werden und in Verbindung mit Digitalrekordern lassen sich wichtige Sequenzen bei Bedarf aufzeichnen. Aus datenschutzrechtlichen Gründen sollten Rekorder passwortgeschützt sein, um unberechtigten Zugriff zu verhindern und eine mindestens in Tagesschritten einstellbare Löschung des aufgezeichneten Bildmaterials bieten. Einsetzbar sind heutzutage Rekorder, die nicht rund um die Uhr laufen müssen, sondern speziell nach Geschäftsschluss erst durch Bewegungs- und Aktivitätserkennung gestartet werden.

Videoüberwachungsanlagen reduzieren Inventurdifferenzen! Trotz dieser einfachen Wahrheit schrecken viele Unternehmen vor den Investitionskosten zurück. Dabei ist eine professionelle Beratung durch seriöse Anbieter in der Regel kostenlos und die Kalkulation durchaus lohnenswert. Denn Investitionen in Sicherheit amortisieren sich schon in den ersten beiden Jahren, in den meisten Fällen sogar innerhalb des ersten Jahres.

Mit Vorschaumonitoren, wie einer hier an der Decke hängt, weiß jeder Kunde sofort, woran er im Laden ist.

WWW.AASSET-SECURITY.DE

Wegfahrsperre für Speicherkarte, Handy & Co.

Für Consumer-Electronic-Produkte gibt es jetzt eine Alternative zur klassischen Warensicherung

Von Birgit Bruns

Es hat Jahrzehnte gedauert, bis das Auto zu seiner Wegfahrsperre kam. Dazu musste freilich erst die Elektronik in die Fahrzeugtechnik einziehen. Allerdings ist es angesichts der immer kürzeren Innovationszyklen auf dem Gebiet der Digitaltechnik doch erstaunlich, wie lange es gedauert hat, bis man das Prinzip der Wegfahrsperre auch als Diebstahlschutz für andere elektronische Produkte entdeckte. Nun ist eine solche Lösung marktreif und in der Praxis auch schon im Einsatz. Für Hersteller, Logistiker und Einzelhandel gleichermaßen gibt es damit für Speicherkarte, Laptop, Handy, USB-Stick, Navi & Co. eine Alternative zur klassischen Warensicherung.

Für die Freischaltung des Codes benötigt jede Kasse einen „DiSa-Activator". Dieser wird mit einem PC verbunden, der wiederum via Internet mit dem DiSa-Server in Verbindung steht und so ständig Sicherungs- und Freischaltcodes speichern und überwachen kann.

Die Idee, Consumer-Electronics-Produkte SB-fähig zu machen, treibt Uwe Bremeyer schon lange an: „Trendprodukte von der SD-Speicherkarte über MP3-Player bis zu hochwertigen Handys stehen auf der Liste der ‚Diebstahlrenner' ganz oben. Ohne Sicherheitsmaßnahmen geht es also nicht", so der Geschäftsführer der DiSa DigitalSafety GmbH. Eine kundenorientierte SB-Vermarktung in Schütten oder auf Sondertischen praktiziert der Handel meist nur bis zu einem Wert von etwa zehn Euro. Höherwertigere Ware wird – wenn überhaupt – nur gesichert angeboten. Doch gerade in der Einstiegspreisklasse hat Diebstahl auf Grund der geringen absoluten Erträge erheblichen Einfluss auf das Ergebnis.

Stichwort „Quellensicherung"

Um die immer kleiner werdenden Produkte zu schützen, haben Industrie und Handel inzwischen ein ganzes Arsenal von Anti-Diebstahl-Vorrichtungen im Einsatz, angefangen von Blisterverpackungen über Plastikboxen, Vitrinen und Schranken an den Ausgängen bis hin zu den Hochsicherheitslagern der Industrie. Schließlich sind elektronische Trendprodukte nicht nur bei der ehrlichen Kundschaft, sondern auch bei Beschaffungskriminellen und Gelegenheitsdieben extrem begehrt.

Anders als die herkömmlichen Maßnahmen ist der neue digitale Diebstahlschutz von DiSa. Damit gesicherte Produkte funktionieren genau so lange nicht, bis sie an der Kasse des Handels bezahlt worden sind. Dort aktiviert die Kassiererin die Digitalkamera oder das Navigationsgerät oder der Kunde bekommt einen Code ausgehändigt, den er bei der Inbetriebnahme des neuen Geräts einmal eingibt und damit die Funktion wiederherstellt. Der digitale Diebstahlschutz basiert auf einem patentierten Verfahren, bei dem den Produkten bereits während der Produktion (Stichwort „Quellensicherung") – oder später im Logistikprozess – jegliche Funktion genommen wird, sie also blockiert werden. Erst durch die Freischaltung wird die Ware – Prinzip Wegfahrsperre – wieder voll funktionsfähig. In der Zwischenzeit ist sie quasi wertlos.

Die Sicherung der Produkte erfolgt durch eine spezielle Software, die die Industrie, die Fabrik oder der Distributor per Download auf Stückzahlbasis bezieht und

Mit diesem Logo sollte jeder potenzielle Dieb verstehen, dass er nichts ausrichten kann.

Uwe Bremeyer war lange genug im Einzelhandel beschäftigt, um zu wissen, wo es dort in Sachen Diebstahlschutz auf den Nägeln brennt.

aufspielt. Diese Daten werden gespeichert. Der für die Freischaltung notwendige Code wird online direkt im Geschäft bereitgestellt, um die Funktionalität der Ware wieder herzustellen. Dafür benötigt der Handel (pro Kasse) einen „DiSa-Activator". Dieser wird mit einem PC verbunden, der wiederum via Internet mit dem DiSa-Server in Verbindung steht und so ständig Sicherungs- und Freischaltcodes speichern und überwachen kann. Das Verfahren garantiert hohe Sicherheit gegen unautorisiertes Freischalten von Ware auf Standort- und Lieferantenbasis mit der Möglichkeit zeitnaher Gegenmaßnahmen. Außerdem ist auch die Bedienung kinderleicht, wie sich SECURITY *insight* exklusiv bei DiSa in Frankfurt am Main überzeugen konnte.

Hinweisschilder und Kennzeichnung

Damit die digitale Warensicherung präventiv wirkt, ist es wichtig, Kunden darüber zu informieren. Auch potenzielle Diebe müssen wissen, dass es sich nicht lohnt, digital gesicherte Produkte zu entwenden. Plakative Hinweisschilder und die Kennzeichnung der Produkte mit einem speziellen Logo weisen auf die neue Sicherungstechnik hin. „Tests in Zusammenarbeit mit einem SB-Warenhausunternehmen haben gezeigt, dass der lokale Lernprozess etwa eine Woche dauert. Danach sinkt die Diebstahlquote auf das Niveau von Gelegenheitsdiebstahl. Professionelle Beschaffungskriminalität findet dann nahezu nicht mehr statt", so Bremeyer. Wird Personal des Diebstahls verdächtigt, können im rechtlich zulässigen Rahmen auf Wunsch Informationen zur Verfügung gestellt werden, ob Freischaltungen außerhalb der Öffnungszeiten oder größere Mengen gleicher Artikel unmittelbar hintereinander erfolgt sind.

Hama, Marktführer für Zubehör für Consumer Electronics und Multimedia, ist einer der ersten Hersteller, der Ware in dieser Art gesichertem Zustand ausliefert. „Für unsere Produkte wünschen wir uns schon lange ein solches System. Die Lösung kommt genau zur richtigen Zeit. Wir setzen darauf", sagt Christoph Hundhausen, Hama-Vertriebsleiter Consumer Electronics. „Jetzt sind wir in der Lage, zum Beispiel Speicherkarten als Selbstbedienungsartikel zu verkaufen. Damit eröffnen sich dem Handel weitere Absatzkanäle und ein deutlich höheres Absatzpotenzial."

Auch auf die Wegfahrsperre hat man lange gewartet. Heute ist sie praktisch Standard…

WWW.DIGITAL-SAFETY.DE

„Skimming kratzt am Image!"

Über das Ausspähen von Kartendaten am PoS und wie sich der Einzelhandel dagegen schützen kann / Mit Frank Wio von easycash sprach Arne Trapp

Das „Skimming", also das Ausspähen von Kartendaten, hat längst auch den Einzelhandel erreicht. Ursprünglich hatten es Kriminelle auf die Daten von Kredit- oder Bankkarten abgesehen. Der ausgelesene Inhalt der Magnetstreifen führte zusammen mit der geklauten PIN direkt zum Zugriff aufs Bankkonto. Tatort des Ausspähens war in der Regel der Geldausgabeautomat. Doch das geht natürlich auch mit den Terminals am Point oft Sale (PoS) im Einzelhandel. Dem wollen die Betreiber von Supermärkten, Kaufhäusern und kleinen Läden natürlich einen Riegel vorschieben.

SECURITY *insight*: Herr Wio, wie gehen die Täter beim PoS-Skimming vor?

Frank Wio: Wie auch die Festnahmen der Kripo beweisen, sind die Banden perfekt organisiert: Einbruchs- und IT-Experten sind spezialisiert auf diese Form der Straftaten. Das Vorgehen ist in verschiedene Phasen zu kategorisieren: Erst ausspähen, dann in die Geschäfte einbrechen, Terminals manipulieren, Daten auslesen, Dubletten der Karten erstellen. Da deutsche Geldautomaten diese Dubletten erkennen, setzen die Betrüger sie im Ausland ein, um Geld abzuheben.

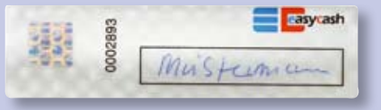
Wie hoch ist das Risiko für Konsumenten und Banken?

Trotz anderslautender Presseberichte: Das Risiko für Konsumenten, Opfer von Skimming-Betrug zu werden, ist vergleichsweise gering. Bei 550.000 Kartengeräten verzeichneten wir 2007 bundesweit gerade mal zwölf Manipulationsfälle an PoS-Terminals. Anders ausgedrückt: Während der Schaden durch Falschgeld-Straftaten in diesem Zeitraum 3,8 Millionen Euro beträgt, verursachte Skimming Schäden von 2,5 Millionen Euro. Das schließt den Betrug am Geldautomaten allerdings nicht ein. Die Polizei meldet überdies mittlerweile durchschlagende Erfolge. Zahlreiche Verhaftungen haben sich als Aderlass für kriminelle Banden erwiesen. Was den finanziellen Schaden der Kartennutzer betrifft, so sind die Banken in der Haftung. Endkunden wird der Schaden ersetzt – im Gegensatz zu Falschgeldschäden. Und auch auf Seiten der deutschen Banken ist das Risiko überschaubar: Da die Abhebungen ausnahmslos im Ausland stattfinden, haften auch hier die ausländischen Geldinstitute, deren Infrastruktur die Abhebungen erst ermöglichen.

Und wie sieht es mit den betroffenen Geschäften aus?

Für sie bedeutet es natürlich zunächst einmal einen Imageschaden. In der Regel waren Filialen großer Fachmarktketten betroffen, da sie über identische Sicherheitsstrukturen und hohe Kassendurchsätze verfügen. Uns liegen jedoch keinerlei Informationen über nachhaltige Umsatzeinbußen vor, die mit den Manipulationsfällen in Verbindung stehen.

Die beiden haben offensichtlich keine Angst davor, beim Bezahlen mit Karte Skimming-Opfer zu werden.



Das Siegel macht Manipulationen am Terminal sichtbar.

easycash hat ein Sicherheitssiegel entwickelt, das die Terminalmanipulation verhindern soll. Wie funktioniert das?

Damit keine Missverständnisse entstehen: Unser neues Siegel verhindert Manipulationen nicht – es macht sie sichtbar. Um PoS-Terminals zu manipulieren, muss man die Geräte öffnen. Unser Siegel ist so beschaffen, dass es, einmal aufgeklebt, nicht ohne Beschädigung entfernt werden kann. Beim Öffnen der Geräteschalen wird es zwangsläufig beschädigt; Manipulationen werden sichtbar, das Ausspähen der Kartendaten wird erschwert. Fälschungssicherheit erreichen wir durch extrem hochwertiges Material und Hologramm-Technologie. Außerdem ist jedes Siegel mit einer eindeutigen, individuellen Nummer und einem Unterschriftenfeld versehen. Durch die spezielle Vollflächen-Laminierung ist der Schutz des Siegels und der aufgebrachten Unterschrift langfristig gewährleistet.

Mal abgesehen von Ihrem Siegel – welche Sicherheitsmechanismen setzt die Zahlungsverkehrsbranche gegen Skimming ein?

Mittelfristig wird der so genannte EMV-Chip den Magnetstreifen auf Debitkarten ersetzen. Diese chipbasierende Lösung gilt als fälschungssicher. Bereits 60 Prozent der im Umlauf befindlichen Karten sind damit ausgestattet, bis 2010 soll diese Funktionalität flächendeckend verfügbar sein. Darüber hinaus gibt es Ansätze, die sich in verschiedenen Umsetzungsstadien befinden. Interessant ist sicher die Entwicklung von Überwachungssystemen, die verdächtige Vorgänge direkt in den Terminals identifizieren und so einen schnellen Eingriff ermöglichen.

Frank Wio ist Geschäftsleiter Operations bei der easycash GmbH. Das Unternehmen bietet seit über zehn Jahren Lösungen zur Abwicklung des kartengestützten bargeldlosen Zahlungsverkehrs am Point of Sale.

Welchen Lösungsansatz halten Sie für viel versprechend?

Die Kombination der verschiedenen Ansätze. Dabei spielt das holografische Sicherheitssiegel eine zentrale Rolle, da es als eine der ersten Maßnahmen flächendeckend verfügbar ist. Der Handel wird dahingehend informiert und ist meiner Meinung nach auch ausreichend für das Thema Skimming sensibilisiert. Zusätzliche Sicherheit bietet die Umstellung des PIN-basierenden Zahlverfahrens auf unser OLV-System. Sämtliche Zahlungen werden dabei mit unserer Sperrdatei *HWD* abgeglichen. Mehr als 2,5 Millionen aktuelle Einträge machen sie zur aussagekräftigsten Blacklist. In Verbindung mit dem Forderungsankauf (Factoring) sind Zahlungsausfälle damit ausgeschlossen. Und da von Manipulation nur PIN-basierende Verfahren betroffen sind, ist das Online-Lastschriftverfahren mehr als eine Alternative.

WWW.EASYCASH.DE