SICHERHEIT IM DIGITALEN ZEITALTER

- Migration von Sicherheitstechnik und Gefahrenmeldeanlagen von ISDN auf IP- und Cloud Technologien

Ein Analyst Report erstellt im Auftrag der ITENOS GmbH

von Dr. Carlo Velten und Meike Buch

crisp RESEARCH

ITENOS

INHALTSVERZEICHNIS

KAPITEL 1: DIGITALER UMBRUCH – WARUM DIE UMSTELLUNG VON ISDN AUF IP-NETZE SICHERHEITSVERANTWORTLICHE ZUM HANDELN ZWINGT

„Mit der neuen IP basierten Technik vereinfachen wir den Betrieb für Leitstellen und reduzieren damit Aufwände und Kosten. Für unsere Endkunden bieten wir hochwertige Bandbreite vor Ort, um beispielsweise eine effektive und kostengünstige Videoüberwachung ergänzend zu der Gefahrenmeldeanlage zu nutzen." (Karsten Lebahn Leiter IPT Sonderdienste, Deutsche Telekom)

Im Mai 2015 hat die deutsche Telekom die finale Ablösung ihrer ISDN-Netze durch eine IP-basierte Plattform bis zum Beginn des Jahres 2018 beschlossen. Um dem technologischen Fortschritt Rechnung zu tragen, werden auch die übrigen deutschen Telekommunikationsanbieter diesem Beispiel zeitnah folgen. Vor allem auf die Nutzer von Gefahrenmeldeanlagen und Leitstellenbetreiber, welche zu großen Teilen auf die ISDN-Technologie gesetzt haben, kommt aus diesem Grund in den kommenden Jahren eine wichtige Umstellung zu, welche die betroffenen Unternehmen zum Handeln zwingt. Unternehmensangaben der Deutschen Telekom zu folge haben erst ca. 15% der KMUs auf die Umstellung reagiert[1] , die übrigen Firmenkunden der deutschen Telekom müssen bis spätestens im Jahr 2018 diesem Beispiel gefolgt sein.

Auf der neu eingeführten IP-Plattform werden alle Dienste (Telefon, Internet, Sonderdienste, etc.), nunmehr gemeinsam über eine Leitung angeboten.

Die Umstellung auf „All-IP" erhöht somit die Flexibilität, da neue Dienste schnell über die IP-Leitung zu- und abgebucht werden können. Ein weiterer Vorteil der IP-Technologie besteht darin, dass eine deutlich höhere Bandbreite (bis zu 1000 mal höher als ISDN-Leitungen) sowie ein höheres Übertragungstempo ermöglicht werden. Die Umstellung ist seitens der Telekom schon im vollen Gange und soll voraussichtlich bis Ende 2018 abgeschlossen sein.

Für Standarddienste, wie z.B. Telefonanlagen und Netzwerke, bietet die Telekom den Kunden neue Verträge an und unterstützt beim Umstellen der Hardware. Anders ist dies jedoch bei angebotenen Sonderdiensten, wie z.B. bei Aufzugnotrufen und Gefahrenmeldeanlagen. Hier liegt es in der Verantwortung der Kundenunternehmen sich mit dem Thema der Umstellung auf IP-basierte Netze aktiv zu beschäftigen und auf die Herstellerfirmen und Dienstleister aktiv zuzugehen.

1 http://www.heise.de/ix/meldung/Telekom-umwirbt-Geschaeftskunden-mit-IP-Angeboten-2737361.html

„Das Ziel der Telekom ist die Umsetzung bis 2018. Man sollte schon angefangen haben sich damit auseinander zu setzen. Insbesondere die Errichter müssen auf ihre Kunden zugehen und informieren, dass es Umstellungen geben wird." (Thomas Urban, Bereichsleiter Security, VdS)

Doch wann ist für die Unternehmen der richtige Zeitpunkt, um sich mit der Umstellung der verwendeten Sonderdienste zu beschäftigen? Und wie sollen sie diese Umstellung am besten angehen? Mit diesen Fragen beschäftigt sich der vorliegende Report, welcher darauf abzielt, IT- und Sicherheitsverantwortliche in Unternehmen sowie Leitstellenbetreiber bei der Analyse, Planung und Konzeption ihrer Migrationsstrategien zu unterstützen.

ALARMANLAGENUMRÜSTUNG VON ISDN AUF IP-NETZE – WINTERREIFENWECHSEL ZUM RICHTIGEN ZEITPUNKT

Zur Beantwortung dieser Fragen kann folgende Analogie als plakatives Beispiel herangezogen werden: Die alljährliche Umstellung von Sommer- auf Winterreifen. Denn durch dieses Beispiel wird schnell und nachvollziehbar deutlich, dass der richtige Zeitpunkt den entscheidenden Einflussfaktor für den Erfolg darstellt:

Denn Autofahrer, die schon im August ihre Sommerreifen wechseln, gehen nicht ökonomisch mit ihren Ressourcen um, da die Winterreifen in den kommenden Monaten noch nicht benötigt werden und daher unnötig abgenutzt werden. Soll auf die Winterreifen zu dem Zeitpunkt umgestiegen werden, in welcher die Mehrzahl an Autofahrern ihre Reifen wechseln, so muss der Fahrer entweder selber das Wissen und die nötige Technik besitzen um die Reifen eigenständig zu wechseln oder aber lange Wartezeiten in den Werkstätten in Kauf nehmen. Die Konsequenz, die daraus entsteht, besteht darin, dass der Fahrer durch die Wartezeit eine Zeit lang nicht ausreichend mobil ist oder er sich die Mobilität teuer erkaufen muss (z.B. durch einen Mietwagen zur Überbrückung). Am schlimmsten trifft es jedoch diejenigen Autofahrer, die den Wechsel bis in den Dezember oder Januar aufschieben und erst den Wintereinbruch abwarten, bis sie handeln. Diese müssen ihr Auto im schlimmsten Falle ganz stehen lassen, da es sich ohne Winterreifen nicht mehr sicher bewegen lässt. Ähnlich verhält es sich bei der Umstellung von der ISDN-Technik auf IP-basierte Netze. Nur die Unternehmen, welche den richtigen Zeitpunkt für die Umstellung abpassen, können den Wechsel schnell, kostengünstig und effizient durchführen. Besitzen Unternehmen nicht das nötige Wissen, so können sie sich analog zum Winterreifen-Beispiel Hilfe von Experten suchen, welche die technologische Umstellung für sie planen und durchführen.

Für die Unternehmen, die ihre Gebäude und Liegenschaften über Gefahrenmeldeanlagen absichern sowie für Leitstellenbetreiber, gilt daher, dass sie sich frühzeitig, am besten sofort, über die weitreichenden Auswirkungen der IP-Umstellung informieren sollten. Denn bis 2018 ist es auch für die ISDN-basierten Gefahrenmeldeanlagen (GMA) an der Zeit, diese an die neue Technik anzupassen. Hierbei ist es nicht nur wichtig, eine Gefahrenmeldeanlage anzuschaffen, welche hardwareseitig IP-fähig ist.

Denn auch bei der Software und den verschiedenen Übertragungswegen gibt es wichtige Unterschiede, welche die Unternehmen beachten sollten. Durch das vergleichsweise geringe Zeitfenster kommen viele der Firmen jedoch in Bedrängnis, die sich bislang noch keine Gedanken über die Umstellung ihrer Anlagen gemacht haben. Denn gerade die zuverlässige Sicherung der Geschäfts- und Ladenflächen ist, nicht erst seit dem Anstieg der Bandenkriminalität und Einbrüchen in den letzten Jahren, für viele Firmen geschäftskritisch.

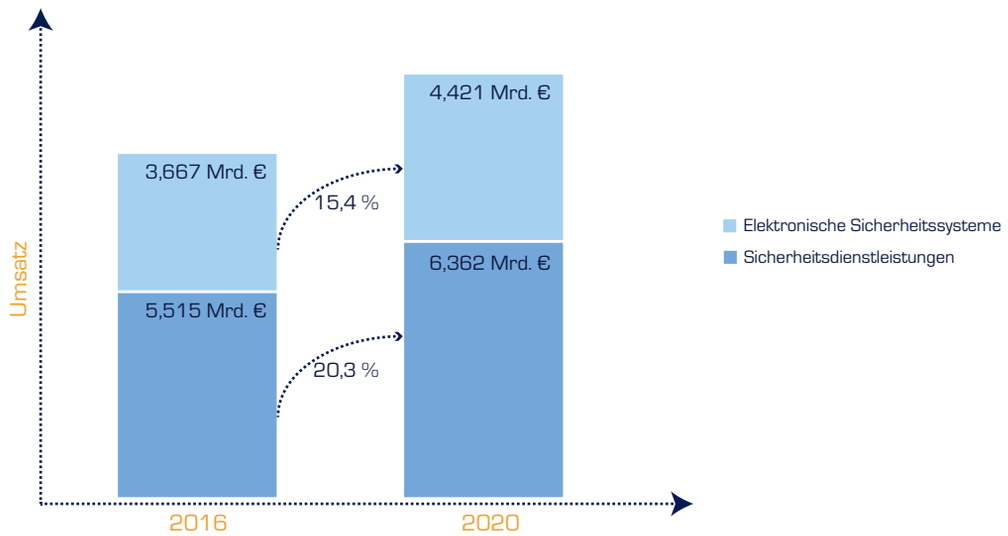
KAPITEL 2: SICHERHEITSMARKT IM DIGITALEN ZEITALTER

„Die Umstellung auf IP läuft auch bei Geschäftskunden auf vollen Touren. Bis Ende 2018 werden wir knapp vier Millionen Anschlüsse bei über zwei Millionen Kunden auf IP umstellen. Die erste Million haben wir schon gepackt." (Karsten Lebahn Leiter IPT Sonderdienste, Deutsche Telekom)

Der Markt für Sicherheitsdienstleistungen und elektronische Sicherheitssysteme unterliegt zusätzlich zu dem schon genannten technologischen Trend in Richtung IP-Übertragung auch den aktuellen politischen und gesellschaftlichen Entwicklungen und wird deshalb in den kommenden Jahren ein deutliches Wachstum aufweisen. So werden Flüchtlingsunterkünfte, welche im Zuge der aktuellen Flüchtlingskrise ausgebaut werden, zumeist von privaten Sicherheitsdienstleistern überwacht. Auch steigen laut Polizei, unter anderem bedingt durch verringerte Grenzkontrollen, die Einbrüche in Privat- und Geschäftsgebäuden stetig an.

Firmen und Privatleute investieren aus diesen Gründen massiv in den Ausbau ihrer Gefahrenmeldetechnik. Betragen die Ausgaben im B2B Sicherheitsmarkt in Deutschland im Jahr 2016 noch rund 9,182 Mrd. €, so werden sie im Jahr 2020 schätzungsweise auf 10,783 Mrd. € anwachsen. Dies entspricht einer Wachstumsrate von 17,4% über die Jahre 2016-2020, wobei das Wachstum zum einen durch die IP-Umstellung im Bereich der elektronischen Sicherheitssysteme voran getrieben wird. Zum anderen wird auch die Nachfrage an Sicherheitsdienstleistungen, wie einer Gebäudeüberwachung durch Wachpersonal und Drohnen, Integrationsdienstleistungen – und Beratung sowie (mobile) Sicherheitssoftware stark anwachsen.

Sicherheitsmarkt in Deutschland



Quelle:
Crisp Research AG, 2016

Bricht man den Sicherheitsmarkt nach Branchen auf, so können vier Hauptbranchen identifiziert werden:

- Gebäudevermietung
- Einzelhandel / Banken
- Industrieunternehmen
- Öffentliche Einrichtungen

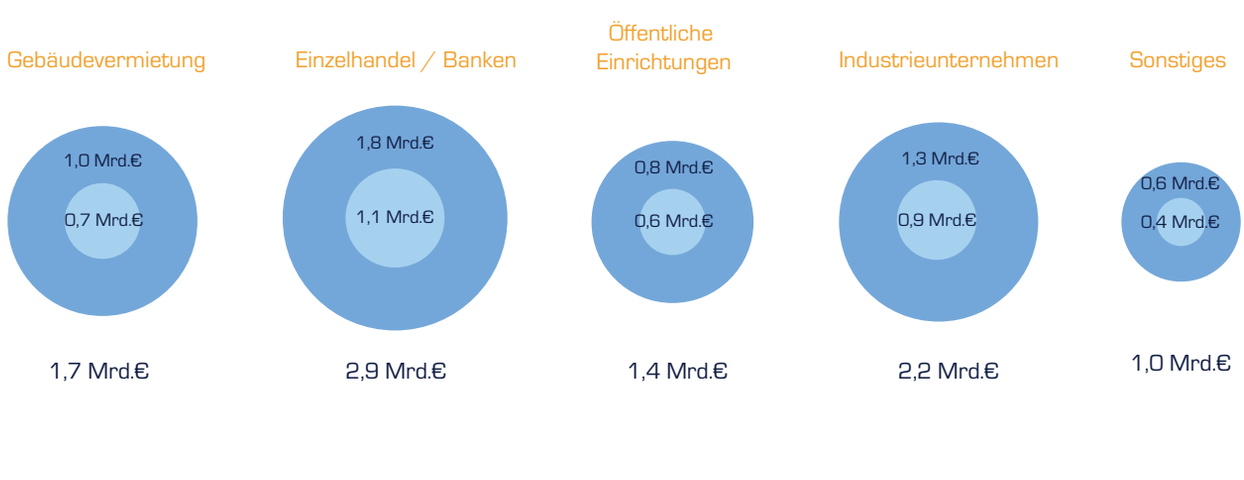
Der Einzelhandel stellt hierbei mit rund 2,9 Mrd. € Investitionskosten im Jahr 2016 den größten Zielmarkt dar, denn hier kommt es immer häufiger zu Ladendiebstählen, weshalb viele Einzelhändler auf moderne Überwachungstechnik setzen und entsprechend viel Geld investieren.

Innerhalb der öffentlichen Einrichtungen schwanken die Sicherheitsbedarfe stark. Während bei Gefängnissen oder Polizeistationen zumeist hohe Sicherheitsstufen gelten und dementsprechend viel in die neuste Sicherheitstechnik investiert wird, reicht es für Bibliotheken oder Verwaltungsgebäude zumeist, wenn eine installierte Gefahrenmeldeanlage weiterhin wie gewünscht funktioniert. Für öffentliche Einrichtungen belaufen sich die geschätzten Investitionskosten im Jahr 2016 auf ca. 1,4 Mrd. €.

Vor allem die größeren Industrieunternehmen investieren stark in neue Überwachungstechnologien und versuchen neben dem Erhalt des Status Quo, die sich aus den neusten technologischen Trends, wie Internet of Things (IoT) oder Smart Factory, ergebenden Potentiale zu heben. Die Investitionskosten für Industrieunternehmen belaufen sich daher aktuellen Schätzungen von Crisp Research zufolge auf rund 2,2 Mrd. € im Jahr 2016. Einen weiteren großen Investitionsblock stellt die gewerbliche Gebäudevermietung mit insgesamt 1,7 Mrd. € dar.

Während der Sicherheitsmarkt in der Vergangenheit eher ein Markt der langfristigen Investitionen war, so wird sich der Markt zukünftig dynamischer entwickeln, da vermehrt in moderne Sicherheitstechnik investiert werden wird. Dies liegt zunächst vor allem an der fortschreitenden Technikevolution mit immer geringeren Innovationszyklen und den daraus resultierenden Technologietrends (siehe Kapitel 6), welche neben der reinen Gebäudeüberwachung noch weitere Vorteile für die Unternehmen bereithalten.

Ausgaben je Branche im Jahr 2016



Quelle:
Crisp Research AG, 2016

Durch die Umstellung der ISDN-Leitungen auf die IP-Netze und dem damit verbundenen Wegfall von den hauptsächlich verwendeten Diensten im Kontext von Gefahrenmeldeanlagen, welche häufig auf Datex-P beruhen, wird auf die Unternehmen vor allem in den Jahren 2017 / 2018 zusätzlich ein Investitionspeak insbesondere für Gefahrenmeldeanlagen, Übertragungseinrichtungen und die Umrüstung und Beratung der internen Übertragungsnetze zukommen.

Die Risiken einer nicht-funktions- und einsatzfähigen Gefahrenmeldeanlage können sich weder Unternehmensentscheider noch deren Sicherheitsdienstleister erlauben. Denn gesetzliche Haftungstatbestände sowie unternehmensinterne Compliance-Richtlinien setzen hier in vielen Fällen klare Regeln und Verantwortlichkeiten. Laut Schätzungen von Crisp Research AG liegt der Anteil der kommerziellen Gefahrenmeldeanlagen, die eine teilweise oder vollständige Umrüstung benötigen bei über 70%.

KAPITEL 3: HERAUSFORDERUNGEN FÜR DIE STAKEHOLDER IM ZUGE DER UMSTELLUNG AUF DIGITALE NETZE

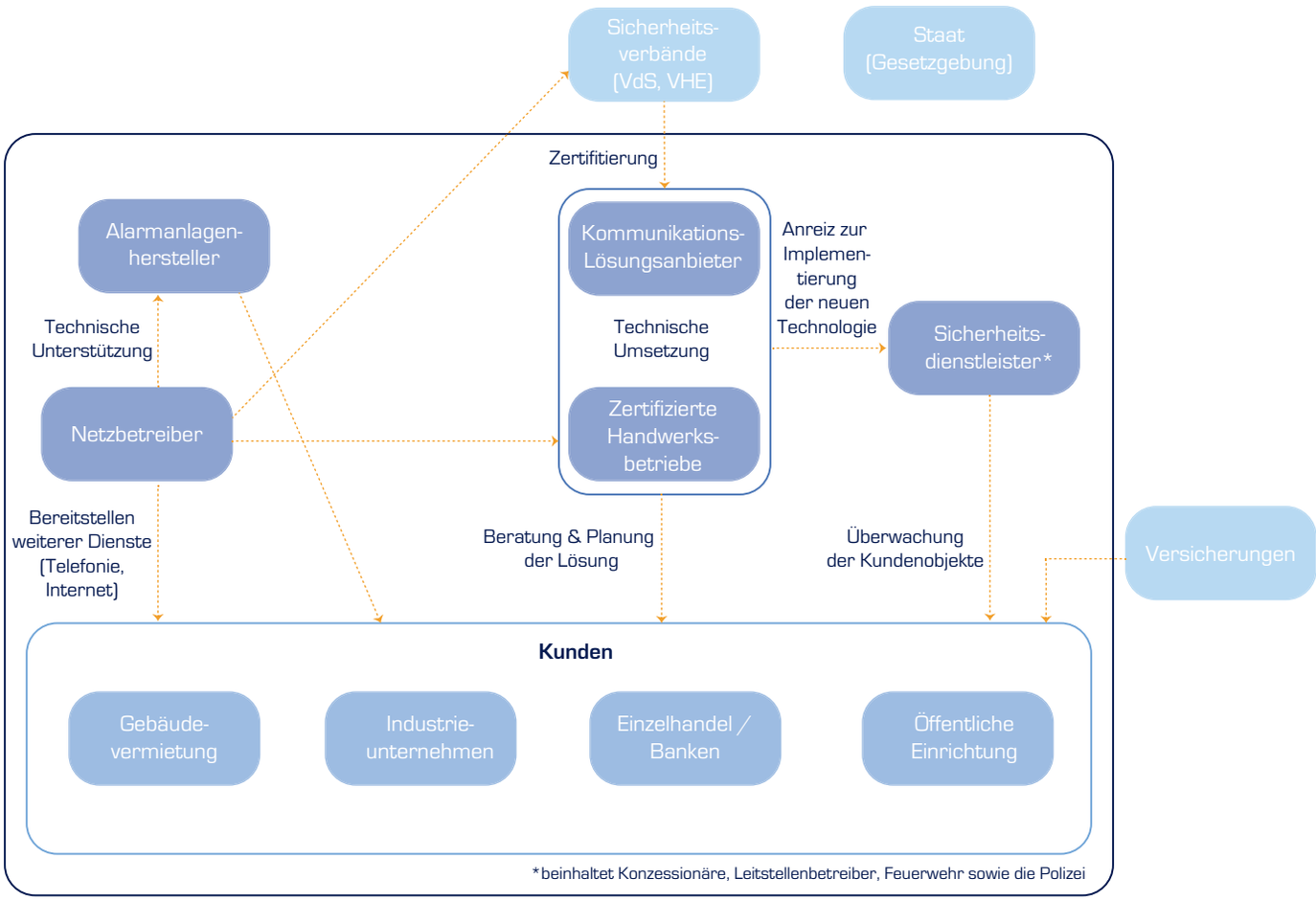
„In der elektronischen Sicherheitsbranche haben wir neben komplexer Technik auch noch komplexe Geschäftsmodelle und Verantwortlichkeiten. Die spezialisierten Errichterbetriebe, die Leitstellenbetreiber und die Hersteller von Gefahrenmeldeanlagen bilden ein komplexes Zusammenspiel mit dem Kunden und uns als Provider."
(Karsten Lebahn
Leiter IPT Sonderdienste, Deutsche Telekom)

Die Vergangenheit hat gezeigt: Jede technologische Innovation hat sowohl positive als auch negative Auswirkungen auf eine Vielzahl von Stakeholdern, wie z.B. auf Kunden, Anbieter, Dienstleister, Verbände, den Staat und eine Vielzahl von weiteren Anspruchsgruppen. Denn bei einer technologischen Innovation entsteht zunächst eine Informationsasymmetrie zwischen dem Innovator und seinen Anspruchsgruppen, welche für viele dieser Stakeholdergruppen im Verlauf der Umstellung auf die neue Technologie zu Herausforderungen führt. Doch nicht alle Interessengruppen sind dabei im gleichen Ausmaß betroffen.

Für die Klärung der Aufgaben, Verantwortlichkeiten und Risiken der beteiligten Personen- und Entscheiderkreise im Kontext von Gefahrenmeldeanlagen müssen daher zunächst alle betroffenen Stakeholder identifiziert werden und anschließend die Rolle, welche sie im Rahmen der Technologietransformation spielen, herausgearbeitet werden.

Der Telekom, bzw. den anderen Netzbetreibern, kommt im Rahmen der Umstellung der Telekommunikationsnetze auf die IP-Technik die Rolle des Innovators zu. Diese Umstellung hat nicht nur Auswirkungen auf den Innovator, welcher die alten Technologien abschafft und neue Übertragungswege einrichten muss.

Stakeholder „Umstellung ISDN - IP“



Quelle:
Crisp Research AG, 2016

Zu den betroffenen Stakehol-dern zählen neben dem Netzbe-treiber unter anderem:

- Kunden
- Hersteller von Gefahrenmeldeanla-gen
- Lösungsanbieter
- Zertifizierte Handwerker
- Konzessionäre / Leitstellenbetreiber (inkl. Feuerwehr & Polizei)
- Sicherheitsverbände
- Staat (Gesetzgebung)
- Versicherungen

Dabei werden die verschiedenen Anspruchsgruppen vor eine Vielzahl an Herausforderungen gestellt, welche sie im Rahmen der Umstellung lösen müssen.

Diese Herausforderungen werden für die betroffenen Personen umso dringlicher, je länger die verschiedenen Stakeholder warten, um sich mit diesen Herausforderungen zu beschäftigen.

Stakeholder und Ihre Herausforderungen im Rahmen der IP-Umstellung

Stakeholder	Herausforderung im Rahmen der IP-Umstellung bezogen auf Gefahrenmeldeanlagen (GMA)	Bester Handlungszeitraum	Einfluss der IP-Umstellung
Netzbetreiber	Netzabbau ISDN & analog / Einführung IP Technologie / Umrüstung bei den Kunden (Standarddienste)	2015-2018	Sehr hoch
GMA Hersteller	Entwicklung und Produktion von IP-fähigen Geräten & Software	Ab 2015	Hoch
Lösungsanbieter	Kundenaufklärung / Beratung sowie Planung und Umrüstung von Kunden GMA sowie der Leitstellen-Technik	2016-2018	Hoch
Handwerker (zertif.)	Kundenaufklärung / Beratung sowie Planung und Umrüstung von Kunden GMA / Leitstellen-Technik	2016-2018	Hoch
Leitstellenbetreiber	Umstellen der eigenen verwendeten Technologie und Software in der Leitstelle / Verantwortung für Übertragungssicherheit, Verschlüsselung, Zertifikatverwaltung usw. der angebundenen Kunden / Kundenaufklärung	2016-2016	Sehr hoch
Kunden	Aufrüstung der eigenen GMA / interne Umstellung der Leitungsnetze / Herausarbeiten einer IT- und Sicherheitsstrategie	Ab sofort	Sehr hoch
Sicherheitsverbände	Mitgliederaufklärung / Überarbeiten der Zertifizierungen bezüglich der Besonderheiten von der IP-Technik	2015-2018	Mittelmäßig
Staat (Gesetzgebung)	Aufklärung der betroffenen Kundengruppen / Anpassen der Gesetze an die neue Technologie	2015-2018	Gering
Versicherungen	Einbindung einer Klausel, die Schäden bei Nutzung von veralteter Technik (analog und ISDN) ausschließt	2018	Mittelmäßig

Quelle: Crisp Research AG, 2016

Während die Netzbetreiber, die Hersteller von Gefahrenmeldeanlagen sowie weite Teile der betroffenen Leitstellenbetreiber schon relativ weit in der technischen Transformation fortgeschritten sind, haben vor allem die kleineren und mittelständischen Betriebe aus Mangel an Informationen über die Dringlichkeit der Umstellung zumeist noch keinerlei Transformationsstrategien für ihre Unternehmen entwickelt. Aus diesem Grund ist die Aufklärung der Endkunden über die weitreichenden Auswirkungen der Umstellung der analogen und ISDN Netze hin zur Übertragung über das Internet Protokoll zunächst die wichtigste Aufgabe von Sicherheitsverbänden, dem Gesetzgeber sowie der Lösungsanbieter. Die Leitstellenbetreiber, insbesondere die Polizei und die Feuerwehr, müssen für die Sicherstellung der kontinuierlichen Verbindung mit den Kunden zeitweise beide Technologien unterstützen und daher schon sehr frühzeitig ihre internen Übertragungsnetze auf die IP-Technologie umrüsten. Rollen & Verantwortung der zentralen Stakeholder im Detail:

Netzbetreiber - Die Innovatoren: Durch den Abbau der veralteten ISDN-Netze und der zeitgleichen Einführung der neuen IP-Technologie kommt den Netzbetreibern die Rolle der Innovatoren zu. Neben der technischen Umrüstung der eigenen Netze sollten die Netzbetreiber ihre Kunden über die Neuerungen aufklären und die Vorteile der Umstellung herausstellen. Denn viele Betroffene wissen nicht, dass im Zuge der IP-Einführung auch über ISDN hinaus andere Kommunikationsnetze, wie z.B. „Datex-P" der Telekom, ihrem Ende nahe gekommen sind. War Datex-P zunächst nur über Spezialanschlüsse zugänglich, so ist es vor allem durch die Möglichkeit zur Verbindung über ISDN (X.31) auch für die Anbindung von Gefahrenmeldeanlagen an die Leitstellen populär geworden. Daher sollten im Rahmen der Umstellung auf die IP-Technik die Kunden auch auf diese Problematik sowie auf die Auswirkungen auf weitere betroffene Sonderdienste hingewiesen werden. Neben den Herausforderungen gibt es allerdings auch Vorteile, welche die Umstellung auf die IP-Technik mit sich bringt. So bietet die Übertragung über das Internet Protocol eine größere Bandbreite und ein höheres Übertragungstempo als es über ISDN-Netze möglich war, welches vor allem für die Übertragung von Videoaufnahmen von Überwachungskameras einen Vorteil bietet.

„Besonders bei zu migrierenden Leitstellen müssen wir immer eine Ende-zu-Ende Funktion im Hinterkopf haben und ein individuelles Migrations-konzept mit dem Leitstellenbetreiber entwickeln. Art und Umfang der Aufschaltungen, vorhandene Empfangstechnik, effiziente Interimslösungen für die Migrationsphase sowie ein neues technologisches Zielbild für die Leitstelle finden dabei Berücksichtung.“(Karsten Lebahn Leiter IPT Sonderdienste, Deutsche Telekom)

Leitstellenbetreiber – Die mit der Doppelrolle: Leitstellenbetreibern kommt im Rahmen der IP-Umstellung eine Doppelrolle zu. Zum einen sind sie direkte Betroffene der Umstellung. Da sie dafür Sorge tragen müssen, dass sie die Alarmmeldung ihrer Kunden auch mit dem neuen Übertragungsweg weiterhin zuverlässig erreichen können, müssen sie selbst frühzeitig ihre eigenen Netze und Empfangseinrichtungen auf die IP-Technik umrüsten. Zum anderen haben sie die Verantwortung, ihre Kunden aktiv über die Konsequenzen der IP-Umstellung aufzuklären. Denn viele Kunden wissen nichts von den Auswirkungen, die diese Umstellung über die Telefonnetze hinaus, zum Beispiel im Hinblick auf ihre Gefahrenmeldeanlagen, haben kann. Zusätzlich ergeben sich mit der Einführung einer neuen EU Norm Änderungen für die Leitstellenbetreiber, die nicht mit der technischen Umstellung erledigt sind.

Ganz konkret bedeutet die Reform für die Leitstellenbetreiber eine erhöhte Verantwortung ihren Kunden gegenüber, denn durch das neue Gesetz verlagern sich Zuständigkeiten, die historisch bedingt vom Übertragungsnetzbetreiber übernommen worden sind. So müssen zum Beispiel Themen der Übertragungssicherheit, Verschlüsselung und Adresskonzepte zukünftig vom Administrator der Leitstelle verwaltet werden, da sie zu großen Teilen nicht mehr wie unter ISDN und X.31 üblich, in den technischen Produkteigenschaften verankert sind. Eine zusätzliche Herausforderung besteht bei der Übertragung über das Internet Protocol bei der Priorisierung der Signalübermittlung. Denn über ein und dieselbe Leitung werden durch die Umstellung sowohl Telefon, Streaming als auch Signale der Gefahrenmeldeanlage übertragen.

„Für viele Kunden stellt der Technologiewandel von ISDN respektive Datex-P hin zu IP einen grossen Einschnitt dar. Umso wichtiger ist es daher für diese, dass sie von einem kompetenten Partner mit massgeschneiderten Lösungen für die Alarmübertragung und langjähriger Expertise, vor allem auch im Bereich der All-IP-Kommunikationslösungen, unterstützt werden. Denn nur durch eine klare Migrations-strategie können Kunden die Potentiale, welche die IP Technik bereithält, heben und gemeinsam mit einem starken Partner zu einer zukünftsfähigen Lösung mit einem höheren Servicestandard und innovativen Features verwandeln.“

(Wolfgang Heck , Geschäftsleitung,

ITENOS GmbH)

Lösungsanbieter - Die aktiven Unterstützer:

Die Lösungsanbieter treten dann auf den Plan, wenn die Kunden für sich erkannt haben, dass sie die internen Übertragungsnetze sowie die Gefahrenmeldeanlagen analog der neusten technologischen Entwicklungen umbauen müssen. Sie sind die aktiven Helfer der Umrüstung und können entweder allumfassend von der Auswahl der passenden Hard- und Software, über die Installation der Gefahrenmeldeanlage bis hin zum Umbau der internen Übertragungsnetze beim Kunden unterstützen oder sich aber auf einzelne Teilbereiche davon spezialisieren. Denn gerade an den Stellen, wo die Umstellung auf die IP-Technik bei den meisten Kunden und Leitstellenbetreibern Fragen aufwirft, können diese Stakeholder aktiv unterstützen. So beraten sie zum Beispiel ihre Kundenunternehmen...

- ...wie die Alarmübertragung auch im Falle von hohen Telefon- und Streamingbelastungen der IP-Netze sichergestellt werden kann
- ...bezüglich sekundären Übertragungswegen, z.B. über Mobilfunk, wenn die IP-Übertragung zum Beispiel durch Stromausfälle nicht funktioniert
- ...wie Hochverfügbarkeit durch georedundante Plattformen sichergestellt werden kann
- ...über die Vorteile von festen IP-Adressen für den Erst- und Zweitweg
- ...bezüglich Themen wie Übertragungssicherheit, Adressenkonzepte, Verschlüsselung und VPN-Betrieb im Kontext von IP-Netzen

Kunden / Unternehmen - Die Adressaten: Viele Unternehmen, welche neben ihren Telefonanlagen auch ihre Gefahrenmeldeanlagen über ISDN-Netze mit den Leitstellen der Feuerwehr, der Polizei und den Sicherheitsdienstleistern vernetzt haben, wissen bislang nur wenig über die Auswirkungen der Umstellung auf die IP-Netze auf ihre gebuchten Sonderdienste. Denn viele Unternehmen verbinden die Abschaffung der ISDN-Netze einzig und allein mit ihren Telefonanlagen. Doch die Umstellung betrifft auch die mit dem ISDN-Netz verbundenen Netze, wie zum Beispiel Datex-P, welches von vielen Firmen vor allem im Kontext von Gefahrenmeldeanlagen zur Anbindung an die Leitstelle genutzt wird.

Die Umstellung hat somit nicht nur auf die Telefonanlagen und die Internetbereitstellung einen direkten Einfluss, sondern auch auf weitere Unternehmensbereiche. Aus diesem Grund ist es gerade für Kundenunternehmen, die ihre Gebäude und Liegenschaften mit Gefahrenmeldeanlagen gesichert haben, höchste Zeit sich allumfassend über die Auswirkungen der Umstellung zu informieren und Strategien für die Umstellung auszuarbeiten.

KAPITEL 4: IP-UMRÜSTUNG – FLUCH ODER SEGEN? HERAUSFORDERUNGEN FÜR SICHERHEITSVERANTWORTLICHE

„Durch den Wegfall von ISDN und DSL-Übertragungsmedien müssen auch Konzessionäre für die Interventionsalarmierung auf moderne Übertragungsverfahren umstellen. IP-Netzwerke sind dazu bestens geeignet und werden durch Funkübertragungswege redundant ergänzt, um auch zukünftige Anforderungen sicherheitsbewusst, schnell und zuverlässig erfüllen zu können." (Frank Herstix, Regional Marketing Manager Germany, Honeywell I Security and Fire)

Die physische Sicherung von Unternehmen durch Gefahrenmeldeanlagen wird zukünftig, auch vor dem Hintergrund von steigenden Einbruchsquoten, immer wichtiger. Daher ist es vor allem für die IT-Sicherheitsexperten sowie die Geschäftsführung in den Kundenunternehmen enorm wichtig, immer über die neusten Änderungen und technischen Neuerungen informiert zu sein. Der von der Gefahrenmeldeanlage im Unternehmen verwendete Übertragungsweg bestimmt (z.B. Datex-P), ob sie direkt von der Umstellung auf die IP-Technologie betroffen ist. IT-Sicherheitsexperten und Geschäftsführer sollten daher, wenn sie unsicher sind, ob sie auf die Umstellung reagieren sollen, zunächst auf die Herstellerfirmen ihrer Gefahrenmeldeanlagen oder auf den zuständigen Netzbetreiber zugehen und diese aktiv auf das Thema IP-Migration ansprechen.

Stellt sich hierbei heraus, dass die installierte Gefahrenmeldeanlage von der Umstellung betroffen ist, so können die Unternehmen die Umstellung entweder bei vorliegendem umfassenden technischen Wissen selbst in die Wege leiten oder aber einen erfahrenden Lösungsanbieter für Gefahrenmeldeanlagen mit einbeziehen. Da die Dringlichkeit jedoch branchenspezifisch voneinander abweichen kann, werden an dieser Stelle die vier Branchen vorgestellt, welche aufgrund der zuvor schon erwähnten umfangreichen Ausgaben für Sicherheitstechnik hauptsächlich von der Umstellung betroffen sind:

- (Wohn-) Gebäudevermietung
- Industrieunternehmen
- Einzelhandel / Banken
- Öffentliche Einrichtungen

(WOHN-) GEBÄUDEVERMIETUNG

Bei einer (Wohn-) Gebäudevermietung ist vor allem der Gebäudeverwalter der Hauptverantwortliche, wenn es darum geht, die Sicherheit und Instandhaltung der Vermietungsobjekte zu gewährleisten. Da es sich bei den Gefahrenmeldeanlagen jedoch um technische Lösungen handelt, die mehrere Gebäude und Zuständigkeitsbereiche umfassen, ist der Gebäudeverwalter unter Umständen nicht der alleinige Verantwortliche. Hinzu kommt an dieser Stelle, dass die Umstellung einen hohen Grad an technischem Wissen benötigt, welches zumeist bei den Gebäudeverwaltern, welche sich vor allem um verwaltende Tätigkeiten kümmern, nur im geringen Maße vorhanden ist. Für viele Gebäudeverwalter ist es daher Rahmen der Umstellung vorteilhaft auf einen versierten Partner zurückzugreifen, der eine ganzheitliche Strategie erarbeitet und von der Planung bis hin zur technischen Umsetzung unterstützt.

INDUSTRIEUNTERNEHMEN

In Industrieunternehmen liegt die Sachlage etwas anders: Hier sind es entweder die Sicherheitsbeauftragten oder aber die IT-Abteilung mit Fokus auf Sicherheitstechnik, die für die Umstellung auf die IP-Technologie verantwortlich sind. Da die Sicherheitsbeauftragten aus verschiedenen Abteilungen der Unternehmen kommen können, variieren hier die technischen Erfahrungsstufen der Verantwortlichen stark. Eine individuelle und realistische Fähigkeiten-Analyse sollte der Entscheidung vorgeschaltet werden, ob die Umstellung eigenständig oder mit Hilfe eines Dienstleisters erfolgt. Zielführend kann an dieser Stelle auch die Einbindung der IT-Abteilung sein, um eine möglichst gewinnbringende Transformation zu gewährleisten. Denn ohne eine fachmännische und zielführende Umstellung der Gefahrenmeldeanlagen, kann ein Compliance-konformer Betriebsablauf oftmals nicht aufrechterhalten werden. Dieser ist jedoch essentiell wichtig, um das Vertrauen der Kunden in einen hohen Sicherheitsstandard des Unternehmens zu stärken.

EINZELHANDEL / BANKEN

Im Einzelhandel kommt es vor allem auf die Größe des Einzelhandels an, von wem und in welchem Ausmaß die Transformation vorangetrieben wird. Auch muss hier eine klare Unterscheidung getroffen werden, wie kritisch die Gefahrenmeldeanlagen für die Sicherung der Unternehmen sind. Während kleinere Unternehmen mit wenig hochwertigen Waren, wie z.B. Restaurants oder Eisdielen vor allem ihre Einnahmen sichern müssen und somit wenig gebundenes Kapital in Form von Waren in ihren Läden haben, müssen Tankstellenbetreiber, Einzelhändler und Juweliere zusätzlich zu den Einnahmen auch die Waren sichern. Bei der zweitgenannten Personengruppe ist die Absicherung durch Gefahrenmeldeanlagen, hier insbesondere die Einbruchmeldeanlagen, daher besonders geschäftskritisch. In diesem Fall sollte daher eine sichere, vom VdS-zertifizierte Gefahrenmeldeanlage installiert werden. Hierbei empfiehlt es sich daher umfassende Hilfe bei der Umstellung der Gefahrenmeldeanlagen von einem zertifizierten Dienstleister einzufordern, damit die Umstellung reibungslos und die Einführung der Lösung ohne Schwachstellen erfolgt.

Bei großen filialisierten Einzelhändlern, wie z.B. Rewe oder Edeka, gibt es entweder eine IT-Abteilung, die sich um die Sicherheitstechnik kümmert oder aber es besteht eine enge Partnerschaft mit einem großen Sicherheitsdienstleister, der an dieser Stelle beratend zur Seite stehen kann. Franchise-Nehmer sollten sich mit ihren Franchise-Gebern in Verbindung setzen, um die Verteilung der Verantwortlichkeit bezüglich einer Umstellung der Gefahrenmeldetechnik zu klären. Ein besonderes Augenmerk liegt auch bei den Banken auf der Sicherung ihrer Gebäude und den Geldbeständen. Auch hier empfiehlt es sich, auf Grund der Wichtigkeit der Gefahrenmeldeanlagen für den reibungslosen und sicheren Betriebsablauf sich einen kompetenten Partner für die Umrüstung und Installation an die Seite zu holen, um Automatendiebstähle, -sprengungen und Überfälle auf die Filialen zu verhindern.

ÖFFENTLICHE EINRICHTUNGEN

Öffentliche Einrichtungen sind entweder öffentlich-rechtliche Organisationen und daher den Gemeinden, den Ländern oder dem Bund unterstellt oder können in einer Rechtsform des Privatrechts (z.B. Stiftung des öffentlichen Rechts, GmbH, AG) betrieben werden. Unabhängig von der Rechtsform gelten auch hier die schon erwähnten Fragen bezüglich der eigenen Fähigkeiten im Rahmen der Umstellung sowie bei den öffentlich-rechtlichen Organisationen die Vorgaben der nächsten höheren Verwaltungsstelle. Da jedoch die Sicherheitsbedarfe im Bereich der öffentlichen Einrichtungen stark schwanken (z.B. Gefängnisse vs. Bibliotheken) kann man hier keine allgemeinen Empfehlungen treffen.

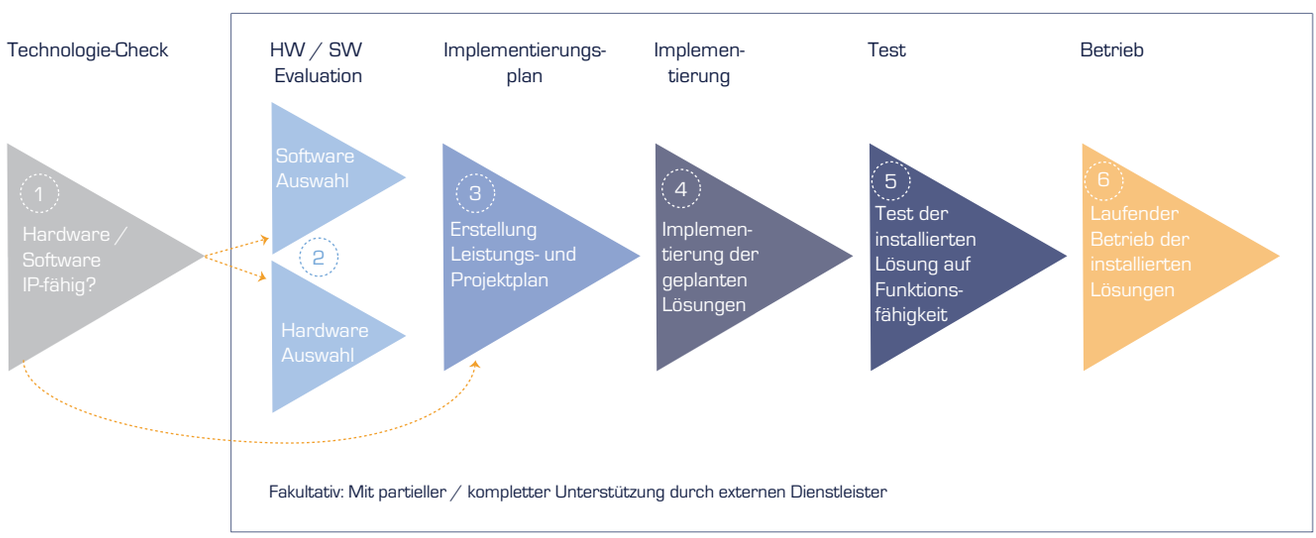
Aus diesem Grund sollten je nach Risikobewertung die Verantwortlichen für die Absicherung der öffentlichen Gebäude ausreichend früh damit beginnen, sich Gedanken um die Umstellung der Sicherheitstechnologie zu machen. Anders sieht das jedoch bei den Feuerwehrleitstellen aus, welche z.B. mit den Brandmeldeanlagen von Industrieunternehmen, Banken und filialisierten Einzelhändlern verbunden sind. Diese stehen in der Pflicht die Anbindung der verbundenen Unternehmen zu ihren Empfangseinrichtungen auch mit Umstellung auf die IP-Technik sicherzustellen. Zu diesem Zweck bietet z.B. der VdS eine Zertifizierung der Leitstelle und seiner Empfangseinrichtung (VdS 3138), an.

KAPITEL 5: HANDLUNGSMÖGLICHKEITEN UND TRANSFORMATIONS-STRATEGIEN FÜR UNTERNEHMEN

Haben die IT-Sicherheitsbeauftragten und die Geschäftsführer im Unternehmen ihre Verantwortlichkeiten erkannt und kennen sie die Herausforderungen, die auf sie zukommen können, so stellt sich ihnen zunächst die Frage, wie sie am besten auf die Umstellung reagieren können. Prinzipiell sollte zunächst identifiziert werden, welche Dienste und welche Hardware konkret betroffen sind.

Sollte eine Umrüstung notwendig sein, so haben die Verantwortlichen prinzipiell zwei Möglichkeiten – die Umstellung in Eigenleistung durchzuführen oder auf einen erfahrenen Lösungspartner zurückzugreifen. Unabhängig davon, ob das Projekt alleine realisiert wird oder ein Lösungspartner hinzugezogen werden soll, werden im Verlauf der Umstellung folgende Schritte erfolgen:

Projektphasen der IP-Umstellung



Quelle:
Crisp Research AG, 2016

„Die All-IP Umstellung stellt grosse Herausforderungen an die Übertragungstechnik, sowohl auf der Seite der Einbruchmeldeanlagen, als auch auf der Empfangsseite."
(Thomas Urban, Bereichsleiter Security, VdS)

1. Technologie-Check: In vielen Fällen müssen nicht komplett neue Gefahrenmeldeanlagen eingebaut werden, um auf die Umstellung auf das Internet Protocol zu reagieren. Oftmals reicht es die verwendete Software zu aktualisieren und die internen Übertragungsnetze sowie die Übertragungseinrichtung umzurüsten, wenn diese einzeln ausgetauscht werden kann. Hierzu sollte am besten der Hersteller der Gefahrenmeldeanlage und der Netzbetreiber kontaktiert werden, um weitere Informationen zu erhalten.

2. Software / Hardware Auswahl: Stellt sich heraus, dass neue Lösungen eingeführt werden müssen, so sollte das Unternehmen die verschiedenen zur Verfügung stehenden Lösungen sichten und ihre Vor- und Nachteile gegenüberstellen. Denn in die Auswahl geeigneter Sicherheitssoftware- und Hardwarelösungen spielen viele individuelle Entscheidungskriterien mit hinein, wie z.B. die Zufriedenheit mit der bestehenden Lösung, die zukünftige IT- und Sicherheitsstrategie im Unternehmen, wie z.B. der Einsatz von Videoübertragungen, sowie natürlich Kosten- und Leistungsaspekte.

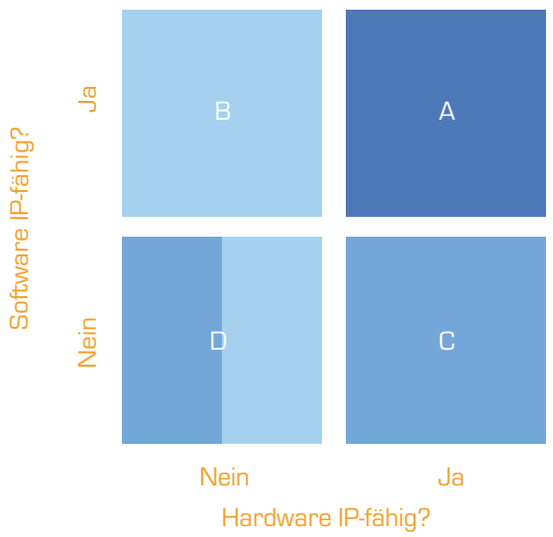
3. Erstellung eines Implementierungsplans: In dieser Phase sollte zunächst ein Projektplan erstellt werden, welcher den zeitlichen Rahmen der Umstellung sowie alle Meilensteine umfasst. Außerdem sollten mittels Lasten- und Pflichtenheft alle Anforderungen an die neue Lösung erhoben sowie alle benötigten Leitungspläne erarbeitet werden. Hierbei müssen eine Vielzahl an Entscheidungen getroffen werden, wie z.B. ob eine stehende oder bedarfsgerechte Verbindung eingerichtet werden soll, ob ein Ersatzweg eingeführt werden muss, ob Testmeldungen eingesetzt werden und wie die Stromversorgung der Übertragungseinheit im Falle eines Stromausfalls abgesichert werden muss. Wenn Unternehmen sicher gehen wollen, dass ihre Gefahrenmeldeanlage den höchsten Standards genügt, so sollten sie ihre geplante Gefahrenmeldeanlage von einer unabhängigen Stelle, z.B. dem VdS, zertifizieren lassen oder bei der Planung direkt auf einen Partner mit zertifizierter Lösung zurück greifen.

4. Implementierung: In dieser Phase findet die tatsächliche technische Umrüstung statt. Hier werden – je nach vorher erstelltem Implementierungsplan - die Hard- und Software erneuert sowie die internen Übertragungsnetze von ISDN auf die IP-Technologie umgestellt. Vor allem für die Umrüstung der internen Übertragungsnetze empfiehlt es sich, einen von dem Netzbetreiber autorisierten, fachkundigen Partner, wie z.B. ITENOS, eine Tochtergesellschaft der Deutschen Telekom, einzubinden. Auch sollten Unternehmen darauf achten, dass der Lösungsanbieter von unabhängiger Stelle, wie zum Beispiel dem VdS zertifiziert ist. Dies begünstigt eine reibungslose und schnelle Umstellung.

5. Testphase: Nach der erfolgten Umstellung sollte zunächst ein Testbetrieb der neuen Gefahrenmeldeanlage vor der tatsächlichen Inbetriebnahme durchgeführt werden, um eine lückenlose Sicherung der Betriebsgebäude zu gewährleisten. Auch sollte die installierte Lösung, falls sie nicht durch einen zertifizierten Lösungsanbieter installiert worden ist, durch Zertifizierungsstellen, wie z.B. dem VdS, ein Unternehmen des Gesamtverbandes der Deutschen Sicherheitswirtschaft, vor finaler Inbetriebnahme überprüft und analog den gängigen Richtlinien zertifiziert werden.

6. Betrieb: Wenn der Testbetrieb gezeigt hat, dass alle installierten Gefahrenmeldeanlagen reibungslos laufen, kann in die Produktivphase übergeleitet werden. Ein kontinuierliches Monitoring sowie regelmäßige Systemupdates und Sicherheitspatches sollten während des Betriebes durchgeführt werden, um Sicherheitslücken vorzubeugen. Auch ist ein kontinuierliches Management der installierten internen Übertragungsnetze wichtig, um einen reibungslosen Betrieb sicher zu stellen.

Szenarien der Transformationsstrategie



Quelle: Crisp Research AG, 2016

Für die Umstellung der Gefahrenmeldeanlagen können grundsätzlich vier verschiedene Szenarien unterschieden werden, welche in der folgenden Grafik exemplarisch dargestellt sind:

FALL A: SOWOHL DIE HARD- ALS AUCH DIE SOFTWARE IST IP-FÄHIG

Hard- und Softwareseitig muss an dieser Stelle von der betroffenen Firma keine Umstellung erfolgen. Allerdings sollte trotzdem frühzeitig eine Umstellung der internen Übertragungsnetze sowie eine Einrichtung eines zweiten Übertragungsweges (z.B. Funk) für den Fall eines Stromausfalles, einer Sabotage oder ähnlichem, eingeplant werden.

Denn mit der Einführung der IP-Übertragung kommen neue sicherheitsrelevante Faktoren zum Tragen (z.B. mögliche Zugriffe von Dritten über das Internet, Überlastung der Übertragungsnetze durch konkurrierende Dienste, wie z.B. Streaming), die keineswegs zu vernachlässigen sind. Daher sollte das Unternehmen bei Projektschritt 3 ansetzen und eventuell für die Absicherung der Funktionsfähigkeit der Gefahrenmeldeanlagen einen kompetenten Partner hinzuziehen.

FALL B: DIE INSTALLIERTE SOFTWARE IST IP-FÄHIG, DIE VERWENDETE HARDWARE JEDOCH VERALTET

In diesem Fall ist die verwendete Software IP-kompatibel, die im Unternehmen installierte Hardware ist jedoch zum derzeitigen Stand nicht auf IP eingestellt. Hier ist zunächst zu überprüfen, ob die verwendete Gefahrenmeldeanlage auf IP umrüstbar ist (z.B. durch Austausch der Übertragungseinheit), oder ob eine komplett neue Anlage angeschafft werden muss. Viele Gefahrenmeldeanlagenhersteller haben sich schon intensiv mit der Umstellung auf die IP-Technik beschäftigt und bieten derzeit eine Fülle an passenden Lösungen für ihre Kunden an. Folgende Firmen bieten derzeit IP fähige Gefahrenmeldeanlagen an:

- Abus
- Bosch
- Esser / Honeywell
- MS AG
- TAS
- Telenot

FALL C: DIE INSTALLIERTE SOFTWARE IST NICHT IP-FÄHIG, DIE VERWENDETE HARDWARE IST IP-FÄHIG

Dieser Fall kann bei Unternehmen auftreten, die kürzlich in neuere Hardware investiert haben, allerdings in diesem Zuge auf eine Umstellung der Software verzichtet haben. Hier empfiehlt es sich, den Softwarehersteller direkt anzusprechen, ob für die veraltete Software Updates verfügbar sind oder ob sie durch Upgrades Internet Protocol fähig gemacht werden kann. Sollte dies nicht der Fall sein, so kann der Hersteller der Gefahrenmeldeanlagen kontaktiert werden, um zu erfragen, welche Software er für seine Gefahrenmeldeanlagen empfiehlt.

FALL D: SOWOHL DIE INSTALLIERTE SOFTWARE ALS AUCH DIE VERWENDETE HARDWARE SIND NICHT IP-FÄHIG

Wenn sowohl die Soft- als auch die Hardware die Übertragung über das Internetprotokoll nicht unterstützen, sollte das Unternehmen zunächst gemäß Schritt 2 alle relevanten Lösungen der Hersteller bezüglich Kosten-Nutzen Aspekten evaluieren. Hierbei empfiehlt es sich, ggf. nicht nur den alten Status Quo wiederherstellen zu wollen, sondern auch neue sich ergebende Chancen (z.B. IoT, Smart Factory, Videoübertragung) mit in die Überlegungen einzubeziehen, um aus den entstehenden Investitionen noch weitere Vorteile herauszuholen.

KAPITEL 6: SICHERHEIT IM DIGITALEN ZEITALTER - CHANCEN UND POTENTIALE DER IP-UMSTELLUNG VON ALARMANLAGEN

„Im Zeitalter von VoIP (Voice over IP) und mit der Nutzung von Telefon, Internet und Fernsehen über einen einzigen Anschluss, werden zunehmend auch Aspekte berücksichtigt wie die Erweiterung der Glasfasernetzwerke, Datenspeicherung in Clouds und Funkübertragung von sensiblen Informationen. Für Hersteller innovativer Gefahrenmeldetechnik ist es erforderlich, die Vorteile der modernen Infrastruktur zukünftig zu nutzen und steigende Anforderungen zu erfüllen." (Frank Herstix Regional Marketing Manager Germany Honeywell I Security and Fire)

Durch die zunehmende Nutzung von Technologien im Security Bereich wird der Sicherheitsmarkt immer enger mit dem IT-Markt verzahnt. Für die Unternehmen bedeutet das in der Konsequenz, dass es somit nicht ausreicht, einen Sicherheitsbeauftragten im Unternehmen zu beschäftigten, der sich mit den Leitungsnetzen, den verwaltungstechnischen sowie rechtlichen Fragen auskennt. Vielmehr sollten Unternehmen gezielt IT-Sicherheitsexperten ausbilden und einen besonderen Fokus auf neue Technologietrends legen, um daraus resultierende IT-Sicherheitsbedarfe und Chancen zu antizipieren. Denn nur durch die Einbindung von IT-Sicherheitstechnologien in die gesamte Unternehmensstrategie lässt sich ein informationstechnischer Fortschritt dauerhaft realisieren. Durch diese Integration ergeben sich für das Unternehmen Chancen, um Prozesse zu optimieren und somit Abläufe zu verschlanken. Folgende Trends sollten in den kommenden Jahren von Sicherheitsbeauftragten und IT-Sicherheitsexperten besondere Beachtung finden, um möglichst viele Innovationspotentiale für das Unternehmen zu identifizieren:

- **Smart Building / Connected Building:** Beim Smart Building geht es um eine intelligente Gebäudevernetzung, die sowohl die Türsteuerungen, die Sicherheitstechnik, das Licht, die Heizung und alle weiteren Komponenten der Gebäude miteinander in der Art verknüpft, dass alle Aktionen energiesparender und effizienter für die Nutzer der Gebäude ausgelegt werden. Gerade auch im Kontext der Einführung der neuen IP-Technologie ist dieser Trend interessant, denn hieraus ergeben sich z.B. durch die Einbindung von Echtzeit-Videoanalysen und Gesichtserkennung neue Potentiale für die intelligente Absicherung der Gebäude.

- **Smart Factory:** Die so genannte intelligente Fabrik ist Teil des von der Bundesregierung gestarteten Projektes Internet 4.0 und beschäftigt sich mit der automatisierten Fertigung innerhalb einer Produktionsstätte mit Hilfe von vernetzten Maschinen und Werkstücken. Dieser Trend ist vor allem für die Industrieunternehmen interessant und kann zur Verschlankung und Effizienzsteigerung der Produktion beitragen.

- **Internet of Things:** Beim Internet of Things werden Gegenstände des Alltags (z.B. Kühlschränke, Autos, Überwachungskameras) durch RFID Chips oder QR-Codes eindeutig identifizierbar gemacht, so dass sie durch eingebaute Mini-Computer sowohl untereinander als auch mit Menschen kommunizieren können. Hieraus ergibt sich eine Fülle an möglichen Einsatzszenarios in den verschiedensten Branchen.

Allerdings kommen mit den neuen Möglichkeiten auch neue potentielle Gefahrenquellen auf Unternehmen zu. Denn auch mögliche Angreifer können auf die voranschreitende Technik zugreifen und sind häufig sehr kreativ, wenn es um deren Einsatz geht. So hat sich zum Beispiel das Unternehmen Dedrone (http://www.dedrone.com/de/) darauf spezialisiert, mit Hilfe von Drohnen-Trackern Gebäude und Liegenschaften gegen Luftraumspionage und Angriffe abzusichern.

Es empfiehlt sich daher neben einem regelmäßigen Screening von neuen Technologien nach Potentialen und möglichen Gefahrenquellen für das eigene Unternehmen, auch Anstrengungen von konkurrierenden Unternehmen sowie Unternehmen aus anderen Branchen im Auge zu behalten.

KAPITEL 7: EMPFEHLUNGEN FÜR CIOS UND SICHERHEITSVERANTWORTLICHE

Zusammenfassend lassen sich dem Sicherheitsverantwortlichen der jeweiligen Unternehmen folgende Empfehlungen mit auf den Weg geben, damit die vorangetriebene Umstellung auf die IP-Technik für sie und ihre Unternehmen kein Fallstrick wird:

- **Risikobewertung für eigenes Unternehmen:** Eine der wichtigsten Empfehlungen stellt die interne Risikobewertung des Unternehmens dar. Denn nur wenn der Verantwortliche die individuellen Herausforderungen und ihre Auswirkungen auf den laufenden Betrieb einschätzen kann, kann er auch handeln, um das Unternehmen fortlaufend vor Gefahren abzusichern.

- **Entwicklung einer Migrations-Roadmap:** Bei einer Technologiemigration sollten im Vorhinein klare Ziele und Meilensteine festgelegt werden, an welchen man kontinuierlich den Projektfortschritt kontrollieren kann. Diese so genannte Roadmap enthält alle Projektinformationen und definiert die Verantwortlichkeiten der beteiligten Projektmitglieder. Sie stellt somit einen wichtigen Grundpfeiler für eine reibungslose Transformation dar.

- **Festlegung Make-or-Buy:** Die Make-or-Buy Entscheidung sollte von dem Sicherheitsverantwortlichen in Abhängigkeit von mehreren Faktoren getroffen werden. Neben den Auswirkungen der Umstellung auf das Unternehmen (Risikobewertung) spielt auch das eigene Können bzw. das der internen Mitarbeiter eine entscheidende Rolle. Ein weiterer wichtiger Faktor ist, vor allem im Rahmen der IP-Transformation, der zeitliche Hintergrund. Denn die Abschaffung der „alten" Netze (ISDN / Datex P) ist im vollen Gange. Durch die Einbindung eines erfahrenen und zertifizierten Dienstleisters kann aufgrund der Erfahrungskurve durch die Durchführung von früheren Projekten das Zeitfenster meist verringert werden.

Evaluierung geeigneter Dienstleister: Die Wahl eines sowohl erfahrenen als auch fähigen Dienstleisters ist vor allem bei dem kritischen Thema der Umstellung von Gefahrenmeldeanlagen essentiell, wenn man sich dafür entscheidet, Hilfe im Rahmen der Transformation in Anspruch zu nehmen. Denn nicht jeder Dienstleister ist im gleichen Maß dafür geeignet, wenn es darum geht die Planung, die technische Migration und die technologische Strategie zu planen. Bei der Auswahl der Dienstleister können daher Referenzprojekte, Zertifizierungen, intensive Beratung und die technologische Nähe zu den Netzbetreibern als Auswahlkriterien dienen.

Konzept „Digitale Sicherheit“: Unter strategischen Gesichtspunkten ist es für Unternehmen sinnvoll, wenn die Umstellung auf die IP-Technologie nicht als einzelnes Transformationsprojekt betrachtet wird. Vielmehr sollte es als Anreiz dazu gesehen werden, ein ganzheitliches Unternehmenskonzept zur digitalen Unternehmenssicherheit zu erarbeiten und als Teil der Digitalisierungs-Strategie des Unternehmens einzuführen.

METHODIK

Die vorliegenden Einschätzungen zur derzeitigen und zukünftigen Marktsituation im deutschen B2B Markt für Sicherheitsdienstleistungen und elektronische Sicherheitssysteme wurden auf Basis von detaillierten Analysen und Marktprognosen von Crisp Research erstellt. Diese basieren auf einer Vielzahl von externen sowie internen Quellen und Marktinformationen, die nach bestem Wissen und Gewissen ausgewertet wurden. Um die weitreichenden Auswirkungen der IP-Umstellung auf alle Stakeholder realistisch einschätzen zu können, wurden zudem zahlreiche Gespräche mit Personen aus den betroffenen Interessengruppen geführt.

Folgende Experten haben zugestimmt Zitate für die Thematik der IP-Umstellung im Kontext von Gefahrenmeldeanlagen bereitzustellen:

- Frank Herstix, Regional Marketing Manager Germany, Honeywell Security and Fire
- Jörg Frey, Geschäftsführer, Stanley Security
- Karsten Lebahn, Leiter IPT Sonderdienste, Deutsche Telekom
- Thomas Urban, Bereichsleiter Security, VdS
- Wolfgang Heck, Leiter Business Unit Netze, ITENOS GmbH

ÜBER ITENOS

Die ITENOS GmbH mit Hauptsitz in Bonn hat sich auf sichere IT-Lösungen spezialisiert. Als eigenständiges Unternehmen, das zum Konzernverbund der Deutschen Telekom AG gehört, plant und realisiert ITENOS kundenspezifische Lösungen in den Bereichen Cloud, Housing und Networks und betreibt die entsprechenden Systeme in eigenen Rechenzentren. Der Kundenstamm besteht vorwiegend aus mittelständischen Unternehmen. Ihnen steht ITENOS seit über 20 Jahren als kompetenter Partner in IT- und Telekommunikationsfragen zur Seite.

Lievelingsweg 125
D-53119 Bonn
TEL +49 228 72 93 0
FAX +49 228 72 93 4799
EMAIL info@intenos.de
http://www.itenos.de/
https://twitter.com/itenos

AUTOREN

Meike Buch (M. Sc. in Business Studies) ist Junior Analyst des IT-Research- und Beratungsunternehmens Crisp Research AG. Sie beschäftigt sich vorwiegend mit den Themenschwerpunkten Cloud Computing, IT-Infrastrukturen und Internet of Things. Zuvor war Meike Buch, neben ihrem Masterstudium im Bereich Information, Innovation und Management an der Universität Kassel, als wissenschaftliche Hilfskraft am Fachgebiet Wirtschaftsinformatik der Universität Kassel tätig. Dort beschäftigte sie sich unter anderem mit den Themen Cloud Computing, IT-Nutzung und Location Based Services.

Dr. Carlo Velten ist CEO des IT-Research- und Beratungsunternehmens Crisp Research. Seit über 15 Jahren berät Carlo Velten als IT-Analyst namhafte Unternehmen in Technologie- und Strategiefragen. Seine Schwerpunktthemen sind Digitale Transformation, Cloud Computing und datenbasierte Geschäftsmodelle. Zuvor leitete er 8 Jahre lang gemeinsam mit Steve Janata bei der Experton Group die „Cloud Computing & Innovation Practice". Davor war Carlo Velten verantwortlicher Senior Analyst bei der TechConsult und dort für die Themen Open Source und Web Computing verantwortlich. Dr. Carlo Velten ist Mitinitiator und Jurymitglied der „Digital Leader Awards" und engagiert sich im Branchenverband BITKOM. Als Business Angel unterstützt er junge Startups und ist politisch als Vorstand des Managerkreises der Friedrich Ebert Stiftung aktiv.

ÜBER CRISP RESEARCH

Die Crisp Research AG ist ein unabhängiges IT-Research- und Beratungsunternehmen. Mit einem Team erfahrener Analysten, Berater und Software-Entwickler bewertet Crisp Research aktuelle und kommende Technologie- und Markttrends. Crisp Research unterstützt Unternehmen bei der digitalen Transformation ihrer IT- und Geschäftsprozesse.

Die Analysen und Kommentare von Crisp Research werden auf einer Vielzahl von Wirtschafts-, IT-Fachzeitschriften und Social Media-Plattformen veröffentlicht und diskutiert. Als „Contributing Editors" bei den führenden IT-Publikationen (Computerwoche, CIO, Silicon et al.), engagierte BITKOM-Mitglieder und nachgefragte Key-Note-Speaker tragen die Analysten von Crisp Research aktiv zu den Debatten um neue Technologien, Standards und Markttrends bei und zählen zu relevanten Influencern der Branche.

Crisp Research wurde im Jahr 2013 von Steve Janata und Dr. Carlo Velten gegründet und fokussiert seinen Research und seine Beratungsleistungen auf „Emerging Technologies" wie Cloud, Analytics oder Digital Marketing und deren strategische und operative Implikationen für CIOs und Business Entscheider in Unternehmen.

KONTAKT

Weißenburgstraße 10
D-34117 Kassel
TEL +49-561-2207 4080
FAX +49-561-2207 4081
info@crisp-research.com
http://www.crisp-research.com/
https://twitter.com/crisp_research

COPYRIGHT