Szene-Trends nachgefragt – in dieser Ausgabe bei Sebastian Schreiber

Seine Mission: Hacken, um Unheil abzuwenden. Deutschlands „Meister-Hacker" Sebastian Schreiber (SySS GmbH) betont im JS-Interview:

„Sicherheit ist eine ‚softe Sache', wenn sie nicht als Projektziel in der Softwareentwicklung vorgegeben wird"

JavaSPEKTRUM sprach mit Deutschlands „Meister-Hacker" Sebastian Schreiber über Sicherheits-Todsünden in Unternehmen. Er wurde bekannt, als es 2013 seiner Firma SySS gelang, alle WhatsApp-Messages auszuspähen.

Der Name täuscht – Sebastian Schreiber ist Auftrags-Hacker. Fotonachweis: Annegret Handel-Kempf

Sebastian Schreiber, *Jahrgang 1972, ist geprägt von seiner Geburtsstadt Tübingen. Ebendort lässt er gerade ein neues Gebäude für die von ihm gegründete SySS GmbH errichten – mit Platz für 300 Mitarbeiter. Die Frage, ob es denn so viele werden, bringt den Absolventen eines Mathe-, Informatik-, BWL- und Physik-Studiums ins Philosophieren. Derzeit hat die Firma von Deutschlands „Meister-Hacker" rund 62 Mitarbeiter. „Wo liegen die Grenzen der Expansion?", fragt der humanistisch gebildete und kulturell vielseitig interessierte Laufsport-Freund beim Interview mit JavaSPEKTRUM und weiß die Antwort darauf derzeit selbst nicht. Beharrlich fragt er weiter, will es wissen. Wie Schreiber alles erkunden will, seit er es schon mit zwölf Jahren geschafft hat, ein Computerspiel zu knacken. Sein Nachdenken über die Welt und ihre Strukturen hat der Schwabe früh in die Idee umgesetzt, die IT-Systeme von Unternehmen auf Sicherheitslücken hin zu untersuchen. Seit 1998 bieten der Pionier in Sachen Penetrationstests und seine Mitarbeiter „Auftrags-Hacking" für Unternehmen an – nach strikt objektiven, produktunabhängigen Kriterien. Ganz legal.*

▼ **JavaSPEKTRUM:** *Herr Schreiber, was sind die drei häufigsten Sicherheitsprobleme bei Firmen?*

Sebastian Schreiber: Einmal *Webapplikationen.* Überall, wo Komplexität herrscht, schleichen sich Fehler ein. Da werden Dinge übersehen, falsch konzipiert. Es gibt Missverständnisse und unklare Zuständigkeiten. Eine Virus-Infektion kann daraus resultieren, dass Firmen eine Vielzahl von Webapplikationen betreiben, die jede für sich relativ einfach angreifbar sind.

Das Zweite sind *Verzeichnisstrukturen in Unternehmen.* Die meisten Unternehmen setzen Active Directory ein, den Verzeichnisdienst von Microsoft. Dieser birgt eine Vielzahl von Schwachstellen, die sich in komplexen Umgebungen gar nicht so einfach beseitigen lassen.

Das dritte Problem sind *unverschlüsselte Kommunikationen.* Ich reise seit sechzehneinhalb Jahren durch die Welt, um mit Entscheidern, Softwareherstellern und anderen zu sprechen. Diese Jahre waren in Bezug auf Verschlüsselung vergebens. Es wird immer noch viel zu wenig verschlüsselt.

▼ *Wenn ich im ICE fahre und jemand telefoniert, höre ich auch Dinge, die ich besser nicht hören sollte.*

Dieses Gehörte entsprechend zu verwerten, ist aber gar nicht so einfach. Wenn ich über den Kaufpreis meines Unternehmens rede, das ich für 24 Millionen Euro verkaufen möchte, ist die Wahrscheinlichkeit, dass jemand vor mir sitzt, der das in den richtigen Kontext einordnet und entsprechend monetär zu meinem Schaden ausnützt, extrem gering.

Bei der E-Mail-Verschlüsselung sieht das jedoch anders aus. Wenn ein Internet-Service-Provider in München einen vollständigen E-Mail-Verkehr unberechtigterweise aufzeichnet, kann ich diesen automatisiert auswerten. Ich weiß, woher die E-Mails kommen, wohin sie gehen. Da wird der Kontext gleich mitgeliefert. Und diese E-Mails sind sehr zahlreich. Unverschlüsselte Kommunikation im Internet hat eine ganz andere Dimension als ein mitgehörter Satz.

▼ *Also kommt es darauf an, beim Abhören auch den Kontext zu kennen?*

Genauso ist es. Der eine Satz im ICE oder ein offener Ferrari mit Schlüssel auf dem Beifahrersitz in der Tiefgarage sehen nach Sicherheits-Todsünden aus, sind es aber – mit klarem Kopf betrachtet – gar nicht. Die Wahrscheinlichkeit, dass da etwas passiert, ist sehr gering. Aller Vermutung nach würde niemand die Tür auch nur anfassen, obwohl sie offen ist.

▼ *Warum wird so wenig verschlüsselt?*

Die Menschen sind glücklich, ihre Peer-Groups kostenlos und unkompliziert zu erreichen. Dann ist es ihnen egal, ob irgendwelche dubiosen Geheimdienste, von denen man gar nicht genau weiß, was sie mit den erspähten Daten anfangen, von ihrer Kommunikation wissen.

▼ *Nach dem Motto: Was interessiert die schon, was ich mache?*

Genau. Am schlimmsten war für mich, dass wir von der Firma SySS Ende 2013 alle WhatsApp-Messages ausspähen konnten. Das ging durch die Presse: „Große Schwachstelle!" Und das war genau dasselbe Jahr, in dem WhatsApp eine riesige Menge an Kunden gewonnen hat und den Eigenwert auf 18 Milliarden Dollar steigern konnte. Das heißt, weder die Börse noch die Anwender bestrafen es, wenn ein Unternehmen Sicherheitslücken hat.

▼ *Sony hatte auch eine Menge Probleme.*

Das war eine andere Dimension, weil es da zu akuten Vorfällen gekommen ist. Die Tatsache, dass ein abstrakter Gegner Ihre Daten ausspähen kann, nehmen Sie billigend in Kauf. Wenn jemand *tatsächlich Ihre* E-Mails ausspäht und diese ins Internet stellt, dann reagieren Sie auch entsprechend betroffen.

▼ *Was bewegt die Täterseite?*

Alles Mögliche. Weil sie's können, weil sie's üben wollen, weil es ihnen Spaß macht. Auftrags-Hacker. Täter, die auf eigene Rechnung arbeiten, Daten stehlen und meistbietend weiterverkaufen. Personen, die so etwas aus politischen Gründen machen. Diejenigen, die im Auftrag eines Kunden einem Wettbewerber schaden wollen. Alle möglichen Konstruktionen sind da möglich.

▼ *Warum entstehen insgesamt Sicherheitsprobleme?*

Generell aufgrund von Komplexität und wegen des mangelnden Interesses der Nutzer. Dienste wie WhatsApp werden gerne genutzt, weil sie kostenlos sind. Hinzu kommt der Wunsch, IT-Projekte schnell umzusetzen. Eine schnelle Umsetzung würde durch IT-Security gebremst. Meine Mitarbeiter und ich stellen überbordende Wünsche hinsichtlich Komfort und Kosteneinsparung fest. Das wird sich die nächsten Jahre noch zuspitzen. Wir werden immer mehr IT einsetzen und dabei auf eine steigende Zahl von heterogenen Standards zurückgreifen.

▼ *Wo sind die Schwachpunkte von Java, speziell der Java-Plattform?*

Es gibt Fehler, die können Sie mit Java nicht mehr machen. Bei den Applikationen ist die Frage, ob die Sandbox funktioniert. Heute kann ich bei Java nur signierte Applets laufen lassen. Da muss der Täter schon einiges machen, um Code auf Ihrem Rechner zum Laufen zu bringen.

▼ *Twitter benutzt beispielsweise Scala, das wiederum auf einer Java Virtual Machine*

läuft. Es gibt etwa 40 oder 50 Sprachen, die auf der Java-Plattform laufen, aber nicht Java sind. Wenn die Plattform unsicher ist und jemand programmiert, egal mit welcher Sprache, gegen die Plattform, die ja die Java Virtual Machine ist …

… dann haben wir uns das Problem wieder ins Haus geholt. Schauen wir dennoch zu anderen Produkten: Bei Flash und Microsoft Silverlight erwarten uns mehr Schwierigkeiten in den nächsten Jahren.

▼ *Die meisten Applikationsserver, ausgenommen Microsoft, sind am Backend auf Java aufgebaut. Haben Sie hier bereits kritische Sicherheitserfahrungen gemacht?*

Täglich, meistens ist das Input Validation. Eingänge werden dahin gehend gefiltert, ob irgendwo ein Escape ist. Klassische Schwachstellen von Webapplikationen kommen auf Webservern, die Java-basiert sind, zum Vorschein. Injection-Attacken aller Art, Cross-Site-Scripting, Cross-Site-Request-Forgery …

▼ *Woher kommen die Angstszenarien um Java?*

Java ist für Hacker interessant, weil es oft eingesetzt wird. Java war mit seinen Applets eine revolutionäre Idee. Aufgrund dieses Szenarios war es sehr früh eine Herausforderung für Angreifer. Sandbox-Hacks gab es eben erstmals bei Java. Wenn der Code serverbasiert läuft, brauchen Sie keine Sandbox mehr und sind nicht angreifbar.

▼ *Verursachen die Entwickler, sei es bei Java oder anderen Plattformen, die von Ihnen angesprochenen Sicherheitsprobleme?*

Entwickler sind Dienstleister. Sie machen im Großen und Ganzen, was ihr Chef ihnen sagt. Die Firma hat andere Ziele als der Anwender – Profitmaximierung. Wenn sehr viele Unternehmen mitmischen, kommt es zu skurrilen Geflechten. Wir haben am Ende Systeme, die teuer und unzuverlässig sind. An den Entwicklern liegt es nicht, sondern an den Strukturen. An unterschiedlichen Protokollen und Regeltechniken. Jedes Unternehmen hat das Ziel, vom Profitshare ein möglichst großes Stück abzukriegen und nicht in erster Linie ein besonders hochwertiges Produkt zu erstellen.

▼ *Bei der Softwareentwicklung selbst gibt es also keine Probleme?*

Nicht beim einzelnen Informatiker, der nur versucht umzusetzen, was man ihm vorgibt. Die Software-Unternehmen und deren Management müssen Verantwortung zeigen.

▼ *Welche konkreten Maßnahmen würden Sie vorschlagen?*

Der Chef muss die Mitarbeiter auf Schulungen schicken, die vermitteln, wo in der Entwicklung auf Sicherheit geachtet werden muss. Von ihm muss die Vorgabe kommen, dass man sich dem SDL anschließen will und sie dessen Standards erfüllen müssen (Anmerkung der Redaktion: *Trustworthy Computing Security Development Lifecycle* – SDL, zu Deutsch Entwicklungszyklus für vertrauenswürdigen Computereinsatz, ist ein 2004 von Microsoft veröffentlichtes Konzept zur Entwicklung von sicherer Software und richtet sich an Softwareentwickler, die Software entwickeln, die böswilligen Angriffen standhalten muss). Nach Abschluss einer Softwareentwicklung – etwa einer Webapplikation – kann natürlich auch ein standardmäßig durchgeführter Penetrationstest ein probates Mittel der Kontrolle sein. Denn die Kette ist nur so stark, wie ihr schwächstes Glied. Und der Hacker wählt genau dieses aus. Er entscheidet, ob er durch die dreifach gesicherte Eingangstür reinkommt oder durch das offene Dachfenster. Mein Unternehmen boomt, weil wir genau diese Form der Qualitätssicherung anbieten. Penetrationstests sind die letzte Bastion, die überprüft, ob etwas nicht sicher ist. Die Praxis zeigt, dass konventionelle Tests zur Qualitätssicherung nicht greifen.

▼ *Wie kann Sicherheit in einer Software-Mannschaft wirklich gelebt werden?*

Entwickler werden von ihrem Chef eingeschworen, wie schnell etwas fertig sein soll. Da ist Sicherheit so eine „softe Sache“. Wenn Sicherheit nicht als Projektziel vorgegeben wird, kann sie von Mitarbeitern in einem ohnehin schon ambitionierten Projekt nicht erwartet werden. Wenn nicht klar ist, dass Sicherheit eines der Projektziele ist, wird sie bei all dem Druck und all den Kompromissen in der Softwareentwicklung nicht als Zufallsprodukt nebenher mit erledigt.

▼ *Fehlt der Sicherheit Entschlossenheit?*

Mehr Entschlossenheit, mehr Commitment: „Wir wollen das haben, wir messen uns daran.“ Unser Weg dahin ist der Penetrationstest als definiertes Abnahmekriterium des Werkvertrags. Damit wird Sicherheit messbar. Wenn meine Mitarbeiter mittels eines Penetrationstests in ein System eindringen können, dann ist in diesem Fall eben der Werkvertrag nicht erfüllt und die Abnahme erfolgt nicht. Wenn ein System hackbar ist, dann kann es kein sauberes System sein, egal welche Top-Entwickler mitgearbeitet haben und welche Zertifizierungen berücksichtigt wurden. Dieser Lernprozess ist das eigentliche Ziel unserer Penetrationstests. Die Unternehmen müssen sich fragen: „Wie konnte es zu den Schwachstellen kommen, obwohl wir doch Top-Entwickler haben?“

▼ *Woher haben Sie das Know-how?*

In sechzehneinhalb Jahren sammelt sich Know-how an. Es gibt kein großes, deutsches Unternehmen, in das wir noch nicht eingedrungen sind. Das heißt natürlich, dass uns erst der Kunde hereingebeten hat und wir dann das eine oder andere System gehackt haben. Wir waren im vergangenen Jahr auf drei großen Hacker-Kongressen im Ausland. Budapest, Moskau, Wien – in Deutschland auch auf vielen. Wir sind hinter neuem Wissen her. Auf dem *Chaos Communication Congress* Ende Dezember 2014 mit über 11.000 Teilnehmern waren wir mit 21 Mitarbeitern vertreten. Wir sind im ständigen, regen Austausch und erhalten die Informationen meist vor der Öffentlichkeit. Natürlich sind wir auch Mitglied in der Allianz für Cyber Security.

▼ *Haben Sie Kontakte zur „Hinterhof-Hacker-Szene“?*

Die Situation ist schwierig. Unsere Kunden erwarten, dass wir keinerlei Berührungspunkte zur Hacker-Szene haben. Gleichzeitig sollen wir unser Wissen möglichst zwei Jahre vor der Hacker-Szene besitzen.

▼ *Gehen Sie nach einer Checkliste zu technischen Applikationen, Design, Netzwerk, Router und vielen weiteren Möglichkeiten vor?*

Unser Vorgehen ist systematisch, aber nicht strikt, sondern beinhaltet viel Kreativität, Kunst und Talent. Wir hacken nicht nach einer Checkliste, sind aber auch keine Zombie-Walk-Hacker. Das wäre zu aufwendig. Mit cleveren, pfiffigen Methoden haben wir das nötige Maß an Freiheit, ohne unter Beliebigkeit zu leiden.

▼ *Gibt es für Ihre Mitarbeiter entsprechende Schulungen?*

Auch, aber sie lernen in den Projekten selbst, die sehr unterschiedlich sind. Gleichzeitig müssen sie erhebliches Vertrauen genießen und das notwendige Know-how mitbringen.

Wird das Thema IT-Sicherheit in Zukunft noch größer werden?

IT und Netzwerke durchdringen den privaten und geschäftlichen Alltag in immer stärkerem Maße. Ich bin gespannt, wie schnell wir von 62 Mitarbeitern auf 300 kommen.

Interview:
Michael Stal, Annegret Handel-Kempf

Kunden-orientierte Kultur aus Sicht eines Java-Insiders

Die Kultur im Umgang miteinander, mit Arbeit und Aufgabenstellern – in vielen Gesprächen geht es in der IT- und Java-Szene derzeit um die Form der täglichen Arbeit. Darum, wie die Vorgehensweise und das Umfeld das, was hinten herauskommt, massiv beeinflussen.

„Don't fuck the customer". Ein Satz, den man so nicht unbedingt mit Kultur verbinden würde. Für Sven Peters von Atlassian, Keynote-Speaker bei der OOP in München und Mitglied der Java User Group Hamburg, jedoch das Kernstück einer ehrlichen und erfolgreichen Unternehmenskultur.

Vier weitere wichtige Werte gibt es in der australischen Firma, die mit Softwarelösungen für Softwareentwickler groß wurde. So groß, dass sich viele fragen, ob sich das vertrauensvolle Miteinander und die Optimierungsorientierung des Riesen auch auf kleine und mittelgroße Geschäftsgebilde übertragen lassen. Was zu erproben wäre.

Etwa die „DO-Ocracy" – die Kunden vertrauen darauf, dass ihre Auftragnehmer den Code nicht kaputt machen. Auch wenn sie selbst Vorgaben setzen, die kaum einen anderen Weg übrig lassen. Dennoch müsse gelten: „Don't fuck the customer."

Das „Nein"-Sagen praktizieren: „Don't write crappy code." Und immer nach einer besseren Lösung suchen. Das Gleichgewicht ausbalancieren: „Code nicht vergessen – Kunden nicht vergessen."

Selbst auf dem stillen Örtchen werden die Mitarbeiter bei Atlassian mit angepinnten Motto-Sprüchen stets an ihre Mission erinnert. Etwa mit: „Produkte kommen und gehen. Die Kultur bleibt." So werden die Entwickler an passender Stelle daran erinnert, dass alles vergänglich ist. Nur die Kultur nicht.

Keynote-Speaker Sven Peters auf der OOP

Echt strange: Menschliche Haut als Smartphone-Tastatur, implementiert auf Java-Basis

Saarbrücker Informatiker entwickeln beachtliche Innovationen. Merkwürdig mutet jedoch dieses ganz spezielle M(ensch)2M(aschine) an, das in Zusammenarbeit mit Forschern von der Carnegie Mellon University in den Vereinigten Staaten entstanden ist: Das Verfahren „iSkin" soll den menschlichen Körper enger mit der Technikwelt verknüpfen, ihn sogar als berührungsempfindliche Oberfläche für mobile Geräte einsetzen.

Die Forscher haben aus flexiblem Silikon und leitfähigen Elektrosensoren berührungsempfindliche Sticker für die Haut entwickelt. Diese können wie eine Eingabefläche technische Befehle empfangen, ausführen und so mobile Geräte fernsteuern. Drückt man auf einen Sticker, kann man, je nach Modell, zum Beispiel einen Anruf annehmen oder die Lautstärke eines Musikspielers regulieren. „Mit den Stickern erweitern wir die interaktive Oberfläche für den Nutzer, da praktisch der ganze Körper als Eingabefläche eingebunden werden kann", erklärt Martin Weigel, der als Doktorand im Team von Jürgen Steimle am Exzellenzcluster der Universität des Saarlandes forscht. Das flexible Material ermöglicht es, die Sensoren in verschiedenen Formen und Größen und mit persönlichem Design herzustellen. Mit einem Tastatursticker wäre es beispielsweise möglich, Nachrichten zu verfassen und zu verschicken.

Die elastischen Sensoren (und Interaktionen) selbst sind unabhängig von Plattformen und Programmiersprachen. Ganz ohne Java kommen die Wearable-Forscher jedoch nicht aus. Weigel: „In unserer konkreten Implementierung programmierten wir unter anderem in Processing (`https://processing.org`), welches auf Java basiert. Wir nutzen es insbesondere für die schnelle Visualisierung von Sensordaten und bei der Entwicklung von Anwendungsprototypen."

iSkin-Tattoo

(Fotonachweis: Universität des Saarlandes – Oliver Dietze)

Kino zum Mitmachen

Die digitale Welt verknüpft sich mit der Realität. Nicht nur in der Industrie 4.0, sondern auch im Kino, auf Fan-Meilen oder vor „Big Screens" in Einkaufszentren. Bereits in 100 US-Filmtheatern können die Zuschauer aufgrund einer Software des New Yorker Start-ups „Audience Entertainment" in Filmszenen live mitspielen. *Die Anwendungen entstanden mithilfe eines Entwicklungs-Kits*, das immer noch hungrig auf Inhalte ist (Link: `http://audienceentertainment.com/sdk`).

Und so rücken Wirklichkeit und digitale Daten zusammen: Kameras und Mikros, die mitten im Publikum angesiedelt sind, werden mit Server und Projektionstechnologie verbunden. Das Ergebnis aus vorhandenen Szenen und Interaktion wird live auf einem großen Bildschirm dargestellt. Damit wird es möglich, dass sich große Menschenmengen, die normalerweise fest in ihren Kinosesseln sitzen, frei in virtuellen Naturlandschaften und anderen Filmszenen bewegen.

„Interaktives Super-Theater" nennt das Start-up das physische Miteinander-Spielen auf Softwarebasis. Die Gruppeninteraktion vor einem gemeinsamen Szenerie-Kontext beruht auf „iD", einer Software, deren Grundlage ein patentierter, intelligenter Algorithmus ist.

Public Cloud verunsichert

Jedem seine eigene Wolke, so die dominante Strategie deutscher Unternehmen. BITKOM-Vizepräsident Achim Berg: „Unternehmen richten sich überwiegend interne Clouds ein, die öffentlich nicht zugänglich und oft vom Internet entkoppelt sind." Fast die Hälfte der deutschen Unternehmen setzen mittlerweile Cloud-Services ein, wobei Sicherheitsbedenken eine schnellere Verbreitung verhindern.

In fast jedem vierten deutschen Unternehmen (24 Prozent) wird der Einsatz der „Wolken-IT" bereits geplant oder diskutiert. Für ein Drittel (32 Prozent) ist die Nutzung der Big-Data-Technologie, bei der die Server nicht im Unternehmen stehen müssen, derzeit kein Thema. Das ist das Ergebnis einer repräsentativen Umfrage unter 458 Unternehmen im Auftrag der Wirtschaftsprüfungs- und Beratungsgesellschaft KPMG in Zusammenarbeit mit dem Digitalverband BITKOM.

„Cloud-Computing hat sich zu einer der zentralen Technologien der digitalen Welt entwickelt", sagte Ex-Microsoft- und Ex-Telekom-Manager Berg bei der Vorstellung des „Cloud-Monitors 2015". Nach den Ergebnissen der Umfrage nutzen 39 Prozent der Unternehmen IT-Services aus einer Private Cloud. Das sind drei Prozentpunkte mehr als im Vorjahr. Das Public-Cloud-Computing kommt dagegen kaum von der Stelle. Der An-

teil der Nutzer stieg lediglich um einen Punkt auf aktuell 16 Prozent.

Big-Data-Analyse via Java-Bibliothek Flume

Mit einer anderen Art von Offenheit sollen Cloud-Dienste zögerlichen Unternehmen Big Data und digitale Wirtschaft näherbringen. *Cloud Dataflow,* beispielsweise, soll manche lästigen Aufgaben erleichtern: „Cloud Dataflow macht es Anwendern einfach, geschäftskritische Informationen aus ihren Daten zu gewinnen, und das mit niedrigeren operativen Kosten und ohne den Aufwand, eine eigene Infrastruktur aufbauen, verwalten und skalieren zu müssen“, schreibt Greg DeMichillie vom Google Platform Team im Developers Blog des Unternehmens.

Er will „Herz und Verstand“ von Entwicklern erobern, weil dann „gute Dinge passieren“, sagt DeMichillie laut `http://bits.blogs.nytimes.com`. Der Google-Cloud-Manager weiter: „Einfachheit wird ein großes Geschäft sein – was Entwickler gerne machen, ist Code schreiben, nicht Infrastruktur managen.“

Dataflow ist ein Cloud-Dienst, der aus der Java-Bibliothek Flume und dem Framework MillWheel entstand, die intern von Google-Entwicklern genutzt wurden. Google hat bereits ein Cloud-Dataflow-SDK für Java als Open Source freigegeben. Cloud Dataflow wurde im Juni 2014 zur Entwicklerkonferenz Google I/O öffentlich vorgestellt und dient der Big-Data-Analyse. Google sieht es als eine „Plattform zur Demokratisierung der Datenverarbeitung im großen Maßstab, indem Datenforscher, Datenanalysten und datenzentrierte Entwickler einfacheren und besser skalierbaren Zugang zu Informationen erhalten“. Der Dienst richtet sich an Unternehmen jeder Größe, die große, vor allem online generierte Datenmengen analysieren und sich dabei keine Gedanken über die verwendete Infrastruktur machen wollen.

Telefonieren in der Cloud – mithilfe von Java

Dunkle Wolken hängen über allen, die sich noch verbal über Festnetzleitungen verständigen und auf diesem Weg die Störungsstelle informieren wollen, wenn die IP-Leitung mal ausfällt. Die Deutsche Telekom setzt die geplante Komplettumstellung ihres Netzes auf die All-IP Technik konsequent, man könnte auch sagen „erbarmungslos“, fort, um die teuren ISDN-Leitungen los zu werden. Herkömmliche analoge und ISDN-basierte Anschlüsse sollen bald der Vergangenheit angehören. Künftig werden alle Telefongespräche über Voice-over-IP (VoIP), also die Internetleitung, abgewickelt.

„All IP“ kommt ohne Ausnahme und mit ihr die Telekommunikations-Cloud. Die Telekom will bis 2016 in Großstädten und bis 2018 deutschlandweit alle ISDN- und Analog-Verträge kündigen. Voraus gehen schriftliche Aufforderungen, sich innerhalb von vier Wochen zu melden und freiwillig auf IP-Verträge umzusteigen. Sonst geht nach Ablauf der Analog- beziehungsweise ISDN-Vertragslaufzeit nichts mehr in der Telekommunikation von Unternehmen und Heim, fürchten die Empfänger der IP-Zeitenwende-Briefe.

Router, die noch S0-Ports für den Anschluss von ISDN-Telefonanlagen bieten, sucht man im aktuellen Angebot der Telekom vergeblich. Mancher hat aber noch ein älteres, derartiges Modell in Betrieb, das er weiter nutzen kann und seine ISDN-Telefone gleich mit. Nutzt man jedoch ISDN-Telefone an Telekom-IP-Routern, die zugleich Telefonanlagen ohne S0-Port sind, taugen sie maximal als „Sprachrohre“, ohne Anruferlisten und ähnliche, nützliche Features.

Wie können Elektroschrott und Investitionen in neue Endgeräte in Zeiten der Cloud-TK dennoch vermieden werden?

Circa 20 Millionen Systemtelefone sind in Deutschland noch im Einsatz. Viele Menschen wollen sich keine IP-Telefone anschaffen, solange die bisherigen Endgeräte gut funktionieren. Für Unternehmen von ein bis 100.000 Nebenstellen macht beispielsweise eine neue Inhouse-Entwicklung der NFON AG, die Ncloudbox+, die Umstellung auf All IP einfacher: Vorhandene Systemtelefone werden an das Mini-Device angeschlossen und mit dem Ethernet verbunden. Die gewohnten Leistungsmerkmale bleiben erhalten und werden automatisch durch die NFON-Cloud abgebildet.

Ebenfalls „Made in Germany“ ist eine Lösung von Gigaset. Gigaset schwebt schon länger in den Wolken und produziert deshalb nicht nur geeignete Hardware, sondern sucht auch Java-Entwickler für die Gigaset-Cloud. Diese bringt Festnetz-Telefonie, Tablets, Smartphones, Business Telephony, Partner Services und Home Solutions, inklusive Hausüberwachung, zueinander und macht deren Infos überall verfügbar.

Eine kleine Wunderbox des Münchner Unternehmens soll bei der Umstellung auf VoIP helfen: Die auf der CeBIT vorgestellte Basisstation Gigaset GO-Box 100 verfügt, für den nahtlosen Übergang von der analogen zur IP-basierten Telefonie, weiterhin über einen analogen Festnetzanschluss, sowie einen zusätzlichen LAN-Anschluss und einen VoIP-Client für zwei parallele Gespräche und sechs Rufnummern. Die Gigaset GO-Box 100 ist die DECT-Basisstation aller GO-Telefone und Schnittstelle für neue Kommunikationsmöglichkeiten. Alte und neue Gigaset-Endgeräte sollen wie gewohnt über diese Box funktionieren.

Beispielsweise sieht man über eine App unterwegs, wer zu Hause angerufen hat. Sobald ein Gigaset GO-Telefon Internetzugang hat, kann über dieses Endgerät weltweit kostenlos mit anderen Gigaset-Endgeräten, die im „gigaet.net“ angemeldet sind, telefoniert werden. Alles Cloud …