

Die Sicherheitsphilosophie der Banken – Nutzen für den Handel



Alexander von Stülpnagel

Sprecher der
Geschäftsführung
Informatikzentrum der
Sparkassenorganisation
GmbH / SIZ

Grüß Gott, Frau Straub, meine Damen und Herren.
Ich bin mir nicht sicher ob ich an dieser Stelle so ganz richtig platziert bin, weil ich weder aus Baden-Württemberg noch direkt aus dem Handel bin. Aber, was uns verbindet, ist das gemeinsame Interesse am Thema Sicherheit. Ich will Ihnen heute vorstellen, was wir zum Thema Sicherheit in der Sparkassen-Finanzgruppe machen, was wir für die Zukunft erwarten und wie der Handel von diesem Wissen profitieren kann.

Das Thema Sicherheit wird generell in der Wirtschaft, im Handel und für Sie als Unternehmer immer wichtiger. Ich habe Ihnen dazu eine ganz aktuelle Umfrage mit dem Titel „Wirtschaft bangt um Sicherheit“ mitgebracht, die in der Süddeutschen Zeitung publiziert wurde. Darin heißt es: „In der deutschen Wirtschaft wächst die Angst vor Angriffen aus dem Internet. Drei von vier Sicherheitsbeauftragten in den Unternehmen erwarten eine Zunahme der Gefährdung, vor allem durch Hacker und Viren, ergab eine Umfrage der Arbeitsgemeinschaft der Sicherheit der Wirtschaft.“ Dabei ist es wichtig, dass es weniger um Datenspiionage geht, als vielmehr die Unternehmen befürchten müssen, durch solche Angriffe in ihren internen Abläufen beeinträchtigt zu werden.

Die Angriffe bekommen also eine ganz andere Qualität. Es geht nicht mehr nur um Themen wie sicheres Bezahlen, Datendiebstahl, Produktpiraterie, Korruption oder Kriminalität im Internet

im Allgemeinen, sondern es geht um die Infrastruktur in den jeweiligen Unternehmen. Wir stehen noch am Anfang dieser Thematik und ich fürchte, die Gefahren werden hier leider zunehmen. Und im Zusammenhang mit der verstärkten Nutzung des Internet werden sich Unternehmen jeder Größenordnung immer mehr mit diesem Thema befassen müssen.

Ich möchte Ihnen davon berichten, was die Banken respektive die Sparkassen in diesem Bereich machen. Schon lange bevor es das Internet gab sind die Banken und Sparkassen ja mit dem Thema Sicherheit in besonderem Maße konfrontiert worden, denn das Geld soll und muss bei den Sparkassen oder Banken sicher sein, und das bedeutet letztlich, die Dinge auch in anderen Bereichen sicher zu gestalten.

Wir, das SIZ, sind als Unternehmen innerhalb der Sparkassen-Finanzgruppe mit diesem Thema befasst. Darüber hinaus betreuen wir aber auch weitere Institute der Finanz- und Versicherungswirtschaft, Industrie- und Handelsunternehmen und wir entwickeln konkrete Lösungen z.B. im Elektronik Banking. Sie werden von mir jetzt jedoch keine Verkaufsveranstaltung für irgendwelche Technik bekommen, mit der alles sicher wird, vielmehr möchte ich zu Ihnen über das Thema IT und IT-Sicherheitsmanagement sprechen. Darüber, dass es nicht genügt, nur Technik aufzubauen, sondern dass man sich auch organisatorisch damit befassen muss. Sicherheit ist ein Thema für jeden – es

trifft uns alle, im Privatleben wie im Unternehmen. Wir als SIZ sind der Meinung, dass es da grundsätzliche, branchenunabhängige Anforderungen gibt. Ich möchte Ihnen zeigen, dass Sie die Erfahrungen aus dem Bankensektor auch in die Unternehmen übertragen können, dass dort auch ähnliche Lösungen vorstellbar und einsetzbar sind. Und schließlich möchte ich auch noch kurz auf etwas eingehen, mit dem Sie im Handel täglich zu tun haben - auf den Zahlungsverkehr.

Lassen Sie uns zuerst kurz darauf kommen, warum Sicherheit uns alle angeht. Immer mehr Geschäftsprozesse bei den Banken, wie auch in Unternehmen werden durch IT-Anwendungen und IT-Systeme abgebildet oder unterstützt. Diese IT-Prozesse gilt es entsprechend abzusichern. Denn wenn die IT nicht mehr läuft, läuft der Prozess nicht mehr, läuft das Geschäft nicht mehr. Der Unternehmenserfolg ist direkt mit der Infrastruktur verzahnt. Denken Sie einfach mal daran, was passieren würde, wenn Ihre IT abgeschaltet wird. Könnten Sie dann noch so weiterarbeiten wie bisher? Haben Sie dafür ein Notfallkonzept, damit Sie zumindest für einen bestimmten Zeitraum weiter arbeiten können? So etwas muss eine Bank natürlich besonders überprüfen und dafür vorsorgen, denn wir könnten ja immer mit einem Ausfall konfrontiert werden.

In der Finanzwelt haben wir strenge Vorgaben seitens des Gesetzgebers bzw. der Aufsicht, welche von ihrer Seite darauf achtet dass die Infrastruktur möglichst sicher ist. Auch die Wirtschaftsprüfer sind entsprechend aufgestellt. Ebenfalls ein wichtiger Punkt ist die Internationalisierung des Handels und der Finanzdienstleistungen. Dabei gilt, je mehr sich die IT-Unterstützung von Geschäftsprozessen für Unternehmen als wirtschaftlich sinnvoll darstellt, je mehr Angriffsfläche entsteht. Und entsprechend nimmt die darauf spezialisierte Kriminalität zu.

Es gibt immer mehr elektronischen Geschäftsverkehr zwischen Kunden und Unternehmen und zwischen den Unternehmen. Wenn hier neue technische Felder erschlossen beziehungsweise Prozesse verbessert werden, bedeutet das eben

auch neue Risiken. Wenn ich die Informationstechnologie nutze, dann muss ich auch für den Fall vorsorgen, dass diese Technologie angegriffen wird oder nicht mehr zur Verfügung steht. Ein Beispiel wie es erst kürzlich vorgekommen ist: Wenn an der Schnittstelle zum Kartenleser am POS manipuliert wird, Geräte illegal ausgetauscht oder dazwischen geschaltet werden - erleben Sie unmittelbar die Problematik der Infrastruktur. Den Schaden hat das Unternehmen, den Schaden hat der Kunde. Hier muss man vorbeugen.

Wir meinen, dass es dabei ganz wichtig ist, dieses Thema nicht nur rein technisch, sondern ganzheitlich zu betrachten. Sich nicht nur einen bestimmten Baustein im Unternehmen anzusehen nach dem Motto: „Jetzt schaue ich mir mal an, ob meine Sicherheits-Türen auch wirklich alle zugeschlossen sind.“ Denn was uns eigentlich fordert, sind die ganzen Zusammenhänge, weil die Welt immer komplexer wird.

Schauen Sie sich hier Gefahren an, wie sie uns in der Sparkassenwelt begegnen. Wir beobachten bestimmte Sicherheitsangriffe schon seit einigen Jahren. Und Sie sehen, dass die zunehmen. Und was noch schlimmer ist, es nehmen vor allem die Angriffe mit dem höheren Risiko zu. Nicht die einfachen, die man schnell in den Griff bekommen kann, sondern es nehmen die roten und gelben Balken zu, die einen größeren Schaden verursachen, beziehungsweise ein größeres Ausmaß haben. Das ist Fakt und ich fürchte, die Kurve wird auch die nächsten Jahre weiter so steigen. Trotz aller Maßnahmen, die wir treffen, wird es also immer ein Wettlauf zwischen Hase und Igel sein. Wenn wir etwas Neues machen, werden auf der anderen Seite wieder neue Angriffsmöglichkeiten entwickelt. Ein zweites Phänomen, das Sie auch alle kennen: Heute geht alles viel schneller. Wenn irgendein PC befallen wurde, dauerte es vor einiger Zeit noch 26 Stunden, bis 350.000 PCs befallen waren. Heute werden bestimmte Viren in 15 Minuten verbreitet, weil wir eben so vernetzt sind, wie wir sind. Dieses Phänomen lässt sich nicht ändern und insofern geht es umso mehr darum Vorsorge zu treffen.

Wenn ich Sie jetzt frage, ob Sie schon einmal Sicherheitsprobleme in Ihrem Unternehmen hatten, würde ich die Antwort erwarten: „Na ja, eigentlich ist noch nicht so viel passiert“. Vielleicht sind Sie aber auch schon lahm gelegt worden, durch einen Virus, ein trojanisches Pferd oder dadurch, dass tatsächlich die Daten selbst korrumpiert wurden.

Auf dieser Folie sehen sie, dass es Dinge gibt, die nicht so häufig auftreten und in der Presse stehen, deren Schadenspotenzial aber sehr hoch ist. Zum Beispiel, wenn wirklich jemand ins Netzwerk eindringt und sich über einen bestimmten Zeitraum Daten holt oder Dinge manipuliert, ohne dass Sie es merken. Man hat zwar entsprechende Kontrollen, aber es dauert immer einige Zeit, bis man merkt, dass da etwas nicht stimmt.

Umso wichtiger ist es, hier rechtzeitig Vorsorge zu treffen. Denn wenn so etwas passiert, ist es meist schlimmer, als wenn ein PC von einem Virus befallen ist. Den PC kann man abhängen, saubermachen und dann ist die Welt wieder in Ordnung. Die finanziellen Schäden wieder auszugleichen macht dagegen unendlich viel mehr Mühe.

Sicherheitsprobleme sind meist direkt oder indirekt mit finanziellen Schäden verbunden. Denn Arbeitsstillstand kostet nun mal Geld. Wenn ein Unternehmen Ergebnisse verliert, kostet es Geld, sie wieder herzustellen. Wenn Sie kompromittiert werden und dann beim Konkurrenten bestimmte Dinge wiederfinden, ist das mit Sicherheit auch finanziell von Nachteil. Wenn Sie nicht mehr mit einem anderen Partner, Lieferanten oder mit dem Kunden kommunizieren können, weil bestimmte E-Mails nicht mehr funktionieren, ist es wirtschaftlich ebenfalls schädlich. Unter Umständen müssen Sie auch dem Gesetzgeber Rede und Antwort stehen, wenn Sie bestimmte Vorschriften nicht befolgen.

Für den Handel habe ich an dieser Stelle noch zwei Punkte dazu genommen. Das Problem, eine ungedeckte Lastschrift wieder zurückbekommen. Oder dass ein Terminal selbst manipuliert wird.

Fazit 1: Wir haben alle in der einen oder anderen Weise mit dem Thema Sicher-

heit zu tun. Und das wird in Zukunft noch deutlich zunehmen. Was ist jetzt zu tun? Das erste, was ich Ihnen mitgeben möchte ist, wie wir eine Lösung für die Sparkassen-Finanzgruppe gemacht haben und dass diese Lösung auch auf andere Branchen übertragbar ist. Schauen Sie sich einmal an, wie Ihre Geschäftsprozesse mit IT unterlegt sind. Wie ist was wo hinterlegt und beschrieben? Kennt jemand die Zusammenhänge - was mit wem wie läuft, wie kommuniziert, ersetzt wird und so weiter? Denn Sie werden immer wieder neue Hardware und neue Software benötigen. Da findet ein ständiger Wechsel statt und deshalb müssen Sie wissen, wie Ihre Infrastruktur aussieht, angefangen von Kunde und Handel über die Niederlassung bis hin zur Unternehmenszentrale oder einem entsprechenden Rechenzentrum.

Wenn Sie diesen Überblick haben, gibt es zwei ganz große Themen. Was passiert in den Niederlassungen? Sind dort die Dinge tatsächlich so hinterlegt und abgesichert, wie es notwendig ist? Und dann: Wie steht es um die Anbindung an die Zentrale und um den Zugriff auf die Niederlassung selbst? Das ist zum Beispiel wichtig für die Sparkassen, die selbst eine große IT haben, aber auch von den Großsystemen der Rechenzentren beliefert werden. Ein Teil läuft in den Zweigstellen, ein Teil läuft in der Hauptstelle und ein Teil läuft auf dem zentralen Rechner, mit dem eben viele Sparkassen bedient werden. Hier geht es darum, dass aus der Sicht der Sparkasse alles ineinander greift und jedes Teil für sich, aber auch die Kommunikation untereinander sicher ist. Die einzelne Sparkasse kann sich nicht allein darauf berufen, dass das externe Rechenzentrum das schon alles erledigt. Es muss, zumindest nach unserer Gesetzgebung, selbst überprüfen, ob das Rechenzentrum sicher aufgestellt ist und beispielsweise Notfallübung macht. Wenn ein Industrie- oder Handelsunternehmen eine entsprechende Infrastruktur hat, gilt das natürlich genauso.

Deutlicher wird es, wenn Sie einmal die Kommunikation zwischen einzelnen Firmen, Lieferanten, Unterlieferanten und Kunden betrachten: Hier wird heute in vielen Fällen per E-Mail kommuniziert.

Und man geht davon aus, dass das, was ich sende, tatsächlich auch das ist, was ankommt. Dass die E-Mail nicht manipuliert ist und dann auch die gewünschte Reaktion erfolgt. In der Regel verschicken wir Dinge unverschlüsselt, unsigned, damit alles einfacher ist, aber genau dort ist natürlich eine Angriffsfläche für entsprechende Hacker. Man muss sich daher fragen, wie sensibel bestimmte Dinge für das Unternehmen sind, ob ich sie zum Beispiel verschlüsseln oder gar nicht über einen solchen Kanal schicken soll, der trotz aller Firewalls einfach doch nicht hundertprozentig sicher ist.

Eine der Maßnahmen ist: Sich zu überlegen, welche Information so sensibel ist, dass sie auf keinen Fall kompromittiert werden darf. Denn dann fragen Sie sich auch, was sind die jeweiligen Auswirkungen, wenn ein Angriff passiert? Wenn jemand nur zufällig mitliest, macht es zunächst einmal nichts. Aber wie gerade auch in dem erwähnten Zeitungsartikel stand: Das ist oft nicht nur ein zufälliges Mitlesen, sondern ein bewusstes Angreifen. Man will sehen, welche Daten versendet werden. Man will diese dann auch bewusst verändern und vielleicht auch Zugangsdaten auslesen oder Informationen weitergeben – zum Beispiel an die Presse. Wir kennen das heute vor allem aus den USA. Weil dort meines Erachtens noch viel zu wenig die Managementseite gesehen wird. Da wird viel Technik aufgebaut, um Sicherheit zu erreichen. Aber es wird weniger der ganzheitlich systematische Ansatz verfolgt, den ich Ihnen hier nahe bringen will.

Meine Botschaft ist, nicht nur den technischen Aspekt zu betrachten - dass ich dieses und jenes auf meiner Firewall mache oder auch die richtige Schließanlage habe, wenn ich einmal nicht nur die IT-Seite sehe. Es geht vor allem darum, und das ist unsere Erfahrung, die Dinge organisatorisch in den Griff zu bekommen und die Mitarbeiter für das Thema zu sensibilisieren.

Ich möchte Ihnen bewusst machen, dass Sie sich selbst fragen: „Wie ist es denn bei uns eigentlich geregelt? Gibt es Bereiche, wo ich nicht genau weiß, ob alles wie geplant funktioniert und bin ich si-

cher?“ Dabei ist die Sensibilisierung der Mitarbeiter ein ganz wichtiges Thema.

Und nun zur Lösung, die die Sparkassen-Finanzgruppe gewählt hat.

Sie hat sich gesagt: Wir haben ein gewisses Gesamtrisiko. Das müssen wir erstmal zur Kenntnis nehmen und uns dann überlegen wie wir dieses dann verringern können. Wir haben mehrere Möglichkeiten. Wir können das tun, was jeder andere auch tut. Wir bauen Technik auf und konfigurieren sie so, damit wir von der Seite nicht so leicht angegriffen werden können und uns dem „state of the art“ entsprechend abschotten.

Das machen Sie in der Regel heute auch. Sie nehmen keine unbekannt technischen Komponenten ins Haus, sondern nur solche, von denen Sie zumindest annehmen, dass sie sicher sind oder Ihre entsprechenden Systeme sicher machen.

Damit kommen wir zu der Stufe des vermeidbaren Risikos. Was sich bei uns bewährt hat und ich deshalb der Wirtschaft generell empfehlen würde, das heißt „Ganzheitliches Sicherheitsmanagement“. Genau wie man z.B. ein ganzheitliches Personalwirtschaftskonzept hat, bei dem man sich fragt: „Wo will ich denn hin mit meinem Unternehmen, was steht da an, wie bekomme ich den entsprechenden Nachwuchs, welche Möglichkeiten muss ich bieten?“, genauso geht es auch hier darum, das Sicherheitsmanagement als Prozess aufzusetzen. Das fängt damit an, dass ich jemanden habe, der dafür verantwortlich ist. Nämlich den Sicherheitsbeauftragten, der in dem schon erwähnten Zeitungsartikel befragt wurde. Aber wer hat überhaupt Sicherheitsbeauftragte? Meistens macht das irgendjemand so nebenher mit. Fragen Sie den dann auch mindestens alle drei Monate einmal danach, was denn eigentlich gewesen ist, was als nächstes ansteht, ob diese und jene Dinge umgesetzt und das alles auch dokumentiert wurde?

Das sind die Fragen aus dem Sicherheitsmanagement, mit dem Sie Ihr Risiko zumindest um das verringern können, was Sie selbst steuern können. Wir können natürlich immer noch angegriffen

werden, und das werden wir auch, wie ich eben schon dargestellt habe. Und auch dagegen gibt es Mechanismen. Wir haben in der Finanzgruppe ein CERT, ein Computer Emergency Response Team oder auf deutsch: ein Notfallteam. Das ist eine Hotline mit Experten, die bei einem Virus oder anderen Angriffen angerufen werden und dann wissen, was zu tun ist und auch herauszufinden versuchen, woher der Angriff kommt und dann entsprechende Gegenmaßnahmen einleiten. Das gilt jetzt nur für die Sparkassen-Finanzgruppe, aber soweit ich weiß, gibt es bereits eine Initiative, so etwas auch für den Mittelstand zu entwickeln. Man kann dann Leistungen bündeln, Angriffe schneller beantworten, damit nicht jeder Einzelne alleine vor dem Problem steht.

So kommen wir auf das Restrisiko, das man dann akzeptieren kann und muss. Wir können ja nicht jeden Preis bezahlen, sondern müssen uns auf eine bestimmte Größenordnung einigen. Aber genau diese Frage ist immer die erste, die wir einer Sparkasse stellen: „Wie viel Risiko willst Du denn am Ende des Tages eingehen?“ Mit welchem Ausmaß an Risiko können Sie leben? Wenn Sie sagen, ich kann damit leben, dass dies und jenes nicht überprüft ist, dann wissen Sie das zumindest und kennen Ihre Restrisiken. Man muss sich dieses Risikos bewusst werden, es weitestgehend minimieren, dann kann man es akzeptieren. Unser Vorschlag ist, die Risikobetrachtung systematisch anzugehen. Durch einen Sicherheitsbeauftragten, der berichtet, durch die entsprechende Technik aber auch durch physikalische Sicherheitsmaßnahmen, um beispielsweise einen Einbruch zu verhindern.

Wie sehen die entsprechenden Szenarien aus, wie lauten die Fragen? Habe ich an alles gedacht, alles überprüft – auch für den Fall, dass es mal nicht funktioniert. Beispielsweise sind Vertragsbeziehungen ein häufig unterschätztes Thema: Was passiert, wenn mein Zulieferer mal drei Stunden lang nicht kommt? Wer trägt dann die Verantwortung wofür? Auch ist zu prüfen, wo man Kosten optimieren kann. Ebenso wichtig ist auch der Bereich des generellen Betriebs einer solchen wie auch immer gearteten technischen Infrastruk-

tur. Das alles gehört zum Thema Sicherheitsmanagement dazu.

Und so fassen das jetzt die Banken und Sparkassen an: Sie gehen nicht nur punktuell in logische und technische Sicherheit, sie machen nicht nur Notfallplanung, sondern gehen das ganze Thema umfassend an. Wir haben dafür ein Konzept entwickelt, an das sich inzwischen die gesamte Sparkassen-Finanzgruppe angeschlossen und auch implementiert hat. Die einzelnen Sparkassen und Verbundpartner haben die jeweilige Ausprägung gewählt und unser Konzept ist zum de facto-Standard geworden. Und wenn das bei so vielen Unternehmen erfolgreich war, dann müsste das eigentlich auch bei allen anderen Unternehmen funktionieren, die sich um das Thema Sicherheit Gedanken machen. Deshalb stelle ich Ihnen das Konzept hier vor.

Wir fangen in der Regel damit an, dass wir in die Häuser gehen und Fragen stellen, um den Stand des Sicherheitsmanagements des Unternehmens zu erfassen. Dabei können wir die typischen Fragen relativ schnell gemeinsam durchgehen und dann auch aufzeigen, ob und wo es Handlungsbedarf gibt. Dies stellt dann auch schon einen wichtigen Mehrwert dar.

Welche Prozesse sind für mich überhaupt relevant, welche muss ich von der Sicherheit her anders betrachten als andere. Denn während der eine Prozess 24 Stunden stillsteht, macht es mir vielleicht nichts aus, bei einem anderen aber schon. Ich muss das entsprechend bewerten, zuordnen und mich dann fragen: „Was habe ich bereits getan? Welche Dinge liegen vor, dokumentiert oder verfahrensmäßig?“ Die eigentliche Kernfrage ist: „Will ich daran etwas ändern? Kann ich damit leben? Ist mir diese Änderung auch das Geld wert, das sie kostet?“ Und dann haben Sie einen Maßnahmenkatalog, mit dem Sie wissen, wo Sie stehen und wie Sie weiter vorgehen.

Die erste wichtige Erkenntnis ist: Wir müssen diesen Prozess umfassend sehen und bekommen dann am Ende des Tages einen umfassenden Blick auf die Dinge. Das ist für jedes Unterneh-

men ein zentraler Mehrwert: Alle meine Sicherheitsanforderungen sind definiert, die Verantwortlichkeiten benannt, die Sicherheitslücken identifiziert und der Umsetzungsbedarf festgelegt. Das alles wird dann bei uns in einem technischen System hinterlegt. Darin sind alle Aspekte bereits vorformuliert. Sie müssen nur noch Ihre Ergebnisse dort eintragen.

Und damit kommen wir zu Erkenntnis Nummer 2:

Das, was wir hier in der Sparkassen-Finanzgruppe schon einige 100mal angewendet haben, die gleichen Fragen, die gleiche Thematik – das lässt sich auch auf den Mittelstand anwenden. Die Geschäfte einer Sparkasse sind natürlich andere als die im Handel. Aber es sind immer Geschäftsprozesse, die per IT unterstützt werden. Diese Übertragung haben wir in mehreren mittelständischen Unternehmen getestet.

Die Kunden waren sehr angetan und haben gesagt: „Jawohl, wir haben das gleiche Problem. Wir müssen manche Dinge vielleicht nicht so intensiv machen, wir haben keine Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), die uns beäugt. Wir haben nur die Wirtschaftsprüfer. Aber wir sind trotzdem der Meinung, dass wir Handlungsbedarf haben.“ Das unterstreicht unsere Botschaft, dass unsere Erfahrungen übertragbar sind.

Lassen Sie mich zum Ende noch einmal auf das Thema Sicherheit im Zahlungsverkehr eingehen, denn wir sind hier ja auf einem Handelsforum. Als Informatikzentrum befassen wir uns mit anderen Partnern intensiv mit diesem Thema. Denn natürlich tun die Banken alles, um einen sicheren Zahlungsverkehr zu ermöglichen. Das geschieht in der Regel in Abstimmung mit allen Bankengruppen über den so genannten Zentralen Kreditausschuss (ZKA). In dieser Hinsicht sind wir in Deutschland ganz gut aufgestellt. Das gibt es nicht in jedem europäischen Land, dass an dieser Stelle so eng zusammengearbeitet wird. Auch im Bezug auf Sicherheit sind wir überhaupt nicht im Wettbewerb. Sondern gemeinsam daran interessiert, alles so sicher wie möglich zu machen, damit der Unternehmer, der Kunde und der Händler davon profitieren.

Sie kennen vermutlich die Diskussion um den Wechsel vom Magnetstreifen zum Chip. Das wird kommen, denn das bringt deutlich mehr Sicherheit. Außerdem kann man damit auch viele Zusatzfunktionen realisieren und in den Markt bringen, auf die ich jetzt aber nicht weiter eingehen will.

Wir haben festgestellt, dass ein Chip die Infrastruktur viel sicherer macht als ein Magnetstreifen. Den Chip kann man nicht ohne weiteres kopieren, den kann man auch nicht auslesen.

Diese Umstellung liegt also in Ihrem Interesse, damit der Handel an dieser Stelle sicherer wird. Natürlich kostet das etwas mehr als eine Lastschrift. Dafür haben Sie aber auch die Zahlungsgarantie. Dahinter steht die EMV-Initiative der Kreditkartenhersteller, d. h. dieser Chip ist standardisiert, wird also weltweit in dieser Form eingeführt. Die letzten Zahlen, die ich dazu habe sind von 2007. Da waren die Herausgeber der Karten europaweit schon bei fast 70 % EMV-Unterstützung und auch die Händlerseite schon bei 65 % Akzeptanz von EMV-Karten. Es gibt auch schon einige Erfolgsbeispiele dafür, dass durch diese Technologie Kartenausfälle reduziert werden können.

Das Thema Chip wird auch durch das Thema SEPA, die Single Euro Payment Area, getrieben. Parallel zum Euro wird jetzt auch ein einheitlicher europäischer Zahlungsraum mit einer gemeinsamen technischen Lösung für Debit-Zahlungen, Überweisungen und Lastschriften entstehen.

Das bringt sowohl für Kunden viele Vorteile, aber auch für die Händler, die in verschiedenen Ländern aktiv sind. Viele Dinge im europäischen Zahlungsverkehr vereinfachen sich dann sehr. Das hat natürlich auch Migrationsaspekte. Stellen Sie sich zeitig auf EMV ein, nutzen Sie Verfahren, die das unterstützen. Denn das ELV-Verfahren ist in dieser Form nicht mehr vorgesehen. Die technische Umsetzung wird hinter den Kulissen stattfinden. Als Händler werden Sie das an Ihren Terminals merken und als Unternehmer auch daran, dass Sie dann europaweit Lastschriften machen können.

Das war also mein kleiner Ausblick zum Thema Sicherheit für den Handel. Mein Fazit besteht aus zwei Teilen: Zum einen geht es darum, die Menschen zu sensibilisieren. Es gilt Sicherheitsbewusstsein zu schaffen. Zum anderen sollte man sich nicht sagen: „Das passiert mir nicht, wird schon gut gehen“. Das ist natürlich auch eine Art Sicherheitsstrategie. Aber wenn dann doch einmal etwas passiert, kann es sehr unangenehm werden. Im Verhältnis zu diesem Risiko ist es sicherlich besser sich vorher einen Überblick zu verschaffen und entsprechende Maßnahmen zu ergreifen. Nach dem Motto: „Die beste Alarmanlage nützt nichts, wenn sie nicht eingeschaltet wird.“

Das ist meine Botschaft an Sie.
Vielen Dank!